Innehållsförteckning

Regeringskansliet

Faktapromemoria
Riksdagsår: 2025/26
FPM-nummer: 78
2026-02-23

Cybersäkerhetspaket; förändringar i EU:s cybersäkerhetsakt och i NIS 2-direktivet

Försvarsdepartementet

Dokumentbeteckning

COM(2026) 11 Celexnummer 52026PC0011

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

COM(2026) 13 Celexnummer 52026PC0013

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

Sammanfattning

Kommissionen presenterade den 20 januari 2026 ett cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555).

I förordningen om ändringar i cybersäkerhetsakten (CSA 2) föreslås ändringar avseende mandatet för EU:s cybersäkerhetsbyrå (Enisa) i syfte att bl.a. klargöra och i vissa fall utöka Enisas ansvar och uppgifter. Därtill föreslås ändringar i ramverket för europeisk cybersäkerhetscertifiering syftandes till att effektivisera och förtydliga processerna i ramverket. Vidare finns också förslag om ett nytt ramverk för säkerhet i leveranskedjor för informations- och kommunikationsteknik (IKT) som syftar till att harmonisera och stärka EU:s arbete med säkerhet i IKT-leveranskedjor.

I direktivet föreslås riktade ändringar i NIS 2-direktivet. Förslagen innebär bl.a. vissa ändringar i vilka entiteter som omfattas av NIS 2-direktivet och följdändringar utifrån CSA 2-förslaget. Regeringen är preliminärt positiv till förtydliganden av Enisas existerande uppgifter avseende bl.a. policyutveckling, kunskapsbyggnad och kunskapsspridning, stödjande verksamhet kring standardisering och övningar. Regeringen anser dock att mer analys behövs i frågan om utvidgningen av Enisas mandat, vilket hänför sig till att

Enisa ska inta en mer operativ roll samt att byrån ska kunna ta ut avgifter för viss verksamhet.

Regeringen är också preliminärt positiv till att ramverket för cybersäkerhetscertifiering effektiviseras och förtydligas. Regeringens ingångsvärde i förhandlingarna är att verka för förändringar som får verkliga effekter.

Regeringen välkomnar att kommissionen undersöker sätt att stärka säkerheten i kritiska IKT-leveranskedjor. Hur ramverket är tänkt att fungera och vilka effekter det kan få kräver emellertid ytterligare analys.

Slutligen välkomnar regeringen kommissionens förslag om att införa ändringar i NIS 2-direktivet som syftar till att förtydliga hur regelverket ska tillämpas.

Regeringen avser verka för att regler och processer utformas så att konsekvenserna är proportionerliga och inte medför större begränsningar eller kostnader än vad som är nödvändigt.

1. Förslaget

1.1 Ärendets bakgrund

Mot bakgrund av bl.a. ökade hot och sårbarheter i cyberrymden, kopplat till EU:s inre marknad, har kommissionen under de senaste åren tagit fram en rad bindande rättsakter och rekommendationer.

1.1.1 EU:s verktygslåda för 5G-säkerhet

Baserat på bl.a. EU:s samordnade riskanalys av cybersäkerheten i 5G-nät publicerade samarbetsgruppen[1] den 29 januari 2020 EU:s verktygslåda för 5G-säkerhet. Verktygslådan innehåller rekommenderade åtgärder som kan vidtas för att reducera identifierade risker. Åtgärderna, vilka inte är bindande för medlemsstaterna, omfattar bland annat att stärka säkerhetskraven för operatörer av mobilnät, bedöma leverantörers riskprofil och tillämpa relevanta begränsningar eller uteslutningar av leverantörer som utgör en hög risk samt säkerställa att varje operatör har en strategi för att undvika eller begränsa beroendet av en enda leverantör.

1.1.2 Cybersäkerhetsakten

Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) innehåller två huvudsakliga delar: (1) ett mandat för EU:s cybersäkerhetsbyrå, Enisa, och (2) ett ramverk för europeisk cybersäkerhetscertifiering (ECCF). ECCF infördes för att ersätta nationella certifieringsordningar med europeiska ordningar som möjliggör harmoniserade och

[1] *Samarbetsgruppen för nät- och informationssäkerhet*, inrättades genom Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).

standardiserade bedömningar av cybersäkerhetsnivån för produkter och tjänster på den inre marknaden. Europeiska certifieringsordningar bedömdes också kunna skapa förenklade villkor för både kunder och leverantörer. Enisa fick i cybersäkerhetsakten en central roll i att stötta kommissionen i certifieringsarbetet, bl.a. att bistå kommissionen i dess roll som ordförande för den europeiska gruppen för cybersäkerhetscertifiering (ECCG) och uppgiften att ta fram utkast på certifieringsordningar som beställs av kommissionen.

1.1.3 NIS 2-direktivet

Europaparlamentet och rådet antog den 14 december 2022 direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet). NIS 2-direktivet, som ersatte det tidigare NIS-direktivet från 2016, syftar till att höja den gemensamma cybersäkerhetsnivån inom EU. Direktivet omfattar 18 sektorer och innehåller skärpta cybersäkerhetskrav för både privata och offentliga aktörer. I Sverige har NIS 2-direktivet genomförts i huvudsak genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507).

1.1.4 Inre säkerhetsstrategin

Kommissionen presenterade i april 2025 dokumentet ProtectEU: Europeisk strategi för inre säkerhet[2]. I strategin aviserade kommissionen delar av det som nu presenteras i CSA 2-förslaget. I strategin anges bland annat att EU behöver en gemensam strategi om säkerhet och motståndskraft för IKT-leveranskedjor och IKT-infrastruktur, i syfte att motverka rådande fragmentering på den inre marknaden samt för att undvika kritiska beroenden och att säkra EU:s kritiska infrastruktur. Molntjänster och telekommunikationstjänster uppges vara centrala för leveranskedjorna för kritisk infrastruktur och kommissionen indikerar att kritiska entiteter bör välja sådana tjänster utifrån en lämplig cybersäkerhetsnivå, med beaktande av inte bara tekniska risker utan också strategiska risker och beroendeförhållanden. I strategin framhålls att EU:s verktygslåda för 5G-cybersäkerhet[3] har varit en lämplig ram för att skydda 5G-näten men att medlemsstaterna inte tillämpat verktygslådan tillräckligt effektivt. Allvarliga säkerhetsbrister beskrivs därför vara olösta, särskilt avseende utfasning av leverantörer som bedömts utgöra hög risk.

[2] Meddelande från Kommissionen till Europaparlamentet, Rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om ProtectEU: Europeisk strategi för inre säkerhet, KOM 2025/148.

[3] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt regionkommittén - Säker 5G utbyggnad i EU – Genomförande av EU:s verktygslå, KOM (2020) 50.

1.1.5 Förslaget om förordning om digitala nät

I samband med CSA 2-förslaget presenterade kommissionen den 21 januari ett förslag till förordning om digitala nät (Digital Networks Act, DNA).[4] Förslaget innehåller bland annat villkor som får förenas med anmälan och radiospektrumtillstånd som avser efterlevnad av de krav som föreslås i CSA 2.

1.2 Förslagets innehåll

1.2.1 Ändringar i Cybersäkerhetsakten

Enisas mandat uppdateras för att reflektera nya uppgifter i EU:s samlade cyberreglering

Enisas mandat föreslås förtydligas för att inkorporera alla de uppgifter som tillkommit Enisa i och med nya rättsakter som har införts sedan EU:s cybersäkerhetsakt trädde i kraft 2019. I vissa delar utökas också Enisas roll enligt kommissionens förslag. Kommissionen uppskattar också att förslaget skulle kräva en budgetökning för Enisa där byråns årliga budget från 2028 blir 49 miljoner EUR.

Förslaget innehåller nya uppgifter för Enisa kopplat till byråns operativa arbete. Bl.a. föreslås upprättande av en ny stödfunktion för att bemöta utpressningsangrepp, s.k. ransomware, samt uppgifter att tillhandahålla verktyg för säker kommunikation och verktyg som kan användas vid bedömning av överenstämmelse

[4] COM(2026) 16: Proposal Regulation Digital Networks Act (DNA).

med certifieringsordningar. I förslag på nya bestämmelser ska Enisa kunna ta ut avgifter för vissa tjänster och verktyg som byrån tillhandahåller. Därtill föreslås en ökad roll och nya funktioner inom sårbarhetshantering och hotunderrättelser. Vidare föreslås Enisa ingå som fast medlem i det nätverk för enheter för hantering av it-säkerhetsincidenter som inrättats enligt artikel 15 i NIS 2-direktivet (CSIRT-nätverket) samtidigt som byrån behåller sin sekretariatsroll inom nätverket. Enisa föreslås även få en tydligare roll avseende utvecklingen av en europeisk ram för cybersäkerhetskompetenser (ECSF). ECSF är ett ramverk med profiler för yrkesroller inom cybersäkerhet och utgör enligt kommissionens meddelande om ”Cybersecurity Skills Academy” (COM(2023) 207) grunden för att bedöma EU:s kompetensförsörjningsbehov inom cybersäkerhet.

Det tidigare nätverket för nationella sambandspersoner (NLO-nätverk) finns inte med i det nya förslaget. Medlemsstaterna ska istället enligt förslagen utse minst två nationella sambandspersoner som ska fungera dels som kontaktyta för medlemsstaternas förfrågningar mot Enisa och dels arbeta med Enisas ordinarie verksamhet. I fråga om arbetet i Enisas styrelse föreslås kommissionens godkännande krävas vid större beslut. Därtill föreslås att styrelsen primärt ska utgöras av chefer, eller i andra hand högre beslutsfattare, från medlemsstaternas cybersäkerhetsmyndigheter.

Effektivare och tydligare processer i ramverket för cybersäkerhetscertifiering

Kommissionen föreslår ändringar i ramverket för cybersäkerhetscertifiering som syftar till att effektivisera och förtydliga processerna för framtagandet av certifieringsordningar. De föreslagna ändringarna innebär bl.a. nya bestämmelser om hur kommissionen ska beställa utkast till certifieringsordningar från Enisa och vilken information en sådan beställning måste innehålla. Därtill finns nya bestämmelser om hur ordningar ska tas fram och hur de ska förvaltas. När det gäller förvaltning föreslås en tydlig roll för Enisa att i samverkan med medlemsstater, unionsorgan och privat sektor besluta om hur ordningar ska förvaltas. Det föreslås också nya tidsbestämmelser om de ingående stegen i framtagande av certifieringsordningar inklusive att framtagandet av nya ordningar ska ta högst 12 månader. Vidare utökas de säkerhetsmål som certifieringsordningar ska eftersträva, bl.a. i syfte att harmonisera ordningarna med nya bestämmelser i EU:s cyberresiliensförordning och NIS 2-direktivet. I förslagen stärks också Enisas möjlighet att ta fram egna specifikationer som kan ligga till grund för nya certifieringsordningar, t.ex. om tillämpliga harmoniserade internationella eller europeiska standarder bedöms saknas. Det framgår även tydligare skrivningar vilka premierar europeiska framför nationella certifieringsordningar. Bl.a. föreslås kommissionen kunna be medlemsstater att upphäva en nationell certifieringsordning. Europeiska cybersäkerhetscertifieringsgruppen (ECCG), där medlemsstaternas

certifieringsmyndigheter ingår, skulle dock i vissa fall kunna föreslå för kommissionen att beställa en ny certifieringsordning.

Därtill finns ett antal nya förslag i förhållande till ramverkets utformning i EU:s cybersäkerhetsakt av idag. Bland dessa finns att kommissionen aviserar en ny certifieringsordning för NIS 2-entiteters cybersäkerhet. Denna ska kunna användas för certifiering mot kraven på rikshanteringsåtgärder i NIS 2-direktivet, bl.a. för att entiteter med gränsöverskridande verksamhet ska kunna uppvisa efterlevnad av riskhanteringsåtgärderna i NIS 2-direktivet men också efterlevnad av andra unionsöverskridande eller sektoriella regelverk med säkerhetskrav. Den nya certifieringsordningen går i linje med att innehav av certifikat utfärdade från europeiska certifieringsordningar föreslås kunna innebära presumtion om regelefterlevnad av EU:s cyber- och digitala reglering i tillämpliga delar.

Vidare föreslås ett råd (European Cybersecurity Certification Assembly) inrättas för att på minst årlig basis samla relevanta intressenter för strategiska diskussioner om cybersäkerhetscertifiering inom unionen. Den intressentgrupp för cybersäkerhetscertifiering som etablerades i första cybersäkerhetsakten finns inte heller i det nya förslaget. Istället ska Enisa, utöver ovan nämnda råd, löpande samverka med relevant industri och andra parter inom ramen för ett brett externt samverkansmandat.

Ett nytt ramverk för EU-harmoniserat tillvägagångssätt avseende stärkt säkerhet i IKT-leveranskedjor

Kommissionen föreslår ett ramverk för att adressera icke-tekniska risker i IKT-leveranskedjor i högkritiska sektorer och andra kritiska sektorer enligt direktiv (EU) 2022/2555. Mekanismen som föreslås syftar till att identifiera viktiga IKT-tillgångar i kritiska IKT-leveranskedjor och föreslå lämpliga och proportionerliga åtgärder för de entiteter som framgår av bilaga I och II till direktiv (EU) 2022/2555.

Ramverket tar sin utgångspunkt i artikel 22 i NIS 2-direktivet om samordnade säkerhetsriskbedömningar för kritiska leveranskedjor och kompletterar denna med ytterligare bestämmelser om roller och processer för hur sådana bedömningar ska genomföras. Innebörden av förslagen är bl.a. att kommissionen, med utgångspunkt i bedömningar genomförda enligt artikel 22 i NIS 2-direktivet eller utifrån andra specificerade underlag, bl.a. ska kunna anta genomförandeakter om utnämning av tredjeländer som utgör cybersäkerhetsrisk och identifiera högriskleverantörer från sådana länder. Innan sådana genomförandeakter tas fram ska kommissionen också analysera om landet i fråga har lagar eller bevisad praxis som kräver att företag rapporterar sårbarheter i mjuk- och hårdvara till nationella myndigheterna innan de uppmärksammats offentligt, om landet saknar effektiva rättsmedel och oberoende demokratisk kontroll som kan korrigera identifierade risker. Vidare ska bedömas huruvida hotaktörer som

kontrolleras från landet bedriver skadlig cyberaktivitet samt om landet saknar förmåga eller vilja att samarbeta med kommissionen eller medlemsstaterna för att hantera identifierade risker. Ramverket innehåller också en interventionsmekanism för att, under särskilda omständigheter, kunna tillämpas på leverantörer på den inre marknaden som står under kontroll av tredjeländer eller leverantörer som utgör hög risk eller som kontrolleras av medborgare från ett sådant land.

För identifierade högriskleverantörer föreslås flera begränsningar som ska kunna införas bl.a. i förhållande till hur NIS 2-entiteter får nyttja sådana leverantörer, där kommissionen via genomförandeförordningar ska kunna förbjuda respektive kräva utfasning av utrustning från leverantörerna eller införa krav på riskreducerande åtgärder avseende användning av utrustning från leverantörerna. Enligt förslaget ska dock åtgärder som vidtas utifrån ramverket inte hindra medlemsstater från att anta eller bibehålla nationella bestämmelser för att säkerställa ett högre skydd. Därtill föreslås begränsningar avseende bl.a. högriskleverantörers möjlighet att delta i offentliga upphandlingar inom EU som rör tillhandahållande av komponenter för viktiga IKT-tillgångar, att ta del av EU-finansiering eller ingå i europeiskt standardiseringsarbete.

Av förslaget framgår särskilda bestämmelser rörande utfasning av utrustning från högriskleverantörer respektive förbud mot att

installera ny utrustning från sådana leverantörer i mobilnät, fibernät och satellitnät för elektroniska kommunikationer. För mobilnät gäller att sådan utfasning ska ske inom 36 månader från publicering av en genomförandeakt där högriskleverantören i fråga definieras.

Leverantörer ska, innan de definieras som högriskleverantörer, enligt förslagen kunna höras. Vidare ska det gå att ansöka om undantag för att ingå i IKT-leveranskedjor hos NIS 2-entiteter eller för att deltaga i offentlig upphandling av komponenter som ingår i viktiga IKT-tillgångar. Därtill finns i förslaget bestämmelser om tillsyn och verkställighetsåtgärder. Sanktioner ska också kunna utfärdas mot NIS 2-entiteter vid överträdelser av sådana genomförandeaktörer som förbjuder nyttjande av komponenter från högriskleverantörer inom viktiga IKT-tillgångar eller av krav på riskreducerande åtgärder enligt antagna genomförandeakter. Det föreslås vidare att den nationella myndigheten enligt CSA 2 ska kunna begära att en regleringsmyndighet enligt DNA-förslaget återkallar tillhandahållares radiospekrumtillstånd eller rätt att tillhandahålla elektroniska kommunikationsnät eller -tjänster. Detta föreslås gälla vid bristande efterlevnad av säkerhetskraven i CSA 2.

1.2.2 Ändringar i NIS 2-direktivet

Direktivets tillämpningsområde

Förslaget innebär bl.a. att tillämpningsområdet för NIS 2-direktivet utökas då nya aktörer inkluderas som NIS 2-entiteter. Det berör leverantörer av europeiska digitala identitetsplånböcker och europeiska företagsplånböcker, som föreslås klassificeras som väsentliga entiteter, oavsett storlek. Vidare föreslås alla operatörer av undervattensinfrastruktur för elektronisk kommunikation ingå i direktivets omfattning, såväl tillhandahållare av allmänna som icke-allmänna elektroniska kommunikationsnät. Även alla entiteter som ansvarar för strategisk infrastruktur med både civil och militär användning (dubbla användningsområden) ska omfattas av direktivets tillämpningsområde.

Förslaget innebär också att vissa aktörer inte längre ska omfattas av direktivet. Endast elproducenter med en produktionskapacitet på över en megawatt ska omfattas av direktivet, förutsatt att de i övrigt uppfyller storlekskravet i direktivet. Kravet om produktionskapacitet gäller även elproducenter som driver flera anläggningar vars sammanlagda produktionskapacitet överstiger en megawatt.

Kommissionen föreslår att en ny storlekskategori av företag inkluderas i direktivet, små midcapföretag, vilket omfattar företag som sysselsätter färre än 750 personer och har en årlig omsättning som inte överstiger 150 miljoner euro eller en årlig

balansomslutning som inte överstiger 129 miljoner euro. Kommissionen föreslår vidare att entiteter som överstiger trösklarna för små midcap-företag ska klassificeras som väsentliga. Kommissionen föreslår även att den allmänna storleksregeln ska tillämpas på leverantörer av domännamnssystemstjänster (DNS-tjänsteleverantörer) vilket medför att mindre sådana aktörer inte längre kommer att omfattas av direktivet.

Förslaget innehåller också vissa förtydliganden i direktivets bilagor I och II avseende vårdgivare, elproducenter, vätgasverksamheter och aktörer inom kemisektorn, som har till syfte säkerställa rättssäkerhet och minska bördan för både verksamheter och nationella myndigheter.

Enisas och kommissionens uppgifter

Enisa ska enligt förslaget stödja medlemsstater i tillsynen av entiteter som tillhandahåller tjänster inom flera medlemsstater. Det innebär också att nationella tillsynsmyndigheter ska skicka in information till Enisa om bland annat de cybersäkerhetsrelaterade riskhanteringsåtgärder som den väsentliga eller viktiga entiteten har vidtagit. Enisa ska också genomföra analyser av gränsöverskridande cybersäkerhetskrav och lämna rekommendationer om tillsyn i samverkan mellan berörda medlemsstater. Vidare föreslås att kommissionen ska utvärdera behovet av genomförandeakter. I det fall kommissionen antar

genomförandeakter får medlemsstaterna inte införa ytterligare nationella krav avseende de åtgärder som avses i artikel 21.2 i NIS 2-direktivet.

I förslaget anges även att kommissionen bör utveckla riktlinjer för NIS 2-entiteters krav på leverantörer avseende säkerhet i leveranskedjor. Syftet är att säkerställa rättslig tydlighet och förhindra att skyldigheter på ett otillbörligt sätt överförs till aktörer som inte omfattas av NIS 2-direktivet.

Nya krav på rapportering av utpressningsprogram

Förslaget innehåller krav på harmoniserad insamling av uppgifter om utpressningsprogram, s.k. ransomware-angrepp. NIS 2-entiteter ska enligt förslaget ange information om en incident har sitt ursprung i ett ransomware-angrepp samt hur entiteten hanterat incidenten, inklusive om något lösenbelopp begärts samt huruvida entiteten gjort någon sådan betalning.

1.3 Gällande svenska regler och förslagets effekt på dessa

Cybersäkerhetsakten är en förordning och därför direkt tillämplig i svensk rätt utan att den behövs genomföras i nationell lagstiftning. De ändringar som enligt förslaget ska göras i förordningen blir även de direkt tillämpliga. Viss kompletterande svensk lagstiftning kan eventuellt komma att behöva ses över, såsom lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt och förordning (2021:555) med kompletterande bestämmelser till EU:s

cybersäkerhetsakt. Förslaget bedöms också påverka lagen (2022:482) om elektronisk kommunikation. Detta bland annat genom förslag om åtgärder mot högriskleverantörer i mobilnät, fasta nät och satellitnät för elektroniska kommunikationer.

Direktivförslaget bedöms påverka nationella regler som genomför NIS 2-direktivet i svensk rätt. Sverige har genomfört direktivet i huvudsak genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507). Även ändringar av myndigheters föreskrifter kan bli aktuella.

Vilka ytterligare ändringar i svensk lagstiftning som kan behöva göras är föremål för fortsatt analys.

1.4 Budgetära konsekvenser och konsekvensanalys

Enligt kommissionen skulle förslaget innebära att Enisas budget ökar med 81,5 procent till cirka 49 miljoner EUR från år 2028. Kommissionen har angett att detta ska finansieras genom omprioriteringar i den innevarande fleråriga budgetramen (MFF) och till viss del genom att Enisa kan ta ut nya avgifter bl.a. inom ramen för ECCF och för byråns verktyg för it-säkerhet. Huruvida detta träffar primärt näringslivets gränsytor mot Enisa, eller om det också kan innebära ekonomiska konsekvenser för offentlig sektor i Sverige, behöver analyseras vidare.

Inrättandet av ett europeiskt ramverk för säkerhet i IKT-leveranskedjor skulle innebära budgetmässiga åtaganden då det

skulle ge nya uppgifter för de myndigheter som utövar tillsyn under den svenska NIS 2-regleringen då dessa också föreslås utöva tillsyn av bestämmelserna i det nya ramverket. Krav på att vidta riskreducerande åtgärder inom IKT-leveranskedjor eller krav på utfasning av, eller förbud mot, användning av vissa leverantörers komponenter inom viktiga IKT-tillgångar kommer också påverka svenska NIS 2-entiter.

2. Ståndpunkter

2.1 Preliminär svensk ståndpunkt

2.1.1 Budgetära konsekvenser

Regeringen anser att huruvida det finns utrymme att öka Enisas budget är något som bör beslutas inom ramen för förhandlingarna om EU:s långtidsbudget. Regeringen har en budgetrestriktiv hållning och anser att eventuella utgiftsökningar inom EU:s budget ska finansieras genom omprioriteringar inom befintliga ramar. Regeringen värnar även principen om en sund ekonomisk förvaltning.

2.1.2 Cybersäkerhetsakten

Enisas mandat

Det är positivt att kommissionen presenterat ändringar som omhändertar det faktum att Enisas roll utvecklats organiskt de senaste åren. Regeringen ser att Enisa i största möjliga

utsträckning bör ha ett renodlat mandat fokuserat på stöd för implementering av EU-reglering, expertishjälp och vägledning samt att byråns roll inte bör överlappa med nationella eller andra EU-myndigheter. Vidare bör Enisas arbete i största möjliga mån vara horisontellt inriktat. Som huvudregel bör inte, utan särskilda skäl, verksamhet med fokus på särskilda sektorer eller andra verksamhetsmässiga delområden tillföras. Nya uppgifter för byrån bör följas av tydliga krav på informationsdelning och samverkan med nationella myndigheter, samt finansieras inom befintliga ekonomiska ramar.

Att förslaget utgår från att Enisa ska ha en självständig roll inom ramen för certifieringsramverket (ECCF), är också positivt och kan bidra till ökad effektivitet i Enisas verksamhet inom ramen för ECCF.

Nya uppgifter som föreslås för Enisa bör alltid föregås av analys av byråns kapacitet, befintliga resurser och huruvida Enisa är bäst lämpat att utföra uppgiften. I sammanhanget är det en nyckelfaktor att Enisas styrelse involveras i sådana överväganden och kan vägleda byrån genom att bidra till vilka prioriteringar som görs för byråns verksamhet. Vidare anser regeringen att det är centralt att eventuella ambitionshöjningar hanteras inom ramen för befintliga resurser.

Regeringen ställer sig positiv till att det nuvarande nätverket för nationella sambandspersoner inte finns med i det nya förslaget, då ett avvecklande av nätverket kan frigöra resurser och istället främja användning av uppbyggda kanaler för kommunikation mellan intressenter i medlemsstater och EU-nivå (såsom via nationella samordningscentrum i NCC-nätverket). Regeringen behöver dock ytterligare analysera den föreslagna modellen där varje medlemsstat åläggs att bidra med två sekonderade nationella experter till Enisa som ska utgöra sambandspersoner.

Regeringen ser att de förslag som innebär att medlemsstaternas ges en stark, drivande roll via Enisas styrelse är positiva. CSA 2 bör inte precisera tjänstenivå eller yrkeskategori för medlemsstaternas delegater i Enisas styrelse. Sådana överväganden sköts bäst av medlemsstaterna själva.

Regeringen ämnar slå vakt om att Enisas roll inte blir övervägande operativ i förhållande till övriga uppgifter av stödjande karaktär. Det är centralt att EU-nivån inte duplicerar sådant som redan görs på nationell nivå och att arbetet bedrivs på ett kostnadseffektivt sätt. I sammanhanget krävs ytterligare analys av Enisas roll att ta fram vissa verktyg, inklusive sådana som byrån ska kunna ta ut avgifter för, men också förslaget att Enisa ska ingå i CSIRT-nätverket. Upprättandet av ett stödcenter inriktat på utpressningsprogram, s.k. ransomware, kan riskera att dels påverka Enisa i en operativ inriktning och dels förflytta byråns

tonvikt från en horisontell ansats till att fokusera på särskilda delområden. Sverige bör dock ställa sig positivt till att kompetensramverket ECSF vidareutvecklas enligt förslaget i CSA 2, med beaktande av att ECSF bör utgöra ett efterfrågestyrt och flexibelt verktyg som är frivilligt för medlemsstaterna. Att ramverket utökas med ett certifieringsliknande förfarande där kompetenser ska attesteras kräver dock ytterligare överväganden.

Certifieringsramverket (ECCF)

Regeringen ser positivt på tydligare och mer transparenta bestämmelser rörande framtagande av certifieringsordningar och att ramverket effektiviseras i syfte att öka takten i framtagandet av certifieringsordningar. Nya tidsgränser behöver dock vara realistiska och får inte innebära att viktiga säkerhetsaspekter missas i framtagandet av ordningar. Regeringen ser positivt på att förslagen understryker Enisas självständiga roll och mandat för extern intressentsamverkan. När Intressentgruppen för certifiering samtidigt föreslås utgå krävs att Enisa agerar självständigt inom ECCF samtidigt som byrån säkerställer adekvat samverkan med och faktainhämtning från experter både från medlemsstater och industri. Här bör det nya rådet för certifiering spela en roll avseende externa intressenters möjlighet till insyn och påverkan i ECCF. Detta gäller också vid förvaltning av certifieringsordningar, där både medlemsstater och industri har nyckelfunktioner.

Regeringen avser även värna om att privata certifieringsorgan fortsatt kan utfärda certifikat enligt ECCF.

Regeringen ser positivt på förslag syftandes till att certifieringsordningar ska kunna omhänderta bestämmelser i reglering som tillkommit sedan cybersäkerhetsakten trädde i kraft 2019 då det kan förenkla regelefterlevnad. Samtidigt är det viktigt att certifiering som grundregel fortsatt är frivilligt. Regeringen bedömer att förslag rörande att certifieringsordningar ska kunna nyttjas som ett instrument för aktörer att uppnå och demonstrera regelefterlevnad kan bidra till minskad administrativ börda. Regeringen vill understryka att certifieringar utgör en delmängd i detta arbete, och att nationella tillsynsmyndigheter alltid har rätt att inleda tillsyn – och att ytterst finna att ett tillsynsobjekt inte efterlever tillämplig reglering – trots innehav av certifikat som utfärdats inom ECCF.

Regeringen tillstyrker att europeisk certifiering bör ha företräde framför nationella certifieringsordningar. Det är väsentligt att undvika fragmentering på den inre marknaden som det kan innebära om aktörer behöver förhålla sig till olika nationella system och tillvägagångssätt inom certifiering.

Regeringen välkomnar att de säkerhetsmål som certifieringsordningar ska ta i beaktande inte inkluderar geopolitiska, icke-tekniska krav då sådana krav inte bör ingå i

tekniska certifieringsordningar. Samtidigt krävs mer analys av de utökade säkerhetsmålen som föreslås i CSA 2. Vidare anser regeringen att certifieringsordningar primärt bör bygga på internationell eller europeisk standardisering.

Ramverk för säkerhet i IKT-leveranskedjor

Regeringen ser att nya, unionsöverskridande regler avseende icke-tekniska risker i IKT-leveranskedjor i högkritiska och kritiska sektorer kan ge framåtdrift i EU:s samlade säkerhetsarbete under förutsättning att dessa är väl utformade och balanserade. Regeringen välkomnar därför kommissionens ambition om att få framdrift i och ökad harmonisering av medlemsstaternas säkerhetsarbete i förhållande till icke-tekniska faktorer för IKT-leveranskedjor. Regeringen noterar att förslaget också omfattar vissa tekniska cybersäkerhetsåtgärder och anser även att det är viktigt att dessa harmoniserar med den horisontella regleringen i NIS 2- och CER-direktiven.

Regeringen noterar vidare att medlemsstaternas nationella regelverk för att åtgärda icke-tekniska risker i mobilnät är fragmenterade, och att rekommendationerna i EU:s verktygslåda för 5G-säkerhet inte genomförts fullt ut i flera EU-länder. Regeringen välkomnar därför kommissionens förslag som syftar till att säkerställa en harmoniserad ansats till icke-tekniska sårbarheter i 5G-nät. I nu gällande svensk lagstiftning är frågan om identifiering av och åtgärder mot högriskleverantörer i mobilnät en

fråga för bedömning i relation till vilket hot sådana utgör mot Sveriges säkerhet. Målsättningen med den lagstiftningen överensstämmer i stora delar med CSA 2-förslaget. Vidare konstateras att förslagen om krav på utfasning av högriskleverantörer i fasta nät och satellitnät för elektroniska kommunikationer är långtgående och regeringen ser att närmare analys är nödvändig, i synnerhet i förhållande till vilka inverkningar de får för svenska företag. De föreslagna reglerna bedöms därutöver få konsekvenser för Sveriges nationella bestämmelser på området.

Vidare noterar regeringen att frågor om säkerhet i IKT-leveranskedjor tangerar frågor om nationell säkerhet som är medlemsstaters eget ansvar enligt fördraget om Europeiska unionen. Regeringen erinrar därför om att gemensamma åtgärder aldrig kan hindra medlemsstaterna från att vidta åtgärder för att säkerställa ett högre skydd än vad som krävs av EU-rätten i de fall det är nödvändigt av nationella säkerhetsskäl.

Riskbedömningar som föreslås ligga till grund för utpekande av länder och leverantörer med hög risk bör vara principbaserade och präglas av gedigen analys som medlemsstaterna deltar eller ges insyn i. Det är centralt att ramverket är proportionerligt och används i linje med EU:s åtaganden i handelsavtal samt inte nyttjas för omotiverad protektionism. Regeringen noterar att förslagen innehåller mekanismer för hur företag som pekas ut

genom ramverket ska kunna höras innan kommissionens beslut fattas samt möjlighet för företagen att ansöka om undantag, vilket torde vara nödvändigt men kräver ytterligare analys.

2.1.3 NIS 2-direktivet

Sverige välkomnar kommissionens förslag till direktiv. Förslaget innehåller bestämmelser om ändringar i tillämpningsområdet för NIS 2-direktivet som väntas bidra till ökad regelefterlevnad och minska den administrativa bördan för berörda aktörer och tillsynsmyndigheter.

Regeringen ställer sig vidare positiv till att leverantörer av europeiska digitala identitetsplånböcker och företagsplånböcker omfattas av direktivet, då detta väntas stärka unionens samlade cyberresiliens. Det är dock viktigt att särskilja plånböckerna från varandra gällande kraven i direktivet, då den dimensionerande säkerhetsnivån skiljer sig mellan respektive plånbok, och detta är något regeringen kommer att verka för. Mot bakgrund av den rådande hotbilden mot undervattensinfrastruktur anser regeringen att relevanta operatörer av sådan infrastruktur bör omfattas av direktivet cybersäkerhetskrav.

Regeringen bedömer vidare att det krävs en noggrann analys av vilka aktörer som är relevanta att inkludera vad gäller strategisk infrastruktur med både civil och militär användning (dubbla användningsområden) för att säkerställa en väl avvägd reglering.

Vidare bedömer regeringen att en väl avvägd reglering även behöver åstadkommas vad gäller det nationella utrymmet för ytterligare cybersäkerhetskrav i förhållande till sådana som kan finnas i genomförandeakter. Kommissionens förslag om Enisas utökade stöd till nationella myndigheter behöver samtidigt ses i ljuset av de förslag som presenteras i cybersäkerhetsakten avseende Enisas roll och mandat. Regeringen är i grunden positiv till byråns stödjande roll vid genomförande av regelverk. Förslaget om att fler uppgifter ska överföras till Enisa från nationella myndigheter behöver dock vägas noggrant mot risken att detta leder till onödig hög administrativ belastning, ökade kostnader och minskad kostnadseffektivitet.

Regeringen avser verka för att direktivet inte ska medföra en högre regelbörda för offentliga såväl som privata aktörer. Det pågår beredning inom Regeringskansliet om närmare ståndpunkter för direktivförslaget.

2.2 Medlemsstaternas ståndpunkter

Medlemsstaternas ståndpunkter gällande förslagen så som de nu presenterats är ännu inte kända, men flera medlemsstater har förmedlat preliminära ståndpunkter i informella ståndpunktspapper. Några av huvuddragen i dessa redogörs för nedan.

Flera länder (bl.a. **Finland** och **Frankrike**) har välkomnat att EU:s cybersäkerhetsreglering förenklas och harmoniseras. Samtidigt har båda medlemsstater betonat att det, innan nya uppgifter tilldelas Enisa, krävs noggrann utvärdering och motivering av nya uppdrag samt att Enisas mandat bör vara fokuserat och komplettera (inte överlappa med) nationella myndigheters eller andra EU-organs roller.

Flera länder (bl.a. **Tyskland** och **Tjeckien**) har välkomnat en revidering av EU:s cybersäkerhetsakt men noterar att den borde föregåtts av en utvärdering av akten som skulle ha presenterats för medlemsstaterna redan under 2024. Att istället publicera utvärderingen tillsammans med förslaget har därför beskrivits som icke-ändamålsenligt.

Flera länder (bl.a. **Tyskland, Frankrike** och **Tjeckien**) har lyft att nya rättsakter sedan 2019 inneburit ett antal nya uppgifter för Enisa och att detta skett utan att åtföljas av en långsiktigt stabil ökning av Enisas resurser.

Ett antal medlemsstater (**Österrike, Belgien, Bulgarien, Kroatien, Tjeckien, Estland, Finland, Frankrike, Tyskland, Ungern, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Slovakien, Slovenien**) har gemensamt framfört önskan att Enisa får en roll som expertcentrum för cybersäkerhet som stödjer medlemsstaterna och fungerar som en kunskaps-

och/informationsspridande, horisontell och tvärsektoriell myndighet samt en möjliggörare för EU-samarbete utan att bli en operativ entitet (såsom en CSIRT). Vidare nämns stärkt samarbete med europeiska standardiseringsorgan samt att Enisas styrelse får stärkt mandat att ge byrån vägledning och prioriteringar som viktiga frågor.

Flera medlemsstater (bl.a. **Spanien, Irland** och **Belgien**) har framfört att certifieringsramverket behöver förändras och att dess processer behöver förtydligas för att bli effektivt. De har bl.a. föreslagit ändringar i roller, i hur ECCG fungerar och kring hur certifieringsordningar tas fram och förvaltas.

Polen har argumenterat för att ändringarna i EU:s cybersäkerhetsakt bör användas för att göra Enisa till referensmyndighet för all cybersäkerhet och att Enisa bör involveras tidigt i processer som kan leda till lagstiftningsförslag.

2.3 Institutionernas ståndpunkter

Inga ståndpunkter är kända för närvarande.

2.4 Remissinstansernas och andra intressenters ståndpunkter

Förslagen har inte skickats ut på remiss.

3. Förslagets förutsättningar

3.1 Rättslig grund och beslutsförfarande

Som rättslig grund har kommissionen angett artikel 114 i Fördraget om Europeiska unionens funktionssätt (EUF). Beslut fattas enligt ordinarie lagstiftningsförfarande, dvs. Europaparlamentet och rådet fattar beslut gemensamt.

3.2 Subsidiaritets- och proportionalitetsprinciperna

Eftersom de rättsakter som det föreslås ändringar i antogs på EU-nivå bedömer kommissionen att de bara kan ändras på EU-nivå. Kommissionen bedömer även att förslagen som lagts fram likväl upprätthåller subsidiaritetsprincipen.

Kommissionen bedömer vidare att initiativet till förslagen inte går längre än vad som är nödvändigt för att uppnå syftet med förenklingsåtgärderna utan att minska skyddet för hälsa, säkerhet och grundläggande rättigheter, samt att förslagen bevarar och optimerar de syften som de ändrade rättsakterna bygger på.

Regeringen delar preliminärt kommissionens bedömningar.

4. Övrigt

4.1 Fortsatt behandling av ärendet

Kommissionens förslag presenterades i rådet den 26 januari 2026. Förslagen förhandlas i rådet under våren 2026. Ordförandeskapet i

rådet har kommunicerat en förväntan om att kunna avsluta förhandlingarna om Enisas mandat i CSA 2 under våren 2026. Förslagen väntas huvudsakligen diskuteras och förhandlas i den horisontella arbetsgruppen för cyberfrågor (HWP CI).

4.2 Fackuttryck och termer

CSIRT: enheter för hantering av it-säkerhetsincidenter (computer security incident response teams).

Cybersäkerhet: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

IKT: Informations- och kommunikationsteknik.

IKT-leveranskedjor: en summa av IKT-tjänster, IKT-produkter och IKT-processer som omfattar aktiviteter och aktörer som är inblandade i alla stadier innan en produkt blir tillgänglig eller en tjänst levereras på marknaden.

Kritiska entiteter: en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan i CER-direktivet.

Kritisk infrastruktur: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning,

utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst.

Ransomware: utpressningsvirus och program som krypterar hela eller delar av en verksamhets information som lagras på drabbade informationssystem och gör informationen otillgänglig.

EUROPEISKA
KOMMISSIONEN

Strasbourg den 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan samt om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2)

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Sedan cybersäkerhetsakten antogs 2019 har hotbilden på cybersäkerhetsområdet utvecklats avsevärt[1] i en alltmer komplex geopolitisk verklighet. Antalet cyberattacker har ökat och de har blivit mer sofistikerade och inriktade på kritisk infrastruktur, företag och allmänheten, med utpressningsprogram som ett centralt inslag[2]. Framväxande teknik som artificiell intelligens (AI) och kvantdatorteknik omformar försvarsverktygen och fiendens taktik. I Mario Draghis **rapport om EU:s framtida konkurrenskraft** från 2024 framhölls behovet av att öka säkerheten och minska beroendet som ett viktigt åtgärdsområde i EU[3]. Både EU:s strategi för en beredskapsunion[4] och den europeiska strategin för inre säkerhet (ProtectEU)[5] har satt cybersäkerheten i centrum för EU:s agenda för motståndskraft. Inom ramen för dessa strategier erkänns att bestående cybersäkerhetshot inte bara utgör tekniska utmaningar, utan även strategiska risker för vår demokrati, ekonomi och livsstil. I meddelandet om att stärka EU:s ekonomiska säkerhet[6] fastställs även som prioriterade mål att förhindra tillgången till känslig information och känsliga uppgifter som skulle kunna undergräva unionens ekonomiska säkerhet samt att förebygga och mildra störningar av EU:s kritiska infrastruktur som påverkar unionens ekonomi. I detta sammanhang spelar effektiva cybersäkerhetsåtgärder en avgörande roll.

Mot denna bakgrund **finns det fyra huvudsakliga problem** som denna föreslagna översyn av cybersäkerhetsakten syftar till att ta itu med: i) den bristande överensstämmelsen mellan unionens policyram för cybersäkerhet och berörda parters behov i en alltmer fientlig hotmiljö, ii) det avstannade genomförandet av det europeiska ramverket för cybersäkerhetscertifiering, iii) komplexiteten och mångfalden hos den cybersäkerhetsrelaterade politiken, som påverkar unionens cybersäkerhetsstatus, och iv) ökade säkerhetsrisker för IKT-leveranskedjor.

På grundval av de huvudsakliga problem som konstaterats är de **två allmänna målen** för insatsen att öka kapaciteten och resiliensen på cybersäkerhetsområdet samt att förhindra fragmentering på den inre marknaden genom att

- bidra till att stärka unionens styrning av cybersäkerheten och hjälpa till att säkerställa att de relevanta institutionerna och myndigheterna samt andra berörda parter är bättre rustade för att förebygga, upptäcka och reagera på cybersäkerhetshot på ett samordnat och effektivt sätt, och
- stödja utvecklingen, genomförandet och användningen av unionens gemensamma cybersäkerhetsinstrument, såsom certifieringsordningar, samt tillhandahålla harmoniserade ramar som skapar förtroende och interoperabilitet mellan medlemsstaterna.

---

1 Enisas hotbildsrapport 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
2 Enisas hotbildsrapport 2025.
3 Europeiska kommissionen, *The future of European Competitiveness*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
4 JOIN(2025) 130 final.
5 COM(2025) 148 final.
6 JOIN(2025) 977 final.

Dessa allmänna mål motsvarar de centrala utmaningar som konstaterades i problemformuleringen. De återspeglar det övergripande politiska målet att stärka cybersäkerhetsstyrningen i unionen och stödja utvecklingen av en säker, resilient och konkurrenskraftig digital inre marknad.

För att bidra till att uppnå de allmänna mål som anges ovan har denna insats följande **specifika mål**:

- Ta itu med den bristande överensstämmelsen mellan unionens policyram för cybersäkerhet och berörda parters behov:
  - Specifikt mål nr 1: skapa kapacitet att effektivt genomföra unionens cybersäkerhetspolitik och kontinuerliga operativa samarbete som möjliggör ett mer strukturerat samarbete mellan medlemsstaterna.
  - Specifikt mål nr 2: utveckla och genomföra medel och mekanismer för att effektivt stödja och tillgodose behoven hos medlemsstaterna, näringslivet och andra berörda parter.
- Ta itu med den begränsade användningen av och effektiviteten hos det europeiska ramverket för cybersäkerhetscertifiering:
  - Specifikt mål nr 3: skapa förutsättningar för ett snabbare genomförande av ordningar för cybersäkerhetscertifiering som drivs av marknadsbehov genom att utvidga tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering, säkerställa effektivt underhåll och smidiga förfaranden samt öka öppenheten.
- Ta itu med det fragmenterade efterlevnadslandskapet och komplexiteten i övergripande och sektorsspecifika ramar:
  - Specifikt mål nr 4: skapa mekanismer och villkor för att underlätta efterlevnaden av cybersäkerhetskraven och därigenom göra genomförandet mer samstämmigt och effektivt.
- Ta itu med cybersäkerhetsrisker i leveranskedjan:
  - Specifikt mål nr 5: minska de risker för kritiska IKT-leveranskedjor som orsakas av entiteter som är etablerade i eller kontrolleras av entiteter från tredjeländer som utgör cybersäkerhetsproblem (högriskleverantörer) och minska kritiska beroenden genom att utarbeta en samstämmig och ändamålsenlig ram på EU-nivå för att hantera säkerhetsrisker för IKT-leveranskedjan.

Översynen av cybersäkerhetsakten omfattas av **programmet om lagstiftningens ändamålsenlighet och resultat (Refit-programmet)**. Den bidrar starkt till att öka tydligheten, råda bot på ineffektivitet och anpassa förfarandena inom de rättsliga ramarna. Översynen bidrar även till att den inre marknaden fungerar väl och säkerställer samtidigt unionens säkerhet och strategiska oberoende.

Mer konkret föreslås en fullständig reform av mandatet för Europeiska unionens cybersäkerhetsbyrå (Enisa) som ger effektivt stöd för genomförandet av politiken och mervärde i form av stöd till operativt samarbete mellan medlemsstaterna.

Med tanke på de ökande cybersäkerhetsrisker och cybersäkerhetsutmaningar som unionen står inför syftar förslaget till att öka Enisas ekonomiska resurser och personalresurser för att återspegla dess förstärkta roll och uppgifter och dess centrala position när det gäller att försvara unionens digitala ekosystem, så att Enisa effektivt kan utföra de uppgifter som byrån tilldelas genom detta förslag.

Översynen kommer också att bidra till att undanröja fragmenterade metoder, förbättra samordningen och samtidigt sänka efterlevnads- och driftskostnaderna på lång sikt. Genom att upphäva den nuvarande cybersäkerhetsakten och införa ett reformerat europeiskt ramverk för cybersäkerhetscertifiering tillhandahåller förslaget ett mer effektivt och ändamålsenligt verktyg som både främjar förtroendet mellan företag, allmänheten och offentliga myndigheter och underlättar efterlevnaden av relevant unionslagstiftning. Förslaget medför en effektivisering genom att styrningsmodellen ses över och mer förutsägbara, samstämmiga och smidiga certifieringsförfaranden stöds, så att ordningarna kan utvecklas och genomföras snabbare.

De större synergieffekterna med relevanta befintliga unionsrättsliga ramar kommer att främja certifiering som ett efterlevnadsverktyg för företag och minska den administrativa bördan för organ för bedömning av överensstämmelse som är verksamma inom flera delar av cybersäkerhetslagstiftningen. Genom att utvidga tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering och göra det möjligt att utveckla en ordning för entiteters cybersäkerhetsstatus minskar förslaget dessutom efterlevnadskostnaderna för entiteter som omfattas av relevant unionslagstiftning om cybersäkerhet, i första hand entiteter som omfattas av NIS 2-direktivet. Detta tillvägagångssätt kommer att avsevärt förenkla regleringsskyldigheterna för entiteter som omfattas av flera efterlevnadskrav samt säkerställa att de nationella myndigheterna använder sina resurser mer effektivt. Utöver denna översyn finns ett förslag till direktiv om införande av riktade ändringar av NIS 2-direktivet som syftar till att förenkla efterlevnaden och säkerställa ett smidigt och samstämmigt genomförande av särskilda aspekter av cybersäkerhetsramen, bland annat i fråga om tillämpningsområde, definitioner, rapportering om incidenter med utpressningsprogram samt tillsyn av entiteter som tillhandahåller gränsöverskridande tjänster.

Genom den nya förordningen skapas även en harmoniserad ram för att hantera icke-tekniska risker som påverkar IKT-leveranskedjor, i syfte att minska den nuvarande fragmenteringen av strategier i medlemsstaterna. Tillsammans utgör dessa aspekter en betydande förenkling och modernisering av unionens rättsliga ram för cybersäkerhet, helt i linje med Refit-programmets principer om tydlighet, effektivitet och digital beredskap.

- **Förenlighet med befintliga bestämmelser inom området**

Unionen har utökat sina rättsliga och politiska verktyg genom att anta ett antal rättsliga instrument och politiska åtgärder: i) NIS 2-direktivet syftar till att stärka cybersäkerheten för kritisk infrastruktur. ii) I dess ”systerdirektiv”, närmare bestämt direktivet om kritiska entiteters motståndskraft, fastställs fysiska säkerhetsåtgärder. iii) Genom cyberresiliensförordningen höjs cybersäkerheten för produkter. iv) Genom cybersolidaritetsakten skapas EU-omfattande insatskapacitet. v) EU:s cyberplan[7] stöder krishanteringssamarbete på EU-nivå inom ramen för vilket kommissionen och den höga

[7] COM(2025) 66 final.

representanten spelar en viktig roll i förberedelserna inför och hanteringen av storskaliga cybersäkerhetsincidenter. vi) Verktygslådan för 5G-cybersäkerhet stöder cybersäkerhet i 5G-nätverk. vii) Den europeiska handlingsplanen för cybersäkerhet för sjukhus och vårdgivare[8] bidrar till att förbättra deras cybersäkerhet. viii) EU-akademin för cyberkompetens[9] bemöter den växande utmaning som kompetensbristen på cybersäkerhetsområdet utgör.

Den ovannämnda rättsliga ramen för cybersäkerhet kompletterades med sektorsspecifik lagstiftning, dvs. förordningen om digital operativ motståndskraft för finanssektorn, nätföreskrifter om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden för delsektorn för elektricitet eller informationssäkerhetsregler (DEL-IS[10]) för delsektorn lufttransport.

Översynen av cybersäkerhetsakten är anpassad till och stärker de bestämmelser i NIS 2-direktivet som rör Enisas roll när det gäller att stödja genomförandet av NIS 2-direktivet, även i fråga om stöd för operativt samarbete. Den är också anpassad till cyberresiliensförordningen, bland annat vad gäller översikten och hanteringen av sårbarheter på den inre marknaden, och den ökar även mervärdet av gemensam situationsmedvetenhet. Vad beträffar det europeiska ramverket för cybersäkerhetscertifiering är översynen av cybersäkerhetsakten anpassad till cyberresiliensförordningen angående produktsäkerhetsmålen och hanteringen av sårbarheter, och till den nya lagstiftningsramen avseende ackreditering. Vidare finns det starka synergieffekter som härrör från utvecklingen av certifiering av cybersäkerhetsstatus för NIS 2-direktivet och potentiellt för att underlätta efterlevnaden av andra relevanta unionsrättsakter såsom den allmänna dataskyddsförordningen, utan att det påverkar tillämpningen av deras särskilda certifieringskrav. Den övergripande ram som hanterar cybersäkerhetsrisker för IKT-leveranskedjor stöder dessutom NIS 2-direktivets övergripande mål att skapa en hög gemensam cybersäkerhetsnivå i hela unionen och bygger på den riskbaserade metoden i NIS 2-direktivet.

Genom översynen av cybersäkerhetsakten, i kombination med förslaget till direktiv om införande av riktade ändringar av NIS 2-direktivet i förenklingssyfte, tillhandahålls de nödvändiga verktygen för att göra denna heltäckande ram mer effektiv och ändamålsenlig i syfte att uppnå de förväntade resultaten, tillhandahålla en starkare europeisk dimension och täppa igen de återstående luckorna i lagstiftningen.

- **Förenlighet med unionens politik inom andra områden**

Översynen av cybersäkerhetsakten skulle komplettera direktivet om kritiska entiteters motståndskraft, som omfattar överväganden avseende leveranskedjan som en del av kritiska entiteters åtgärder för motståndskraft. Den skulle dessutom komplettera kommande initiativ, såsom i) EU-rättsakten om moln och AI-utveckling, som bland annat syftar till att åtgärda bristen på ett konkurrenskraftigt unionsbaserat erbjudande av molntjänster i tillräcklig omfattning för att kunna vara till nytta för mycket kritiska användningsfall eller sektorer, ii) förslaget till rättsakt om digitala nät, iii) den kommande översynen av förordning (EU) 2023/1781[11], iv) ramen för offentlig upphandling[12], som för närvarande håller på att

[8] COM(2025) 10 final.

[9] COM(2023) 207 final.

[10] Kommissionens genomförandeförordning (EU) 2023/203 och kommissionens delegerade förordning (EU) 2022/1645.

[11] Europaparlamentets och rådets förordning (EU) 2023/1781 av den 13 september 2023 om en ram med åtgärder för att stärka Europas halvledarekosystem och om ändring av förordning (EU) 2021/694 (förordning om halvledare), EUT L 229, 18.9.2023, s. 1.

utvärderas[13], och förslaget till förordning om förenkling av den digitala lagstiftningen (*det digitala omnibuspaketet*)[14], där det fastställs att Enisa ska utveckla en gemensam kontaktpunkt för rapportering av incidenter genom vilken de olika entiteterna samtidigt kan fullgöra sina skyldigheter att rapportera incidenter inom ramen för flera rättsakter. Översynen skulle dessutom stärka ställningen för unionens myndigheter och operatörer i samarbetet med partner i södra Medelhavsområdet, särskilt genom att främja sammankoppling genom säker och tillförlitlig digital infrastruktur i hela Medelhavsområdet, vilket är ett grundläggande mål för pakten för Medelhavsområdet.

Översynen av cybersäkerhetsakten är också i linje med unionens strategiska dokument, särskilt när det gäller ramen för säkerheten i IKT-leveranskedjor. Inom ProtectEU angav kommissionen vidare att en harmoniserad strategi för säkerheten i IKT-leveranskedjan kan ta itu med den nuvarande fragmenteringen av den inre marknaden på grund av olika strategier på nationell nivå, undvika kritiska beroendeförhållanden och minska de risker för IKT-leveranskedjor som högriskleverantörer medför och på detta sätt säkra den kritiska infrastrukturen. I strategin för ekonomisk säkerhet framhölls även behovet av att göra EU:s ekonomi och leveranskedja mer resilienta för att främja EU:s konkurrenskraft[15]. Behovet av att ta itu med avbrott i leveranskedjor samt cyberattacker betonades också i EU:s strategi för en beredskapsunion och i vitboken om europeisk försvarsberedskap[16]. Översynen är även anpassad till Mario Draghis rapport om EU:s framtida konkurrenskraft, vilket betonas ovan. Sist men inte minst överensstämmer översynen av cybersäkerhetsakten på området säkerhet i IKT-leveranskedjan med det nyligen antagna gemensamma meddelandet till Europaparlamentet och rådet om att stärka EU:s ekonomiska säkerhet[17].

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

• Rättslig grund

Den rättsliga grunden för detta förslag är artikel 114 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*). Enligt artikel 114 i EUF-fördraget ska sådana åtgärder vidtas som syftar till att upprätta den inre marknaden och få den att fungera. Förordning (EU) 2019/881 om Enisa och om cybersäkerhetscertifiering av informations- och kommunikationsteknik, allmänt känd som cybersäkerhetsakten[18], antogs ursprungligen i enlighet med denna bestämmelse.

När det gäller cybersäkerheten i IKT-leveranskedjan medför fragmenteringen av de nationella ramarna för att hantera icke-tekniska riskfaktorer negativa effekter på den inre marknadens funktion, eftersom skillnaderna mellan nationella strategier i förlängningen kan göra vissa medlemsstater mer sårbara, vilket kan få spridningseffekter i hela unionen och därmed påverka den övergripande motståndskraften och även tillförlitligheten.

---

12 I synnerhet direktiven 2014/23/EU, 2014/24/EU och 2014/25/EU.

13 *Commission launches call for evidence and public consultation on the evaluation of the Public Procurement Directives*, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_sv.

14 COM(2025) 837 final.

15 JOIN(2023) 20 final.

16 JOIN(2025) 120 final.

17 JOIN(2025) 977 final.

18 Förordning - 2019/881 - SV - EUR-Lex.

Med tanke på cybersäkerhetshotens föränderliga karaktär och det ökande ömsesidiga beroendet mellan medlemsstaternas digitala system utgör artikel 114 i EUF-fördraget fortsatt den motiverade rättsliga grunden för översynen av cybersäkerhetsakten. Den föreslagna förordningen återspeglar den senaste utvecklingen inom cybersäkerhetslagstiftningen, särskilt med tanke på Enisas växande ansvar och den utökade omfattningen av certifieringar och riskhantering.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Subsidiaritetsprincipen kräver att det görs en bedömning av nödvändigheten och mervärdet av en åtgärd på unionsnivå. Överensstämmelse med subsidiaritetsprincipen på detta område erkändes redan när den nuvarande cybersäkerhetsakten antogs.

Såsom redan analyserats i samband med cybersäkerhetsakten är åtgärder på unionsnivå av avgörande betydelse, eftersom cybersäkerhetshoten och de därmed sammanhängande utmaningarna sträcker sig utanför de enskilda medlemsstaterna. Fragmenterade nationella lösningar har visat sig vara otillräckliga för att uppnå marknadsomfattande förtroende och samordning. Det krävs en reviderad rättslig ram för unionen för att undanröja hinder, säkerställa ett konsekvent genomförande och stödja medlemsstaterna i en alltmer komplex lagstiftnings- och hotmiljö. Cybersäkerhet är en fråga av gemensamt intresse för unionen.

De åtgärder som omfattas av den föreslagna förordningen ger ett tydligt mervärde genom att stödja harmonisering, rättslig klarhet och samordnade insatser mot cybersäkerhetsutmaningar.

Enisas nuvarande uppgifter har utvidgats genom senare lagstiftning utan att det har gjorts någon omfattande översyn av byråns huvudsakliga ansvarsområden och resurser. Detta har skapat ineffektivitet och otillräcklig prioritering av centrala uppgifter till stöd för medlemsstaterna. Förslaget till insatser syftar därför till att renodla och prioritera de nuvarande uppgifterna för att stärka Enisas mandat så att byrån kan fungera som en gemensam kontaktpunkt för cybersäkerhetsexpertis på unionsnivå. På denna punkt finns det ingen betydande skillnad i fråga om subsidiaritet jämfört med cybersäkerhetsakten. Dessutom skapar skillnaderna i medlemsstaternas nationella certifieringsordningar och regleringsmetoder en marknadsfragmentering och ytterligare efterlevnadsbördor som undergräver konkurrenskraften.

I det nya förslaget planeras även nya åtgärder kopplade till politiken för leveranskedjan och förenklingsinsatser på unionsnivå. Det innebär en ytterligare förstärkning av säkerheten i leveranskedjan och cybersäkerhetssektorn inom unionen och en ökning av medlemsstaternas och näringslivets beredskap och motståndskraft.

Beroendet av entiteter som är etablerade i ett tredjeland som utgör cybersäkerhetsproblem eller som kontrolleras av ett sådant tredjeland, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland (högriskleverantörer) påverkar entiteter i hela unionen, samtidigt som betydande cybersäkerhetsincidenter i leveranskedjan ofta sprids över nationsgränserna. Eftersom IKT-leveranskedjorna är gränsöverskridande skulle fragmenteringen av efterlevnadskraven på den inre marknaden dessutom undergräva rättssäkerheten för entiteterna. I förslagen till flerårig budgetram föreskrivs vidare att högriskleverantörer ska uteslutas för att skydda EU:s budget och säkerhetsintressen. I den ram för leveranskedjan som ingår i denna förordning föreskrivs en mekanism för att identifiera länder som utgör cybersäkerhetsproblem, en verksamhet som endast kan genomföras effektivt på EU-nivå. När det gäller säkerhet i IKT-leveranskedjan är det endast insatser på EU-nivå

som kan säkerställa samma minimisäkerhetsnivå i hela unionen och den nödvändiga harmoniseringen av strategier.

Syftet med cybersäkerhetsakten bibehålls och vidareutvecklas i denna översyn. Detta kan inte i tillräcklig utsträckning uppnås av medlemsstaterna, utan kan bättre uppnås på unionsnivå, i enlighet med artikel 5 i fördraget om Europeiska unionen.

- **Proportionalitetsprincipen**

De föreslagna åtgärderna går inte utöver vad som är nödvändigt för att uppnå de politiska målen i förslaget. Vidare bör räckvidden hos unionens insatser inte hindra ytterligare nationella åtgärder med avseende på den nationella säkerheten. Insatser på unionsnivå är därför motiverade av subsidiaritetsskäl och proportionalitetsskäl.

Förslaget syftar till att, ur ett rättsligt perspektiv, bättre återspegla Enisas mandat och processen för utveckling, antagande och underhåll av europeiska cybersäkerhetscertifikat. Förslaget innehåller vissa nya uppgifter för Enisa, men syftet med dem är att stödja medlemsstaterna på de områden där betydande brister har konstaterats. Enisa kommer inte att ersätta medlemsstaternas enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*). När det gäller det europeiska ramverket för cybersäkerhetscertifiering är certifieringen fortsatt frivillig och kan hjälpa entiteter att visa att de uppfyller unionens cybersäkerhetskrav. På så sätt säkerställs att proportionalitetsprincipen iakttas.

Beträffande de lösningar som föreslås i samband med säkerheten i IKT-leveranskedjan föreskrivs det i ramen att man ska samla in bevis på vad som utgör viktiga tillgångar och vilka åtgärder som skulle vara proportionerliga och nödvändiga för att minska riskerna för de kritiska leveranskedjorna. Innan dessa åtgärder fastställs kommer en bedömning av de ekonomiska konsekvenserna att göras, där man bland annat undersöker den ekonomiska genomförbarheten, de tillgängliga alternativen på marknaden och de specifika produkternas livscykel. Denna bedömning kommer att hjälpa till att fastställa vilka riskbaserade åtgärder som behövs och är lämpligast.

- **Val av instrument**

Genom detta förslag görs en översyn av förordning (EU) 2019/881, där Enisas nuvarande mandat och uppgifter fastställs, liksom det europeiska ramverket för cybersäkerhetscertifiering. Ändringarna av Enisas mandat och av det europeiska ramverket för cybersäkerhetscertifiering görs därför bäst i form av samma rättsliga instrument, dvs. en förordning. Den föreslagna lagstiftningen medför även en ändamålsenlig ram på EU-nivå för att hantera säkerhetsrisker för IKT-leveranskedjan, för vilken en förordning på ett effektivare sätt skulle lösa de konstaterade problemen och uppnå de angivna målen, eftersom endast insatser på EU-nivå kan säkerställa samma säkerhetsnivå i hela unionen och den nödvändiga harmoniseringen av strategier. För en sådan åtgärd skulle ett direktivs införlivandeprocess lämna ett alltför stort utrymme för avgöranden på nationell nivå, vilket kan leda till bristande enhetlighet för vissa väsentliga cybersäkerhetskrav samt till rättsosäkerhet, fortsatt fragmentering och till och med diskriminerande gränsöverskridande situationer.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Europeiska kommissionen bedömde, i enlighet med artikel 67 i förordning (EU) 2019/881, relevansen, effekterna och mervärdet av samt ändamålsenligheten, effektiviteten och samstämmigheten hos Enisa och det europeiska ramverket för cybersäkerhetscertifiering, med hänsyn till det föränderliga tekniska och lagstiftningsmässiga landskapet. Denna utvärdering, som slutfördes i december 2024 och omfattade perioden 2017–2023, syftade till att se över Enisas mandat och verksamhet samt till att bedöma den roll som det europeiska ramverket för cybersäkerhetscertifiering spelar för att främja en säker cybermiljö i hela EU. De viktigaste slutsatserna kan sammanfattas enligt följande:

- **Relevans:** Enisas relevans på cybersäkerhetsområdet framhävs av dess lyhördhet för de berörda parternas föränderliga behov och dess förmåga att anpassa sig till ett skiftande landskap. De berörda parterna är i regel nöjda med Enisas insatser, men det finns utrymme för att öka Enisas genomslagskraft. Detta kan uppnås genom att man förbättrar stödet till och synligheten för olika sektorer, särskilt små och medelstora företag, som ofta har svårt att uppfylla cybersäkerhetskraven. En bättre planering av resurser och tydligare samordning med nationella myndigheter spelar en avgörande roll. Genom en omprioritering av verksamheten och optimering av de befintliga resurserna kommer Enisa att bli bättre anpassat till de dynamiska behoven i det europeiska cybersäkerhetslandskapet.

  Vad gäller det europeiska ramverket för cybersäkerhetscertifiering anses ramverket, trots dess lovande grundval, fortfarande ha mer potential än praktiska effekter, eftersom endast en certifieringsordning nyligen har tagits i bruk. Ramverket är utformat för att sömlöst integreras med andra unionsrättsakter i syfte att effektivisera förfaranden och underlätta den gränsöverskridande handeln. Dess betydelse framhävs inom högriskområden som molntjänster och 5G-infrastruktur.

- **Ändamålsenlighet:** Enisa har framgångsrikt uppfyllt sitt mandat genom att uppnå nästan all planerad output och har visat upp flexibilitet och motståndskraft under kriser som covid-19-pandemin och Rysslands anfallskrig mot Ukraina. För att öka effektiviteten krävs dock bättre prioritering, ett tydligt fokus och en strategisk resursfördelning. En mer flexibel strategi för intern styrning är nödvändig för att Enisa ska kunna anpassa sig till nya cybersäkerhetskrav och minska förseningarna.

  Syftet med det europeiska ramverket för cybersäkerhetscertifiering var att harmonisera cybersäkerhetscertifieringen i hela unionen, men man stötte på betydande utmaningar, bland annat processuella begränsningar och fragmentering, vilket ledde till förseningar och ineffektivitet, såsom förseningar i antagandet av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering. Externa faktorer, såsom geopolitiska spänningar och covid-19-pandemin, komplicerade ytterligare uppnåendet av målen för det europeiska ramverket för cybersäkerhetscertifiering, vilket visade på behovet av flexibla åtgärder och en konsekvent resursfördelning bland berörda parter för att göra cybersäkerhetscertifieringen enhetlig och ändamålsenlig. Trots dessa hinder har man åstadkommit positiva resultat – framför allt när det gäller att öka medlemsstaternas medvetenhet om vikten av och svårigheterna med cybersäkerhetscertifiering.

- **Effektivitet:** Enisa har arbetat effektivt inom ramen för sin matrisbaserade organisatoriska ram och har främjat samarbete och prioritering av uppgifter. Enisa har dock ställts inför utmaningar när det gäller att uppfylla de allt högre ställda kraven och tillsätta specialiserade befattningar, en situation som förvärrades av en global brist på it-specialister, vilket ledde till förseningar och en stor arbetsbörda. För att åtgärda dessa problem skulle Enisa kunna optimera sin interna arbetskraft och omfördela resurserna på ett ändamålsenligt sätt, vilket framgår av strategiska justeringar såsom 2022 års förflyttning av resurser till stödåtgärden för cybersäkerhet. Byrån skulle dessutom kunna öka sin operativa effektivitet ytterligare genom att förbättra budgetförvaltningen och minska de administrativa utgifterna.

  Effektiviteten i det europeiska ramverket för cybersäkerhetscertifiering har kritiserats på grund av förlängda tidsfrister för antagande av ordningar för cybersäkerhetscertifiering och den därmed sammanhängande komplexiteten; den första ordningen antogs först i början av 2024, nästan fem år efter det att cybersäkerhetsakten antogs. Politiska och tekniska utmaningar, såsom debatter om datasuveränitet och svårigheter med att omvandla utkast till rättsakter, har bidragit till förseningarna. De politiska utmaningarna och tekniska kraven har hindrat framstegen, vilket framgick i samband med EU-ordningen för cybersäkerhetscertifiering av molntjänster och EU-ordningen för cybersäkerhetscertifiering av 5G-nät. Trots denna ineffektivitet har ramverket medfört flera positiva aspekter. Det krävs dock fortfarande förbättringar när det gäller deltagandet av berörda parter och den interna styrningen för att säkerställa en optimal funktion och strategiska bidrag.

- **Samstämmighet:** Enisas samstämmighet stöds av ett omfattande deltagande av berörda parter och anpassning till den senaste lagstiftningen. För ökad samstämmighet och en bättre resursfördelning är det dock viktigt att förbättra synergierna med såväl andra unionsorgan, såsom Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, som de nationella myndigheterna. Dessutom krävs en renodling av den interna kommunikationen och resursförvaltningen inom Enisa, kombinerat med en öppen samverkan med privata berörda parter. En tydlig avgränsning av Enisas uppgifter, i överensstämmelse med cyberresiliensförordningen och NIS 2-direktivet, kommer att förbättra både effektiviteten och konsekvensen i lagstiftningen.

  När det gäller det europeiska ramverket för cybersäkerhetscertifiering är en fullständig överensstämmelse mellan ramverket och andra unionslagstiftningsinstrument, däribland NIS 2-direktivet och cyberresiliensförordningen, avgörande för att säkerställa en enhetlig cybersäkerhetsstrategi. Trots att ramverket visar en teoretisk anpassning till dessa lagstiftningsåtgärder är den faktiska integreringen fortfarande komplex och kräver noggrann tillsyn. Genomförandet av den antagna europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering inom ramen för cyberresiliensförordningen kommer att vara ett viktigt test i detta avseende.

- **EU-mervärde:** Enisa har bidragit stort till unionens cybersäkerhetsekosystem genom att främja samarbete och anpassa praxis. Byråns roll när det gäller att underlätta de nationella insatserna och ge insikter om nya hot har varit av avgörande betydelse. Kritiken från berörda parter inom den privata sektorn om behovet av ett mer skräddarsytt stöd tyder dock på att det behövs ett ökat deltagande av intressenter och ett bättre samarbete med näringslivet. En strategisk omprövning av resursförvaltningen skulle göra det möjligt för Enisa att bättre anpassa sig till nya

cybersäkerhetsutmaningar och mer effektivt stödja olika berörda parter. Det europeiska ramverket för cybersäkerhetscertifiering syftade till att införa harmoniserade certifieringsprocesser men ställdes inför utmaningar i samband med genomförandet på grund av förlängda tidsfrister och fragmentering. Ramverkets mervärde har begränsats på grund av dess brister när det gäller att uppnå målen och dess bristande effektivitet. Trots dessa utmaningar har ramverket förbättrat harmoniseringen bland medlemsstaterna och medfört bättre samarbetsmöjligheter, särskilt genom att skapa forum för samarbete med berörda parter såsom den europeiska gruppen för cybersäkerhetscertifiering.

- **Samråd med berörda parter**

Mellan 2023 och 2025 genomfördes flera samråd med berörda parter både i samband med utvärderingen av cybersäkerhetsakten och översynen av cybersäkerhetsakten enligt nedan.

– **Under 2023** genomfördes 65 intervjuer (varav 52 var mer inriktade på Enisa och 13 främst på det europeiska ramverket för cybersäkerhetscertifiering), ett undersökningsprogram, där 209 svar inkom (varav 70 gällde ramverket), ett offentligt samråd och två workshoppar om swot-analys och rekommendationer, med 26 respektive 70 deltagare. Syftet med dessa verksamheter var framför allt att samla in synpunkter från berörda parter för att utvärdera Enisas effekter, effektivitet och ändamålsenlighet. Slutrapporten från studien (*Study to Support the Evaluation of the European Union Agency for Cybersecurity [ENISA] and the European Cybersecurity Certification Framework*), som utfördes av PwC, Intellera Consulting och PPMI på kommissionens uppdrag (2024), färdigställdes i december 2024.

– **År 2025** utlyste kommissionen en inbjudan att lämna synpunkter. Framför allt uppmanades berörda parter att lämna in skriftliga bidrag, inklusive ståndpunktsdokument, tekniska rapporter eller kommentarer om specifika reformförslag. Sammanlagt mottogs 184 enskilda bidrag från en rad olika kategorier av berörda parter, däribland branschorganisationer, cybersäkerhetsföretag, små och medelstora företag, akademiska institutioner och intresseorganisationer.

– **Mellan april och juni 2025** anordnade kommissionen ett offentligt samråd som en del av översynen av cybersäkerhetsakten och mottog 193 svar. Samrådet bestod av 38 frågor, både öppna och slutna, om Enisas mandat, det europeiska ramverket för cybersäkerhetscertifiering, säkerheten i IKT-leveranskedjan och förenkling.

– **Riktat samråd (intervjuer):** Ett antal halvstrukturerade intervjuer genomfördes med utvalda berörda parter. Dessa omfattade Enisas företrädare samt nationella myndigheter som har utvecklat eller förvaltar nationella rapporteringsplattformar. Intervjuerna inriktades på Enisas roll och kapacitet, den operativa funktionen hos det europeiska ramverket för cybersäkerhetscertifiering, praktiska utmaningar med att harmonisera certifieringsförfaranden på nationell nivå och unionsnivå samt rapporteringsbördor och genomförandehinder. Dessa diskussioner gav kvalitativa insikter som berikade tolkningen av resultaten av det offentliga samrådet och bidrog till att renodla de politiska alternativen.

– **Samråd med medlemsstaternas företrädare inom ramen för rådets arbetsgrupp[19] och i bilaterala diskussioner**, där medlemsstaterna kunde yttra sig om översynen av cybersäkerhetsakten.

– **Riktat samråd (grupper för det europeiska ramverket för cybersäkerhetscertifiering – den europeiska gruppen för cybersäkerhetscertifiering, intressentgruppen för**

[19] Den övergripande arbetsgruppen för cyberfrågor.

cybersäkerhetscertifiering): I egenskap av ordförande för båda grupperna redogjorde kommissionen för läget i fråga om översynen av cybersäkerhetsakten vid mötena i den europeiska gruppen för cybersäkerhetscertifiering den 12 mars och 3 juli 2025 samt vid mötet i intressentgruppen för cybersäkerhetscertifiering den 17 mars 2025. Genom frågeformulär inhämtades dessutom kompletterande expertutlåtanden från medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering.

Samrådet inriktades på följande fem huvudområden som konstaterats vara centrala för att unionens framtida cybersäkerhetsram ska fungera och vara samstämmig:

- **Enisas mandat och operativa roll**, inbegripet stöd till medlemsstaterna och expertis inom ny teknik.
- **Ändamålsenligheten hos det europeiska ramverket för cybersäkerhetscertifiering**, inklusive styrnings- och utvecklingsprocesser.
- **Komplexiteten i och fragmenteringen av cybersäkerhetsskyldigheterna**, med fokus på rapporteringsbördor och potentiell förenkling.
- **Proportionaliteten i kraven för små och medelstora företag** och möjligheten till differentierade efterlevnadsvägar.
- **De samhällsmässiga och ekonomiska konsekvenserna** av harmoniserade cybersäkerhetsregler, inbegripet effekter på konsumenter, rättigheter, innovation och konkurrenskraft.
- **Konsekvensbedömning**

Översynen av cybersäkerhetsakten, tillsammans med förslaget till direktiv om införande av riktade ändringar av NIS 2-direktivet, åtföljdes av en konsekvensbedömning (se sammanfattningen nedan). Nämnden för lagstiftningskontroll avgav ett positivt yttrande med reservationer om det på nytt inlämnade utkastet till konsekvensbedömningsrapport om översynen av cybersäkerhetsakten[20]. Konsekvensbedömningen justerades för att ta hänsyn till nämndens rekommendationer och kommentarer.

Det slutliga politiska förslaget avviker inte från de bedömda alternativen i konsekvensbedömningen.

Kommissionen undersökte alternativ på fyra insatsområden, mot bakgrund av de särskilda mål som skulle uppnås: 1) Enisas mandat (som även är en del av den nuvarande cybersäkerhetsakten), 2) det europeiska ramverket för cybersäkerhetscertifiering (som även är en del av den nuvarande cybersäkerhetsakten), 3) riktade ändringar av NIS 2-direktivet i förenklingssyfte, men även i samband med Enisas mandat och det europeiska ramverket för cybersäkerhetscertifiering, och 4) säkerheten i IKT-leveranskedjan, som även är av betydelse för både NIS 2-ekosystemet och det europeiska ramverket för cybersäkerhetscertifiering. Varje uppsättning alternativ motsvarar ett insatsområde, men de är samtidigt sammankopplade och relevanta sinsemellan.

Alternativ för att ta itu med den bristande överensstämmelsen mellan unionens policyram för cybersäkerhet och berörda parters behov i en alltmer fientlig miljö

[20] Förordning (EU) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj).

Alternativ A.1: *förtydliga Enisas mandat och underlätta för prioritering* – Detta alternativ skulle ge en tydlig och stabil ram för Enisas uppgifter genom att införliva de uppgifter som fastställs i annan lagstiftning.

Alternativ A.2: *reformera Enisas mandat* – Detta alternativ skulle leda till att cybersäkerhetsakten upphävs och ersätts och att byråns mandat ses över.

Alternativ A.3: *reformera Enisas mandat med ett starkt fokus på operativt stöd* – Detta alternativ skulle bygga vidare på alternativ A.2. Dessutom skulle Enisa utveckla kapacitet för att direkt stödja entiteter enligt NIS 2-direktivet när det gäller att reagera på och återhämta sig från cybersäkerhetsincidenter på en medlemsstats begäran.

Alternativ för det europeiska ramverket för cybersäkerhetscertifiering

Alternativ B.1: *förtydliga tillämpningsområdet för, inslagen i och målen med det europeiska ramverket för cybersäkerhetscertifiering samt införa en underhållsmekanism* – Genom detta alternativ skulle en ny underhållsmekanism införas för de ordningar som Enisa ska genomföra, efter det att de antagits.

Alternativ B.2: *reformera det europeiska ramverket för cybersäkerhetscertifiering genom att se över dess förfaranden samt utvidga tillämpningsområdet för att underlätta förenkling av regelefterlevnaden* – Detta alternativ skulle upphäva cybersäkerhetsakten och ersätta den med en ny förordning. Utöver alternativ B.1 skulle förfarandena för begäran, utveckling och antagande av ordningar ses över för att förbättra ansvarsskyldigheten och effektiviteten.

Alternativ B.3: *reformera det europeiska ramverket för cybersäkerhetscertifiering i enlighet med alternativ B.2 och införa obligatorisk certifiering för cybersäkerhetsstatus* – Detta alternativ bygger vidare på alternativ B.2 och syftar till att ytterligare öka ramverkets effekter genom att införa obligatorisk certifiering av väsentliga entiteter med beaktande av särskilda riskscenarier, i stället för att enbart förlita sig på frivillig certifiering av entiteter.

Alternativ för förenkling

Alternativ C.1: *anta en strategi med icke-bindande icke-lagstiftningsinstrument, bland annat genom att använda befintliga befogenheter (anta genomförandeakter enligt artiklarna 21.5 och 23.11 i NIS 2-direktivet)* – Inom detta alternativ planeras antagandet av genomförandeakter genom användning av de befintliga befogenheterna enligt NIS 2-direktivet för att säkerställa en högre grad av harmonisering av riskhanteringsåtgärder för cybersäkerhet, tröskelvärden för incidentrapportering samt typen av information i och formaten och förfarandet för underrättelser. Inom alternativet planeras även antagandet av en uppsättning riktlinjer för ökad rättssäkerhet och ett mer harmoniserat genomförande.

Alternativ C.2: *riktade insatser – ytterligare förenkling av efterlevnaden av den relevanta unionslagstiftningen för cybersäkerhet* – Detta alternativ omfattar begränsade insatser genom ändringar av cybersäkerhetsakten och NIS 2-direktivet i syfte att förenkla särskilda aspekter av cybersäkerhetsramen, inklusive anpassningar av tillämpningsområdet, maximal harmonisering för genomförandeakter, bevis på efterlevnad genom certifiering och antagande av den uppsättning riktlinjer som planeras inom alternativ C.1.

Alternativ C.3: *harmonisera de cybersäkerhetsrelaterade åtgärder som fastställs i unionslagstiftningen* – Detta alternativ bygger vidare på alternativ C.2 och skulle avlägsna alla de riskhanteringsåtgärder för cybersäkerhet som ingår i den sektorsspecifika lagstiftningen samt befogenheter i förhållande till sådana åtgärder. I stället skulle NIS 2-ekosystemet ändras genom att kraven förenklas för alla typer av entiteter, i syfte att främja harmonisering.

Alternativ för säkerheten i IKT-leveranskedjan

Alternativ D.1: *anta en icke-bindande strategi för att hantera cybersäkerhetsrisker för IKT-leveranskedjor* – Med detta alternativ skulle inga regleringsåtgärder vidtas på EU-nivå. I stället skulle kommissionen öka antalet samordnade riskbedömningar och frivilliga verktygslådor.

Alternativ D.2: *ad hoc-regleringsåtgärder för att kodifiera 5G-verktygslådan* – Detta alternativ skulle kodifiera åtgärderna i 5G-verktygslådan. Genom alternativet skulle medlemsstaterna bli skyldiga att se till att komponenter från högriskleverantörer inte används i viktiga tillgångar i nätet.

Alternativ D.3: *utarbeta en heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor* – Genom detta alternativ skulle en övergripande, teknik- och sektorsneutral ram inrättas för att hantera icke-tekniska cybersäkerhetsrisker för IKT-leveranskedjor.

Efter en omfattande analys framkom följande kombination av alternativ som det rekommenderade policypaketet: alternativ A.2 (reformera Enisas mandat), alternativ B.2 (reformera det europeiska ramverket för cybersäkerhetscertifiering genom att se över dess förfaranden samt utvidga tillämpningsområdet för att underlätta förenkling av regelefterlevnaden), alternativ C.2 (riktade insatser – ytterligare förenkling av efterlevnaden av den relevanta unionslagstiftningen för cybersäkerhet) och alternativ D.3 (inrätta en heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor).

Denna kombination erbjuder ett välbalanserat svar på de konstaterade politiska utmaningarna och medför en avsevärt ökad effektivitet, ändamålsenlighet och samstämmighet i hela unionen.

Övergången till det föreslagna rekommenderade alternativet till ram kommer att medföra kostnader, både för Enisa i fullgörandet av sina nya uppgifter (uppskattningsvis upp till 161,3 miljoner EUR under fem år) och för de offentliga myndigheterna i hela unionen för tillsyn (uppskattningsvis upp till 80 miljoner EUR under fem år, med beaktande av relevanta kostnadsbesparingar). När det gäller företagen kan utfasningen av specifik högriskutrustning under fem år leda till årliga kostnader på 3,4–4,3 miljarder EUR för mobilnätsoperatörer, medan investeringarna i betrodda leverantörer kan öka med upp till 2 miljarder EUR per år.

Samtidigt förväntas de förenklade och minskade efterlevnadskraven generera kostnadsbesparingar på upp till 15,3 miljarder EUR för företagen under fem år. En förbättring av unionens övergripande cybersäkerhetsstatus och tekniska suveränitet kombinerat med stimulerad innovation och konkurrenskraft skulle dessutom ge stora fördelar för allmänheten, myndigheter och företag. Detta förväntas till stor del uppväga de ursprungliga utgifterna på lång sikt.

Genom minskad marknadsfragmentering och harmoniserade lagstiftningskrav medför de rekommenderade alternativen ökad konkurrenskraft i hela unionen, vilket förser företagen med tydligare vägar till efterlevnad och innovation.

De rekommenderade alternativen skulle också bidra till förenkling genom tydlig vägledning och integrerade system, vilket skulle minska den administrativa bördan. Alternativen är förenliga med principen ”en in och en ut” genom att det säkerställs att nya skyldigheter uppvägs av minskningar på annat håll.

- **Lagstiftningens ändamålsenlighet och förenkling**

Översynen av cybersäkerhetsakten, genom de valda politiska alternativen A.2, B.2, C.2 och D.3, bidrar starkt till att förbättra tydligheten, undanröja ineffektivitet och anpassa förfarandena inom de rättsliga ramarna. Mer konkret föreslås i alternativ A.2 en fullständig reform av Enisas mandat som effektivt stöder genomförandet av politiken och det operativa samarbetet mellan medlemsstaterna. Denna konsolidering kommer också att bidra till att undanröja fragmenterade metoder, förbättra samordningen och samtidigt sänka efterlevnads- och driftskostnaderna på lång sikt. Alternativ B.2, som innebär att man upphäver den nuvarande cybersäkerhetsakten och inför ett reformerat europeiskt ramverk för cybersäkerhetscertifiering, ökar effektiviteten genom en översyn av styrningsmodellen och främjande av mer förutsägbara, samstämmiga och smidiga certifieringsförfaranden. Detta kommer att möjliggöra ett snabbare antagande av ordningar och bättre anpassning till övergripande lagstiftning, vilket leder till minskad splittring av lagstiftningen och en minskad börda för både offentliga och privata berörda parter. Genom alternativ C.2 sänks efterlevnadskostnaderna för entiteter som omfattas av relevant unionslagstiftning om cybersäkerhet genom ändringar av tillämpningsområdet och genom att organisatoriska ordningar för cybersäkerhetscertifiering möjliggörs för entiteter som omfattas av NIS 2-direktivet och andra rättsakter. Detta tillvägagångssätt kommer att avsevärt förenkla regleringsskyldigheterna för entiteter som omfattas av flera krav samt säkerställa att de nationella myndigheterna använder sina resurser mer effektivt. Genom alternativ D.3 skapas en harmoniserad ram för att hantera icke-tekniska risker som påverkar IKT-leveranskedjor, i syfte att minska den nuvarande fragmenteringen av strategier i medlemsstaterna. Tillsammans utgör dessa alternativ en betydande förenkling och modernisering av unionens rättsliga ram för cybersäkerhet, helt i linje med Refit-programmets principer om tydlighet, effektivitet och digital beredskap.

Förslaget är förenligt med den s.k. digitala kontrollen, eftersom dess tonvikt på förenklade digitala processer visar på unionens åtagande för en strategi enligt principen ”digitalt först”, för att säkerställa ett snabbare och mer tillförlitligt datautbyte och beslutsfattande. Alternativ D.3 skulle också kunna ha en stor inverkan på digitaliseringen, eftersom det skulle innebära ersättning av komponenter från entiteter som är etablerade i eller kontrolleras av entiteter från tredjeländer som utgör cybersäkerhetsproblem (högriskleverantörer).

- **Grundläggande rättigheter**

Lagstiftningsförslaget bedömdes på grundval av dess potential att stärka eller äventyra grundläggande rättigheter och främja jämlikhet och förtroende, med särskilt fokus på samhällspåverkan och rättigheter, inbegripet integritet, dataskydd och enskilda personers förmåga att förstå, utöva och hävda sina rättigheter.

Utvidgningen av Enisas mandat kommer att bidra till ökad cyberresiliens i hela ekonomin och samhället i allmänhet, vilket kommer att leda till ett bättre skydd av människors integritet och personuppgifter. Förslaget kommer även att stödja cybersäkerhetsutbildning, i och med att det klargör Enisas roll när det gäller att utveckla kompetensen hos arbetskraften inom cybersäkerhet.

Vidare kommer det europeiska ramverket för cybersäkerhetscertifiering att öka allmänhetens och företagens förtroende för certifierade IKT-lösningar som används i vardagen. Att införa ytterligare ordningar skulle öka denna effekt.

Förslaget bidrar till människors förtroende genom att uppmuntra entiteter i kritiska sektorer att erhålla cybersäkerhetscertifiering och därmed offentligt visa att de håller en hög cybersäkerhetsnivå. Genom att säkerställa en harmoniserad rapportering om incidenter med

utpressningsprogram och vidta åtgärder för en övergång till postkvantkryptografi skulle man dessutom öka allmänhetens förtroende för skyddet av känsliga uppgifter i kritiska sektorer.

Bestämmelserna om säkerhet i leveranskedjan kommer att ha en viss inverkan på skyddet av de grundläggande rättigheterna genom att antalet utländska påverkansförsök begränsas. Verksamhet som spionage och övervakning undergräver kraftigt medborgarnas grundläggande rättigheter. Denna övergripande ram skulle kunna förbättra förtroendet, säkerheten och integriteten inom olika typer av teknik och digitala lösningar.

4. BUDGETKONSEKVENSER

Enisas beräknade budget, som kommer att bidra till en betydande ökning av EU:s säkerhet, uppskattades till 341 miljoner EUR för sju år eller en årlig genomsnittlig budget på 49 miljoner EUR (prognos för 2028–2034). Detta innebär en ökning med 81,5 % av byråns budget jämfört med 2025. Enligt analysen i konsekvensbedömningen kommer det föreslagna initiativet att generera stora fördelar i form av kostnadsbesparingar på upp till 14,6 miljarder EUR för företag. Även om de potentiella kostnadsbesparingarna i samband med den övergripande förbättringen av unionens beredskap mot cybersäkerhetsincidenter till sin natur är svåra att kvantifiera uppskattas de snabbare insatserna och den bromsade spridningen av cybersäkerhetsincidenter kunna leda till kostnadsbesparingar på mellan 3,7 och 4,4 miljarder EUR under fem år. Inom ramen för kommande politiska initiativ kommer kommissionen att undersöka den övergripande fördelningen av resurser för och inom EU:s institutioner, organ och byråer på området cybersäkerhet för att utnyttja kunskap och expertis och för att identifiera och utveckla synergier.
De ytterligare resurser som föreslås för att stärka byrån omsätts i 118 heltidsekvivalenter och ytterligare driftskostnader som kommer att täcka de nuvarande överenskommelserna om medverkan mellan Enisa och kommissionen, såsom underhållet av den gemensamma rapporteringsplattformen, de heltidsekvivalenter som arbetar med driften och förvaltningen av EU-cybersäkerhetsreserven samt viktiga kommissionsinitiativ såsom utvecklingen av den gemensamma kontaktpunkten enligt förslaget om ett digitalt omnibuspaket. Andra driftskostnader är kopplade till programmet för samordnad information om sårbarheter, insamling och analys av underrättelser om cybersäkerhetshot, säker kommunikation och uppbyggnad av cybersäkerhetsmognad för Enisa. Driftskostnaderna för underhållet av de europeiska ordningarna för cybersäkerhetscertifiering, auktoriseringen avseende cybersäkerhetskompetens och tjänsten för testverktyg läggs också till i denna budget, även om dessa kostnader även omfattar mekanismer för självfinansiering genom avgifter.

En viktig aspekt av förslaget är införandet av avgiftsmekanismer som kommer att bidra till olika politiska mål, inklusive en hållbar ekonomihanteringsprocess inom byrån. Den reviderade cybersäkerhetsakten innehåller tre typer av avgifter som kommer att bidra till Enisas budget, närmare bestämt avgifter från utfärdandet av auktorisation för kompetensintyg, avgifter från tjänsten för testverktyg och avgifter från stödet till underhållet av de europeiska ordningarna för cybersäkerhetscertifiering. Den förväntade nyttan för EU:s budget uppskattas till cirka 18,5 miljoner EUR under sjuårsperioden 2028–2034.

Kommissionens budgetbegäran omsätts i ytterligare 50 heltidsekvivalenter, som kommer att genomföra ramen för leveranskedjan, samt uppgifter i samband med utarbetandet av genomförandeakter för avgiftsmekanismer, underhållet av certifieringsordningar, standardisering och stöd till operativt samarbete m.m. Kommissionens kostnader för att genomföra ramen för leveranskedjan väntas framför allt påverkas av de olika bedömningar av ägar- och kontrollförhållanden som kommissionen kommer att genomföra. Resultaten av

denna uppgift kommer dock i hög grad att bidra till besparingar för medlemsstaterna i deras övervakning av genomförandet av begränsningsåtgärder och fullgörandet av de skyldigheter som NIS 2-entiteterna åläggs genom ramen. Medlemsstaterna kommer att kunna utnyttja resultaten av bedömningarna av ägar- och kontrollförhållanden direkt, snarare än att varje medlemsstat måste lägga resurser på samma bedömningsbehov.

Se den finansieringsöversikt som åtföljer cyberpaketet för mer detaljerad information.

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Kommissionen kommer att övervaka tillämpningen av den föreslagna förordningen och lägga fram en rapport om utvärderingen för Europaparlamentet och rådet vart femte år. Dessa rapporter kommer att vara offentliga och redogöra för den praktiska tillämpningen och kontrollen av efterlevnaden när det gäller den föreslagna förordningen.

- **Förklarande dokument (för direktiv)**

Inte tillämpligt eftersom förslaget är en förordning.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

I förslaget förtydligas Enisas roll och Enisa tilldelas konkreta uppgifter som består i att stödja berörda parter, i första hand medlemsstaterna, särskilt med genomförandet av unionens politik och lagstiftning, operativt samarbete, kapacitetsuppbyggnad, cybersäkerhetscertifiering och standardisering samt förbättring av arbetskraften inom cybersäkerhet och dess rörlighet i hela unionen. Förslaget syftar vidare till att göra det europeiska ramverket för cybersäkerhetscertifiering effektivare och mer ändamålsenligt för att förbättra cybersäkerheten inom unionen och ge kunderna möjlighet att göra väl underbyggda val när de upphandlar IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster på den inre marknaden. I kombination med förslaget till direktiv om införande av riktade ändringar av NIS 2-direktivet syftar detta förslag dessutom till att underlätta efterlevnaden av cybersäkerhetsskyldigheter och till att frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter inom unionens kritiska sektorer. Slutligen tar förslaget upp behovet av att göra unionens ekonomi och IKT-leveranskedja mer motståndskraftiga för att främja EU:s egen säkerhet och konkurrenskraft. Närmare uppgifter finns nedan.

AVDELNING I: ALLMÄNNA BESTÄMMELSER

Avdelning I i den föreslagna förordningen innehåller de allmänna bestämmelserna: syftet (artikel 1) och definitionerna (artikel 2), inbegripet hänvisningar till relevanta definitioner från andra unionsinstrument, såsom direktiv (EU) 2022/2555[21] (NIS 2-direktivet), förordning (EG) nr 765/2008[22] och förordning (EU) nr 1025/2012[23].

AVDELNING II: ENISA (EUROPEISKA UNIONENS CYBERSÄKERHETSBYRÅ)

[21] http://data.europa.eu/eli/dir/2022/2555/oj.
[22] http://data.europa.eu/eli/reg/2008/765/oj.
[23] http://data.europa.eu/eli/reg/2012/1025/oj.

Avdelning II i den föreslagna förordningen innehåller de viktigaste bestämmelserna om Enisa.

I kapitel I beskrivs Enisas uppdrag (artikel 3) och mål (artikel 4).

I kapitel II presenteras byråns uppgifter i tre avsnitt.

Avsnitt 1 innehåller bestämmelser om de uppgifter som rör stöd till genomförandet av unionens politik och lagstiftning. Där anges vilka entiteter och organisationer som ska få stöd och hur det ska gå till (artikel 5). I artikel 6 beskrivs byråns ansvar vad gäller kapacitetsuppbyggnad; den ska bland annat tillhandahålla medlemsstaterna kunskap och expertis om förebyggande och hantering av cyberhot, uppdatering av cybersäkerhetsstrategier och utökande av arbetskraften inom cybersäkerhet. Enisa kommer även att hjälpa medlemsstaterna med deras medvetandehöjande verksamhet (artikel 7) och kommer att analysera den viktigaste marknadsutvecklingen inom cybersäkerhet samt sprida tekniska råd och analyser (artikel 8). Enisa kommer också att bidra till och främja internationellt samarbete i cybersäkerhetsfrågor, enligt beskrivningen i artikel 9.

I avsnitt 2 fastställs Enisas uppgifter i samband med det operativa samarbetet mellan medlemsstaterna, unionsentiteter och cybersäkerhetstjänsten för unionens institutioner, organ och byråer (CERT-EU), nätverket för enheter för hantering av it-säkerhetsincidenter (CSIRT-nätverket), Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) och andra berörda parter, inbegripet utfärdande av riktlinjer och genomförande av säkra kommunikationsverktyg (artikel 10). Enisa kommer även att hjälpa till att förbättra situationsmedvetenheten om cyberhot och cyberincidenter genom att (bland annat) utveckla en eller flera databaser med underrättelser om cyberhot för att utföra analyser och utfärda tidiga varningar (artikel 11). Reglerna för sådana tidiga varningar (innehåll, tidpunkt, tjänst) fastställs i artikel 12. För att hjälpa väsentliga och viktiga entiteter att förbereda sig inför, svara på och återhämta sig från incidenter med utpressningsprogram ska Enisa driva EU-cybersäkerhetsreserven i enlighet med artikel 13 och i samarbete med Europol och CSIRT-enheter eller andra behöriga myndigheter, beroende på vad som är tillämpligt. Artikel 14 innehåller bestämmelser om Enisas roll vid cybersäkerhetsövningar på unionsnivå, inbegripet sammanställning av ett årligt rullande program för cybersäkerhetsövningar på unionsnivå. Utöver dessa uppgifter bör Enisa tillhandahålla verktyg och plattformar, särskilt den gemensamma rapporteringsplattform som inrättades i enlighet med artikel 16.1 i förordning (EU) 2024/2847 (artikel 15). Slutligen ska byrån utveckla en gemensam kapacitet för sårbarhetshanteringstjänster på unionsnivå och tillhandahålla sårbarhetshanteringstjänster (artikel 16).

I avsnitt 3 om cybersäkerhetscertifiering och standardisering anges byråns uppgifter i detta avseende. I artikel 17 beskrivs Enisas roll i utvecklingen och genomförandet av det europeiska ramverket för cybersäkerhetscertifiering, inklusive byråns ledande roll när det gäller att utarbeta ordningar och säkerställa deras underhåll och kapacitetsuppbyggnad, medan det i artikel 18 fastställs hur Enisa bör delta i utarbetandet av tekniska specifikationer och bidra till standardiseringsverksamhet på europeisk och internationell nivå, även på området krypteringsalgoritmer.

I avsnitt 4 beskrivs byråns uppgifter i samband med genomförandet av EU-akademin för cyberkompetens. Artikel 19 innehåller bestämmelser om Enisas roll inom den europeiska kompetensramen för cybersäkerhet, och i artikel 20 fastställs byråns uppgifter kopplade till utvecklingen och underhållet av ordningar för europeiska individuella intyg om cybersäkerhetskompetens. Kraven för att bli en auktoriserad tillhandahållare av intyg fastställs i artikel 21, medan kraven kopplade till behandlingen av ansökningar anges i artikel 22. Enisa

måste tillhandahålla offentlig information om den europeiska kompetensramen för cybersäkerhet och individuella intyg om cybersäkerhetskompetens (artikel 23).

Kapitel III gäller Enisas organisation. Byråns förvaltnings- och ledningsstruktur omfattar även en vice verkställande direktör (artikel 24). Bestämmelser om styrelsen, inklusive dess sammansättning, ordförande, möten, funktioner och omröstningsbestämmelser, finns i avsnitt 1 (artiklarna 25–29). Styrelsen ska bistås av direktionen, i enlighet med artikel 30 i avsnitt 2. Avsnitt 3 innehåller bestämmelser om utnämning och avsättning av samt förlängning av mandatet för den verkställande direktören (artikel 31) och bestämmelser om den verkställande direktörens uppgifter och ansvarsområden (artikel 32). Styrelsen får besluta att inrätta rollen som vice verkställande direktör för att bistå den verkställande direktören (avsnitt 4, artiklarna 33 och 34). Styrelsen ska inrätta Enisas rådgivande grupp, som ska ge Enisa råd i enlighet med bestämmelserna i artikel 35. I avsnitt 6 fastställs bestämmelser om överklagandenämndens inrättande och sammansättning (artikel 36) och dess ledamöter (artikel 37). I artikel 38 anges under vilka omständigheter överklagandenämndens ledamöter måste avstå från att delta i överklagandeförfarandet och skälen för att invända mot en ledamot av nämnden. Enisas beslut eller underlåtenhet att agera får överklagas till överklagandenämnden (artikel 39). Artikel 40 innehåller bestämmelser om vilka personer som har rätt att överklaga samt tidsfristen och överklagandeformen. I artiklarna 41–43 fastställs bestämmelser om omprövning, prövning av beslut om överklaganden och talan vid domstolen. Slutligen föreskrivs i artikel 44 processen för det samlade programdokumentet.

Kapitel IV rör inrättandet av byråns budget och budgetens struktur, liksom bestämmelserna om dess presentation och genomförande (artiklarna 45–55). Det innehåller även bestämmelser som underlättar kampen mot bedrägeri, korruption och andra olagliga handlingar (artikel 51).

Kapitel V avser byråns personalstyrka. Det innehåller allmänna bestämmelser om tjänsteföreskrifterna och anställningsvillkoren för övriga anställda samt bestämmelser om immunitet och privilegier (artiklarna 56 och 57). I kapitlet införs krav på att medlemsstaterna ska utse kontaktpersoner som utstationerade nationella experter vid Enisa och bestämmelser om deras roll vid byrån (artikel 58). Det innehåller även bestämmelser om användningen av utstationerade nationella experter och annan personal som inte är anställd av byrån (artikel 59).

Avslutningsvis innehåller kapitel VI allmänna bestämmelser om byrån. Här beskrivs byråns rättsliga ställning (artikel 60) och dess säte fastställs (artikel 61); dessutom finns bestämmelser om byråns överenskommelse om säte och villkor för verksamheten samt om ombudsmannens administrativa kontroll (artiklarna 62 och 63). Kapitlet innehåller bestämmelser om ansvar, språkordning och skydd av personuppgifter (artiklarna 64–66) samt säkerhetsbestämmelser om skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade uppgifter (artikel 67). Det innehåller bestämmelser om samarbetet med unionsentiteter och nationella myndigheter (artikel 68) och andra berörda parter (artikel 69). Dessutom beskrivs bestämmelserna om byråns samarbete med tredjeländer och internationella organisationer (artikel 70).

AVDELNING III: EUROPEISKT RAMVERK FÖR CYBERSÄKERHETSCERTIFIERING

Genom avdelning III i den föreslagna förordningen inrättas det europeiska ramverket för cybersäkerhetscertifiering.

I kapitel I redogörs för ramverkets mål, tillämpningsområde och förfaranden. Målen (artikel 71) är bland annat att stärka cybersäkerheten i hela unionen och underlätta en harmoniserad strategi för certifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus. Ramverket bör också främja certifiering för att förenkla efterlevnaden av tillämplig unionslagstiftning genom presumtion om överensstämmelse och därigenom minska bördan för företagen (artikel 78). Därefter beskrivs förfarandeaspekterna, med utgångspunkt i samråden om strategiska prioriteringar för europeisk cybersäkerhetscertifiering och offentlig information om kommissionens utveckling av ordningar samt inrättandet av en ny europeisk församling för cybersäkerhetscertifiering (artikel 72). Efter en detaljerad begäran från kommissionen (artikel 73) förväntas Enisa lämna in ett förslag till certifieringsordning inom tolv månader. I artikel 74 föreskrivs ytterligare tidsfrister för inlämningen av yttrandet från den europeiska gruppen för cybersäkerhetscertifiering samt inlämningen av ordningen för antagande av kommissionen. Genom artikel 75 införs en tydlig underhållsmekanism för befintliga ordningar, som kan leda till att sådana ordningar ses över (artikel 76). Översynen av en ordning kan även bygga vidare på en periodisk utvärdering av ordningens ändamålsenlighet och effekter på den inre marknaden. I artikel 77 ges Enisa en grund för att utarbeta tekniska specifikationer till stöd för utvecklingen och underhållet av europeiska ordningar för cybersäkerhetscertifiering. När kommissionen antar eller ser över en ordning får den inkludera hänvisningar till sådana tekniska specifikationer (artikel 74). Genom de olika förfarandena säkerställs öppenhet och kvalitet genom att experter och allmänna berörda parter involveras i olika skeden av planeringen, utvecklingen, antagandet och underhållet av certifieringsordningar. I artikel 79 föreskrivs att Enisa ska ha en särskild webbplats om europeiska ordningar för cybersäkerhetscertifiering, med information om antagna ordningar samt europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse som utfärdats inom ramen för dessa ordningar.

Kapitel II innehåller allmänna regler för innehållet i europeiska ordningar för cybersäkerhetscertifiering.

I artikel 80 fastställs en förteckning över säkerhetsmål enligt vilka Enisa ska utforma en ordning och som säkerställer anpassning till relevant cybersäkerhetslagstiftning. Varje europeisk ordning för cybersäkerhetscertifiering får innehålla de komponenter som anges i artikel 81. Dessa komponenter ska vara förenliga med unionslagstiftningen och får harmoniseras mellan olika ordningar med hjälp av standardbestämmelser. Båda bestämmelserna ger den flexibilitet som krävs för anpassning till olika typer av ordningar. Dessutom finns ytterligare bestämmelser om reglerna för assuransnivåer (artikel 82) och självbedömning av överensstämmelse (artikel 83). Kapitlet innehåller även en förteckning över kompletterande information (artikel 84) som ska lämnas av tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer.

Slutligen innehåller kapitel III styrningsreglerna för det europeiska ramverket för cybersäkerhetscertifiering, uppdelade i tre olika avsnitt.

Avsnitt 1 avser regler för utfärdande av europeiska cybersäkerhetscertifikat, inbegripet certifikat med assuransnivån ”hög” (artikel 85). Där fastställs dessutom reglerna för harmonisering av europeiska ordningar för cybersäkerhetscertifiering med nationella ordningar för cybersäkerhetscertifiering och cybersäkerhetscertifikat (artikel 86), och i samma avsnitt föreskrivs även möjligheten till internationellt erkännande av europeiska cybersäkerhetscertifikat, på grundval av likvärdighetsprincipen (artikel 87). Avsnittet innehåller också en beskrivning av den roll som de nationella myndigheterna för

cybersäkerhetscertifiering spelar och de bestämmelser som gäller för dem (artikel 88) samt reglerna för en mekanism för inbördes granskning mellan dessa myndigheter för att säkerställa likvärdiga standarder i hela unionen (artikel 89) och reglerna för samarbete mellan dessa myndigheter i den europeiska gruppen för cybersäkerhetscertifiering (artikel 90).

I avsnitt 2 föreskrivs i) harmoniserade regler för ackreditering och auktorisering av organ för bedömning av överensstämmelse (artiklarna 91–92), ii) anmälningsregler, inbegripet en befogenhet att säkerställa ytterligare anpassning till relevant unionslagstiftning och den nya lagstiftningsramen (artikel 93), och iii) ett överprövningsförfarande (artikel 94) som säkerställer att kraven på organ för bedömning av överensstämmelse upprätthålls.

Slutligen föreskrivs i avsnitt 3 rättigheter och rättsmedel i förhållande till certifieringsrelaterade beslut (artikel 96), och medlemsstaterna åläggs att fastställa och verkställa proportionella sanktioner för regelöverträdelser.

AVDELNING IV

I kapitel I artikel 98 fastställs tillämpningsområdet för ramen för en tillförlitlig IKT-leveranskedja. Ramen kommer att behandla icke-tekniska risker inom högkritiska sektorer och andra kritiska sektorer som avses i direktiv (EU) 2022/2555. Mekanismen ska användas för att identifiera viktiga IKT-tillgångar i kritiska IKT-leveranskedjor och fastställa lämpliga och proportionella begränsningsåtgärder för den typ av entiteter som avses i bilaga I och bilaga II till direktiv (EU) 2022/2555. Ramen kommer att bygga på samordnade säkerhetsriskbedömningar på unionsnivå, på begäran av kommissionen eller minst tre medlemsstater. I artikel 99 beskrivs hur dessa riskbedömningar kommer att genomföras, och det anges att man vid riskbedömningarna även bör fastställa begränsningsåtgärder. Dessa riskbedömningar bör slutföras inom sex månader från begäran. På begäran av kommissionen kan samarbetsgruppen för nät- och informationssäkerhet gå med på en kortare period. Inom ramen föreskrivs en möjlighet till ett nödförfarande om ett omedelbart ingripande är motiverat för att bevara en korrekt fungerande inre marknad och om kommissionen har tillräckliga skäl att anse att det föreligger ett betydande cyberhot mot unionens säkerhet i samband med kritiska IKT-leveranskedjor. I sådana fall ska kommissionen samråda med medlemsstaterna om behovet av att vidta en eller flera begränsningsåtgärder och göra en riskbedömning. I artikel 100 föreskrivs att om det till följd av den riskbedömning som avses i artikel 99 eller på grundval av andra källor, såsom ett offentligt uttalande på unionens eller en medlemsstats vägnar, visar sig att ett tredjeland utgör en allvarlig och strukturell icke-teknisk risk för IKT-leveranskedjor ska kommissionen kontrollera det hot som detta land utgör, med beaktande av de komponenter som anges i artikel 100. Om kommissionen konstaterar att ett tredjeland utgör en allvarlig och strukturell icke-teknisk risk för IKT-leveranskedjor föreskrivs i artikel 100 ett förfarande enligt vilket kommissionen fastställer ett sådant tredjeland till ett land som utgör cybersäkerhetsproblem för IKT-leveranskedjor. Entiteter som är etablerade i ett tredjeland som har fastställts utgöra cybersäkerhetsproblem i enlighet med den artikeln, eller som kontrolleras av ett sådant tredjeland, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland, kommer inte att tillåtas att utföra ett antal av de verksamheter som anges i den artikeln. I artikel 101 föreskrivs en allmän mekanism för IKT-leveranskedjan enligt vilken kommissionen får vidta åtgärder enligt artiklarna 102 och 103 när samarbetsgruppen för nät- och informationssäkerhet eller kommissionen har slutfört säkerhetsriskbedömningen enligt artikel 99.

Kommissionen kan genom genomförandeakter identifiera viktiga IKT-tillgångar som används av de typer av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 för att

tillverka produkter eller tillhandahålla tjänster. Artikel 102 innehåller en närmare beskrivning av de komponenter som ska beaktas vid identifieringen av viktiga IKT-tillgångar. I artikel 103 fastställs potentiella begränsningsåtgärder i IKT-leveranskedjan. Kommissionen kan genom genomförandeakter besluta att entiteter som är verksamma inom högkritiska sektorer och andra kritiska sektorer måste omfattas av särskilda begränsningsåtgärder, vilka beskrivs närmare i artikeln.

Kommissionen ska genom genomförandeakter upprätta förteckningar över högriskleverantörer som är relevanta för förbuden i de genomförandeakter som antagits i enlighet med artikel 103.1 och 103.7 eller det förbud som avses i artikel 110.1, efter att ha gjort en bedömning av etablering samt av ägar- och kontrollförhållanden. Kommissionen bör samråda med berörda leverantörer och behöriga myndigheter (artikel 104).

En entitet som är etablerad i eller kontrolleras av entiteter från ett tredjeland som har fastställts utgöra cybersäkerhetsproblem i enlighet med artikel 100 får begära tillåtelse att tillhandahålla IKT-komponenter i viktiga IKT-tillgångar tillhörande entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 och att delta i offentlig upphandling i samband med tillhandahållandet av sådana IKT-komponenter. I artikel 105 anges vad begäran ska innehålla och vilket förfarande som gäller för ett sådant undantag. I artikel 106 beskrivs rätten till försvar för entiteten i fråga. Kommissionen ska föra ett offentligt register över besluten om undantag (artikel 107). I artiklarna 108 och 109 anges regler om konfidentialitet samt avgifter i samband med undantagsförfarandet.

I kapitel II föreskrivs tillämpningen av ramen för en tillförlitlig IKT-leveranskedja på mobila, fasta och satellitbaserade elektroniska kommunikationsnät, vilket säkerställer anpassning till den föreslagna rättsakten om digitala nät.

De viktigaste IKT-tillgångarna för mobila, fasta och satellitbaserade elektroniska kommunikationsnät anges i bilaga II. Övergångsperioden för utfasning av IKT-komponenter från högriskleverantörer för viktiga IKT-tillgångar i det mobila elektroniska kommunikationsnätet får inte överstiga 36 månader från och med denna förordnings ikraftträdande. Övergångsperioderna för fasta och satellitbaserade elektroniska kommunikationsnät ska fastställas av kommissionen genom genomförandeakter. Kommissionen ges befogenhet att anta delegerade akter för att ändra de angivna viktiga IKT-tillgångarna och övergångsperioderna, även för framtida mobila generationer (artikel 110). Enligt artikel 111 får leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät inte i någon form använda, installera eller integrera IKT-komponenter från högriskleverantörer, och de kan inte heller beviljas allmän eller individuell auktorisation.

Behöriga myndigheter, tillsyn och verkställighet, jurisdiktion och rätt till försvar (kapitel III)

I kapitel III fastställs regler om behöriga myndigheter, tillsyn och verkställighet samt jurisdiktion.

I artiklarna 112–114 beskrivs medlemsstaternas befogenheter, medel och ansvar när det gäller att säkerställa genomförandet och verkställigheten av bestämmelserna i avdelning IV. Medlemsstaterna måste utse en eller flera behöriga myndigheter och anmäla dessa till kommissionen. Enligt artikel 113 ska kommissionen inrätta ett nätverk för samarbete mellan medlemsstaternas behöriga myndigheter och kommissionen i syfte att underlätta efterlevnaden, och i artikel 114 anges vilka tillsyns- och verkställighetsåtgärder de behöriga myndigheterna har rätt att vidta. I artikel 115 anges vilka sanktioner som gäller vid överträdelse av bestämmelserna i avdelning IV. I artikel 116 beskrivs möjligheten för

medlemsstaterna att ömsesidigt bistå varandra när entiteter bedriver gränsöverskridande verksamhet eller när deras viktiga IKT-tillgångar är belägna i flera medlemsstater. Artikel 117 innehåller regler om jurisdiktion och territorialitet.

AVDELNING VI: SLUTBESTÄMMELSER

Avdelning VI i den föreslagna förordningen innehåller slutbestämmelser, inklusive reglerna för antagande av genomförandeakter och delegerade akter, utvärderingsprocessen för den föreslagna förordningen samt upphävandet av och övergången från förordning (EU) 2019/881. Där anges även dagen för ikraftträdande av den föreslagna förordningen.

2026/0011 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan samt om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[24],

med beaktande av Regionkommitténs yttrande[25],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Sedan Europaparlamentets och rådets förordning (EU) 2019/881[26] antogs har det geopolitiska, tekniska och politiska landskapet förändrats på ett genomgripande sätt. Antalet cybersäkerhetsincidenter, oavsett om de är orsakade av systemfel, den mänskliga faktorn, fientliga handlingar eller naturfenomen, har ökat och cyberattackerna har blivit mer sofistikerade, vilket påverkar väsentliga entiteter, företag och allmänheten. Ekosystemet för cyberbrottslighet har vuxit, med användning av utpressningsprogram som själva kärnan. Incidenterna i leveranskedjan har intensifierats, både sådana som orsakas av brottslingar för ekonomisk vinning och sådana som orsakas av statliga aktörer i störningssyfte eller för spionage, desinformation eller krigföring. Som ett led i en bredare hybridstrategi sprider sig incidenter orsakade av fientlig cyberverksamhet och systemfel utåt och medför störning av väsentliga tjänster, undergräver förtroendet för institutioner och påverkar unionens samhälleliga beredskap och försvarsberedskap. Sådana incidenter har visat sig ha potential att påverka ekonomisk verksamhet, finansiell stabilitet och människors liv. Samtidigt utgör sårbarhet hos kritiska civila infrastrukturer och system en risk för försvarsförmågorna när de är beroende av dessa infrastrukturer och system.

---

[24] EUT C , , s. .

[25] EUT C , , s. .

[26] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(2) Samtidigt har ny teknik, såsom artificiell intelligens och kvantdatorteknik, disruptiva effekter på cybersäkerheten och cyberförsvaret. De omformar försvarsverktygen och angriparnas taktik, vilket innebär hot för cybersäkerheten och cyberförsvaret men också möjligheter för tekniska framsteg. De kan visserligen bidra till cybersäkerheten genom förbättrad detektering av hot eller automatiserad incidenthantering, men de ökar samtidigt den totala attackytan för organisationer, utgör potentiella mål för manipulation och kan undergräva den långsiktiga livskraften för säkerhetsåtgärder, som t.ex. kryptering.

(3) För att hantera denna utveckling har unionen stärkt sina rättsliga och politiska verktyg. Europaparlamentets och rådets direktiv (EU) 2022/2555[27], som stärker cybersäkerheten för kritisk infrastruktur, kompletteras av Europaparlamentets och rådets direktiv (EU) 2022/2557[28] när det gäller fysisk säkerhet. Europaparlamentets och rådets förordning (EU) 2024/2847[29] stärker cybersäkerheten för produkter med digitala element. Europaparlamentets och rådets förordning (EU) 2025/38[30] bygger upp kapaciteten i unionen för hantering av incidenter, och rådets rekommendation av den 6 juni 2025 om en EU-plan för hantering av cyberkriser[31] stöder krishanteringssamarbete på unionsnivå. Verktygslådan för 5G-cybersäkerhet[32] är första steget mot en samordnad strategi på unionsnivå för att säkra 5G-näten. Kommissionens meddelande om EU-akademin för cyberkompetens[33] behandlar den ökande kompetensbristen på cybersäkerhetsområdet. Cybersäkerhetsramen har också stärkts genom sektorsspecifik lagstiftning, i synnerhet Europaparlamentets och rådets förordning (EU) 2022/2554[34] för finanssektorn, kommissionens delegerade förordning (EU) 2024/1366[35] för delsektorn för elektricitet, kommissionens delegerade förordning

---

27 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

28 Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cybersäkerhetshot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (cybersolidaritetsakten) (EUT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 EUT C, C/2025/3445, 20.6.2025. ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, Samarbetsgruppen för nät- och informationssäkerhet, 1/2020, finns på: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Meddelande från kommissionen till Europaparlamentet och rådet, *Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens (EU-akademin för cyberkompetens)*, COM(2023) 207 final, 18 april 2023.

34 Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (EUT L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

(EU) 2022/1645[36] och kommissionens genomförandeförordning (EU) 2023/203[37] (Del-IS) samt relevanta luftfartsskyddsregler som fastställs i kommissionens förordning (EU) 2019/1583[38] för delsektorn för luftfart, och andra policydokument såsom kommissionens meddelande om en EU-handlingsplan för cybersäkerhet för sjukhus och vårdgivare[39]. Unionsentiteterna stärks också genom Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841[40], som fastställer åtgärder som syftar till en hög gemensam nivå av cybersäkerhet inom unionens institutioner, organ och byråer. Genom denna stärkta rättsliga ram för cybersäkerhet har Enisas uppgifter specificerats ytterligare.

(4) I detta sammanhang och i enlighet med ProtectEU: Europeisk strategi för inre säkerhet[41] och EU:s strategi för en beredskapsunion[42] krävs stark europeisk samordning, förtroende och informationsutbyte mellan berörda parter, robusta ramar för att säkerställa säkerheten för IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster, samt utökad och stärkt arbetskraft på cybersäkerhetsområdet, för att säkerställa beredskap, säkerhet och resiliens för unionens samhälle och ekonomi. Detta förutsätter åtgärder för att stärka IKT-leveranskedjorna genom säkerställande av europeisk teknisk suveränitet över viktiga tillgångar, vilket skulle öka unionens resiliens och gagna cyberförsvarsinsatserna. I

---

36 Kommissionens delegerade förordning (EU) 2022/1645 av den 14 juli 2022 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och (EU) nr 139/2014 (EUT L 248, s. 18, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Kommissionens genomförandeförordning (EU) 2023/203 av den 27 oktober 2022 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340, kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664, och för behöriga myndigheter som omfattas av kommissionens förordningar (EU) nr 748/2012, (EU) nr 1321/2014, (EU) nr 965/2012, (EU) nr 1178/2011, (EU) 2015/340 och (EU) nr 139/2014, kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664 och om ändring av kommissionens förordningar (EU) nr 1178/2011, (EU) nr 748/2012, (EU) nr 965/2012, (EU) nr 139/2014, (EU) nr 1321/2014, (EU) 2015/340, och kommissionens genomförandeförordningar (EU) 2017/373 och (EU) 2021/664 (EUT L 31, 2.2.2023, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Kommissionens genomförandeförordning (EU) 2019/1583 av den 25 september 2019 om ändring av genomförandeförordning (EU) 2015/1998 om detaljerade bestämmelser för genomförande av de gemensamma grundläggande standarderna avseende luftfartsskydd, vad gäller cybersäkerhetsåtgärder (EUT L 246, 26.9.2019, s. 15, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Europeisk handlingsplan för cybersäkerhet för sjukhus och vårdgivare*, COM(2025) 10 final, 15 januari 2025.

40 Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 av den 13 december 2023 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer (EUT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

41 Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om ProtectEU: Europeisk strategi för inre säkerhet, COM(2025)148 final, 1 april 2025.

42 Gemensamt meddelande till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén om EU:s strategi för en beredskapsunion, JOIN(2025) 130 final.

meddelandet om att stärka EU:s ekonomiska säkerhet[43] anges som ett prioriterat mål att förhindra tillgång till känslig information och känsliga uppgifter som skulle kunna undergräva EU:s ekonomiska säkerhet och att förebygga och mildra störningar av EU:s kritiska infrastruktur som påverkar EU:s ekonomi. Det konstateras att cybersäkerhetsåtgärder har mycket stor betydelse i det hänseendet.

(5) Storskaliga cybersäkerhetsincidenter som påverkar kritisk infrastruktur, digitala tjänster eller väsentliga samhällsfunktioner kan ha konsekvenser för befolkningen som gör det nödvändigt med civilskydds- och krishanteringsåtgärder som samordnas på unionsnivå. I linje med allriskstrategin i EU:s strategi för en beredskapsunion och beslut nr 1313/2013/EU om en civilskyddsmekanism för unionen ska arrangemang för situationsmedvetenhet, incidenthantering och övningar enligt denna förordning ligga till grund för unionens krishantering, i synnerhet genom Centrumet för samordning av katastrofberedskap (ERCC).

(6) Detta förslag är förenligt med och kompletteras av [förslag till direktiv om komplettering av [översynen av förordning (EU) 2019/881] och ändring av direktiv (EU) 2022/2555 vad gäller förenkling av genomförandet av åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen] och [förslag till förordning om förenkling av lagstiftningsramen på det digitala området (det digitala omnibuspaketet)][44], som ålägger Enisa att utveckla en gemensam kontaktpunkt för incidentrapportering där entiteter kan fullgöra sina skyldigheter att rapportera incidenter inom ramen för flera rättsakter samtidigt.

(7) Genom Europaparlamentets och rådets förordning (EG) nr 460/2004[45] inrättades Enisa med syftet att bidra till målet att säkerställa en hög och effektiv nivå på nätverks- och informationssäkerheten i unionen och utveckla en kultur av nätverks- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga administrationen. Enisas mandat förlängdes tre gånger innan ett permanent mandat beviljades genom förordning (EU) 2019/881. För att bättre hantera de behov som uppstår till följd av den föränderliga hotbilden och teknikutvecklingen, i synnerhet när det gäller operativt samarbete och det ökade behovet av cybersäkerhetspersonal bör Enisas mandat stärkas ytterligare. Av rättssäkerhetsskäl bör förordning (EU) 2019/881 ersättas.

(8) Med en föränderlig hotbild som innebär att cybersäkerhetsincidenter blir allt mer betydande är det viktigare än någonsin att se till att individer, offentliga myndigheter och företag kan känna förtroende i sin dagliga teknikanvändning. Ett ökat förtroende kan underlättas genom stärkt unionsomfattande certifiering inom det europeiska ramverket för cybersäkerhetscertifiering (ECCF) som föreskriver gemensamma cybersäkerhetskrav och utvärderingskriterier för olika nationella marknader och sektorer. Det nya ramverket bör fastställa de viktigaste övergripande kraven för europeiska ordningar för cybersäkerhetscertifiering och tillåta att europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse erkänns och används i alla medlemsstater. Den bör därför inrätta en förfarande- och styrningsram som gör det möjligt att i rätt tid och på ett förutsebart sätt utveckla och underhålla

---

43 Gemensamt meddelande till Europaparlamentet och rådet – *Stärka EU:s ekonomiska säkerhet*, JOIN(2025) 977 final.

44 COM/2025/837 final.

45 Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet (EUT L 77, 13.3.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

europeiska ordningar för cybersäkerhetscertifiering. De europeiska ordningarna för cybersäkerhetscertifiering bör tillämpas enhetligt i alla medlemsstater för att säkerställa ett harmoniserat genomförande av cybersäkerhetskrav och lika villkor för alla och förhindra ”certifieringsshopping” till följd av olika kravnivåer i olika medlemsstater. Enisa bör ha en viktig roll i utvecklingen av ordningarna genom tekniska specifikationer och säkerställande av att sådana ordningar förblir tekniskt uppdaterade. För att tillgodose marknadens behov på ett effektivt sätt bör ramverket omfatta en möjlighet till certifiering av riskhanteringsåtgärder för cybersäkerhet som omfattar entiteter och främja överensstämmelse med annan tillämplig unionslagstiftning på cybersäkerhetsområdet. Anpassning till befintlig unionslagstiftning, såsom förordning (EU) 2024/2847 och direktiv (EU) 2022/2555, är avgörande för att de europeiska ordningarna för cybersäkerhetscertifiering ska kunna bidra till att minska efterlevnadsbördan för företag, öka deras attraktionskraft och stärka cyberresiliensen i unionen.

(9) Enisas uppdrag bör vara att stödja medlemsstaterna och unionsentiteterna för att uppnå en hög nivå av cybersäkerhet, resiliens och förtroende i unionen. Därför bör Enisa fungera som en referenspunkt för rådgivning och expertis på cybersäkerhetsområdet och Enisas arbete bör främst kretsa kring fyra nyckelområden för cybersäkerhet på unionsnivå. För det första bör Enisa hjälpa medlemsstaterna att genomföra unionens politik och lagstiftning på cybersäkerhetsområdet på ett konsekvent sätt och bistå medlemsstaterna genom kapacitetsuppbyggnadsåtgärder för att kontinuerligt förbättra deras kapacitet för beredskap, resiliens och insatser. För det andra bör Enisa bidra till operativt samarbete på unionsnivå mellan medlemsstaterna och till att stärka den gemensamma situationsmedvetenheten om cyberhot och incidenter hos medlemsstaterna och unionsentiteterna. Det tredje nyckelområdet bör vara cybersäkerhetscertifiering och standardisering, medan det fjärde bör vara genomförandet av EU-akademin för cyberkompetens, som bör bidra till utvecklingen av en stark europeisk arbetskraft på cybersäkerhetsområdet med färdigheter som bör vara gångbara i alla medlemsstater.

(10) I Europaparlamentets och rådets förordning (EU, Euratom) 2023/2841 om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer fastställs mandatet för CERT-EU, som inrättas som cybersäkerhetstjänsten för unionens institutioner, organ och byråer för att bidra till säkerheten i unionsentiteters icke-säkerhetsskyddsklassificerade IKT-miljö genom att ge dem råd om cybersäkerhet, hjälpa dem att förebygga, upptäcka, hantera, begränsa, bemöta och återhämta sig efter incidenter och genom att fungera som deras nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering. CERT-EU får även i uppdrag att erbjuda unionsentiteter relevanta cybersäkerhetstjänster. Stöd till unionsentiteter bör också vara en del av Enisas uppdrag. Enisa bör i synnerhet göra detta genom att bedriva ett strukturerat samarbete med CERT-EU om kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot. När så är relevant får Enisa mobilisera det strukturerade samarbetet med CERT-EU för Enisas cybersäkerhetstjänster eller stöd som kan innebära ett mervärde för unionsentiteter, på ett samordnat sätt för att säkerställa synergier för CERT-EU:s insatser.

(11) En av Enisas centrala uppgifter bör vara att hjälpa medlemsstaterna att genomföra unionens politik och lagstiftning på cybersäkerhetsområdet på ett konsekvent sätt, i synnerhet när det gäller direktiv (EU) 2022/2555, förordning (EU) 2024/2847 och förordning (EU) 2025/38. För att bidra till ett konsekvent och effektivt genomförande

av unionens cybersäkerhetsregelverk bör Enisa utfärda teknisk vägledning och rapporter, tillhandahålla rådgivning och bästa praxis och främja ett utbyte av bästa praxis mellan behöriga myndigheter i detta syfte. Enisa gör också en bedömning av cybersäkerhetssituationen i unionen och antar en rapport om denna i enlighet med artikel 18 i direktiv (EU) 2022/2555. Enisa bör även kunna tillgodose förfrågningar om råd och bistånd från medlemsstaterna och, i tillämpliga fall, unionsentiteter om frågor som omfattas av Enisas mandat.

(12) För att främja samarbete mellan offentlig och privat sektor och inom den privata sektorn, i synnerhet för att stödja skyddet av kritisk infrastruktur, bör Enisa stödja informationsutbyte inom och mellan sektorer, i synnerhet de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, och information om produkter med digitala element som omfattas av förordning (EU) 2024/2847. Sådant stöd kan ha formen av tillhandahållande av bästa praxis och vägledning om tillgängliga verktyg och förfaranden samt vägledning om hanteringen av regleringsfrågor som rör informationsutbyte, t.ex. genom att främja inrättandet av sektorsbaserade informations- och analyscentraler (ISAC).

(13) För att stödja och främja strategiskt samarbete och informationsutbyte bör Enisa bidra till arbetet i den samarbetsgrupp som inrättats genom direktiv (EU) 2022/2555 (*samarbetsgruppen för nät- och informationssäkerhet*), i synnerhet genom att tillhandahålla expertis och råd och genom att främja ett utbyte av bästa praxis, bland annat när det gäller gränsöverskridande beroenden, risker och incidenter. Enisa bör också bidra till arbetet i den europeiska samarbetsgruppen för digital identitet, som inrättades genom Europaparlamentets och rådets förordning (EU) nr 910/2014[46], den europeiska gruppen för cybersäkerhetscertifiering och den administrativa samarbetsgrupp (*Adco-gruppen*) som inrättades genom förordning (EU) 2024/2847.

(14) Den offentliga kärnan av det öppna internet, nämligen dess huvudsakliga protokoll och infrastruktur, utgör globala allmänna nyttigheter, tillhandahåller de grundläggande funktionerna för internet som helhet och underbygger dess normala funktion. Inom ramen för sitt mandat bör Enisa stödja säkerheten och resiliensen för den offentliga kärnan av det öppna internet och stabiliteten i dess funktionssätt, inbegripet men inte begränsat till ett säkert ibruktagande och säker drift av viktiga protokoll (i synnerhet domännamnssystem, BGP – Border Gateway Protocol och IPv6 – Internet Protocol version 6) och driften av domännamnssystemet (såsom driften av alla toppdomäner), genom att främja bästa praxis, vägledning och samarbete, i enlighet med etablerade globala flerpartsarrangemang för internetstyrning och relevanta internationella tekniska och operativa organs respektive roller och ansvarsområden.

(15) Enisa fungerar som referenspunkt för rådgivning och expertis på cybersäkerhetsområdet. Därför bör Enisa på kommissionens begäran bistå kommissionen med expertis, teknisk rådgivning, information och analyser, inbegripet genomförbarhetsstudier, yttranden och förberedande arbete i specifika frågor som rör cybersäkerhet, som kan användas som underlag för kommissionens beslutsfattande och underlätta kommissionens övervakning av genomförandet av unionens cybersäkerhetslagstiftning.

---

[46] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(16) Mot bakgrund av dess expertis bör Enisa bistå medlemsstaterna i deras arbete med att bygga upp och förbättra kapaciteten och beredskapen för att förebygga, upptäcka och reagera på cyberhot och cyberincidenter samt i fråga om säkerheten i nätverks- och informationssystem. Enisa bör särskilt stödja utvecklingen och stärkandet av enheterna för hantering av it-säkerhetsincidenter (*Computer Security Incident Response Teams*, *CSIRT-enheter*) enligt direktiv (EU) 2022/2555, i syfte att uppnå en hög gemensam mognadsnivå för dem i unionen.

(17) Enisa har stött och bör fortsätta att stödja medlemsstaterna i utarbetandet och genomförandet av riktlinjer för deras nationella cybersäkerhetsstrategier och bidra till antagandet och genomförandet av cybersäkerhetsstrategier i alla medlemsstater. Enisa bör främja spridningen av sådana strategier genom den interaktiva kartan över nationella cybersäkerhetsstrategier (*den interaktiva NCSS-kartan*) och bör vidare följa hur genomförandet av dem fortlöper, däribland genom att tillhandahålla stöd för utvecklingen av centrala resultatindikatorer i detta sammanhang.

(18) Genom förordning (EU, Euratom) 2023/2841 fick interinstitutionella cybersäkerhetsstyrelsen i uppdrag att hjälpa unionsentiteter att höja sin cybersäkerhetsstatus och CERT-EU i uppdrag att bidra till säkerheten i unionsentiteters icke-säkerhetsskyddsklassificerade IKT-miljö. Enisa bör, på grundval av sin cybersäkerhetserfarenhet, stödja den interinstitutionella cybersäkerhetsstyrelsen och CERT-EU i deras uppgifter i enlighet med förordning (EU, Euratom) 2023/2841, bland annat genom att bidra till analys av cyberhot, situationsmedvetenhet, cybersäkerhetsövningar, samordning av incidenthantering och utbyte av kunnande och bästa praxis.

(19) På grundval av Enisas expertis och för att komplettera förmågorna hos offentliga myndigheter på nationell nivå och unionsnivå bör Enisa tillhandahålla utbildning baserad på den europeiska kompetensramen för cybersäkerhet (ECSF), särskilt för att stödja ett effektivt genomförande av politiken, operativt samarbete och medvetandehöjande åtgärder.

(20) För att säkerställa synergier med Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning (ECCC) och nätverket av nationella samordningscentrum, som inrättats i enlighet med Europaparlamentets och rådets förordning (EU) 2021/887[47], bör Enisa stödja dessa genom att förmedla information om befintliga och framväxande risker och cyberhot, inbegripet risker och hot som rör informations- och kommunikationsteknik.

(21) EU:s strategi för en beredskapsunion belyser att digital kompetens, som bygger på förvärvandet av grundläggande digitala färdigheter, är nödvändig för att göra medborgarna mer resilienta inför potentiella kriser. Som lyfts fram i kommissionens meddelande om kompetensunionen[48] saknar emellertid nästan halva den vuxna befolkningen grundläggande digitala färdigheter, trots att mer än 90 % av arbetstillfällena kräver sådana. För att säkerställa att den nuvarande och potentiella framtida arbetskraften har de färdigheter som krävs i den snabbt föränderliga digitala

[47] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EUT L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[48] Meddelande från kommissionen till Europaparlamentet, Europeiska rådet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Kompetensunionen*, COM(2025) 90 final av den 5 mars 2025.

miljön, och för att bidra till utvecklingen av den europeiska talangreserven på cybersäkerhetsområdet, bör Enisa stödja medvetandehöjande åtgärder på cybersäkerhetsområdet som syftar till att locka begåvningar och hjälpa till med att informera om vilken utbildning och vilka färdigheter som behövs på cybersäkerhetsområdet, såsom EU:s cybersäkerhetsutmaning. Enisa bör därför samordna cybersäkerhetstävlingar, CTF-evenemang (capture-the-flag) och liknande praktiska övningar, som ett sätt att utveckla cybersäkerhetsfärdigheter och främja kapacitetsuppbyggnad i hela unionen. Vid genomförandet av medvetandehöjande åtgärder bör Enisa säkerställa att dessa åtgärder tillgodoser de nationella offentliga myndigheternas och unionsentiteternas behov, liksom företagens (i synnerhet små och medelstora företag) och utbildningsinstitutionernas behov, genom att upprätthålla praktiska ramar och utbildningsåtgärder, såsom ”awareness-raising-in-a-box”. Enisa bör fortsätta att utarbeta praktisk och tillämpbar vägledning för att stödja genomförandet av unionens politik och lagstiftning på cybersäkerhetsområdet. Enisa bör även sträva efter att tillhandahålla relevant information om gällande certifieringsordningar, t.ex. genom att tillhandahålla riktlinjer och rekommendationer.

(22) För att stödja företag med verksamhet inom cybersäkerhetssektorn och användare av cybersäkerhetslösningar, samt för att säkerställa ett effektivt genomförande av avdelning III i denna förordning, bör Enisa utveckla och upprätthålla en marknadsobservationsgrupp, genom att göra regelbundna analyser och sprida information om de viktigaste trenderna på cybersäkerhetsmarknaden, på både efterfråge- och utbudssidan. För att stödja användarna av den EU-cybersäkerhetsreserv som inrättats i enlighet med förordning (EU) 2025/38 bör Enisa också förbereda en kartläggning av de tjänster som sådana användare behöver och av tillgången till sådana tjänster, i enlighet med den förordningen.

(23) Cyberhot är en global fråga. Det behövs ett närmare internationellt samarbete för att förbättra cybersäkerheten, inbegripet för att fastställa gemensamma beteendenormer och tillvägagångssätt. Därför bör Enisa stödja unionens samarbete med tredjeländer, med fokus på länder som är kandidatländer för anslutning till unionen, och internationella organisationer, som Nato, genom att tillhandahålla den expertis och analys som kommissionen och berörda unionsentiteter behöver, när så är lämpligt. Enisas verksamhet på internationell nivå bör alltid vara i linje med unionens prioriteringar.

(24) För att bidra till en hög cybersäkerhetsnivå i unionen bör Enisa stödja operativt samarbete mellan medlemsstater, i samarbete med CERT-EU, samt mellan unionsentiteter och mellan berörda parter. Därför bör Enisas roll stärkas. Enisa bör bli medlem i CSIRT-nätverket och bidra till nätverkets informationsutbyte och analys. Enisa bör även främja och stödja samarbete mellan berörda CSIRT-enheter i händelse av incidenter, attacker mot eller störningar i de nät eller den infrastruktur som förvaltas eller skyddas av dem. Enisas aktiva stöd till arbetet i CSIRT-nätverket och det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) bör göra det möjligt för dessa nätverk att fortsätta stärka sin mognadsnivå. Enisas roll i stödet till detta samarbete inbegriper bekämpande av hot mot säkerheten och integriteten när det gäller demokratiska institutioner, val och andra processer samt den kritiska infrastruktur som de är beroende av, i linje med *Europeiskt demokratiförsvar: att främja starka och motståndskraftiga demokratier*[49].

[49] JOIN(2025) 791 final.

(25) För att stödja kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot bör Enisa utnyttja tillgänglig teknisk och operativ expertis hos CERT-EU genom strukturerat samarbete, t.ex. genom särskilda arrangemang.

(26) För att stärka cybersäkerheten i unionen och säkerställa snabba och effektiva insatser mot cyberhot bör Enisa stödja medlemsstaterna på deras begäran, t.ex. genom att ge råd om förbättringar av deras förmåga att förebygga, upptäcka, hantera och återhämta sig från incidenter, genom att underlätta den tekniska hanteringen av betydande incidenter i den mening som avses i direktiv (EU) 2022/2555, i synnerhet genom att stödja ett frivilligt utbyte av tekniska lösningar mellan medlemsstater, eller genom att säkerställa att cyberhot och incidenter analyseras. Enisa bör också bistå EU-CyCLONe i utarbetandet av rapporter till unionen och medlemsstaterna på politisk nivå.

(27) För att minska exponeringen för utländsk inblandning, manipulering av leveranskedjan och strategisk dataexfiltrering bör Enisa inom CSIRT-nätverket och EU-CyCLONe använda säkra kommunikationsverktyg. Sådana verktyg bör bygga på rekommendationen om en EU-plan för hantering av cyberkriser och bör tillhandahållas av juridiska enheter som är etablerade eller bedöms vara etablerade i unionen och som kontrolleras av medlemsstater eller av medborgare i medlemsstater.

(28) För att bidra till beredskapen och insatserna på unionsnivå i samband med storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser bör Enisa genomföra åtgärder avseende situationsmedvetenheten på cybersäkerhetsområdet.

(29) Tillgång i realtid till verifierad, tillförlitlig underrättelseinformation om cyberhot är avgörande för att bygga upp en gemensam situationsmedvetenhet i unionen. Enisa, kommissionen, CERT-EU och Europeiska it-brottscentrumet (EC3) vid Europol har redan utvecklat databaser med underrättelseinformation om cyberhot som är anpassade till deras särskilda behov. Enisa och andra berörda unionsentiteter bör samarbeta, frivilligt, för att utveckla databaser med verifierad och tillförlitlig underrättelseinformation om cyberhot i realtid och sträva efter synergier för att säkerställa stordriftsfördelar och stärka en sund ekonomisk förvaltning. Detta arbete bör även inbegripa sektorsbaserade unionsentiteter, såsom EU:s rymdprogrambyrå. De bör endast utbyta analyser, trender, taktik, tekniker och förfaranden som härletts ur materialet, inte obearbetade källor, och bör respektera entiteternas oberoende när det gäller hanteringen av deras egen livscykel för underrättelseinformation om cyberhot i linje med deras uppdrag och regler om behörighet.

(30) För att bidra till samordnade insatser i rätt tid bör Enisa kunna utfärda tidiga varningar om en potentiell eller pågående betydande eller storskalig incident, eller om ett cyberhot av potentiellt gränsöverskridande art. till den eller de CSIRT-enheter som berörs och, när så är lämpligt, till CSIRT-nätverket och EU-CyCLONe, i synnerhet i samband med entiteter som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555. Informationen i sådana tidiga varningar får innefatta allmänt kända sårbarheter och om de påverkar produkter med digitala element som omfattas av förordning (EU) 2024/2847, samt tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer och rekommendationer om begränsningsåtgärder.

(31) För att upprätthålla förtroendet och inte äventyra informationsutbytet är det viktigt att Enisa använder synliga märkningar som anger i vilken utsträckning som dokument eller information som producerats eller tagits emot av Enisa får förmedlas vidare. På samma sätt bör Enisa använda dokument eller information som inkommer till Enisa

för att utföra sin verksamhet, med förbehåll för eventuella begränsningar genom en synlig märkning som anger villkor för vidareförmedling.

(32) För att bidra till att öka medvetenheten om indikatorer på cyberhot och rekommendationer om begränsningsåtgärder bör Enisa göra en tjänst för tidig varning tillgänglig för entiteter som är verksamma inom sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555. Sådana generiska, frivilliga tidiga varningar bör särskilt gagna små och medelstora företag och bör tillhandahållas i ett maskinläsbart format som görs allmänt tillgängligt. Denna frivilliga tjänst bör alltid vara separat från och inte relaterad till eventuella offentlig-privata partnerskap som Enisa kan komma att inrätta eller redan har inrättat.

(33) För att stödja en gemensam situationsmedvetenhet på cybersäkerhetsområdet i unionen bör Enisa, i nära samarbete med medlemsstaterna, utarbeta en regelbunden djupgående teknisk lägesrapport om cybersäkerheten i EU som behandlar incidenter och cyberhot på grundval av allmänt tillgänglig information, egna analyser och rapporter som delats av den fått från medlemsstaternas CSIRT-enheter eller de nationella gemensamma kontaktpunkter för säkerheten i nätverks- och informationssystem (*gemensamma kontaktpunkter*) som föreskrivs i direktiv (EU) 2022/2555, båda på frivillig grund, samt Europol och CERT-EU. Rapporten bör göras tillgänglig för rådet, Europeiska utrikestjänsten, EU-CyCLONe, CSIRT-nätverket, kommissionen och Europol.

(34) För att stärka berörda parters gemensamma situationsmedvetenhet om cyberhot- och incidentbilden bör Enisa analysera trender i fråga om cyberhot och incidenter. Detta bör inbegripa en regelbunden analys som omfattar högkritiska sektorer och andra kritiska sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, inbegripet hälso- och sjukvård, energi och transport. Denna analys bör omfatta sektorernas mognadsgrad och bland annat kartlägga tänkbara utmaningar som är specifika för enskilda sektorer. När så är lämpligt, och för att identifiera konsekvenser i leveranskedjan, bör analysen omfatta faktaunderlag om cyberhot och trender som rör produktkategorier som omfattas av förordning (EU) 2024/2847. Enisa bör utveckla expertis avseende infrastrukturers cybersäkerhet och deras kritiska beroenden i leveranskedjan, i synnerhet för att stödja de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och genomförandet av förordning (EU) 2024/2847. Därför bör Enisa också samarbeta med andra relevanta unionsentiteter, när så är lämpligt.

(35) För att bättre förstå utmaningarna på cybersäkerhetsområdet behöver Enisa vidare analysera nuvarande och framväxande teknik och tillhandahålla ämnesspecifika bedömningar om tekniska innovationers förväntade samhälleliga, rättsliga, ekonomiska och regleringsrelaterade konsekvenser för cybersäkerheten. För att säkerställa att allmänheten enklare får tillgång till information om cybersäkerhetsrisker och tänkbara åtgärder kan Enisa tillhandahålla relevant information på sin webbplats, på ett användarvänligt och välstrukturerat sätt.

(36) Enisas stärkta roll när det gäller att främja situationsmedvetenhet, analysera hot och tillhandahålla tekniska råd kommer att bidra till att förbättra de kollektiva cybersäkerhetsinsatserna avseende produkter med digitala element och stödja genomförandet av förordning (EU) 2024/2847. I enlighet med förordning (EU) 2024/2847 får Enisa föreslå marknadskontrollmyndigheter gemensamma åtgärder för att kontrollera överensstämmelsen för produkter med digitala element och identifiera kategorier av produkter med digitala element för vilka samordnade tillsynsåtgärder

kan organiseras. Information som härrör från analys av cyberhot och tidiga varningar bör stärka det stöd som Enisa tillhandahåller dessa myndigheter och bidra till en effektiv kontroll av genomförandet av förordning (EU) 2024/2847 för att förhindra att cyberattacker medför leveranskedjeeffekter på den inre marknaden och för att förbättra unionens övergripande beredskap.

(37) Angrepp med utpressningsprogram utgör ett betydande cybersäkerhetshot mot unionen. För att stärka unionens cybersäkerhet och bekämpa utpressningsprogram bör Enisa utveckla kapacitet för situationsmedvetenhet och stöd för incidenthantering och återställning. När Enisa hjälper enskilda väsentliga och viktiga entiteter med insatser för hantering av och återställande från ett angrepp med utpressningsprogram bör denna byrå göra det i nära samarbete med Europol och med CSIRT-enheter eller behöriga myndigheter, såsom tillämpligt, och då utnyttja Europols beprövade erfarenhet av att bekämpa brottslighet baserad på utpressningsprogram. Sådan hjälp bör komplettera CSIRT-enheternas verksamhet till stöd för incidenthantering. För att uppnå synergier i sitt arbete mot utpressningsprogram bör Enisa inrätta en helpdesk och skulle för detta syfte kunna sammanföra relevanta förmågor och tjänster för att motverka utpressningsprogram och säkra enkel tillgång till information, vägledning och verktyg som kan hjälpa väsentliga och viktiga entiteter i deras incidenthantering och återställning efter incidenter förbundna med utpressningsprogram.

(38) Enisa bör tillhandahålla kommissionen teknisk expertis och stöd vid utarbetandet av ett löpande årligt program med cybersäkerhetsövningar på unionsnivå i enlighet med rekommendationen om en EU-plan för hantering av cyberkriser, för att testa cybersäkerhetsnivån hos de entiteter som deltar i dessa övningar och för att minimera dubbelarbetet. Enisa bör exempelvis ge råd om lämpliga typer av övningar, såsom skrivbordsövningar, hybridövningar eller fullskaliga operativa övningar, samt om mål, scenarier och deltagande.

(39) Snabb tillgång till korrekt information om sårbarheter och en robust sårbarhetshantering är en förutsättning för att säkerställa en hög cybersäkerhetsnivå på den inre marknaden. Därför bör Enisa upprätthålla en europeisk sårbarhetsdatabas i enlighet med direktiv (EU) 2022/2555 och skapa en gemensam unionskapacitet för sårbarhetshanteringstjänster, som säkerställer en resilient och hållbar tjänstenivå och minskar risken för störningar. I detta syfte bör Enisa undersöka möjligheterna att fördjupa det strukturerade samarbetet med program, register eller databaser som liknar den europeiska sårbarhetsdatabasen, för att motverka dubbelarbete och sträva efter komplementaritet på internationell nivå, när så är lämpligt. Enisa bör också stödja samordnad sårbarhetsinformation med flerpartsdeltagande på unionsnivå och tillhandahålla mervärdestjänster, såsom sårbarhetsrådgivning, klassificering av allvarlighetsgrad och produktförteckningar, samt tillhandahålla en förbättrad europeisk katalog över kända utnyttjade sårbarheter som kan hjälpa entiteterna i deras sårbarhetshantering.

(40) Enisas roll i utvecklingen av det europeiska ramverket för cybersäkerhetscertifiering bör också vara en central aspekt av dess mandat. Enisa bör tillhandahålla sin tekniska expertis under hela livscykeln för europeiska ordningar för cybersäkerhetscertifiering. Med sikte på en framtida ordning bör Enisa identifiera befintliga standarder eller tekniska specifikationer som kan ligga till grund för en sådan och, när så är relevant, själv utarbeta tekniska specifikationer som det kan hänvisas till i en sådan ordning. Enisa bör ansvara för att utarbeta förslag till certifieringsordningar på begäran av kommissionen. Enisa bör ansvara för underhållet av de ordningar som redan finns. Enisa bör då bidra till uppbyggnaden och utvecklingen av ett ekosystem för

certifiering, där återkoppling från medlemsstater och privata intressenter efterfrågas och deras certifieringskapacitet stärks. Detta bör också inbegripa en särskild webbplats för certifiering där relevant information om antagna ordningar, däribland certifikat och försäkringar om överensstämmelse, kostnadsfritt görs allmänt tillgängliga.

(41) För att stödja genomförandet av relevant unionslagstiftning bör Enisa forma utvecklingen på cybersäkerhetsområdet genom att ta fram tekniska specifikationer till stöd för genomförandet av relevant unionslagstiftning, inbegripet med sikte på deras användning som potentiell referens för europeiska ordningar för cybersäkerhetscertifiering. Enisa bör också övervaka berörda standardiseringsorgans framtagande och utveckling av standarder för att följa standardiseringstrenderna på europeisk och global nivå, och bör vid behov påverka utformningen av sådana standarder genom att delta i standardiseringsorganisationernas verksamhet, exempelvis genom att utarbeta bidrag och leda detta arbete. I detta sammanhang bör Enisa vara opartiskt. Det kan exempelvis finnas situationer där Enisa bör dra sig tillbaka från relevant verksamhet hos standardiseringsorgan, om Enisa ombeds att bedöma europeiska standarder som begärts av kommissionen till stöd för unionslagstiftning. Enisa bör inte bidra till utarbetandet av standarder i de fall då Enisa ansvarar för bedömningen av de berörda standarderna.

(42) För att stödja genomförandet av unionens politik och förbereda potentiell standardiseringsverksamhet bör Enisa bidra till utvecklingen och utvärderingen av krypteringsalgoritmer, i synnerhet på området postkvantkryptografi. I detta sammanhang kan Enisa, på begäran av kommissionen och i enlighet med en överenskommelse om medverkan enligt definitionen i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509[50], inrätta en process för att begära och utvärdera algoritmer för krypteringsalgoritmer av berörda parter, i synnerhet sådana som är verksamma inom kryptografi, den akademiska världen och forskning, men även tillverkare, CSIRT-enheter, nationella myndigheter för cybersäkerhetscertifiering och behöriga myndigheter enligt direktiv (EU) 2022/2555. I de fall då Enisa bidrar till inrättandet av sådana processer bör byrån främja samverkan mellan relevanta berörda parter och genomföra de organisatoriska aspekterna. Processen bör vara formell, öppen, transparent och inkluderande, inbegripet samråd med berörda parter om utkasten till minimikrav och utvärderingsprocessen och utvärderingskriterierna, i synnerhet med tanke på utvärderingarnas säkerhet och genomförande.

(43) För att stödja genomförandet av verksamhet avseende bedömning av överensstämmelse inom ramen för europeiska ordningar för cybersäkerhetscertifiering och annan relevant unionslagstiftning kan Enisa tillhandahålla relevanta tekniska testverktyg för att stödja medlemsstaterna, företagen och organen för bedömning av överensstämmelse i deras utvärderingsverksamhet. Sådana verktyg bör syfta till att skapa synergier på unionsnivå och effektivt fungerande förfaranden för bedömning av överensstämmelse, för att tillgodose medlemsstaternas och marknadens behov. Sådana behov kan uppstå exempelvis på området inbyggd säkerhet (security by design) för att stödja företag, inbegripet små och medelstora företag, i deras genomförandeinsatser i samband med förordning (EU) 2024/2847. I detta sammanhang bör Enisa ta ut avgifter för att täcka relevanta kostnader i samband med fastställande, utformning, utveckling,

[50] Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509 av den 23 september 2024 om finansiella regler för unionens allmänna budget (EUT L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

underhåll och uppdatering av nödvändig programvaru- och hårdvarukapacitet för sådana testverktyg.

(44) För att stödja medlemsstaterna i deras ansträngningar att åtgärda bristen på cybersäkerhetspersonal och det växande behovet av en kvalificerad, diversifierad (även i fråga om könsfördelning) och flexibel arbetskraft och för att främja arbetstagarnas rörlighet och beredskapen i medlemsstaterna bör Enisa bygga vidare på de principer och det arbete som inletts inom EU-akademin för cyberkompetens. Enisa bör i synnerhet etablera den europeiska kompetensramen för cybersäkerhet (ECSF) som en gemensam ram för yrkesprofiler på cybersäkerhetsområdet. Enisa bör även hjälpa medlemsstaterna att uppnå en jämnare könsfördelning i cybersäkerhetsroller. Detta tillvägagångssätt överensstämmer med den vision som beskrivs i kommissionens meddelande om kompetensunionen och skulle bidra till dess mål. En kvalitetsmärkning för europeiska individuella intyg om cybersäkerhetskompetens bör också övervägas.

(45) Den europeiska kompetensramen för cybersäkerhet bör vara ett praktiskt och flexibelt verktyg att använda på frivillig grund som skapar en gemensam förståelse och terminologi för berörda roller och arbetsuppgifter, färdigheter och kunskaper som vanligtvis krävs i cybersäkerhetsroller, med sikte på att stödja en kartläggning av kritiska färdigheter, inbegripet generella färdigheter, som arbetskraften behöver, och bör göra det möjligt för utbildningsanordnare, såsom företag, högre utbildningsanstalter eller yrkesutbildningsaktörer, att utforma program och hjälpa beslutsfattare att utveckla initiativ och åtgärda kompetensbrister. Med potential att användas som en referensram för erkännande av färdigheter bör den också vara kompatibel med den europeiska klassificeringen av färdigheter, kvalifikationer och yrken (Esco) för att hjälpa personalavdelningar att förstå kraven för resursplanering, rekrytering och karriärutveckling till stöd för cybersäkerhetsbehov. Medan DigComp 3.0 beskriver kunskaper, färdigheter och attityder som människor behöver för att vara digitalt kompetenta i vardagsliv, deltagande i samhällslivet, arbete och lärande och kan användas av både vuxna och barn erbjuder den europeiska kompetensramen för cybersäkerhet en enkel ram för identifiering av cybersäkerhetsroller och därmed förbundna uppgifter samt de kunskaper och färdigheter som behövs för att utföra dessa. I detta hänseende riktar den sig till en specialiserad grupp inom cybersäkerheten, alltifrån faktiska eller potentiella yrkesverksamma på cybersäkerhetsområdet till utbildningsinstitutioner och arbetsgivare. Den europeiska kompetensramen för cybersäkerhet bör också stödja utvecklingen av europeiska individuella intyg om cybersäkerhetskompetens genom att vara det centrala instrument som används för att utveckla ordningarna, som möjliggör nya aktörers inträde på marknaden och stöder marknadskonkurrens inom en gemensam ram. Den europeiska kompetensramen för cybersäkerhet bör regelbundet utvärderas och uppdateras så att det säkerställs att den på lämpligt sätt återspeglar cybersäkerhetsarbetsmarknadens behov och den tekniska och politiska utvecklingen. Enisa bör stödja användningen av den europeiska kompetensramen för cybersäkerhet hos och inom medlemsstaterna och unionsentiteterna och bör tillhandahålla ändamålsenligt stöd när sådant bistånd behövs.

(46) Cybersäkerhetskompetens och -kvalifikationer bör göras jämförbara, transparenta och tillförlitliga på hela den inre marknaden. Därför bör europeiska individuella intyg om

cybersäkerhetskompetens[51] hjälpa arbetsgivare, inbegripet små och medelstora företag och startupföretag, att på ett effektivt sätt rekrytera faktiska eller potentiella yrkesverksamma på cybersäkerhetsområdet inom och mellan medlemsstater, i linje med de mål som anges i meddelandet om kompetensunionen. För att säkerställa ett konsekvent genomförande i alla medlemsstater bör de europeiska individuella intygen om cybersäkerhetskompetens baseras på en gemensam förståelse på unionsnivå av de färdigheter som behövs för att uppnå dessa mål, och de bör tillhandahållas av leverantörer som auktoriserats av Enisa i enlighet med en gemensam uppsättning kriterier. Detta tillvägagångssätt bör vara förenligt med och bidra till målen i det framtida initiativet för kompetensportabilitet.

(47) Utvecklingen av ordningarna för europeiska individuella intyg om cybersäkerhetskompetens bör syfta till att komplettera medlemsstaternas åtgärder genom att erbjuda offentliga myndigheter och ekonomiska aktörer möjligheten att utnyttja en europeisk intygsmekanism, i linje med unionens stödjande befogenhet när det gäller utbildning och yrkesutbildning, i enlighet med artikel 6 e och artiklarna 165.1 och 166.1 i EUF-fördraget. Ordningarna kan också, tillsammans med EU-akademin för cyberkompetens, ligga till grund för program för högre utbildning, såsom sektorsbaserade europeiska examina, och för utvecklingen av mikromeriter. Därför bör ordningarna för europeiska individuella intyg om cybersäkerhetskompetens inte syfta till att harmonisera medlemsstaternas lagar och andra författningar, utan snarare ses som en möjliggörande faktor och en möjlighet som medlemsstater och ekonomiska aktörer kan vilja anamma och främja.

(48) Enisa bör alltid säkerställa att ordningarna för europeiska individuella intyg om cybersäkerhetskompetens förblir anpassade till marknadens behov och bygger på erfarenheter från både offentliga och privata leverantörer av individuell certifiering, inbegripet medlemsstater, högre utbildningsanstalter, yrkesutbildningsinstitutioner och företag. Enisa bör konsultera kommissionen om prioriteringar i fråga om ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, med vederbörlig hänsyn till genomförandet av politiken och marknadens behov.

(49) För att säkerställa att den europeiska kompetensramen för cybersäkerhet och dessa ordningar är anpassade till varandra bör ändringar av en ECSF-yrkesprofil automatiskt utlösa en utvärdering av ändamålsenligheten för berörda ordningar för europeiska individuella intyg om cybersäkerhetskompetens, vilken kan leda till en översyn av dessa.

(50) Med beaktande av mångfalden av yrkesprofiler på cybersäkerhetsområdet och de därmed förbundna arbetsuppgifterna, färdigheterna och kunskaperna kan bedömningen av individer och bedömningsmetoderna behöva anpassas i de enskilda ordningarna för europeiska individuella intyg om cybersäkerhetskompetens. Varje ordning bör säkerställa att bedömningen av de färdigheter som en individ behöver när det gäller läranderesultat, när så är relevant inbegripet utvärderingen av kompetensnivån, systematiskt utvärderas mot en ECSF-yrkesprofil eller undergrupp av dessa. Bedömningsmetoderna kan innefatta sådana aspekter som test av teoretiska kunskaper,

[51] De europeiska individuella intygen om cybersäkerhetskompetens bör anses ha ett liknande upplägg som det som marknaden erkänner som ”cybersäkerhetscertifieringar”. För att undvika förvirring i förhållande till det europeiska ramverket för cybersäkerhetscertifiering föredras emellertid begreppet ”intyg” (på engelska används ”attestation” i enlighet med meddelandet om EU-akademin för cyberkompetens).

praktisk examination, förhandskrav och inbördes bedömning. Individers erfarenheter bör vederbörligen beaktas.

(51) För att säkerställa ett konsekvent genomförande av ordningar för europeiska individuella intyg om cybersäkerhetskompetens, i synnerhet när det gäller bedömning av individer, bör Enisa tillhandahålla obligatorisk utbildning av den personal som utför bedömningen av individer. Sådan personal bör ha erfarenhet från cybersäkerhetsområdet som kan påvisas genom innehav av ett europeiskt individuellt intyg om cybersäkerhetskompetens för den yrkesprofil som den utför bedömningen av, på en kompetensnivå som minst motsvarar kompetensnivån hos den individ som de bedömer.

(52) Auktoriserade tillhandahållare av intyg har uppgiften att intyga att en individ har den kunskap och kompetens som behövs för att kunna utföra det som ingår i en av ECSF-yrkesprofilerna och tillhandahålla en kvalitetssäkring för arbetsgivarna i unionen. I och med att även arbetsgivare som driver kritisk infrastruktur i unionen tittar på kvalitetssäkringen av färdigheter och kompetenser hos de individer som förvärvar europeiska individuella intyg om cybersäkerhetskompetens bör de auktoriserade tillhandahållare som intygar nivån på färdigheter och kompetenser vara tillförlitliga ur cybersäkerhetssynpunkt och inte vara föremål för otillbörlig påverkan från tredjeländer som kan utgöra cybersäkerhetsproblem. Därför bör entiteter som är etablerade i ett tredjeland som utgör cybersäkerhetsproblem och som har utpekats i enlighet med denna förordning, eller som kontrolleras av ett sådant land, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland (högriskleverantörer) i enlighet med denna förordning bör inte ha rätt att bli auktoriserad tillhandahållare av intyg för några europeiska individuella intyg om cybersäkerhetskompetens enligt avdelning II avsnitt 4.

(53) För att säkerställa att individer som innehar ett europeiskt intyg om cybersäkerhetskompetens enkelt kan använda och uppvisa detta och att sådana intyg kan användas i alla medlemsstater bör auktoriserade tillhandahållare av intyg säkerställa att elektroniska intyg för de europeiska individuella intygen om cybersäkerhetskompetens på individens begäran utfärdas till den europeiska digitala identitetsplånbok (EUDI-plånboken) som inrättats genom förordning (EU) nr 910/2014. Auktoriserade tillhandahållare av intyg bör anses som tillhandahållare av betrodda tjänster och omfattas av det system för tillsyn och skadeståndsansvar som fastställs i förordning (EU) nr 910/2014. Det system för attributsintyg som används i enlighet med kommissionens genomförandeförordning (EU) 2025/1569[52] bör registreras i katalogen över system för attributsintyg som föreskrivs i den genomförandeförordningen.

(54) För att bidra till utvecklingen av cybersäkerhetsarbetskraften och kompetensportabiliteten i hela unionen bör Enisa se till att ordningarna för europeiska individuella intyg om cybersäkerhetskompetens och förteckningen över auktoriserade tillhandahållare av intyg är tillgängliga för allmänheten via en särskild webbplats.

(55) Enisa bör styras och bedriva sin verksamhet med beaktande av principerna i den gemensamma ansats för unionens decentraliserade byråer som godkändes av

[52] Genomförandeförordning (EU) 2025/1569.

Europaparlamentet, rådet och kommissionen den 19 juli 2012[53]. Rekommendationerna i den gemensamma ansatsen bör också på lämpligt sätt återspeglas i Enisas arbetsprogram, utvärderingar av Enisa och Enisas rapporterings- och förvaltningsmetoder.

(56) För att styrelsen ska kunna utföra sina uppgifter på ett effektivt sätt, i synnerhet när det gäller vägledning i fråga om inriktningen på Enisas verksamhet och fastställande av Enisas strategiska prioriteringar, är det viktigt att styrelsen består av högnivårepresentanter för medlemsstaterna och kommissionen. Därför bör varje medlemsstat till styrelseledamot utse chefen för en nationell behörig myndighet i den medlemsstaten som ansvarar för cybersäkerhet och som utsetts i enlighet med artikel 8.1 i direktiv (EU) 2022/2555.

(57) För att säkerställa att suppleanter i styrelsen kan fullgöra sina uppdrag på lämpligt sätt bör medlemsstaterna utse suppleanter som har lämplig yrkesmässig expertis och erfarenhet. När det gäller suppleanterna bör kommissionen och medlemsstaterna sträva efter en jämn könsfördelning i styrelsen och begränsa omsättningen av suppleanter för att säkerställa kontinuitet i styrelsens arbete.

(58) För att göra det möjligt för Enisa att fullgöra sitt uppdrag effektivt bör styrelsen, bestående av medlemsstaternas och kommissionens företrädare, fastställa den allmänna inriktningen på Enisas arbete, inbegripet dess strategiska prioriteringar, och säkerställa att Enisa utför sina uppgifter i enlighet med denna förordning. Styrelsen bör ha befogenhet att fastställa budgeten och kontrollera att den genomförs, anta lämpliga finansiella bestämmelser, utarbeta transparenta förfaranden för Enisas beslutsfattande, godkänna Enisas samlade programdokument, anta sin egen arbetsordning, utse den verkställande direktören, besluta om förlängning respektive avslutande av den verkställande direktörens mandatperiod och besluta ifall funktionen vice verkställande direktör bör inrättas – och i sådana fall utse den vice verkställande direktören och besluta om förlängning respektive avslutande av den vice verkställande direktörens mandatperiod. Alla personer som utövar en verkställande funktion inom Enisa bör därför utses av styrelsen. Styrelsen bör också ansvara för att utnämna eller avsätta överklagandenämndens medlemmar och fastställa regler för att förhindra eller hantera intressekonflikter i det hänseendet.

(59) För att bidra till att säkerställa att Enisa fastställer sina strategiska prioriteringar och håller dem uppdaterade bör styrelsen minst en gång per år hålla ett sammanträde som helt viks åt Enisas strategiska prioriteringar. För att säkerställa att styrelsen är effektiv och välinformerad får styrelsen till sina sammanträden bjuda in personer vars synpunkter kan vara relevanta och av intresse för de ämnen som diskuteras för att tillhandahålla insikter, sakkunskap eller råd. En sådan person skulle vara en tillfällig observatör utan rösträtt.

(60) Styrelsen bör anta sina beslut med absolut majoritet av sina ledamöter med rösträtt, om inte annat föreskrivs i denna förordning. Mot bakgrund av betydelsen av budget- och personalfrågor – i synnerhet frågor som rör den årliga budgeten, den årliga verksamhetsrapporten, strategin för bedrägeribekämpning, genomföranderegler som ger verkan åt tjänsteföreskrifterna, utnämningen av verkställande direktör, vice

[53] Gemensam ansats som fogats till det gemensamma uttalandet från Europaparlamentet, Europeiska unionens råd och Europeiska kommissionen om decentraliserade organ, som antogs den 19 juli 2012 och finns på: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

verkställande direktör och räkenskapsförare, uppföljning av iakttagelser från Europeiska byrån för bedrägeribekämpning (Olaf) och Europeiska åklagarmyndigheten (Eppo) och antagandet av Enisas finansiella regler – bör styrelsen anta sådana beslut endast om kommissionens företrädare avger en positiv röst. Vid antagandet av ett beslut om antagande av ett slutligt samlat programdokument efter beaktande av kommissionens yttrande, bör en positiv röst från kommissionens företrädare krävas endast med avseende på de delar av beslutet som inte rör Enisas årliga och fleråriga arbetsprogram.

(61) Direktionen bör bidra till att styrelsen fungerar på ett effektivt sätt. Som ett led i det förberedande arbetet i samband med styrelsens beslut bör styrelsen i detalj granska relevant information och utforska tillgängliga alternativ och ge råd och lösningar för att förbereda styrelsens beslut. Den bör också bistå och lämna råd till den verkställande direktören vid genomförandet av styrelsens beslut.

(62) För att Enisa ska fungera väl bör den verkställande direktören utses på grundval av meriter, dokumenterad skicklighet i förvaltning och ledarskap samt kompetens och erfarenheter som rör cybersäkerhet. Den verkställande direktörens uppgifter bör utföras med fullständigt oberoende. Styrelsen bör utse den verkställande direktören på grundval av en förteckning över kandidater som utarbetats av kommissionen, efter ett öppet och transparent förfarande som iakttar principen om jämn könsfördelning.

(63) Den verkställande direktören bör utarbeta ett förslag till Enisas samlade programdokument, efter samråd med kommissionen, och bör vidta alla åtgärder som är nödvändiga för att säkerställa att det samlade programdokumentet genomförs på rätt sätt. Den verkställande direktören bör utarbeta en årsrapport, som föreläggs styrelsen och omfattar genomförandet av Enisas årliga arbetsprogram, samt upprätta en preliminär beräkning av Enisas inkomster och utgifter och genomföra budgeten. Den verkställande direktören bör också ha möjlighet att inrätta tillfälliga arbetsgrupper som i synnerhet ska behandla vetenskapliga, tekniska, rättsliga eller socioekonomiska frågor. Inrättandet av en tillfällig arbetsgrupp anses i synnerhet nödvändigt i samband med utarbetandet av enskilda förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordning*). Det kan också vara nödvändigt att inrätta en tillfällig arbetsgrupp för underhållsverksamhet i samband med särskilda antagna europeiska ordningar för cybersäkerhetscertifiering. Tillfälliga arbetsgrupper bör även inrättas för att utveckla och underhålla ordningar för europeiska individuella intyg om cybersäkerhetskompetens och bistå Enisa i arbetet med styrningen, genomförandet och utvecklingen av den europeiska kompetensramen för cybersäkerhet. Den verkställande direktören bör säkerställa att de tillfälliga arbetsgruppernas medlemmar väljs med utgångspunkt i högsta möjliga standard när det gäller expertkunskaper, med målsättningen att det bör finnas en jämn könsfördelning och, utifrån de specifika frågor som berörs, en lämplig balans mellan medlemsstaternas förvaltningar, unionsentiteter och den privata sektorn, inklusive branschen, användare och akademiska experter på nätverks- och informationssäkerhet liksom akademiska experter på produkter med digitala element.

(64) Styrelsen får besluta att inrätta funktionen vice verkställande direktör för att bistå den verkställande direktören, om styrelsen anser att en sådan funktion är nödvändig för att säkerställa eller upprätthålla en välfungerande verksamhet hos Enisa. När styrelsen beslutar om ett eventuellt inrättande av denna funktion får den beakta den verkställande direktörens synpunkter.

(65) Enisa bör också ha en rådgivande grupp för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda parter. Enisas rådgivande grupp, som inrättats av styrelsen på förslag av den verkställande direktören, bör koncentrera sig på frågor som är relevanta för berörda parter och bör uppmärksamma Enisa på dessa frågor. Enisas rådgivande grupp bör särskilt rådfrågas om utkastet till Enisas årliga arbetsprogram. Sammansättningen av Enisas rådgivande grupp och de uppgifter som anförtrotts den bör säkerställa en tillräcklig representation av berörda parter i Enisas arbete. Företrädare för medlemsstaternas och unionens rättsvårdande myndigheter, dataskyddsmyndigheter och marknadskontrollmyndigheter bör ha rätt att företrädas i Enisas rådgivande grupp.

(66) De som ansöker om att bli auktoriserade tillhandahållare av intyg eller om att förnya sin auktorisation bör ha tillgång till nödvändiga rättsmedel när de påverkas av beslut som fattas av Enisa. Därför bör ett lämpligt överklagandeförfarande fastställas så att byråns beslut kan överklagas till en överklagandenämnd, vars beslut i sin tur kan överklagas till Europeiska unionens domstol (*domstolen*) i enlighet med fördragen. Kravet på att Enisas överklagandeförfarande måste uttömmas innan ett ärende väcks hos Europeiska unionens domstol är endast tillämpligt på personer som har talerätt vid överklagandenämnden.

(67) För att garantera Enisas fullständiga autonomi och oberoende och göra det möjligt för Enisa att utföra sina uppgifter bör Enisa beviljas en tillräcklig och autonom budget som främst finansieras genom bidrag från unionen, men även genom bidrag från tredjeländer som deltar i Enisas arbete och genom avgifter som betalas av auktoriserade tillhandahållare av intyg och organ för bedömning av överensstämmelse som deltar i ordningar och utfärdar europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse. Värdmedlemsstaten, och alla andra medlemsstater, bör ha rätt att lämna frivilliga bidrag till Enisas budget. Inga bidrag, vare sig finansiella eller in natura, till Enisa från medlemsstater, tredjeländer eller andra entiteter eller personer får äventyra Enisas självständighet och opartiskhet. Unionens budgetförfarande bör tillämpas på unionens bidrag och alla andra bidrag från unionens allmänna budget. Revisionsrätten bör granska Enisas räkenskaper för att säkerställa transparens och ansvarighet. För att kunna delta i alla relevanta framtida projekt bör byrån ges möjlighet att ta emot bidrag.

(68) För att säkerställa Enisas kapacitet att tillgodose efterfrågan på de tjänster som Enisa tillhandahåller, i synnerhet när det gäller beslut om att auktorisera tillhandahållare att utfärda europeiska individuella intyg om cybersäkerhetskompetens och när det gäller underhåll av ordningarna för europeisk cybersäkerhetscertifiering och av testverktyg, bör Enisa ges befogenhet att ta ut avgifter. Avgifter i samband med behandlingen av ansökningar om att bli auktoriserad tillhandahållare av intyg bör fastställas på lämpligt sätt, så att de i tillräcklig grad bidrar till att täcka de beräknade kostnaderna för utveckling och underhåll av ordningarna för europeiska individuella intyg om cybersäkerhetskompetens och för utvärdering av om kraven och skyldigheterna för att bli och förbli auktoriserad tillhandahållare av intyg uppfylls och fortsätter att uppfyllas. Avgifter i samband med kostnaderna för att utfärda och förnya auktorisationer till auktoriserade tillhandahållare av intyg bör inkludera kostnaderna för utvärderingar som utförs av Enisa eller under Enisas tillsyn. Avgifter i samband med deltagande i de europeiska ordningarna för cybersäkerhetscertifiering och för utfärdande av certifikat inom sådana ordningar bör fastställas på lämpligt sätt, så att de i tillräcklig grad bidrar till att täcka de beräknade kostnaderna för upprätthållandet av ordningarna. Betalningen av sådana avgifter bör göra det möjligt för anmälda organ

för bedömning av överensstämmelse och, i tillämpliga fall, innehavare av certifikat inom en ordning att delta i sådan verksamhet samt relevant kapacitetsuppbyggnad och PR-verksamhet för att främja utbyte av bästa praxis och ökat genomslag för ordningar och certifierade lösningar.

(69) För att säkerställa proportionalitet, transparens och rättssäkerhet bör avgifterna fastställas på ett transparent och rättvist sätt. Alla Enisas utgifter som kan hänföras till personal som deltar i verksamhet som är avgiftsbelagd, i synnerhet arbetsgivarens proportionella bidrag till pensionssystemet, och kostnader som rör överklagandenämnden, bör återspeglas i den kostnaden. Avgifterna får inte leda till onödiga finansiella eller administrativa bördor för de sökande. Rimliga tidsfrister bör fastställas för betalningen av avgifter.

(70) Det är nödvändigt införa en uppsättning indikatorer för att mäta byråns arbetsbelastning, ändamålsenlighet och effektivitet när det gäller verksamhet som finansieras genom avgifter. Med beaktande av dessa indikatorer bör byrån anpassa sin personalplanering och förvaltning av resurser i samband med avgifter för att på lämpligt sätt kunna tillgodose sådan efterfrågan och eventuella fluktuationer i intäkterna från avgifter.

(71) För att identifiera och korrekt hantera risken för faktiska eller upplevda intressekonflikter bör Enisa ha regler om förebyggande och hantering av intressekonflikter. Enisa bör också tillämpa de regler om tillgång till handlingar som fastställs i Europaparlamentets och rådets förordning (EG) nr 1049/2001[54]. Enisas behandling av personuppgifter bör ske i enlighet med Europaparlamentets och rådets förordning (EU) 2018/1725[55]. Enisa bör efterleva de bestämmelser som gäller för unionsentiteterna och den nationella lagstiftning som rör hantering av information, i synnerhet känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter.

(72) Vid utförandet av sina uppgifter kan Enisa få tillgång till känsliga uppgifter, såsom uppgifter om cyberhot och incidenter. Det är därför viktigt att Enisa bevarar konfidentialiteten för de uppgifter som byrån hanterar. I linje med artikel 339 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*) gäller i synnerhet att tjänstemän och övriga anställda i Enisa, även efter det att deras uppdrag upphört, är förpliktade att inte lämna ut upplysningar som omfattas av tystnadsplikt, särskilt uppgifter om företag, deras affärsförbindelser eller deras kostnadsförhållanden.

(73) För att säkerställa att Enisa fullt ut uppnår sina mål bör byrån samarbeta med berörda EU-tillsynsmyndigheter och andra behöriga myndigheter i unionen, berörda unionsentiteter, däribland CERT-EU, EC3 vid Europol, Europeiska försvarsbyrån (EDA), Europeiska unionens rymdprogrambyrå (EUSPA), Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec), Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (eu-LISA), Europeiska centralbanken (ECB), Europeiska bankmyndigheten

---

[54] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

[55] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(EBA), Europeiska dataskyddsstyrelsen, Byrån för samarbete mellan energitillsynsmyndigheter (Acer), Europeiska unionens byrå för luftfartssäkerhet (Easa) och andra unionsentiteter som arbetar med cybersäkerhet. Enisa bör också samarbeta med behöriga myndigheter enligt direktiv (EU) 2022/2555, marknadskontrollmyndigheter och myndigheter som hanterar dataskydd för att utbyta kunnande och bästa praxis, och bör lämna råd om cybersäkerhetsfrågor som kan påverka deras arbete.

(74) Europol har en viktig roll när det gäller att förebygga och bekämpa cyberbrottslighet, inbegripet cyberbrottslighet kopplad till nät- och informationssäkerhetsincidenter. För att skapa synergier mellan de två byråernas respektive uppgifter bör Enisa samarbeta med Europol, i synnerhet genom att utbyta information om trender i fråga om teknik, krav och konsekvenser i samband med utpressningsprogram. Sådant samarbete kan också omfatta kartläggning av de vanligaste typerna av utpressningsprogram som riktas mot entiteter som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, för att stödja väsentliga och viktiga entiteter i deras incidenthantering och återställning.

(75) För att stödja operativt samarbete och gemensam situationsmedvetenhet när det gäller cyberhot och incidenter är det viktigt att Enisa samarbetar med berörda parter och i synnerhet med företag och organisationer från den privata sektorn, som Enisa kan inrätta offentlig-privata partnerskap med.

(76) För att effektivt uppnå de mål som anges i denna förordning kan Enisa i synnerhet samarbeta med akademiska institutioner som bedriver forskningsinitiativ på relevanta områden och utveckla lämpliga kanaler för synpunkter från konsumentorganisationer och andra organisationer.

(77) I och med att cyberhot och incidenter sträcker sig över gränser kan tredjeländers cybersäkerhetsnivå och beredskap påverka entiteter i unionen. Därför bör Enisa kunna tillhandahålla kapacitetsuppbyggnadsverksamhet, inbegripet utbildning, kapacitetsuppbyggnad, partnersamverkan i tredjeländer och i synnerhet skräddarsydd kapacitetsuppbyggnadsverksamhet för länder som är kandidater för anslutning till unionen eller andra partnerländer, i enlighet med unionens prioriteringar. Sådan verksamhet bör bedrivas efter en särskild förfrågan om adekvat stöd, med beaktande av unionens prioriteringar, och genomföras genom särskilda arrangemang, däribland överenskommelser om medverkan enligt förordning (EU, Euratom) 2024/2509. Det europeiska ramverket för cybersäkerhetscertifiering syftar till att skydda mot cyberhot, såsom fientligt utnyttjande av cybersäkerhetssårbarheter eller cybersäkerhetsincidenter som påverkar funktionerna (utformning och drift) för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus. Genom att fokusera på tekniska risker i samband med IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus bör det europeiska ramverket för cybersäkerhetscertifiering komplettera ramverket för säkerhet i IKT-leveranskedjan, som syftar till att säkerställa en harmoniserad strategi på unionsnivå för att hantera icke-tekniska risker inom högkritiska sektorer och andra kritiska sektorer.

(78) Det bör vara möjligt för medlemsstaterna att använda sig av europeisk cybersäkerhetscertifiering i samband med offentlig upphandling i enlighet med Europaparlamentets och rådets direktiv 2014/24/EU[56].

(79) För att underlätta förenkling av efterlevnaden för entiteter bör det europeiska ramverket för cybersäkerhetscertifiering omfatta en möjlighet att certifiera deras cybersäkerhetsstatus. Entiteter, i synnerhet entiteter som tillhandahåller flera olika typer av tjänster i flera medlemsstater, kan mötas av olika cybersäkerhets- och datasäkerhetsrelaterade skyldigheter enligt övergripande instrument, såsom Europaparlamentets och rådets förordning (EU) 2016/679[57] och Europaparlamentets och rådets direktiv (EU) 2022/2555[58], liksom sektorsspecifika instrument. För att rationalisera genomförandet av det övergripande cybersäkerhetsregelverket och underlätta efterlevnaden av det bör unionslagstiftningen kunna föreskriva en möjlighet för entiteter att visa att de uppfyller kraven på cybersäkerhetsriskhantering genom ett europeiskt cybersäkerhetscertifikat. En berörd ordning skulle kunna bidra till att harmonisera de efterlevnadskrav som följer av olika regleringsinstrument, utan att det påverkar deras specifika certifieringskrav. Sådana förenklingsåtgärder skulle kunna minska den administrativa bördan och därmed frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter inom kritiska sektorer i unionen.

(80) Den europeiska certifiering av krav på cybersäkerhetsriskhantering som utvecklas inom det europeiska ramverket för cybersäkerhetscertifiering bör göra det möjligt för entiteter att visa att de efterlever relevant unionslagstiftning om en ordning täcker de respektive rättsliga krav som fastställs i en sådan akt och om den föreskriver detta. På denna grund kan också en unionsrättsakt föreskriva en presumtion om överensstämmelse med dessa krav. Sådana ordningar kan bidra till att förbättra det sammanhållna genomförandet av cybersäkerhetskrav i unionslagstiftning för att skapa lika villkor i alla medlemsstater och minska efterlevnadsbördan.

(81) Det europeiska ramverket för cybersäkerhetscertifiering bör omfatta en möjlighet att certifiera IKT-processer, definierade som en uppsättning aktiviteter som utförs för att utforma, utveckla, leverera eller underhålla en IKT-produkt eller en IKT-tjänst. En skyddsprofil är ett exempel på en IKT-process, såsom anges i kommissionens genomförandeförordning (EU) 2024/482[59]. Ett annat exempel på en IKT-process är en uppsättning aktiviteter som utförs av en tillverkare för att på ett säkert sätt utforma och utveckla en IKT-produkt, däribland fysiska, logiska, förfarandemässiga och personalrelaterade åtgärder och andra säkerhetsåtgärder som är nödvändiga för att skydda konfidentialiteten och integriteten i samband med utformningen och

---

56 Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

57 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

58 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

59 Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

implementeringen av en IKT-produkt i dess utvecklingsmiljö. Certifieringen av sådana aktiviteter benämns ofta som *anläggningscertifiering* i samband med en certifieringsprocess enligt kommissionens genomförandeförordning (EU) 2024/482.

(82) Definitionen av utlokaliserade säkerhetstjänster i denna förordning bör överensstämma med den för leverantörer av utlokaliserade säkerhetstjänster i direktiv (EU) 2022/2555. Dessa tjänster, som består i att utföra eller tillhandahålla stöd för verksamhet som rör deras kunders hantering av cybersäkerhetsrisker, har blivit allt viktigare när det gäller att förhindra och begränsa incidenter. Leverantörerna av dessa tjänster betraktas därför som väsentliga eller viktiga entiteter som tillhör en högkritisk sektor enligt direktiv (EU) 2022/2555. Leverantörer av utlokaliserade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster har en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Leverantörer av utlokaliserade säkerhetstjänster har dock också själva varit mål för cyberattacker och utgör en särskild risk, eftersom de är nära integrerade i sina kunders verksamhet. Det är därför nödvändigt att väsentliga och viktiga entiteter i den mening som avses i direktiv (EU) 2022/2555 visar större aktsamhet vid valet av leverantörer av utlokaliserade säkerhetstjänster.

(83) Europeiska ordningar för cybersäkerhetscertifiering är relevanta för en bred grupp intressenter, såsom leverantörer av IKT-lösningar, organ för bedömning av överensstämmelse och användare. För att främja ett brett deltagande av intressenter bör den europeiska församlingen för cybersäkerhetscertifiering (*församlingen*) anordnas minst en gång om året i syfte att främja samarbete mellan kommissionen, Enisa, medlemsstaterna och berörda intressenter. Den kommer att ha en avgörande betydelse för arbetet med att identifiera och ta itu med nya cybersäkerhetsutmaningar och strategiska prioriteringar på certifieringsområdet samt att säkerställa att certifieringsordningarna underlättar en säker integrering av digital teknik och är anpassade till användarnas behov. Församlingen bör främja unionens ledarskap inom certifieringsverksamhet och upprätthålla certifieringsramens förmåga att skapa förtroende bland företag, offentliga myndigheter och allmänheten.

(84) Kommissionen bör upprätthålla en särskild webbplats för att säkerställa transparens genom offentliggörande av aktuell information om arbetet med att genomföra det europeiska ramverket för cybersäkerhetscertifiering. Webbplatsen bör omfatta information om certifieringsordningar under utarbetande, strategiska prioriteringar för kommande certifieringsordningar, begäranden till Enisa om utarbetande av förslag till certifieringsordningar och information om antagandet av certifieringsordningar. Kommissionens webbplats kommer att komplettera Enisas webbplats om europeiska ordningar för cybersäkerhetscertifiering, som bör omfatta heltäckande uppgifter om det tekniska utarbetandet av förslag till certifieringsordningar och underhåll av certifieringsordningar, med fokus på utfärdade europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse.

(85) För att stärka dialogen mellan unionens institutioner och bidra till en formell, öppen, transparent och inkluderande samrådsprocess bör kommissionen, när den utvärderar denna förordning, beakta aspekter som anges i synpunkter från Europaparlamentet, rådet och den europeiska församlingen för cybersäkerhetscertifiering.

(86) Genomförbarhetsstudier som utförs av Enisa bör bidra till förberedelserna av planering och utveckling av ordningar för cybersäkerhetscertifiering. De bör ta hänsyn till berörda parters synpunkter och anpassa de framtida certifieringsordningarna till

pågående arbete inom forskning, utveckling och teknisk bedömning, i synnerhet med beaktande av bidrag från unionens och medlemsstaternas forskningsinitiativ. Sådana studier kan bidra till kartläggning av tillgängliga standarder och tekniska specifikationer. De bör utföras på begäran av kommissionen eller i enlighet med unionens strategiska prioriteringar för att säkerställa att de föränderliga tekniska villkoren och cybersäkerhetsbehoven på ett fullgott sätt hanteras och återspeglas när ordningar begärs och utvecklas.

(87) Utformningen av ett förslag till certifieringsordning och det sätt på vilket ordningen täcker säkerhetsmål och säkerhetselement bör stå i proportion till certifieringsföremålets ämne och tillämpningsområde. Därmed kan t.ex. en certifieringsordning för molntjänster omfatta säkerhetsmål som är relevanta för IKT-tjänster och organisatorisk säkerhet. Som ett annat exempel kommer ett säkerhetsmål kopplat till att inte inkludera kända sårbarheter som kan utnyttjas sannolikt inte att vara relevant för certifieringen av IKT-processer.

(88) För att säkerställa att europeiska ordningar för cybersäkerhetscertifiering genomförs på ett harmoniserat sätt i alla medlemsstater är det nödvändigt att föreskriva regler för underhåll av ordningarna. Underhållsarbetet är också nödvändigt för att säkerställa att ordningarna och den styrkande dokumentationen för dem hålls uppdaterade, särskilt på cybersäkerhetsområdet där hotbilden och tekniken ständigt utvecklas. Certifieringsordningarna bör därför utformas och underhållas på ett sätt som undanröjer risken för att de snabbt ska bli föråldrade. Underhållsarbetet bör normalt involvera utarbetande och uppdatering av styrkande dokumentation, inbegripet tekniska specifikationer och riktlinjer, samt kartläggning av standarder eller tekniska specifikationer av relevans för ordningen. En analys av ordningens funktionssätt, dess potentiella brister och nödvändiga förbättringar bör också ingå i underhållsarbetet. Dessutom bör underhållsarbetet omfatta informationsutbyte mellan medlemsstaterna om genomförandet av ordningar samt bidrag till mekanismer för inbördes granskning och inbördes bedömning.

(89) Till följd av underhållsarbetets tekniska karaktär bör Enisa förvalta sådan verksamhet, i samarbete med kommissionen och med stöd av den europeiska gruppen för cybersäkerhetscertifiering (ECCG) och dess undergrupp för underhåll. Inrättandet av en ECCG-undergrupp för underhåll gör det möjligt att samla in tekniska bidrag och insikter från medlemsstaterna med sikte på ett harmoniserat tillvägagångssätt.

(90) Underhållsarbetet bör omfatta interaktion med berörda intressentgrupper för att säkerställa att ordningarna förblir marknadsrelevanta och uppdaterade, bland annat genom delning och mottagande av tekniska bidrag. Sådana intressentgrupper kan utgöras av standardiseringsorganisationer, organ för bedömning av överensstämmelse, leverantörer, användare, offentliga myndigheter eller branschorganisationer. De olika ordningarnas särdrag, inklusive deras motsvarande tekniska forum och industrier, innebär att det bör vara möjligt att samla in tekniska bidrag på olika sätt från olika ordningar. För vissa ordningar bör Enisa kunna använda sig av en tillfällig arbetsgrupp som samlar experter från medlemsstaternas offentliga förvaltningar, unionsentiteter och den privata sektorn. Tekniska bidrag kan också komma från informations- och analyscentraler eller standardiseringsorganisationer. Enisa bör analysera vilket format som är lämpligast för varje ordning och inkludera en underhållsstrategi i varje förslag till certifieringsordning.

(91) Europeiska ordningar för cybersäkerhetscertifiering bör bygga på standarder eller tekniska specifikationer, i synnerhet för definitionen av säkerhetskrav och

utvärderingsmetoder. Enisa bör ges möjlighet att utarbeta tekniska specifikationer till stöd för utarbetandet och underhållet av ordningar, i synnerhet om produkter från standardiseringsorganisationer saknas eller inte är lämpliga i förhållande till ordningens målsättningar. Som ett led i utarbetandet bör Enisa stödjas av den europeiska gruppen för cybersäkerhetscertifiering och, i tillämpliga fall, den tillfälliga arbetsgrupp som inrättats för den berörda ordningen. Enisa bör också efterfråga bidrag från intressentgrupper. Enisa bör beakta marknadsacceptansen och europeiska och internationella standarder. Med beaktande av kvaliteten på de tekniska specifikationerna och ordningens målsättningar bör det vara möjligt för kommissionen att hänvisa till tekniska specifikationer som utarbetats av Enisa i en europeisk ordning för cybersäkerhetscertifiering.

(92) Tekniska specifikationer som utvecklats av Enisa och som det hänvisas till i en ordning bör göras tillgängliga på Enisas webbplats för europeiska ordningar för cybersäkerhetscertifiering, så att alla berörda parter kan få tillgång till dem. I vissa specifika fall kan ett offentliggörande på en webbplats dock utgöra en risk för cybersäkerheten för certifierade IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus och därmed i förlängningen för allmän säkerhet. Exempelvis kan tekniska specifikationer innehålla exakt information om nya angreppsvägar som skulle kunna användas av fientliga aktörer om de görs allmänt tillgängliga. Denna typ av information bör spridas på ett restriktivt sätt baserat på behovsenlig behörighet till berörda parter, såsom nationella myndigheter för cybersäkerhetscertifiering, organ för bedömning av överensstämmelse och leverantörer som är föremål för certifiering. På grund av den restriktiva spridningen av sådana tekniska specifikationer bör ingen hänvisning till dem finnas i europeiska ordningar för cybersäkerhetscertifiering och de bör därför inte vara bindande.

(93) Ordningar för certifiering av cybersäkerhetsstatus bör utformas på ett modulärt sätt, för att göra det möjligt att påvisa efterlevnad och presumtion om överensstämmelse med relevanta cybersäkerhetskrav i annan unionslagstiftning, i de fall då lagstiftningen omfattar den möjligheten. Presumtionen om överensstämmelse med kraven i dessa rättsakter kommer därför endast att få verkan som ett möjligt sätt att påvisa regelefterlevnad om respektive rättsakt möjliggör sådan presumtion om överensstämmelse. Detaljerna i en sådan ordning, närmare bestämt syftet, målsättningarna eller vissa aspekter, kommer därför sannolikt att skilja sig från dem i andra ordningar. I synnerhet bör ordningar för certifiering av entiteters cybersäkerhetsstatus utvecklas för att möjliggöra en bedömning av en entitets kontinuerliga överensstämmelse med unionslagstiftning. Det är därför inte nödvändigt att ordningar för certifiering av entiteters cybersäkerhetsstatus omfattar alla delar av europeiska ordningar för cybersäkerhetscertifiering, såsom assuransnivåer, och detta bör återspeglas i reglerna för ordningarna.

(94) En ram för certifiering av cybersäkerhetsstatus inom det europeiska ramverket för cybersäkerhetscertifiering gör det möjligt att utveckla en ordning som innebär att entiteter som tillhandahåller tjänster i flera medlemsstater kan påvisa regelefterlevnad med avseende på de skyldigheter avseende hantering av cybersäkerhetsrisker som fastställs i Europaparlamentets och rådets direktiv 2022/2555. På grundval av detta kan de entiteter som kan påvisa regelefterlevnad dra nytta av mer enhetliga och mindre betungande tillsynsstrategier på den inre marknaden. Utvecklingen av en sådan certifieringsordning bör underlättas av antagandet av genomförandeakter enligt direktiv (EU) 2022/2555. Genom tilläggsprofiler kan en ordning för certifiering av

cybersäkerhetsstatus påvisa regelefterlevnad av kraven i de fall då en medlemsstat har antagit eller bibehållit bestämmelser som säkerställer en högre cybersäkerhetsnivå i linje med direktiv (EU) 2022/2555. På denna grund kan en entitet som tillhandahåller tjänster i flera medlemsstater påvisa regelefterlevnad av alla relevanta tilläggsprofiler genom ett enda europeiskt cybersäkerhetscertifikat.

(95) De säkerhetsmål och säkerhetskrav som fastställs i europeiska ordningar för cybersäkerhetscertifiering och som hänför sig till produktsäkerhet bör vara samstämmiga med de väsentliga cybersäkerhetskrav som fastställs i bilaga I till förordning (EU) 2024/2847. Denna samstämmighet är nödvändig för att säkerställa att tillverkare vars produkter omfattas av förordning (EU) 2024/2847 inte ställs inför motstridiga krav när de certifierar sina produkter inom en europeisk ordning för cybersäkerhetscertifiering. Konsekventa krav underlättar också presumtion om överensstämmelse enligt artikel 27 i förordning (EU) 2024/2847, som innebär att tillverkare av produkter med digitala element som har certifierats inom en europeisk ordning för cybersäkerhetscertifiering på vissa villkor kan omfattas av presumtion om överensstämmelse med väsentliga cybersäkerhetskrav enligt bilaga I till den förordningen.

(96) Inom den europeiska ordningen för cybersäkerhetscertifiering bör det vara möjligt att specificera en tilläggsprofil, genom att fastställa ytterligare eller specifika krav för användningsfall, inbegripet ytterligare förmågor såsom förbättrade produktegenskaper, specialiserade tjänsteerbjudanden eller tillgångar, optimerade processer och avancerade säkerhetsåtgärder. I och med att tilläggsprofiler inte motsvarar en särskild assuransnivå bör de omfatta en detaljerad beskrivning av deras syfte, inbegripet de säkerhetshot som avses. Tilläggsprofiler är i synnerhet avsedda att påvisa regelefterlevnad med avseende på specifika standarder och lagstadgade krav inbegripet, i tillämpliga fall, krav som rör ytterligare riskhanteringsåtgärder för cybersäkerhet som fastställs av en medlemsstat enligt principen om minimiharmonisering i linje med direktiv (EU) 2022/2555.

(97) Utan att det påverkar det allmänna system för inbördes granskning som bör införas hos alla nationella myndigheter för cybersäkerhetscertifiering inom det europeiska ramverket för cybersäkerhetscertifiering, bör det vara möjligt att i de europeiska ordningarna för cybersäkerhetscertifiering inkludera en mekanism för inbördes bedömning för de organ som utfärdar europeiska cybersäkerhetscertifikat för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus, i synnerhet för de organ som utfärdar certifikat med assuransnivån ”hög” inom ramen för sådana ordningar. Sådana organ bör också omfatta certifieringsorgan hos de nationella myndigheter för cybersäkerhetscertifiering som utfärdar certifikat på assuransnivå ”hög”. Den europeiska gruppen för cybersäkerhetscertifiering bör stödja tillämpningen av sådana mekanismer för inbördes bedömning. De inbördes bedömningarna bör framför allt bedöma om de berörda organen utför sina uppgifter på ett harmoniserat sätt och de kan innefatta mekanismer för att överklaga.

(98) Kriser, som krig, naturkatastrofer och pandemier, kan ha en negativ inverkan på certifieringsverksamheten. I krisscenarier av detta slag är det kanske inte genomförbart att t.ex. säkerställa anläggningssäkerhet på grund av förstörd infrastruktur, cyberattacker, personalbrist och bristande tillgänglighet till anläggningen. En europeisk ordning för cybersäkerhetscertifiering bör därför specificera tillfälliga regler för certifieringsverksamhetens kontinuitet under sådana scenarier.

(99) För att omsätta tekniska förslag till certifieringsordningar i genomförandeakter krävs komplexa tekniska och rättsliga kunskaper vilket kan bli mycket administrativt betungande. Vissa delar av europeiska ordningar för cybersäkerhetscertifiering, såsom sårbarhetshantering eller villkoren för när sådana märken eller etiketter får användas, är sektorsövergripande och skulle kunna gynnas av harmoniserade referensbestämmelser. För att säkerställa kvaliteten på antagna europeiska ordningar för cybersäkerhetscertifiering och minska efterlevnadsbördan för företagen bör kommissionen ges befogenhet att anta standardbestämmelser som omfattar vissa delar av europeiska ordningar för cybersäkerhetscertifiering.

(100) I syfte att säkerställa konsekvens i den europeiska ramen för cybersäkerhetscertifiering bör det vara möjligt att inom en europeisk ordning för cybersäkerhetscertifiering specificera assuransnivåer för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse som utfärdats inom ramen för den ordningen. Ett europeiskt cybersäkerhetscertifikat bör hänvisa till en av assuransnivåerna ”grundläggande”, ”betydande” eller ”hög”, medan EU-försäkran om överensstämmelse endast bör hänvisa till assuransnivån ”grundläggande”. Assuransnivåerna bör tillhandahålla motsvarande stringens och djup i utvärderingen av IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller entitetens cybersäkerhetsstatus och bör kännetecknas av en hänvisning till relaterade tekniska specifikationer, standarder och förfaranden, inbegripet tekniska kontroller, vars syfte är att begränsa eller förebygga incidenter. Varje assuransnivå bör vara konsekvent inom de olika sektoriella områden där certifiering tillämpas.

(101) Det val av lämplig certifiering och tillhörande säkerhetskrav som görs av användarna av europeiska cybersäkerhetscertifikat bör baseras på en analys av de risker som är förknippade med användningen av IKT-produkterna, IKT-tjänsterna, IKT-processerna eller de utlokaliserade säkerhetstjänsterna eller kontexten för certifieringen av entiteterna. Följaktligen bör assuransnivån stå i proportion till nivån på den risk som är förenad med den avsedda användningen av IKT-produkten, IKT-tjänsten, IKT-processen eller den utlokaliserade säkerhetstjänsten, eller den operativa miljön hos och typen av entitet vars cybersäkerhetsstatus är föremål för certifiering.

(102) För assuransnivån ”grundläggande” bör utvärderingen vägledas av åtminstone följande assuranskomponenter: utvärderingen bör åtminstone omfatta en granskning av den tekniska dokumentationen för IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen för en entitet, vilken utförs av organet för bedömning av överensstämmelse. I de fall då certifieringen omfattar IKT-processer bör även den process som används för att utforma, utveckla och underhålla en IKT-produkt, IKT-tjänst eller utlokaliserad säkerhetstjänst eller en entitets cybersäkerhetsstatus omfattas av den tekniska granskningen. I de fall då en europeisk ordning för cybersäkerhetscertifiering föreskriver en självbedömning av överensstämmelse bör det räcka att tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, eller den entitet vars cybersäkerhetsstatus är föremål för certifieringen, har utfört en självbedömning av överensstämmelsen med certifieringsordningen för IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller entitetens cybersäkerhetsstatus.

(103) För assuransnivån ”betydande” bör utvärderingen, utöver kraven för assuransnivån ”grundläggande”, omfatta åtminstone en kontroll av att säkerhetsfunktionerna hos IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen hos entiteten överensstämmer med dess tekniska dokumentation.

(104) För assuransnivån ”hög” bör utvärderingen, utöver kraven för assuransnivån ”betydande”, åtminstone omfatta ett effektivitetstest som bedömer resistensen hos säkerhetsfunktionerna gentemot genomtänkta cyberangrepp som utförs av personer med betydande färdigheter och resurser. Arbetet med bedömning av överensstämmelse bör utföras inom Europeiska ekonomiska samarbetsområdet för assuransnivån ”hög” eller i de fall då en ordning utformats för att påvisa regelefterlevnad och ge presumtion om överensstämmelse med annan unionslagstiftning. Detta krav är motiverat eftersom bedömningar som görs utanför Europeiska ekonomiska samarbetsområdet ger upphov till ytterligare cybersäkerhetshot, i synnerhet vad gäller immateriella rättigheter i samband med utvärderade IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter. Exempelvis skulle en IKT-produkts källkod kunna granskas när den passerar gränsen till ett tredjeland, vilket utgör en risk för immateriella rättigheter. En annan faktor är att testlaboratorier etablerade i tredjeländer inte drivs i en miljö som berörs av de cybersäkerhetsåtgärder som föreskrivs i EU-lagstiftning, såsom direktiv (EU) 2022/2555 eller förordning (EU) 2024/2847. Exempelvis kan ett testlaboratorium förlita sig på en tredjepartsleverantörs molntjänst som inte uppfyller cybersäkerhetskraven i direktiv (EU) 2022/2555. En certifieringsordning bör dock tillåtas att föreskriva undantagsmekanismer när det gäller exempelvis anläggningscertifiering eller andra tillfällen då bedömning av överensstämmelse rimligtvis inte kan utföras i Europeiska ekonomiska samarbetsområdet.

(105) I vissa fall kan det krävas olika strategier för att uppfylla säkerhetsmålen för en viss assuransnivå, mot bakgrund av särdragen hos en IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller entitets cybersäkerhetsstatus. För att möjliggöra en mer detaljerad strategi bör det vara möjligt att i en europeisk ordning för cybersäkerhetscertifiering ange en eller flera utvärderingsnivåer som motsvarar en av assuransnivåerna. Detta kommer att möjliggöra utveckling av ordningar där flera utvärderingsnivåer utformade för olika syften kommer att motsvara den säkerhetsnivå som är förknippad med en viss assuransnivå.

(106) Europeiska ordningar för cybersäkerhetscertifiering bör kunna ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller möjlighet att göra en bedömning av överensstämmelse på eget ansvar (*självbedömning av överensstämmelse*). I sådana fall bör det vara tillräckligt att tillverkaren, leverantören eller den entitet vars cybersäkerhetsstatus är föremål för certifiering själv utför alla kontroller för att säkerställa att IKT-produkterna, IKT-tjänsterna, IKT-processerna, de utlokaliserade säkerhetstjänsterna eller entitetens cybersäkerhetsstatus överensstämmer den europeiska ordningen för cybersäkerhetscertifiering. Självbedömning av överensstämmelse bör anses lämplig för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus med låg komplexitet, låg risk för allmänheten och en enkel utformning eller enkla produktionsmekanismer.

(107) I de fall då en europeisk ordning för cybersäkerhetscertifiering tillåter både självbedömning av överensstämmelse och certifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus bör denna ordning för cybersäkerhetscertifiering omfatta tydliga och begripliga sätt för konsumenter eller andra användare att skilja mellan IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som varit föremål för självbedömning och som certifierats av tredje part.

(108) Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, eller entiteter vars cybersäkerhetsstatus har certifierats, bör kunna utfärda och underteckna en EU-försäkran om överensstämmelse som ett led i förfarandet för bedömning av överensstämmelse. En EU-försäkran om överensstämmelse är ett dokument som anger att en viss IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst, eller cybersäkerhetsstatusen för en entitet, uppfyller kraven i den europeiska ordningen för cybersäkerhetscertifiering. Genom att upprätta och underteckna EU-försäkran om överensstämmelse tar tillverkaren, leverantören eller entiteten ansvar för att IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen överensstämmer med säkerhetskraven i den europeiska ordningen för cybersäkerhetscertifiering. En kopia av EU-försäkran om överensstämmelse bör lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

(109) Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller bör, under en period som fastställs i den berörda europeiska ordningen för cybersäkerhetscertifiering och i linje med tillämplig unionslagstiftning, ge den behöriga nationella myndigheten för cybersäkerhetscertifiering tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende överensstämmelse med certifieringsordningen. Den tekniska dokumentationen bör specificera de krav som är tillgängliga inom ordningen i den utsträckning som är relevant för självbedömningen av överensstämmelse. Den tekniska dokumentationen bör sammanställas på ett sätt som gör det möjligt att bedöma om en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst eller en entitets cybersäkerhetsstatus överensstämmer med de krav som är tillämpliga inom ordningen.

(110) Europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse bör hjälpa användarna att göra välinformerade val. Därför bör relevant information offentliggöras på en webbplats som upprätthålls av Enisa. Vidare bör IKT-produkter, IKT-tjänster och IKT-processer som certifierats eller varit föremål för en EU-försäkran om överensstämmelse åtföljas av strukturerad information som anpassats till den avsedda användarens förväntade tekniska nivå. Alla användare bör ha tillgång till information om certifieringsordningens referensnummer, den utfärdande myndigheten eller det utfärdande organet och, i tillämpliga fall, assuransnivån, eller bör kunna erhålla en kopia av det europeiska cybersäkerhetscertifikatet. Informationen bör uppdateras regelbundet och göras tillgänglig på en särskild webbplats för europeiska ordningar för cybersäkerhetscertifiering. För att säkerställa kontinuerlig tillgång bör tillverkare och leverantörer även åläggas att underrätta det berörda certifieringsorganet om onlineinformationen eller, i förekommande fall, den fysiska informationen flyttas.

(111) Bedömning av överensstämmelse är ett förfarande för att utvärdera om angivna krav för en IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller entitet har uppfyllts. Förfarandet genomförs av en oberoende tredje part som inte är tillverkaren eller leverantören av de IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som är föremål för certifiering, och inte heller den entitet vars cybersäkerhetsstatus bedöms. Ett europeiskt cybersäkerhetscertifikat bör utfärdas efter en framgångsrik utvärdering av en IKT-produkt, en IKT-tjänst, en IKT-process, en utlokaliserad säkerhetstjänst eller en entitets cybersäkerhetsstatus. Ett europeiskt cybersäkerhetscertifikat bör betraktas som en bekräftelse på att en utvärdering har genomförts på ett korrekt sätt.

(112) Det är viktigt med en strikt uppdelning mellan tillsynsverksamheten och certifieringsverksamheten för att undvika snedvridning och inblandning som kan bli följden i situationer där den entitet som utövar tillsyn över marknaden också konkurrerar på samma marknad. Därmed bör verksamhet där de nationella myndigheterna för cybersäkerhetscertifiering endast utför sina tillsynsuppgifter, såsom att förhandsgodkänna utfärdandet av ett certifikat, inte kräva någon ytterligare intern åtskillnad från annan tillsynsverksamhet. Detta inbegriper exempelvis situationer där den nationella myndigheten för cybersäkerhetscertifiering aktivt samlar in information i samband med en certifieringsprocess som utförs av ett privat organ för bedömning av överensstämmelse och sedan avger ett yttrande om dessa organs utfärdande av certifikatet (*modell med förhandsgodkännande*).

(113) Europeiska ordningar för cybersäkerhetscertifiering bör specificera villkoren för när IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus kan behöva omcertifieras eller för när tillämpningsområdet kan behöva begränsas för ett specifikt europeiskt cybersäkerhetscertifikat. Europeiska ordningar för cybersäkerhetscertifiering bör också ta hänsyn till eventuella möjliga negativa effekter av senare upptäckta sårbarheter eller fall av bristande överensstämmelse hos en certifierad IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller cybersäkerhetsstatus när det gäller överensstämmelsen med säkerhetskraven för det certifikatet.

(114) Harmonisering har en avgörande betydelse för att säkerställa en robust cybersäkerhet och förbättra marknadstillträdet för företag. Däremot medför fragmentering och brist på ömsesidigt erkännande av certifikat betydande hinder för ett sömlöst dataflöde, vilket ökar de operativa kostnaderna för unionens näringsliv. För att mildra dessa utmaningar är det viktigt att motverka fragmentering i fråga om både säkerhetskontrollernas omfattning och metoderna för bedömning av överensstämmelse i hela unionen.

(115) Medlemsstaterna bör underrätta kommissionen och den europeiska gruppen för cybersäkerhetscertifiering i tillräckligt god tid före antagandet av nya nationella ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, för att hjälpa kommissionen och den europeiska gruppen för cybersäkerhetscertifiering att utvärdera vilka verkningar den nya nationella ordningen för cybersäkerhetscertifiering har på den inre marknadens funktion, och i ljuset av ett eventuellt strategiskt intresse av att begära en europeisk ordning för cybersäkerhetscertifiering.

(116) Hänvisningar i nationell lagstiftning till nationella standarder som har upphört att ha verkan i och med att en europeisk ordning för cybersäkerhetscertifiering har trätt i kraft kan orsaka förvirring. När så är relevant bör medlemsstaterna därför se till att antagandet av en europeisk ordning för cybersäkerhetscertifiering avspeglas i deras nationella lagstiftning.

(117) För att främja tillväxten av en tillförlitlig inre marknad och samtidigt skapa partnerskap med tredjeländer bör den certifieringsprocess som inrättats inom det europeiska ramverket för cybersäkerhetscertifiering genomföras på ett sätt som främjar internationellt erkännande, ömsesidigt erkännande och anpassning till internationella standarder.

(118) För att ytterligare främja handel och beakta att IKT-leveranskedjorna är internationella får avtal om ömsesidigt erkännande av europeiska cybersäkerhetscertifikat ingås av unionen i enlighet med artikel 218 i EUF-fördraget. Kommissionen bör ges befogenhet

att anta genomförandeakter för att ensidigt erkänna tredjelandscertifikats likvärdighet med europeiska cybersäkerhetscertifikat. Det bör vara möjligt att föreskriva särskilda villkor för sådana erkännanden av tredjelandscertifikat.

(119) För att uppnå ett likvärdigt genomförande av ramverket i hela unionen och för att underlätta ömsesidigt erkännande och främja ett allmänt godtagande av europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse är det nödvändigt att inrätta en ordning för inbördes granskning mellan nationella myndigheter för cybersäkerhetscertifiering. Den inbördes granskningen bör omfatta förfarandena för tillsyn med avseende på överensstämmelse för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus i förhållande till europeiska cybersäkerhetscertifikat, för övervakning av skyldigheter för tillverkare eller leverantörer av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och certifierade entiteter som utför självbedömning av överensstämmelse, för övervakning av organ för bedömning av överensstämmelse, samt för att fastställa om personalen hos organ som utfärdar certifikat för assuransnivån ”hög” har lämpliga sakkunskaper. Enisa bör delta i de inbördes granskningarna som observatör och stödja organiserandet av mekanismen för inbördes granskningar och de inbördes granskningarna, bland annat genom att utarbeta relevanta vägledningsdokument och mallar, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering. På sin webbplats för europeiska ordningar för cybersäkerhetscertifiering bör Enisa också offentliggöra information om schemat för de inbördes granskningarna och förteckningen över de inbördes granskade nationella myndigheter för cybersäkerhetscertifiering som genomför schemat. Kommissionens genomförandeförordning (EU) 2025/2540[60], som antogs i enlighet med förordning (EU) 2019/881, fastställer en plan för inbördes granskning som används av de antagna europeiska ordningarna för cybersäkerhetscertifiering. Det är nödvändigt att säkerställa att den inbördes granskningen fortsätter. Genom genomförandeakter bör dock kommissionen vid behov kunna fastställa en ny plan för inbördes granskning på minst fem år och fastställa kriterier och metoder för verksamheten inom systemet för inbördes granskning.

(120) När en europeisk ordning för cybersäkerhetscertifiering har antagits bör tillverkarna eller leverantörerna av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster, eller de entiteter vars cybersäkerhetsstatus certifieringen gäller, kunna lämna in ansökningar om certifiering av sina IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller sin cybersäkerhetsstatus till ett organ för bedömning av överensstämmelse efter eget val och var som helst i unionen. Organen för bedömning av överensstämmelse bör ackrediteras av ett nationellt ackrediteringsorgan om de uppfyller de krav som anges i denna förordning och, i tillämpliga fall, krav som specificerats av kommissionen i enlighet med denna förordning. Det system som fastställs i denna förordning bör kompletteras av det ackrediteringssystem som föreskrivs i Europaparlamentets och rådets förordning (EG) nr 765/2008[61].

---

60 Kommissionens genomförandeförordning (EU) 2025/2540 av den 9 december 2025 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller fastställande av planen för inbördes granskning (EUT L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

61 Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av

(121) Organ för bedömning av överensstämmelse som har ackrediterats eller anmälts enligt befintlig unionslagstiftning, i synnerhet förordning (EU) 2024/2847 eller genomförandeförordning (EU) 2024/482, kan ha kompetenser av relevans för nyligen antagna europeiska ordningar för cybersäkerhetscertifiering. För att undvika onödiga finansiella och administrativa bördor är det lämpligt att skapa synergier för ackrediteringen av organ för bedömning av överensstämmelse enligt denna förordning. Därför bör ackrediteringskraven för ordningarna fastställas på ett sådant sätt att de i så stor utsträckning som möjligt anpassas till kraven för anmälda organ enligt förordning (EU) 2024/2847 och ackrediteringskraven enligt genomförandeförordning (EU) 2024/482. Dessutom bör organ för bedömning av överensstämmelse som genomgår ett ackrediteringsförfarande i enlighet med denna förordning kunna förlita sig på tidigare resultat av utvärderingar av deras kompetenser enligt annan unionslagstiftning, när ackrediteringskraven överlappar.

(122) För att främja harmoniserade tjänster för bedömning av överensstämmelse i unionen bör det vara möjligt att i en europeiska ordning för cybersäkerhetscertifiering fastställa ytterligare eller särskilda krav för organ för bedömning av överensstämmelse. I samband med certifiering bör en auktorisation förstås som ett beslut av en nationell myndighet för cybersäkerhetscertifiering som fastställer att ett organ för bedömning av överensstämmelse uppfyller de särskilda eller ytterligare krav som anges i en europeisk ordning för cybersäkerhetscertifiering, för utförande av en viss verksamhet avseende bedömning av överensstämmelse.

(123) Om en europeisk ordning för cybersäkerhetscertifiering omfattar ytterligare eller särskilda krav enligt denna förordning bör organ för bedömning av överensstämmelse auktoriseras av den nationella myndigheten för cybersäkerhetscertifiering för att få utföra uppgifter inom ramen för den ordningen. För att undvika dubbelauktorisation, öka acceptansen och erkännandet av auktorisationsbeslut samt utöva effektiv tillsyn över auktoriserade organ för bedömning av överensstämmelse bör organen för bedömning av överensstämmelse begära auktorisation hos den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstat där de är etablerade. Det är dock nödvändigt att säkerställa att ett organ för bedömning av överensstämmelse har möjlighet att begära auktorisation i en annan medlemsstat om det inte finns någon nationell myndighet för cybersäkerhetscertifiering i den egna medlemsstaten, eller om den nationella myndigheten för cybersäkerhetscertifiering inte besitter den nödvändiga kompetensen för att erbjuda de auktorisationstjänster som efterfrågas. I sådana fall bör lämpligt samarbete och informationsutbyte säkerställas mellan de berörda nationella myndigheterna för cybersäkerhetscertifiering. Kommissionen bör ges befogenhet att anta genomförandeakter för att fastställa förfarandena för auktorisation, även för gränsöverskridande samarbete med avseende på auktorisation.

(124) För att säkerställa den skyddsnivå som krävs för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus är det viktigt att underleverantörer och dotterbolag som är involverade i bedömning av överensstämmelse åläggs att uppfylla samma krav som de anmälda organen för bedömning av överensstämmelse när det gäller utförande av arbetsuppgifter som avser bedömning av överensstämmelse. Följaktligen bör ett organ för bedömning av överensstämmelse ha lämplig kompetens och förmåga att kontrollera att de tillämpliga kraven uppfylls av dess underleverantörer.

---

förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(125) Den anmälande myndigheten bör på lämpligt sätt bedöma i vilken utsträckning som organet för bedömning av överensstämmelse avser att förlita sig på underleverantörer som är etablerade utanför unionen eller har tillgång till personal eller anläggningar utanför den anmälande medlemsstaten. Den offentliga myndigheten i en medlemsstat bör ha möjlighet att besluta att den inte kan ta det övergripande ansvaret som nationell myndighet för cybersäkerhetscertifiering i samband med sådana upplägg och att återkalla eller begränsa omfattningen av anmälan.

(126) För att utvärdera cybersäkerhetskraven för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus bör de nationella myndigheterna för cybersäkerhetscertifiering anmäla ackrediterade organ för bedömning av överensstämmelse till kommissionen och övriga medlemsstater. Anmälan av ackrediterade och, i tillämpliga fall, auktoriserade organ för bedömning av överensstämmelse innebär att dessa organ anses tillförlitliga när det gäller att utföra utvärderings- och certifieringsverksamhet i enlighet med denna förordning och den europeiska ordningen för cybersäkerhetscertifiering, vilket bidrar till det allmänna anseendet för europeiska ordningar för cybersäkerhetscertifiering. Det är därför viktigt att säkerställa att de organ för bedömning av överensstämmelse som har anmälts uppfyller sina krav och fullgör sina skyldigheter över tid samt att förteckningen över anmälda organ för bedömning av överensstämmelse hålls uppdaterad.

(127) Kommissionens genomförandeförordning (EU) 2024/3143[62], som antogs i enlighet med förordning (EU) 2019/881, fastställer förutsättningar, format och förfaranden för anmälningar av organ för bedömning av överensstämmelse vilka används av de antagna europeiska ordningarna för europeisk cybersäkerhetscertifiering. Det är därför nödvändigt att säkerställa att anmälningsverksamheten fortsätter. Kommissionen bör dock ges befogenhet att anta genomförandeakter för att justera dessa förutsättningar, förfaranden och format för anmälan av organ för bedömning av överensstämmelse. I detta sammanhang bör kommissionen utnyttja erfarenheterna från befintliga ordningar och sträva efter anpassning till andra relevanta unionsrättsakter och unionsramar, i synnerhet förordning (EU) 2024/2847 och den nya rättsliga ramen, för att minska efterlevnadsbördan för organ för bedömning av överensstämmelse vars verksamhet omfattas av olika rättsliga instrument.

(128) Leveranskedjorna för informations- och kommunikationsteknik (IKT) består av en uppsättning sammankopplade resurser och processer mellan ekonomiska aktörer. IKT-leveranskedjorna är avgörande för upprätthållandet av samhällets stabilitet och fungerar som en motor för ekonomisk verksamhet i hela unionen. De har också en kritisk roll när det gäller att möjliggöra digital infrastruktur i unionen och stöder ett fungerande samhälle och en fungerande ekonomi i unionen. IKT-leveranskedjorna möjliggör tillverkning, produktion, distribution och underhåll av IKT-tjänster, IKT-system och IKT-produkter som behövs för olika kritiska och högkritiska sektorer, däribland hälso- och sjukvård, finanssektorn, transporter, telekommunikation, energi och tull. Säkerheten i IKT-leveranskedjorna för dessa kritiska sektorer kan också inverka på säkerheten för försvarsinfrastruktur och militär infrastruktur, när denna infrastruktur förlitar sig på civila kritiska sektorer och deras IKT-leveranskedjor.

---

62 Kommissionens genomförandeförordning (EU) 2024/3143 av den 18 december 2024 om fastställande av förutsättningar, format och förfaranden för anmälningar enligt artikel 61.5 i Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (EUT L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

Enligt den rapport om läget i fråga om cyberhot som utfärdats av Enisa (*ENISA Threat Landscape 2025*)[63] är attacker mot leveranskedjor ett av de fem främsta hoten mot cybersäkerheten, vilket visar att angripare aktivt utnyttjar indirekta vägar via tredjepartsleverantörer och beroenden. Störningar i IKT-leveranskedjor kan hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera ekonomisk förlust, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför viktigare än någonsin för att den inre marknaden ska fungera väl.

(129) Utöver de tekniska risker som behandlas i Europaparlamentets och rådets direktiv (EU) 2022/55[64], Europaparlamentets och rådets förordning (EU) 2024/2847[65] och det europeiska ramverk för cybersäkerhetscertifiering som fastställs i förordning (EU) 2019/881 exponeras IKT-leveranskedjorna allt oftare för risker av icke-teknisk art. Sådana icke-tekniska risker kan vara kopplade, men inte begränsade, till den jurisdiktion som leverantören av vissa komponenter tillhör, i synnerhet i de fall då tredjeländer eller fientliga aktörer som kontrolleras från det landet ägnar sig åt ekonomiskt spionage, utför fientliga cyberhandlingar eller kampanjer mot unionen eller dess medlemsstater, eller ägnar sig åt oansvarigt statligt beteende i cyberrymden. Icke-tekniska risker kan också vara kopplade till dolda sårbarheter eller bakdörrar eller potentiella systemiska leveransstörningar, särskilt i samband med teknikinlåsning eller leverantörsberoende. Exempelvis kan avstängningsmekanismer (kill switches) användas för att negativt påverka tillgängligheten till kommunikationsnät och elnät.

(130) Det gemensamma meddelandet om att stärka EU:s ekonomiska säkerhet[66] lyfte fram risken för att tredjeländer skulle få tillgång till känsliga uppgifter och data i unionen eller dess medlemsstater, till följd av industrispionage, av att de levererar maskin- eller programvara som används i vissa produkter, eller av att de äger och kontrollerar vissa företag som innehar känsliga uppgifter och data. Det lyfte också fram risken för att unionens kritiska infrastruktur – däribland kritiska transporter och rymdsystem samt kritisk energi- och kommunikationsinfrastruktur, i synnerhet infrastruktur som identifierats som strategisk för militär rörlighet – skulle störas av utländska aktörer, vilket skulle kunna medföra kaskadeffekter på den europeiska ekonomin. Störningar kan uppstå genom fysiska attacker, cyberattacker eller hybridattacker, inklusive sabotage av hela anläggningar eller deras delar eller delkomponenter. De kan också vara kopplade till IKT-leveranskedjor som behövs för tillhandahållandet av kritiska komponenter eller tjänster för kritisk infrastruktur.

(131) För att hantera de utmaningar för säkerheten i IKT-leveranskedjan som icke-tekniska risker utgör har några medlemsstater vidtagit regleringsåtgärder, genom att exempelvis utpeka högriskleverantörer, medan andra medlemsstater sannolikt kommer att göra detta. Detta kan leda till ytterligare skillnader mellan de nationella strategierna och i

---

63 *ENISA Threat Landscape 2025*, oktober 2025.

64 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) (EUT L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

66 Gemensamt meddelande till Europaparlamentet och rådet – *Stärka EU:s ekonomiska säkerhet*, 3 december 2025, JOIN(2025) 977 final.

förlängningen till ökad sårbarhet i vissa medlemsstater, med potentiella spridningseffekter i unionen. Det är därför nödvändigt att harmonisera vissa aspekter som rör icke-tekniska cybersäkerhetsrisker för IKT-leveranskedjan. Ett sådant ingripande på unionsnivå är också motiverat mot bakgrund av behovet av att säkerställa en hög nivå av cybersäkerhet i hela unionen. Bestämmelserna om säkerhet i IKT-leveranskedjan syftar till att undanröja sådana omfattande skillnader mellan medlemsstaterna, i synnerhet genom fastställande av regler för riskbedömningsmekanismer på unionsnivå för säkerhetsrisker i IKT-leveranskedjan och minimistandarder för skyddet mot säkerhetsrisker i IKT-leveranskedjan.

(132) För att minska antalet kritiska beroenden och sårbarheter är det nödvändigt att inrätta ett ramverk för en betrodd IKT-leveranskedja som bör omfatta icke-tekniska risker förknippade med högriskleverantörer och beroenden i högkritiska sektorer och andra kritiska sektorer. Därför är det nödvändigt att tillhandahålla ett objektivt, riskbaserat, framtidssäkrat och teknikneutralt ramverk på unionsnivå, för att identifiera viktiga IKT-tillgångar och föreskriva en uppsättning proportionella begränsningsåtgärder för att hantera riskerna.

(133) Cybersäkerhetsrisker, såsom risker förknippade med beroenden av högriskleverantörer, kan observeras i flera kritiska IKT-leveranskedjor i unionen, exempelvis när det gäller detekteringsutrustning, uppkopplade och automatiserade fordon, elförsörjningssystem och ellagring, vattenförsörjningssystem, drönare och anti-drönarsystem, molntjänster, medicintekniska produkter, övervakningsutrustning, rymdtjänster och halvledare. Sårbarheter i säkerhetsutrustning för detektering kan ge åtkomst till IKT-system så att fientliga aktörer kan manipulera skannrar på ett sådant sätt att förbjudna föremål kan föras genom säkerhetskontroller utan att upptäckas, med potentiellt katastrofala konsekvenser.

(134) Denna förordning bör inte hindra medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå när det gäller säkerheten i IKT-leveranskedjan, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten. Sådana bestämmelser kan exempelvis inbegripa striktare begränsningsåtgärder för viktiga IKT-tillgångar.

(135) För att identifiera potentiella cybersäkerhetsrisker som påverkar specifika IKT-leveranskedjor får den samarbetsgrupp som inrättades genom artikel 14 i direktiv (EU) 2022/2555 (*samarbetsgruppen för nät- och informationssäkerhet*) göra en bedömning av specifika IKT-leveranskedjor genom samordnade säkerhetsriskbedömningar på unionsnivå. De samordnade säkerhetsriskbedömningarna på unionsnivå bör bland annat omfatta de främsta hotaktörer och hot och sårbarheter som påverkar de viktigaste IKT-tillgångarna. Vid de samordnade säkerhetsriskbedömningarna på unionsnivå bör det utarbetas en förteckning över riskscenarier och en förteckning över åtgärder för att begränsa riskerna. De samordnade säkerhetsriskbedömningarna på unionsnivå bör slutföras inom sex månader. I särskilt brådskande fall bör det vara möjligt att korta tidsfristerna.

(136) I de fall då kommissionen har tillräckliga skäl att anta att det finns ett betydande cyberhot mot unionens säkerhet som berör kritiska IKT-leveranskedjor och att det kan vara nödvändigt att agera för att bevara en välfungerande inre marknad bör den utan dröjsmål samråda med medlemsstaterna om behovet av begränsningsåtgärder och göra en säkerhetsriskbedömning, med beaktande av samrådet med medlemsstaterna.

(137) Om det baserat på en säkerhetsriskbedömning som utförts av samarbetsgruppen för nät- och informationssäkerhet eller kommissionen tycks som om ett specifikt

tredjeland utgör en allvarlig och strukturell icke-teknisk cybersäkerhetsrisk för IKT-leveranskedjorna bör kommissionen verifiera det hot som det landet utgör. Kommissionen får inleda en sådan verifiering även på grundval av andra källor, såsom ett offentligt uttalande på unionens eller en medlemsstats vägnar som svar på en förekomst av oansvarigt statligt beteende i cyberrymden som har lett till en cybersäkerhetsincident. För att bedöma hotnivån bör kommissionen beakta sådana faktorer som förekomsten av lagar eller praxis i tredjelandet som kräver att entiteter inom dess jurisdiktion rapporterar information om sårbarheter i programvara eller maskinvara till myndigheterna i tredjelandet innan det är känt att dessa sårbarheter har utnyttjats. En annan relevant faktor är avsaknad av effektiva rättsmedel, och oberoende och demokratiska kontrollmekanismer, som kan avhjälpa säkerhetsproblem, även avseende befintlig praxis, styrkt information om incidenter där fientliga aktörer som verkar från det landets territorium utför skadlig cyberverksamhet eller skadliga cyberkampanjer, och tredjelandets bristande förmåga eller vilja att samarbeta med kommissionen eller medlemsstaterna för att hantera den risk som härrör från sådana fientliga aktörers verksamhet. Kommissionen bör också beakta information som härrör från samordnade säkerhetsriskbedömningar på unionsnivå eller rapporter som utfärdats av medlemsstater eller internationella organisationer som Nato.

(138) Vid tillämpning av denna förordning bör begreppet kontroll förstås som förmågan att utöva ett avgörande inflytande på en rättslig enhet direkt, eller indirekt via en eller flera mellanliggande rättsliga enheter. Kontrollen över entiteter från ett tredjeland som utgör cybersäkerhetsproblem bör också fastställas i situationer där en sådan entitet har strukturer för verkställande ledning i det landet.

(139) Unionen bör inte finansiera projekt som involverar högriskleverantörer, eftersom det skulle äventyra unionens säkerhet, intressen och trovärdighet. Högriskleverantörer som identifieras i enlighet med denna förordning bör därför inte ha rätt att delta i unionens finansieringsprogram eller finansieringsinstrument som genomförs genom direkt och indirekt förvaltning i enlighet med artikel 136 i förordning (EU, Euratom) 2024/2509 och unionens sektorsspecifika regler eller i unionsfinansieringsverksamhet som genomförs genom delad förvaltning, inbegripet inom den nästa fleråriga budgetramen, när det gäller tillhandahållande av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka ska användas i viktiga IKT-tillgångar. Unionens genomförandepartner, såsom Europeiska investeringsbanksgruppen och nationella utvecklingsbanker och -institutioner, bör avstå från att stödja projekt som står i strid med ovanstående, inbegripet verksamhet på egen risk.

(140) Offentlig upphandling kan vara ett kraftfullt verktyg för offentliga myndigheter att bidra till en mer innovativ, hållbar och konkurrenskraftig ekonomi och för en strategisk användning av offentliga medel. Offentlig upphandling som rör IKT-leveranskedjorna bör inte användas för att gagna leverantörer som hotar säkerheten för unionens kritiska infrastruktur. Högriskleverantörer som identifierats i enlighet med denna förordning bör därför inte ha rätt att delta i offentlig upphandling som rör tillhandahållandet av IKT-komponenter eller komponenter som innehåller IKT-komponenter för användning i identifierade viktiga IKT-tillgångar.

(141) Cybersäkerhetscertifiering har en roll när det gäller att stärka den allmänna säkerheten och motverka cyberhot och fungerar som ett riktmärke för förtroende. Detta förtroende kan urholkas om intyg om cybersäkerhetskompetens utfärdas av högriskleverantörer och dessa bör därför inte ha rätt att ansöka om att bli auktoriserade tillhandahållare av några europeiska individuella intyg om cybersäkerhetskompetens. Det är likaså

lämpligt att utesluta högriskleverantörer från att erhålla cybersäkerhetscertifiering inom det europeiska ramverket för cybersäkerhetscertifiering och från att bli ackrediterade organ för bedömning av överensstämmelse för utfärdandet av sådana certifikat.

(142) Cybersäkerhetsstandarder spelar en kritisk roll när det gäller säkerheten och tillförlitligheten för digitala infrastrukturer. Det är nödvändigt att vidta lämpliga åtgärder för att säkerställa standardisering på cybersäkerhetsområdet. Ett deltagande av entiteter som är etablerade i eller kontrolleras från länder som har identifierats som cybersäkerhetsproblem för IKT-leveranskedjan i linje med denna förordning kan medföra att cybersäkerhetsstandarderna påverkas på ett sätt som undergräver standardernas säkerhet och trovärdighet.

(143) Baserat på resultaten av säkerhetsriskbedömningarna kan kommissionen genom genomförandeakter identifiera vilka IKT-tillgångar som bör betraktas som viktiga IKT-tillgångar eftersom de är kritiska och med förbehåll för särskilda begränsningsåtgärder. Enbart det faktum att en tillgång är anslutbar bör vara tillräckligt för beaktande av dess cybersäkerhetsrisk.

(144) I de fall då det är nödvändigt för att säkerställa en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom unionen bör begränsningsåtgärder tillämpas på entiteter med avseende på deras IKT-leveranskedja och i synnerhet med avseende på viktiga IKT-tillgångar som identifierats. De föreslagna begränsningsåtgärderna bör baseras på en bedömning av potentiella risker och beroenden, inbegripet de potentiella ekonomiska och samhälleliga konsekvenserna av sådana åtgärder för de berörda entiteter som är verksamma inom högkritiska eller andra kritiska sektorer och i synnerhet små och medelstora företag. Vid bedömningen av de ekonomiska konsekvenserna bör man beakta kostnaderna för genomförandet av begränsningsåtgärderna, inklusive livscykelns längd för de berörda komponenterna i viktiga IKT-tillgångar i de fall då åtgärderna inbegriper ett leverantörsbyte. Tillgången till alternativa leverantörer på marknaden bör också bedömas så att ett kontinuerligt tillhandahållande av tjänster kan säkerställas.

(145) Eftersom begränsningsåtgärder potentiellt kan ha begränsande effekter på den internationella handeln med varor och tjänster bör de vara proportionella och målinriktade i förhållande till det eftersträvade legitima målet att säkerställa IKT-leverenskedjornas cybersäkerhet när det gäller entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555, i linje med unionens internationella skyldigheter.

(146) Användning, installation eller varje annan integrering av komponenter som tillhandahålls av högriskleverantörer för driften av viktiga IKT-tillgångar kan vara förknippad med en risk att data därefter överförs till ett tredjeland. I synnerhet kan det utgöra en risk om det finns en otillräcklig skyddsnivå för data i tredjelandet, exempelvis när det gäller skydd av grundläggande rättigheter, immateriella rättigheter eller företagshemligheter, eller olaglig tillgång och olagligt utnyttjande av dessa data för eventuella framtida störningar av leveranskedjan och spionageändamål. För att minska sådana risker får begränsningar tillämpas på överföringen av specifika typer av data till tredjeländer.

(147) Betydande sårbarheter beror på en bristande mångfald när det gäller den utrustning som används av entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555. Användning av en enda leverantör skapar ett beroende av specifik utrustning eller specifika lösningar. En bristande mångfald av leverantörer ökar den

totala sårbarheten för kritisk infrastruktur, i synnerhet om entiteter anskaffar sina IKT-komponenter som används i känsliga IKT-tillgångar från en leverantör som utgör en hög grad av risk. Beroenden har också stor inverkan på resiliensen på nationell nivå och unionsnivå och ger upphov till felkritiska systemdelar. För att begränsa sådana risker får krav på mer än en leverantör för specifika viktiga IKT-tillgångar tillämpas.

(148) Det förekommer att även unionsentiteter använder viktiga tillgångar enligt definitionen i denna förordning. Därför bör de regler om säkerhet i IKT-leveranskedjan som fastställs i denna förordning också tillämpas på dem. För att säkerställa att unionsentiteternas särdrag beaktas är det viktigt att ta hänsyn till icke-tekniska risker för unionsentiteter som härrör från IKT-leveranskedjor när samordnade säkerhetsriskbedömningar görs på unionsnivå.

(149) Under exceptionella omständigheter som motiverar ett omedelbart ingripande för att bevara en väl fungerande inre marknad, och om det finns tydliga bevis som ger kommissionen tillräckliga skäl att anse att användningen av IKT-komponenter eller komponenter som innehåller IKT-komponenter från en viss leverantör utgör ett betydande cybersäkerhetshot för ekonomisk eller samhällelig verksamhet i minst tre medlemsstater, får kommissionen, i nära samråd med medlemsstaterna, föreslå att användning, installation eller integrering av sådana komponenter från denna leverantör förbjuds för den typ av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555.

(150) För att säkerställa att de åtgärder som tillämpas är proportionella kan entiteter som är etablerade i ett tredjeland som utgör cybersäkerhetsproblem och som utpekats i enlighet med denna förordning, eller som kontrolleras av ett sådant tredjeland, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland, ansöka om att undantas från detta förbud mot att förse entiteter av en typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 med IKT-komponenter eller komponenter som innehåller IKT-komponenter för användning, installation eller integrering i den entitetens viktiga IKT-tillgångar och mot att delta i offentliga upphandlingsförfaranden anordnade i enlighet med lagstiftning som införlivar Europaparlamentets och rådets direktiv 2014/24/EU[67] och 2014/25/EU[68] när det gäller tillhandahållandet av IKT-komponenter eller komponenter som innehåller IKT-komponenter för användning i identifierade viktiga IKT-tillgångar. För detta ändamål bör entiteten med tydliga bevis påvisa att den tillämpar effektiva åtgärder för att hantera icke-tekniska risker och säkerställa att det inte förekommer någon som helst otillbörlig inblandning från ett tredjeland som utgör cybersäkerhetsproblem.

(151) Elektroniska kommunikationsnät utgör grunden för en rad tjänster som är nödvändiga för den inre marknadens funktion och för upprätthållandet och driften av vitala samhälleliga och ekonomiska funktioner, exempelvis energi, transporter, banktjänster, hälso- och sjukvård, försvar samt industriell processtyrning. Därför är dessa högkritiska nät attraktiva måltavlor för alla typer av cyberattacker och hybridhot, för störningar, spionage och underrättelseinhämtning samt för bedrägerier och ekonomisk brottslighet. I den riskbedömning av cybersäkerheten och resiliensen hos Europas

---

67 Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng).

68 Europaparlamentets och rådets direktiv 2014/25/EU av den 26 februari 2014 om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (EUT L 94, 28.3.2014, s. 243, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj).

kommunikationsinfrastrukturer och kommunikationsnät som gjordes av samarbetsgruppen för nät- och informationssäkerhet identifierades ett antal risker och hot av strategisk betydelse ur ett unionsperspektiv, såsom attacker med minerade skadeprogram och utpressningsprogram, leveranskedjeattacker, nätintrång och samordnade överbelastningsattacker (DDoS).

(152) Mot bakgrund av sammankopplingen av och det ömsesidiga beroendet mellan olika nationella elektroniska kommunikationsnät är det nödvändigt att alla medlemsstater vidtar ändamålsenliga åtgärder för att säkerställa säkerheten i sina nät. Av samma skäl behöver det finnas en effektiv rättslig ram på unionsnivå som omfattar även icke-tekniska risker och säkerställer säkerheten i de sammankopplade elektroniska kommunikationsnäten på ett heltäckande sätt.

(153) I synnerhet är cybersäkerheten i 5G-nät en fråga av strategisk betydelse för unionen eftersom dessa nät är grundläggande för en rad tjänster som är nödvändiga för den inre marknadens funktion och även är centrala för upprättandet av vår försvarsberedskap, bland annat när det gäller militär mobilitet. 5G-nät kan tillhandahålla pålitlig ultrasnabb konnektivitet för exempelvis data och informationsutbyte, detektering av drönare och realtidssamordning på slagfält.

(154) 5G-utbyggnaden utgörs främst av icke-fristående nät, där endast radioaccessnätet uppgraderas till 5G-teknik och resten av nätet fortfarande är beroende av ett befintligt 4G-stamnät. Icke-fristående 5G-nät bygger främst på redan existerande infrastruktur, vilket innebär att säkerheten för framtida 5G-nät i viss mån avgörs av redan existerande nätutrustning och konfigurationen av sådan utrustning. Därför bör begränsningsåtgärder även omfatta 4G-nät som används för 5G-utbyggnaden.

(155) För att hantera betydande säkerhetsutmaningar i 5G-nät utförde medlemsstaterna inom samarbetsgruppen för nät- och informationssäkerhet, tillsammans med kommissionen och Enisa, en samordnad säkerhetsriskbedömning på unionsnivå av 5G-nät, där både tekniska och icke-tekniska risker granskades. I bedömningen identifierades flera risker, inklusive potentiell inblandning från tredjeländer eller aktörer från tredjeländer via leveranskedjan, och tillgångar kategoriserades utifrån grad av kritikalitet. Denna bedömning bör ligga till grund för fastställandet av viktiga IKT-tillgångar för 5G-kommunikationsnät.

(156) För att begränsa de risker som identifierats i den samordnade säkerhetsriskbedömningen på unionsnivå av 5G-nät antog samarbetsgruppen för nät- och informationssäkerhet EU:s verktygslåda för 5G-cybersäkerhet, som omfattar strategiska och tekniska åtgärder. Även om en majoritet av medlemsstaterna har rättsliga ramar som tillåter begränsning eller uteslutande av högriskleverantörer enligt rekommendationerna i 5G-verktygslådan har genomförandet av dessa ramar inte varit enhetligt. Resultatet är att ett stort antal 5G-anläggningar i unionen använder sig av högriskleverantörer enligt kommissionens meddelande om genomförandet av 5G-verktygslådan[69]. Denna situation skapar sårbarheter, såsom strategiskt beroende och potentiell exponering för inblandning från tredjeländer, som även kan påverka framtida 6G-infrastruktur som bygger på befintliga 5G-nät. Det fragmenterade genomförandet av de åtgärder som rekommenderas i 5G-verktygslådan, i synnerhet när det gäller omfattningen av begränsningarna för högriskleverantörer, har lett till skillnader mellan medlemsstaterna, vilket leder till olika spelregler som delar upp den

[69] Meddelande från kommissionen, *Genomförande av verktygslådan för 5G-cybersäkerhet*, 15 juni 2023, C(2023) 4049 final.

inre marknaden och försvagar den allmänna nätsäkerheten. Europeiska revisionsrätten har lyft fram dessa skillnader och varnat för att avsaknaden av en samordnad strategi undergräver den inre marknadens funktion. Ett fortsatt beroende av högriskleverantörer utgör en allvarlig risk för säkerheten i kritisk infrastruktur i unionen och kan urholka förtroendet för den inre marknaden, eftersom varierande säkerhetsnivåer kan leda till att konsumenter och företag avskräcks från att förlita sig på 5G-baserade produkter och tjänster i unionen. Det är därför viktigt med åtgärder på unionsnivå för att säkerställa en harmoniserad strategi för säkerheten i 5G-nät.

(157) Med sikte på införandet av en utfasningsperiod för viktiga IKT-tillgångar i fasta och satellitbaserade elektroniska kommunikationsnät bör kommissionen utföra en bedömning med vederbörlig hänsyn till graden av säkerhetsrisk som är förknippad med varje enskild viktig IKT-tillgång i fasta och satellitbaserade nät, livslängden för relevanta komponenter och de ekonomiska konsekvenser som avlägsnandet av dessa komponenter skulle ha för de berörda operatörerna. Baserat på resultaten av denna bedömning kan kommissionen överväga olika utfasningsperioder för vissa viktiga IKT-tillgångar och deras integrerade element.

(158) För en effektiv tillsyn och kontroll av efterlevnaden av skyldigheter när det gäller leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät bör de berörda behöriga myndigheterna enligt denna förordning säkerställa ett nära samarbete med de behöriga myndigheterna enligt [förslaget till förordning om digitala nätverk]. På begäran av en behörig myndighet som utsetts enligt denna förordning bör nationella regleringsmyndigheter och andra behöriga myndigheter för radiospektrum, när så är lämpligt, återkalla de rättigheter som avses i artiklarna 9 och 20 i [förslaget till förordning om digitala nätverk] om leverantören av allmänna elektroniska kommunikationsnät inte uppfyller skyldigheterna enligt denna förordning, inbegripet om leverantören inte fasar ut IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer i driften av viktiga IKT-tillgångar inom den period som anges i enlighet med denna förordning.

(159) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer bör medlemsstaterna kunna utse eller inrätta en eller flera behöriga myndigheter med ansvar för åtgärder för tillsyn och kontroll av efterlevnad enligt denna förordning.

(160) De behöriga myndigheterna bör tillhandahålla stöd till entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 för uppfyllandet av deras skyldigheter enligt denna förordning. I detta syfte bör kommissionen bedöma om leverantörer som kan påverkas av specifika förbud är etablerade i ett tredjeland som utgör cybersäkerhetsproblem eller kontrolleras av ett sådant tredjeland, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland. Behöriga myndigheter bör ha ett nära samarbete med kommissionen och andra behöriga myndigheter inom det nätverk som inrättas enligt denna förordning. Baserat på kommissionens bedömning bör de behöriga myndigheterna utbyta relevant information om högriskleverantörer med berörda entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555. Entiteter förväntas inte verifiera om en leverantör står under utländsk kontroll utan får helt förlita sig på information som erhålls från behöriga myndigheter. De behöriga myndigheterna bör säkerställa att dessa entiteter inte påläggs några onödiga administrativa bördor.

(161) För att säkerställa en effektiv efterlevnad bör denna förordning föreskriva åtgärder för tillsyn och kontroll av efterlevnad genom vilka de behöriga myndigheterna kan utöva tillsyn över entiteter av den typ som avses i bilagorna I och II till direktiv (EU)

2022/2555. I de fall då de behöriga myndigheterna utövar sina uppgifter avseende tillsyn och efterlevnadskontroll gentemot dessa entiteter bör de inte gå utöver vad som är nödvändigt utan agera i proportion till de identifierade riskerna.

(162) För en effektiv och konsekvent kontroll av efterlevnaden i hela unionen är det nödvändigt att föreskriva efterlevnadskontrollbefogenheter som de behöriga myndigheterna kan utöva när de skyldigheter som fastställs i denna förordning åsidosätts. Vid utövandet av dessa efterlevnadskontrollbefogenheter bör de behöriga myndigheterna ta vederbörlig hänsyn till ett antal faktorer, däribland överträdelsens art, allvarlighetsgrad och varaktighet, de materiella eller immateriella skador som orsakats, om överträdelsen var avsiktlig eller berodde på försumlighet, vilka åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten samt eventuella andra försvårande eller förmildrande omständigheter. Efterlevnadskontrollåtgärderna, inklusive sanktioner, bör vara proportionella och påförandet av dem bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(163) Det är viktigt att även föreskriva en befogenhet att förelägga viten, för att tvinga en entitet av den typ som avses i bilaga I eller II till direktiv (EU) 2022/2555 att upphöra med en överträdelse av denna förordning i enlighet med ett föregående beslut av den behöriga myndigheten.

(164) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i denna förordning bör varje behörig myndighet ha befogenhet att ålägga sanktioner eller begära att sanktioner åläggs.

(165) När en entitet av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 åläggs sanktioner och den entiteten är ett företag, bör företag förstås som ett företag i enlighet med artiklarna 101 och 102 i EUF-fördraget. Om böter påförs en person som inte är ett företag, bör den behöriga myndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation när den tar ställning till lämpligt bötesbelopp. Medlemsstaterna bör fastställa om och i vilken utsträckning som myndigheter bör åläggas böter. Åläggandet av böter bör inte påverka tillämpningen av de behöriga myndigheternas övriga befogenheter.

(166) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för antagandet av genomförandeakter med närmare bestämmelser avseende de avgifter som tas ut av Enisa, genomförandeakter om en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, genomförandeakter om gemensamma principer och referensbestämmelser avsedda att föreskriva element för europeiska ordningar för cybersäkerhetscertifiering, genomförandeakter som specificerar förfaranden för förhandsgodkännande eller modeller för allmän delegering, genomförandeakter om erkännande av ett tredjelands eller en internationell organisations cybersäkerhetscertifikat som likvärdigt med europeiska cybersäkerhetscertifikat, genomförandeakter om fastställande av en plan för inbördes granskning, genomförandeakter om fastställande av förfaranden (inbegripet gränsöverskridande samarbete) för auktorisering av organ för bedömning av överensstämmelse, genomförandeakter om fastställande av förutsättningar, format och förfarande för

anmälan av organ för bedömning av överensstämmelse, genomförandeakter om utpekande av ett tredjeland som ett land som utgör cybersäkerhetsproblem för IKT-leveranskedjor, genomförandeakter om identifiering av viktiga IKT-tillgångar som används för tillverkning av produkter eller tillhandahållande av tjänster som utförs av entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555, genomförandeakter om fastställande av att entiteter som bedriver verksamhet inom högkritiska sektorer och andra kritiska sektorer omfattas av särskilda begränsningsåtgärder och specificering av tidsperioderna för utfasning av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka tillhandahålls av högriskleverantörer och genomförandeakter som ytterligare specificerar villkoren för undantagande av entiteter som är etablerade i eller som kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem, samt antagandet av genomförandeakter med närmare bestämmelser avseende de avgifter som kommissionen tar ut. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 och granskningsförfarandet bör användas. För att säkerställa enhetliga villkor för genomförandet av denna förordning bör kommissionen tilldelas genomförandebefogenheter för upprättandet av en förteckning över högriskleverantörer av relevans för vissa åtgärder som föreskrivs i denna förordning.

(167) De europeiska ordningarna för cybersäkerhetscertifiering bör återspegla den senaste tekniska utvecklingen och nya relaterade hot samt antagandet av ny unionslagstiftning som fastställer påvisande av regelefterlevnad och presumtion om överensstämmelse genom europeisk cybersäkerhetscertifiering med relevanta cybersäkerhetskrav i den lagstiftningen. Därför bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på tillägg till eller ändring av de säkerhetsmål som eftersträvas med de europeiska ordningarna för cybersäkerhetscertifiering. För att upprätta ett ramverk för en betrodd IKT-leveranskedja bör också befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på ändring av bilaga II till denna förordning för att anpassa den till den tekniska utvecklingen. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter bör Europaparlamentet och rådet erhålla alla handlingar samtidigt som medlemsstaternas experter, och deras experter bör ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(168) Enisas verksamhet bör utvärderas regelbundet och på ett oberoende sätt. Utvärderingen bör beakta Enisas mål och relevansen i dess uppgifter, särskilt dess uppgifter rörande operativt samarbete på unionsnivå. I händelse av en översyn bör kommissionen utvärdera hur Enisas roll som referenspunkt för rådgivning och expertis kan stärkas.

(169) Kommissionens genomförandeförordning (EU) 2024/482 fastställer regler för antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC). EUCC är den första och enda europeiska ordningen för cybersäkerhetscertifiering som antagits i enlighet med förordning (EU) 2019/881. Den rör certifieringen av IKT-produkter, inklusive produkter som tillhör teknikdomänerna ”smartkort och liknande anordningar” och ”hårdvaruenheter med

säkerhetsboxar” och skyddsprofiler (som IKT-processer). Det är därför nödvändigt att säkerställa att både certifieringsverksamheten och byråns verksamhet fortsätter.

(170) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.2 i förordning (EU) 2018/1725[70] och de avgav ett gemensamt yttrande den [datum].

(171) Förordning (EU) 2019/881 bör upphävas.

(172) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen (*EU-fördraget*). I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVDELNING I
ALLMÄNNA BESTÄMMELSER

Artikel 1
Innehåll och tillämpningsområde

1. I denna förordning fastställs

   a) uppdrag, mål, uppgifter och organisatoriska frågor som rör Europeiska unionens cybersäkerhetsbyrå (Enisa),

   b) ett ramverk för inrättandet av europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande cybersäkerhetsnivå för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus i unionen samt i syfte att motverka en fragmentering av den inre marknaden när det gäller ordningar för cybersäkerhetscertifiering i unionen, och

   c) ett ramverk för en betrodd IKT-leveranskedja.

2. Tillämpningen av det ramverk som avses i punkt 1 b ska inte påverka tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsrättsakter.

3. Det ramverk som avses i första stycket led c ska tillämpas på offentliga eller privata entiteter av en typ som avses i bilaga I eller II till direktiv (EU) 2022/2555 och som tillhandahåller sina tjänster eller utför sina verksamheter inom unionen.

4. Denna förordning påverkar inte medlemsstaternas väsentliga statliga funktioner, däribland att säkerställa statens territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten även i fortsättningen vara varje medlemsstats eget ansvar.

---

[70] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 2
Definitioner

I denna förordning gäller följande definitioner:

1) *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra personer som berörs av cyberhot.

2) *unionsentiteter*: unionens entiteter enligt definitionen i artikel 3.1 i förordning (EU, Euratom) 2023/2841.

3) *auktoriserade tillhandahållare av intyg*: en offentlig eller privat entitet för vilken Enisa har antagit ett beslut som auktoriserar den entiteten att bevilja europeiska individuella intyg om cybersäkerhetskompetens i enlighet med en ordning för europeiska individuella intyg om cybersäkerhetskompetens.

4) *europeiskt individuellt intyg om cybersäkerhetskompetens*: ett bevis i digital eller fysisk form, som intygar att en individ kan utföra de uppgifter som är förknippade med en yrkesprofil eller en undergrupp till en yrkesprofil i den europeiska kompetensramen för cybersäkerhet (*ECSF*) och har de kunskaper och den förståelse som krävs för detta, efter en bedömning i enlighet med en ordning för europeiska individuella intyg om cybersäkerhetskompetens.

5) *ordning för europeiska individuella intyg om cybersäkerhetskompetens*: en övergripande uppsättning regler, krav, standarder och förfaranden som fastställts av Enisa och som är förknippade med en yrkesprofil i den europeiska kompetensramen för cybersäkerhet eller en undergrupp till denna och som ska tillämpas på och av auktoriserade tillhandahållare av intyg.

6) *nätverks- och informationssystem*: ett nätverks- och informationssystem enligt definitionen i artikel 6.1 i direktiv (EU) 2022/2555.

7) *nationell strategi för cybersäkerhet*: en nationell strategi för cybersäkerhet enligt definitionen i artikel 6.4 i direktiv (EU) 2022/2555.

8) *incident*: en incident enligt definitionen i artikel 6.6 i direktiv (EU) 2022/2555.

9) *storskalig cybersäkerhetsincident*: en storskalig cybersäkerhetsincident enligt definitionen i artikel 6.7 i direktiv (EU) 2022/2555.

10) *incidenthantering*: incidenthantering enligt definitionen i artikel 6.8 i direktiv (EU) 2022/2555.

11) *cyberhot*: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer.

12) *europeisk ordning för cybersäkerhetscertifiering*: en omfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering eller bedömning av överensstämmelse av specifika IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus.

13) *nationell ordning för cybersäkerhetscertifiering*: en omfattande uppsättning regler, tekniska krav, standarder och förfaranden som utvecklas och antas av en nationell

offentlig myndighet och som tillämpas vid certifiering eller bedömning av överensstämmelse av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som omfattas av tillämpningsområdet för den berörda ordningen.

14) *europeiskt cybersäkerhetscertifikat*: ett dokument, utfärdat av ett relevant organ, som intygar att en viss IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller entitets cybersäkerhetsstatus har utvärderats för kontroll av överensstämmelse med specifika säkerhetskrav som fastställs i en europeisk ordning för cybersäkerhetscertifiering.

15) *EU-försäkran om överensstämmelse*: ett dokument som utfärdats av en tillverkare eller leverantör av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller, och som anger att en självbedömning av överensstämmelse har visat att krav motsvarande assuransnivån ”grundläggande” i den europeiska ordningen för cybersäkerhetscertifiering uppfylls.

16) *IKT-produkt*: en del, eller en grupp av delar, i nätverks- och informationssystem.

17) *IKT-tjänst*: en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nätverks- och informationssystem.

18) *IKT-process*: verksamhet som utförs för att utforma, utveckla, tillhandahålla eller underhålla en IKT-produkt eller IKT-tjänst.

19) *utlokaliserad säkerhetstjänst*: en tjänst som tillhandahålls en tredje part och som består i att utföra, eller tillhandahålla stöd för, verksamhet som rör hantering av cybersäkerhetsrisker, såsom incidenthantering, penetrationstester, säkerhetsrevisioner och rådgivning, inbegripet expertrådgivning för tekniskt stöd.

20) *ackreditering*: ackreditering enligt definitionen i artikel 2.10 i förordning (EG) nr 765/2008.

21) *nationellt ackrediteringsorgan*: ett nationellt ackrediteringsorgan enligt definitionen i artikel 2.11 i förordning (EG) nr 765/2008.

22) *bedömning av överensstämmelse*: bedömning av överensstämmelse enligt definitionen i artikel 2.12 i förordning (EG) nr 765/2008.

23) *organ för bedömning av överensstämmelse*: ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008.

24) *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012[71].

25) *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

26) *harmoniserad standard*: harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

---

[71] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

27) *assuransnivå*: förtroendegrund för att en IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller entitets cybersäkerhetsstatus uppfyller säkerhetskraven i en specifik europeisk ordning för cybersäkerhetscertifiering och anger på vilken nivå en IKT-produkt, IKT-tjänst, IKT-process, utlokaliserad säkerhetstjänst eller entitets cybersäkerhetsstatus har utvärderats, men som inte i sig mäter säkerheten i den berörda IKT-produkten, IKT-tjänsten, IKT-processen eller utlokaliserade säkerhetstjänsten eller den berörda entitetens cybersäkerhetsstatus.

28) *självbedömning av överensstämmelse*: en åtgärd som genomförs av en tillverkare eller en leverantör av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller, som utvärderar om dessa IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus uppfyller kraven i en specifik europeisk ordning för cybersäkerhetscertifiering.

29) *entiteters cybersäkerhetsstatus*: entiteters nivå av cybersäkerhet i förhållande till de särskilda säkerhetskraven.

30) *modell med förhandsgodkännande*: en modell där ett organ för bedömning av överensstämmelse får utfärda ett europeiskt cybersäkerhetscertifikat på grundval av en bedömning som gjorts av en nationell myndighet för cybersäkerhetscertifiering i samband med en specifik certifieringsprocess inom ramen för en relevant ordning.

31) *modell med allmän delegering*: en modell där ett organ för bedömning av överensstämmelse får utfärda ett europeiskt cybersäkerhetscertifikat baserat på en delegering av certifieringsverksamhet från en nationell myndighet för cybersäkerhetscertifiering.

32) *enhet för hantering av it-säkerhetsincidenter* eller *CSIRT-enhet*: en enhet som utsetts eller inrättats i enlighet med artikel 10 i direktiv (EU) 2022/2555.

33) *IKT-komponenter*: IKT-produkter, IKT-tjänster eller IKT-processer som kan användas i driften av IKT-tillgångar.

34) *IKT-tillgångar*: programvaru- eller hårdvarutillgångar i nätverks- och informationssystem som används av en entitet av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555.

35) *viktiga IKT-tillgångar*: IKT-tillgångar identifierade i enlighet med artikel 102.

36) *elektroniskt kommunikationsnät*: ett elektroniskt kommunikationsnät enligt definitionen i artikel 2.1 i förordning (EU) XX/XXXX [förslag till förordning om digitala nätverk].

37) *kontroll*: förmågan att utöva ett avgörande inflytande på en rättslig enhet, antingen direkt eller indirekt via en eller flera mellanliggande rättsliga enheter.

38) *etablering*: faktiskt bedrivande av verksamhet genom en stabil struktur i det land där entiteten har sitt huvudkontor eller sitt huvudsakliga verksamhetsställe.

39) *högriskleverantör*: något av följande:

a) En entitet som är etablerad i ett tredjeland som utgör cybersäkerhetsproblem och som har utpekats i enlighet med artikel 100, eller som kontrolleras av ett sådant tredjeland, av en entitet som är etablerad i ett sådant tredjeland eller av en medborgare i ett sådant tredjeland.

b) En entitet som utpekats i enlighet med artikel 103.7 och entiteter som kontrolleras av den entiteten.

40) *IKT-leveranskedja*: en helhet av IKT-tjänster, IKT-produkter och IKT-processer som omfattar de handlingar och aktörer som är involverade i alla stadier uppströms för en produkt som görs tillgänglig eller en tjänst som tillhandahålls på marknaden.

41) *tredjeland*: ett tredjeland enligt definitionen i artikel 3.4 i Europaparlamentets och rådets förordning (EU) 2023/2675[72].

42) *icke-teknisk risk*: sannolikheten för att en leverantör är under påverkan av ett tredjeland med potential att orsaka förlust eller störning av den tjänst som tillhandahålls av eller äventyra den produkt som tillverkas av en entitet eller medföra exfiltrering av data, inbegripet för spionage eller generering av intäkter.

43) *betydande icke-teknisk cybersäkerhetsrisk*: en icke-teknisk cybersäkerhetsrisk som med hög sannolikhet kan antas orsaka en incident som kan medföra allvarliga negativa konsekvenser, inbegripet genom att orsaka betydande materiell eller immateriell förlust eller störning.

44) *centrala nätverksfunktioner i mobilnät för elektronisk kommunikation*: det centrala arkitekturelementet i mobilnät för elektronisk kommunikation som ansluter de viktigaste nätnoderna till internet och hanterar viktiga systemfunktioner, exempelvis autentisering av användarutrustning, funktioner för laglig avläsning, säkerhetsgateways (SeGW) vid nätverkskanten, signalfunktioner för säkerhetsändamål, roaming och sessionshantering, användar- och kontrollplandatatransport, hantering av åtkomstpolicyer, registrering och auktorisering av nätverkstjänster, lagring av slutanvändar- och nätverksdata, kritiska nättjänster inbegripet domännamnssystem (DNS), samtrafik med tredje parts mobilnät, centrala nätverksfunktioners exponering för externa applikationer, samt urval och hantering av nätverksskivning.

45) *virtualisering av nätverksfunktioner (network function virtualisation, NFV)* och *förvaltning och nätverksorkestrering (management and network orchestration, MANO) av mobilnät för elektronisk kommunikation*: den programvara och arkitektoniska ram som säkerställer livscykelhantering, orkestrering och automatisering av virtualiserade nätverksfunktioner (VNF), molnäkta nätverksfunktioner (CNF) och urvalet och hanteringen av nätverksskivning i mobilnät för elektronisk kommunikation.

46) *radioaccessnät (RAN) för mobilnät för elektronisk kommunikation*: det nätverk som ansluter mobilanvändarutrustningen till stamnätet, däribland basstationer (eNodeB för 4G, gNodeB för 5G), RRH (remote radio heads) och basbandsenheter (BBU), aktiva antennsystem (AAS) och i tillämpliga fall disaggregerade RAN-komponenter såsom centraliserade enheter (CU) och distribuerade enheter (DU) samt intelligent RAN-styrenhet (RIC).

47) *centrala nätverksfunktioner i fasta nät för elektronisk kommunikation*: nätverkets stamnätsintelligens som kopplar samman de viktigaste noderna och hanterar en rad väsentliga funktioner, däribland autentisering och auktorisering av användare (AAA), funktioner för laglig avläsning (LI), domännamnssystem (DNS) och IP-

[72] Europaparlamentets och rådets förordning (EU) 2023/2675 av den 22 november 2023 om skydd av unionen och dess medlemsstater mot ekonomiskt tvång från tredjeländer (EUT L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

adresstjänster (DHCP), hantering av åtkomstpolicyer, lagring av slutanvändar- och nätverksdata, IP-byte och IP-dirigering (IP switching and routing) samt internationella internetportaler (IIG).

48) *näthanteringssystem för fasta nät för elektronisk kommunikation*: alla centraliserade plattformar och programvarukomponenter som behövs för nätets drift, förvaltning, underhåll och tillhandahållande (OAM&P) och övervakningen av nätrelaterad information.

49) *transport- och överföringsfunktioner i fasta nät för elektronisk kommunikation*: alla komponenter som behövs för backhaul och aggregering av trafik över nätverket, inklusive optisk transportutrustning, mikrovågslänkar och undervattenskabelsystem som innefattar såväl undervattensutrustning och terminalutrustning för kabelledning under vatten (submarine line terminal equipment, SLTE) som fysiska landningsstationsanläggningar.

50) *accessnät för fasta nät för elektronisk kommunikation*: det nät som ansluter slutanvändarens lokaler till aggregeringsnätet eller stamnätet, inbegripet optisk linjeterminal (OLT) och optisk nätverksterminal (ONT) för fibernät, modemtermineringssystem med koaxialkabel (CMTS) och kabelmodem för koaxialkabelnät samt fasta trådlösa accesskomponenter när de används som substitut för en fast förbindelse.

AVDELNING II
EUROPEISKA UNIONENS CYBERSÄKERHETSBYRÅ

Kapitel I
Uppdrag och mål

Artikel 3
Enisas uppdrag

1. Enisas uppdrag är att stödja medlemsstaterna och unionsentiteterna för att uppnå en hög nivå av cybersäkerhet, cyberresiliens och förtroende i unionen.

2. Enisa ska fungera som en referenspunkt för rådgivning och expertis i fråga om cybersäkerhet för medlemsstaterna och andra aktörer i unionen.

3. Enisa ska bidra till att minska fragmenteringen på den inre marknaden genom att utföra de uppgifter som denna byrå anförtrotts enligt denna förordning.

4. Enisa ska utföra de uppgifter som byrån anförtrotts genom unionsrättsakter.

5. Enisa ska utveckla sina egna förmågor, däribland teknisk och mänsklig kapacitet och kompetens, som krävs för att utföra de uppgifter som byrån tilldelas enligt denna förordning.

Artikel 4
Enisas mål

1. Enisa ska vara ett expertcentrum inom området cybersäkerhet genom sitt oberoende, den vetenskapliga och tekniska kvaliteten på de råd, de bidrag, den assistans och den

information byrån tillhandahåller, transparensen i sina operativa förfaranden, arbetsmetoderna och genom ett kompetent utförande av sina uppgifter.

2. Enisa ska bistå medlemsstaterna och, när så är lämpligt, unionsentiteter vid genomförandet av övergripande och sektorsspecifik unionspolitik och unionslagstiftning på cybersäkerhetsområdet, inklusive marknadskontrollverksamhet.

3. Enisa ska tillhandahålla sin expertis och bistå kommissionen vid utarbetandet av unionens politik och lagstiftning på cybersäkerhetsområdet.

4. Enisa ska stödja kapacitetsuppbyggnad och beredskap i hela unionen genom att bistå medlemsstaterna, unionsentiteter (genom cybersäkerhetstjänsten för unionens institutioner, organ och byråer (CERT-EU) som avses i kapitel IV i förordning (EU, Euratom) 2023/2841) och offentliga och privata intressenter i syfte att öka skyddet av deras nätverks- och informationssystem, för att utveckla och förbättra cyberresiliensen och insatskapaciteten.

5. Enisa ska bidra till genomförandet av EU-akademin för cyberkompetens och till en ökning av cybersäkerhetsarbetskraften i unionen genom att stödja insatser för att utveckla kompetensportabilitet i hela unionen, bland annat genom upprätthållande och spridning av den europeiska kompetensramen för cybersäkerhet, genom utveckling, underhåll och spridning av ordningar för europeiska individuella intyg om cybersäkerhetskompetens i enlighet med kapitel II avsnitt 4 i denna avdelning och genom att säkerställa tillhandahållande av utbildning i enlighet med artikel 6.8.

6. Enisa ska främja samarbete, däribland informationsutbyte och samordning på unionsnivå, mellan medlemsstater, unionsentiteter i enlighet med förordning (EU, Euratom) 2023/2841 samt berörda privata och offentliga intressenter i frågor som rör cybersäkerhet.

7. Enisa ska bidra till att öka cybersäkerhetskapaciteten på unionsnivå i syfte att stödja medlemsstaternas arbete med för att förebygga och hantera cyberhot.

8. Enisa ska stödja operativt samarbete på unionsnivå, bland annat genom att bidra till gemensam situationsmedvetenhet om cyberhot- och incidentbilden, mellan medlemsstaterna och, i samarbete med CERT-EU, mellan unionsentiteter.

9. Enisa ska ha ett nära samarbete med Europol, CSIRT-enheter och andra berörda nationella myndigheter för att förbättra cybersäkerhetsberedskapen och hanteringen av incidenter med utpressningsprogram.

10. Enisa ska bidra till inrättandet och upprätthållandet av ett europeiskt ramverk för cybersäkerhetscertifiering i enlighet med avdelning III i denna förordning. Enisa ska främja användningen av europeisk cybersäkerhetscertifiering, i syfte att motverka en fragmentering av den inre marknaden.

11. Enisa ska bidra till harmoniseringen av den digitala inre marknaden genom att delta i standardiseringsarbete som är relevant för unionens politik på cybersäkerhetsområdet och genom att utarbeta tekniska specifikationer.

12. Enisa ska främja en hög nivå av cybersäkerhetsmedvetenhet hos organisationer och företag.

Kapitel II
Uppgifter

Avsnitt 1
Stöd för genomförandet av unionens politik och lagstiftning

Artikel 5
Stöd för genomförandet av unionens politik och lagstiftning

1. Enisa ska bidra till genomförandet av unionens politik och lagstiftning genom att göra följande:

   a) Hjälpa medlemsstaterna att genomföra unionens politik och lagstiftning på cybersäkerhetsområdet på ett konsekvent sätt, bland annat genom att utfärda teknisk vägledning och rapporter, tillhandahålla rådgivning och bästa praxis och främja ett utbyte av bästa praxis mellan behöriga myndigheter i detta syfte.

   b) Stödja informationsutbyte inom och mellan sektorer, i synnerhet när det gäller de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och produkter med digitala element som omfattas av förordning (EU) 2024/2847, genom att tillhandahålla bästa praxis och vägledning om tillgängliga verktyg och förfaranden.

   c) På begäran av kommissionen bistå medlemsstaterna genom att tillhandahålla stöd, såsom teknisk vägledning – däribland om riskhanteringsåtgärder för cybersäkerhet, verktyg för mognadsbedömning av cybersäkerheten och strategilistor för hantering av cyberincidenter – som är särskilt anpassat till de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, eller tillhandahålla stöd för genomförandet av principer för inbyggd säkerhet för produkter med digitala element i linje med förordning (EU) 2024/2847, för att främja en förbättring av cybersäkerhetens mognadsgrad och efterlevnaden av unionens cybersäkerhetslagstiftning.

   d) Bidra till arbetet i den samarbetsgrupp som inrättats i enlighet med artikel 14.1 i direktiv (EU) 2022/2555 (*samarbetsgruppen för nät- och informationssäkerhet*), den europeiska samarbetsgruppen för digital identitet som inrättats i enlighet med artikel 46e.1 i förordning (EU) nr 910/2014, den europeiska gruppen för cybersäkerhetscertifiering (ECCG) som avses i artikel 90 i denna förordning och den administrativa samarbetsgruppen (Adco-gruppen) som inrättats i enlighet med artikel 52.15 i förordning (EU) 2024/2847.

   e) Hjälpa medlemsstaterna och relevanta unionsentiteter att utveckla och främja politik på cybersäkerhetsområdet som rör upprätthållandet av den allmänna tillgängligheten till och integriteten för den offentliga kärnan av det öppna internet.

   f) I enlighet med förordning (EU) 2024/2847 tillhandahålla teknisk rådgivning och tekniskt stöd för medlemsstaterna och kommissionen när det gäller frågor som rör genomförandet av den förordningen.

   g) Hjälpa medlemsstaterna att genomföra ömsesidigt bistånd och främja sådana samarbetsförfaranden för väsentliga och viktiga entiteter i enlighet med [artikel 37a i direktiv (EU) 2022/2555].

h) På begäran av Europeiska dataskyddsstyrelsen tillhandahålla råd om genomförandet av specifika cybersäkerhetsaspekter av unionens politik och lagstiftning som rör dataskydd och integritet.

2. Enisa ska bidra till samordnade cybersäkerhetsriskbedömningar på unionsnivå, inbegripet de som utförs i enlighet med artikel 22 i direktiv (EU) 2022/2555.

3. Enisa ska utfärda riktlinjer om interoperabiliteten för nätverks- och informationssystem som används för informationsutbyte, även med avseende på gränsöverskridande cybernav enligt artikel 6.3 i förordning (EU) 2025/38.

4. Enisa ska vara medlem i samarbetsgruppen för nät- och informationssäkerhet enligt artikel 14.3 i direktiv (EU) 2022/2555.

5. På begäran av kommissionen ska Enisa tillhandahålla expertis, teknisk rådgivning, information eller analys eller utföra förberedande arbete i specifika frågor som rör cybersäkerhet, som kan användas som underlag för kommissionens beslutsfattande och övervakning av genomförandet av unionslagstiftningen.

Artikel 6
Kapacitetsuppbyggnad

Enisa ska göra följande:

1) Bistå medlemsstaterna i deras ansträngningar för att förbättra förebyggandet, upptäckten och analysen av, samt kapaciteten att hantera, cyberhot och cyberincidenter genom att tillhandahålla kunskaper och nödvändig expertis.

2) På medlemsstaternas begäran hjälpa dem att fastställa och genomföra frivilliga riktlinjer för information om sårbarheter.

3) I enlighet med förordning (EU, Euratom) 2023/2841 bistå CERT-EU och den interinstitutionella cybersäkerhetsstyrelsen i deras insatser för att hjälpa unionsentiteter att stärka sin cybersäkerhet, förbättra förebyggandet, upptäckten och analysen av cyberhot och cyberincidenter samt förbättra sin kapacitet för att hantera sådana cyberhot och incidenter.

4) Bistå medlemsstaterna med inrättandet av nationella CSIRT-enheter, på begäran i enlighet med artikel 10.10 i direktiv (EU) 2022/2555.

5) Bistå medlemsstaterna vid utarbetande eller uppdatering av en nationell strategi för cybersäkerhet och centrala resultatindikatorer för bedömningen av denna strategi, på begäran i enlighet med artikel 7.4 i direktiv (EU) 2022/2555, främja spridning av dessa strategier och notera framstegen med genomförandet av dessa i hela unionen i syfte att främja bästa praxis.

6) På deras begäran bistå unionens institutioner med utarbetandet och översynen av unionens strategier på cybersäkerhetsområdet samt med att främja spridningen och övervaka framstegen i genomförandet av dem.

7) Bistå nationella CSIRT-enheter i deras arbete för att öka sin kapacitet, bland annat genom att främja dialog och informationsutbyte, för att säkerställa att alla CSIRT-enheter när det gäller den tekniska nivån har gemensamma minimikapacitetskrav och att deras verksamhet följer bästa praxis.

8) Bistå medlemsstaterna, unionsentiteterna och offentliga och privata intressenter i deras insatser för att bedöma, öka och förbättra cybersäkerhetsarbetskraften, exempelvis genom att utveckla, underhålla och främja användningen av

relevanta verktyg såsom den europeiska kompetensramen för cybersäkerhet och ordningar för europeiska individuella intyg om cybersäkerhetskompetens i enlighet med avsnitt 4 i detta kapitel.

9) Bistå relevanta offentliga organ och privata intressenter genom att genomföra målinriktade utbildningsinsatser, när så är lämpligt i samarbete med intressenter.

10) Bistå samarbetsgruppen för nät- och informationssäkerhet i utbytet av bästa praxis och information, i synnerhet när det gäller genomförandet av direktiv (EU) 2022/2555 i enlighet med artikel 14.4 c i det direktivet.

11) Bistå marknadskontrollmyndigheter som utsetts i enlighet med förordning (EU) 2024/2847 i deras verksamhet som syftar till att säkerställa ett effektivt genomförande av den förordningen, inbegripet stöd för vägledning och tekniska råd till ekonomiska aktörer, stöd för kontroll av efterlevnad, utvärdering av risker, gemensam verksamhet och samordnade tillsynsåtgärder (sweeps) i enlighet med förordning (EU) 2024/2847.

12) Bistå medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering i utbytet av bästa praxis och, på begäran från enskilda medlemsstater, bistå de nationella myndigheterna för cybersäkerhetscertifiering när det gäller genomförandet av de europeiska ordningarna för cybersäkerhetscertifiering på nationell nivå.

13) Bistå offentliga myndigheter och privata intressenter i samband med bedömning av överensstämmelse och utvärderingsverksamhet, inbegripet organ för bedömning av överensstämmelse och små och medelstora företag, för att stödja ett robust, konkurrenskraftigt, inkluderande och harmoniserat ekosystem för bedömning av överensstämmelse som stöder genomförandet av förordning (EU) 2024/2847 och det europeiska ramverket för cybersäkerhetscertifiering.

14) Bistå Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum, som inrättats i enlighet med förordning (EU) 2021/887, genom informationsutbyte om nuvarande och framväxande risker och cyberhot, inbegripet risker och hot som rör ny och framväxande informations- och kommunikationsteknik.

15) Bistå medlemsstaterna genom att tillhandahålla tekniskt stöd, inbegripet för inrättandet av och verksamhet inom ramen för regulatoriska sandlådor på cybersäkerhetsområdet i enlighet med relevant unionslagstiftning.

Artikel 7
Medvetandehöjande åtgärder och talangreserv

Enisa ska bistå medlemsstaterna i deras insatser för att öka medvetenheten om unionens politik och lagstiftning på cybersäkerhetsområdet och främja politikens och lagstiftningens synlighet genom att utveckla vägledning och konkreta verktyg som kan användas. Enisa ska stödja initiativ som syftar till att öka den europeiska talangreserven på cybersäkerhetsområdet, i synnerhet genom att samordna uttagningsprov.

Artikel 8
Marknadskännedom och marknadsanalyser

1. Enisa ska utföra och sprida analyser av de viktigaste marknadstrenderna på cybersäkerhetsmarknaden på både efterfråge- och utbudssidan, i synnerhet när det gäller områden där det existerar eller planeras europeiska ordningar för cybersäkerhetscertifiering, sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och produktkategorier som omfattas av förordning (EU) 2024/2847, inklusive bilagorna III och IV till den förordningen.
2. Enisa ska utföra och sprida analyser av tekniska cybersäkerhetstrender, i synnerhet när det gäller verksamheter och entiteter som omfattas av direktiv (EU) 2022/2555 och produkter med digitala element som omfattas av förordning (EU) 2024/2847.
3. Enisa ska bygga upp kunskap och sprida tekniska råd och analyser om de senaste cybersäkerhetsverktygen, ramar för standarder samt bästa praxis.

Artikel 9
Internationellt samarbete

Enisa ska bidra till unionens insatser för att samarbeta med tredjeländer och internationella organisationer samt inom relevanta ramar för internationellt samarbete för att främja internationellt samarbete i frågor som rör cybersäkerhet, genom att

a) om lämpligt delta som observatör i anordnandet av internationella övningar samt analysera och rapportera till styrelsen om resultaten av sådana övningar,

b) på begäran av kommissionen underlätta utbyte av bästa praxis med tredjeländer och internationella organisationer,

c) på begäran av kommissionen förse den med expertis,

d) tillhandahålla kommissionen expertråd och stöd om frågor som rör internationellt erkännande av europeiska cybersäkerhetscertifikat i enlighet med artikel 87,

e) tillhandahålla kommissionen expertrådgivning och stöd i frågor som rör internationell standardisering och kontakter med relevanta internationella standardiseringsorganisationer, när så är relevant i samarbete med den europeiska gruppen för cybersäkerhetscertifiering som inrättats enligt artikel 90.

Avsnitt 2

Operativt samarbete

Artikel 10
Operativt samarbete på unionsnivå

1. Enisa ska stödja operativt samarbete mellan medlemsstaterna, unionsentiteter via CERT-EU och mellan andra intressenter.
2. Enisa ska vara medlem i det nätverk av nationella CSIRT-enheter som inrättats i enlighet med artikel 15.1 i direktiv (EU) 2022/2555 och ska tillhandahålla CSIRT-nätverkets sekretariat i enlighet med artikel 15.2 i direktiv (EU) 2022/2555.

3. Enisa ska tillhandahålla sekretariatet för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) i enlighet med artikel 16.2 andra stycket i direktiv (EU) 2022/2555.

4. Enisa ska stödja tekniskt och operativt samarbete mellan medlemsstaterna, i synnerhet genom CSIRT-nätverket och EU-CyCLONe. Detta stöd ska omfatta följande:

   a) Råd om förbättring av kapaciteten att förebygga, upptäcka, hantera och återhämta sig från incidenter.

   b) På begäran av en eller flera medlemsstater tillhandahålla råd och bedömningar med avseende på specifika potentiella eller pågående incidenter eller cyberhot, däribland genom att tillhandahålla expertis och underlätta den tekniska hanteringen av sådana incidenter, och genom att stödja frivilligt utbyte av relevant information och tekniska lösningar mellan medlemsstaterna.

   c) Analysera sårbarheter, hot och incidenter.

   d) På begäran av en eller flera medlemsstater, ge stöd till tekniska efterhandsundersökningar av betydande incidenter i den mening som avses i artikel 23.3 i direktiv (EU) 2022/2555.

   e) Bidra till att stödja den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå, i synnerhet genom att bistå EU-CyCLONe i arbetet med att utarbeta rapporter för den politiska nivån och genom att främja ett snabbt informationsutbyte mellan CSIRT-nätverket och EU-CyCLONe.

5. På begäran av en medlemsstat eller en unionsentitet ska Enisa i samarbete med CERT-EU stödja konsekvent kommunikation till allmänheten om en incident eller ett cyberhot.

6. Enisa ska stödja samarbete mellan medlemsstaterna och genom CERT-EU mellan unionsentiteter när det gäller införandet av säkra kommunikationsverktyg. Enisa ska inom CSIRT-nätverket och EU-CyCLONe använda säkra kommunikationsverktyg som tillhandahålls av juridiska enheter som är etablerade eller bedöms vara etablerade i unionen och som kontrolleras av medlemsstater eller av medborgare i medlemsstater.

Artikel 11
Gemensam situationsmedvetenhet på cybersäkerhetsområdet

1. För att uppnå en förbättrad gemensam situationsmedvetenhet om cyberhot- och incidentbilden hos medlemsstaterna och unionsentiteter ska Enisa göra följande:

   a) I samarbete med EU-CyCLONe, CSIRT-nätverket, kommissionen, CERT-EU, Europol och andra relevanta unionsentiteter utveckla databaser med verifierad och tillförlitlig underrättelseinformation om cyberhot, inbegripet trender i fråga om incidenter, taktik, teknik och förfaranden.

   b) I enlighet med artikel 12 utfärda tidiga varningar vid en potentiell eller pågående betydande eller storskalig incident, eller ett cyberhot av potentiellt gränsöverskridande art, i synnerhet när det gäller sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.

c) Tillhandahålla snabba och aktuella analyser om framväxande trender i fråga om incidenter, på begäran av CSIRT-nätverket, EU-CyCLONe eller kommissionen.

d) På begäran av medlemsstater eller kommissionen tillhandahålla analys eller annan information om faktiska eller uppfattade cybersäkerhetsrisker eller cyberhot.

e) Tillhandahålla analys och tekniska råd om cybersäkerhetsrisker i produkter med digitala element, däribland för att stödja marknadskontrollen och genom att vartannat år utarbeta en teknisk rapport om nya trender i enlighet med artikel 17.3 i förordning (EU) 2024/2847.

f) Utarbeta en regelbunden djupgående teknisk lägesrapport om cybersäkerheten i EU som behandlar incidenter och cyberhot, och göra denna rapport tillgänglig för rådet, EU-CyCLONe, CSIRT-nätverket, kommissionen, Europeiska utrikestjänsten och Europol.

g) Övervaka trender i fråga om tekniker, krav och konsekvenser av angrepp med utpressningsprogram och förse kommissionen, CSIRT-nätverket, EU-CyCLONe och Europol med information om sådana trender.

2. För att uppnå en förbättrad gemensam situationsmedvetenhet om cyberhot- och incidentbilden hos intressenterna ska Enisa göra följande:

a) Utföra analyser av cyberhot, incidenter, trender, framväxande teknik och konsekvenserna av dessa, inklusive en regelbunden analys av sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och relevanta produktkategorier som omfattas av förordning (EU) 2024/2847.

b) I samarbete med kommissionen och, när så är lämpligt, CSIRT-nätverket, utfärda råd, vägledning och bästa praxis avseende säkerheten i nätverks- och informationssystem, i synnerhet säkerheten för infrastrukturer som stöder de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.

c) Göra långsiktiga strategiska analyser av cyberhot och cybersäkerhetsincidenter i syfte att identifiera framväxande trender och bidra till att förebygga incidenter.

3. Enisa får offentliggöra analyser, råd, vägledning, bästa praxis och rapporter som avses i punkt 2, i samförstånd med de bidragande entiteter som avses i punkt 2.

4. Vid utförandet av de uppgifter som anges i punkterna 1 a–d, 1 f och 2 ska Enisa använda sina egna analyser och, när så är lämpligt, information som byrån fått i samband med utförandet av sina uppgifter, däribland följande:

a) Information från allmänt tillgängliga källor, inklusive allmänt kända sårbarheter i IKT-produkter eller IKT-tjänster som finns tillgängliga i den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555.

b) Information som förmedlats av medlemsstater, unionsentiteter, CERT-EU, partner inom privat sektor eller icke-statliga partner samt tredjelandsorganisationer och internationella organisationer, med förbehåll för eventuella begränsningar av vidarespridningen av informationen som anges med en synlig märkning.

5. Enisa ska ha ett nära samarbete med medlemsstaterna vid utarbetandet av den tekniska lägesrapport om cybersäkerheten som avses i punkt 1 e. Lägesrapporten ska baseras på offentlig information, Enisas egna analyser samt rapporter som Enisa får från bland andra medlemsstaternas CSIRT-enheter eller de gemensamma kontaktpunkter som inrättats genom direktiv (EU) 2022/2555, båda på frivillig grund, samt EC3 och CERT-EU. I samförstånd med de bidragande entiteterna får Enisa offentliggöra en aggregerad version av lägesrapporten.

Artikel 12
Tidiga varningar

1. Tidiga varningar enligt artikel 11.1 första stycket b i denna förordning ska innehålla relevant information om en potentiell eller pågående betydande eller storskalig incident, eller ett cyberhot av potentiellt gränsöverskridande art, i synnerhet när det gäller sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555. Sådan information får innefatta allmänt kända sårbarheter och uppgift om huruvida de påverkar produkter med digitala element som omfattas av förordning (EU) 2024/2847, samt tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer och rekommendationer om begränsningsåtgärder.
2. Tidiga varningar enligt artikel 11.1 första stycket b ska utfärdas snarast möjligt till berörd(a) CSIRT-enhet(er) och, när så är lämpligt, till CSIRT-nätverket och EU-CyCLONe.
3. Enisa ska erbjuda en tjänst för tidig varning till entiteter som bedriver verksamhet inom sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.
4. Den tjänst som avses i punkt 3 ska tillhandahållas på entitetens begäran och i ett maskinläsbart format som görs allmänt tillgängligt. Tjänsten ska inbegripa information om indikatorer på cyberhot och rekommendationer om begränsningsåtgärder.
5. Enisa ska inrätta ett förfarande för att sprida de tidiga varningarna till de entiteter som avses i punkt 3.

Artikel 13
Stöd till incidenthantering och granskning

1. Enisa ska driva och administrera EU-cybersäkerhetsreserven, helt eller delvis, i enlighet med förordning (EU) 2025/38.
2. På begäran av kommissionen eller EU-CyCLONe ska Enisa, med stöd av CSIRT-nätverket och med de berörda medlemsstaternas godkännande, granska och analysera betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter i enlighet med artikel 21 i förordning (EU) 2025/38.
3. Enisa ska i samarbete med Europol och CSIRT-enheterna eller andra behöriga myndigheter, såsom tillämpligt, bistå enskilda väsentliga och viktiga entiteter som förtecknas i bilagorna I och II i direktiv (EU) 2022/2555 i samband med beredskapen inför, hanteringen av och återhämtningen från en incident med utpressningsprogram. För detta ändamål ska Enisa inrätta en helpdesk och i synnerhet utnyttja den förbättrade gemensamma situationsmedvetenheten om cyberhot- och incidentbilden i enlighet med artikel 11.1 första stycket a och g i denna förordning.

Artikel 14
Cybersäkerhetsövningar på unionsnivå

1. Enisa ska stödja kommissionen i utarbetandet av ett löpande årligt program med cybersäkerhetsövningar på unionsnivå.

2. Enisa ska upprätthålla en databas över lärdomar från de övningar som avses i punkt 1 och ge medlemsstaterna och, när så är relevant, unionsentiteterna rekommendationer om hur dessa lärdomar ska omsättas i handling på ett ändamålsenligt och effektivt sätt.

3. På begäran av EU-CyCLONe eller kommissionen ska Enisa anordna, eller bidra till anordnandet av, cybersäkerhetsövningar på unionsnivå, inbegripet för att testa beredskapen att hantera storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på unionsnivå.

4. På begäran av medlemsstaterna ska Enisa stödja dessa vid anordnandet av nationella cybersäkerhetsövningar.

5. På begäran av CERT-EU ska Enisa bidra till anordnandet av cybersäkerhetsövningar som anordnas av CERT-EU i enlighet med artikel 13.7 i förordning (EU, Euratom) 2023/2841.

Artikel 15
Tillhandahållande av verktyg och plattformar

1. Enisa ska inrätta, tillhandahålla, driva, underhålla och uppdatera, såsom nödvändigt, operativa tekniska verktyg, inbegripet plattformar för cybersäkerhet på unionsnivå, i synnerhet den gemensamma rapporteringsplattform som inrättats i enlighet med artikel 16.1 i förordning (EU) 2024/2847 [och den gemensamma kontaktpunkt för incidentrapportering som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555], och testverktyg till stöd för genomförandet av förfaranden för bedömning av överensstämmelse i enlighet med relevant unionslagstiftning.

2. När så är lämpligt för tillämpningen av punkt 1 ska Enisa samarbeta och utbyta information med CSIRT-nätverket och, i tillämpliga fall, marknadskontrollmyndigheter.

Artikel 16
Sårbarhetshanteringstjänster

Enisa ska utveckla en gemensam unionskapacitet för sårbarhetshanteringstjänster och erbjuda intressenterna sårbarhetshanteringstjänster genom att

a) underhålla den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555,

b) förse intressenterna med sårbarhetshanteringstjänster, på grundval av den europeiska sårbarhetsdatabasen och med utnyttjande av den relevanta information som Enisa har tillgång till,

c) när så är lämpligt, ingå strukturerat samarbete med organisationer som tillhandahåller program, register eller databaser som liknar den europeiska sårbarhetsdatabasen,

d) aktivt stödja CSIRT-enheter som utsetts till samordnare i enlighet med artikel 12.1 i direktiv (EU) 2022/2555 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat,

e) utveckla och underhålla metoder och styrningsmekanismer för identifiering av sårbarheter och samordnad information om sådana, i samarbete med nationella behöriga myndigheter, CSIRT-enheter, branschen och forskarsamhället.

Avsnitt 3

Cybersäkerhetscertifiering och standardisering

Artikel 17
Cybersäkerhetscertifiering

1. Enisa ska bidra till och främja utvecklingen och genomförandet av unionens politik för cybersäkerhetscertifiering i enlighet med avdelning III i denna förordning. Enisa ska ansvara för följande:

   a) Utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordningar*) för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus i enlighet med artikel 74 och, i tillämpliga fall, utarbeta tekniska specifikationer i enlighet med artikel 77.

   b) Underhålla antagna europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 75, bland annat med sikte på en eventuell översyn av de antagna europeiska ordningarna för cybersäkerhetscertifiering i enlighet med artikel 76.

   c) Främja användningen av antagna ordningar och underhålla en särskild webbplats med information om och offentliggörande av europeiska ordningar för cybersäkerhetscertifiering, europeiska cybersäkerhetscertifikat och EU-intyg om överensstämmelse i enlighet med artikel 79.

   d) Organisera kapacitetsuppbyggnad för certifieringsprocesser, utvärderingsverksamhet, inbördes granskning och inbördes bedömning, däribland genom att ge stöd till medlemsstaterna på deras begäran i enlighet med artikel 6.12.

2. Enisa ska stödja kommissionen i följande arbetsuppgifter:

   a) Styrningen av den europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 90.

   b) Organiserandet av en europeisk församling för cybersäkerhetscertifiering i enlighet med artikel 72.1.

   c) Frågor som rör det internationella erkännandet av europeiska cybersäkerhetscertifikat i enlighet med artikel 87.

   d) Anordnandet av inbördes granskningar enligt artikel 89.

   e) Utarbetandet av standardbestämmelser som det kan hänvisas till i de europeiska ordningarna för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus i enlighet med artikel 81.5.

Artikel 18
Standardisering, tekniska specifikationer och vägledning

1. Enisa ska utarbeta tekniska specifikationer och vägledning till stöd för genomförandet av unionslagstiftningen på cybersäkerhetsområdet. Vid utarbetandet av dessa tekniska specifikationer ska Enisa beakta befintliga europeiska och internationella standarder samt andra relevanta tekniska specifikationer. Enisa ska säkerställa att dess tekniska specifikationer och vägledningar är konsekventa.

2. Enisa ska övervaka och, när så är relevant, delta i och leda arbetet med att utveckla standardiseringen på unionsnivå och, i enlighet med artikel 9, på internationell nivå, för att stödja unionens politik på cybersäkerhetsområdet.

3. Enisa ska stödja utvecklingen och utvärderingen av krypteringsalgoritmer. Vid ett positivt utfall av Enisas utvärdering av en krypteringsalgoritm ska Enisa samarbeta, i enlighet med förordning (EU) nr 1025/2012, med europeiska standardiseringsorgan för att stödja dess standardisering.

4. Enisa ska ge kommissionen och, när så är relevant, medlemsstaterna tekniska råd om lämpliga standarder eller tekniska specifikationer till stöd för unionens cybersäkerhetspolitik, inbegripet harmoniserad unionslagstiftning på cybersäkerhetsområdet, i synnerhet förordning (EU) 2024/2847, tekniska områden enligt artikel 25 i direktiv (EU) 2022/2555 och europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 81.1 d.

5. Enisa ska bistå kommissionen i bedömningen av förslag till harmoniserade standarder för att stödja genomförandet av harmoniserad unionslagstiftning på cybersäkerhetsområdet.

6. Enisa ska främja användningen av europeiska och internationella standarder för cybersäkerhet.

7. Enisa ska utföra de uppgifter som avses i punkterna 1–6 med integritet, opartiskhet och konfidentialitet, vilket inbegriper att avsluta eller pausa sitt deltagande i enskilda tekniska organ när ett sådant deltagande står i strid med andra uppgifter eller mål.

Avsnitt 4
Genomförande av EU-akademin för cyberkompetens

Artikel 19
Den europeiska kompetensramen för cybersäkerhet

1. Enisa ska utarbeta och offentliggöra en europeisk kompetensram för cybersäkerhet (*kompetensramen*). Innan kompetensramen offentliggörs eller uppdateras i enlighet med punkt 4 ska Enisa samråda med kommissionen.

2. Kompetensramen ska fastställa profiler för yrkesverksamma på cybersäkerhetsområdet och kopplingen av specifika uppgifter, färdigheter och kunskaper till en viss yrkesprofil. Användningen av kompetensramen ska vara frivillig för offentliga och privata entiteter.

3. Enisa får samråda med intressenter vid utvecklingen och spridningen av kompetensramen.

4. Enisa ska regelbundet bedöma behovet av uppdateringar av kompetensramen och vid behov uppdatera den.

Artikel 20

Utveckling, antagande och underhåll av ordningar för europeiska individuella intyg om cybersäkerhetskompetens

1. Enisa ska utveckla, anta och underhålla ordningar för europeiska individuella intyg om cybersäkerhetskompetens. Användningen av ordningar för europeiska individuella intyg om cybersäkerhetskompetens ska vara frivillig för nationella offentliga organ och privata entiteter, om inte annat anges i nationell lagstiftning.

2. Innan en ny ordning för europeiska individuella intyg om cybersäkerhetskompetens inleds ska Enisa samråda med kommissionen. Enisa får endast anta en sådan ordning om kommissionen avgett ett positivt yttrande. Vid utarbetandet av en ordning för europeiska individuella intyg om cybersäkerhetskompetens får Enisa konsultera relevanta intressenter.

3. En ordning för europeiska individuella intyg om cybersäkerhetskompetens ska omfatta följande:

   a) Intygsordningens innehåll och tillämpningsområde baserat på kompetensramens yrkesprofiler och undergrupper till dessa.

   b) Krav tillämpliga på individer som utbildats för att göra bedömningar (*bedömare*) i enlighet med artikel 21 samt nödvändiga färdigheter, kunskaper och erfarenheter och utbildningsmetoder.

   c) Analys av marknadsgenomslaget för varje intygsordning.

   d) Läranderesultat, bedömningsmetoder och villkor som auktoriserade tillhandahållare av intyg ska använda för att utvärdera i vilken mån en individ uppvisar de färdigheter som krävs i enlighet med artikel 21.

   e) I tillämpliga fall, en eller flera kompetensnivåer.

   f) Regler om hur auktoriserade tillhandahållare av intyg ska bevara uppgifter.

   g) Innehållet i och formatet för europeiska individuella intyg om cybersäkerhetskompetens, med vederbörlig hänsyn till artikel 21.5 e.

   h) Längsta giltighetstid för europeiska individuella intyg om cybersäkerhetskompetens som utfärdats enligt intygsordningen.

4. En ordning för europeiska individuella intyg om cybersäkerhetskompetens får inkludera den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens.

5. Enisa ska säkerställa ett nära samarbete med medlemsstaterna under hela arbetet med att utarbeta ordningar för europeiska individuella intyg om cybersäkerhetskompetens.

6. En ändring av en ordning för europeiska individuella intyg om cybersäkerhetskompetens ska inte påverka den auktorisation som beviljats i enlighet med artikel 22.3 a utan den ska förbli giltig under den period som den beviljats för.

Artikel 21

Auktoriserade tillhandahållare av intyg

1. Auktoriserade tillhandahållare av intyg ska bedöma om individer uppfyller kraven i en ordning för europeiska individuella intyg om cybersäkerhetskompetens och ska om dessa krav uppfylls utfärda europeiska individuella intyg om cybersäkerhetskompetens. Tillhandahållare av intyg kan inneha flera auktorisationer,

där varje enskild auktorisation beviljats för en viss ordning för europeiska individuella intyg för cybersäkerhetskompetens.

2. Enisa ska tillhandahålla vägledning för och genomföra obligatorisk utbildning av bedömare med avseende på de krav och bedömningsmetoder som ingår i ordningen för europeiska individuella intyg om cybersäkerhetskompetens enligt artikel 20.3 b.

3. Entiteter som önskar bli auktoriserade tillhandahållare av intyg eller som önskar förnya sin auktorisation (*sökande*) ska lämna en ansökan till Enisa. De ska uppfylla följande krav:

   a) De ska vara en juridisk person.

   b) De ska kunna utföra de uppgifter som fastställs i denna förordning när det gäller europeiska individuella intyg om cybersäkerhetskompetens, oavsett om den auktoriserade tillhandahållaren av intyg själv utför bedömningen eller om bedömningen utförs för denna tillhandahållares räkning och på dess ansvar.

   c) De ska ha de nödvändiga medlen för att på lämpligt sätt kunna utföra de tekniska och administrativa uppgifterna i samband med ordningen för europeiska individuella intyg om cybersäkerhetskompetens och ska ha tillgång till all den utrustning och alla de faciliteter som krävs.

   Vid tillämpning av första stycket led b gäller att om underleverantörer eller utomstående konsulter anlitas ska detta vara väl dokumenterat, det ska inte inbegripa mellanhänder och det ska finnas ett skriftligt avtal som bland annat ska innehålla bestämmelser om sekretess och intressekonflikter.

4. Sökande får inte vara högriskleverantörer.

5. Auktoriserade tillhandahållare av intyg ska fullgöra följande skyldigheter:

   a) För genomförandet av varje ordning för europeiska individuella intyg om cybersäkerhetskompetens ska de

      i) förfoga över de bedömare och den personal de behöver för att i rätt tid utföra sin verksamhet i enlighet med den berörda ordningen,

      ii) säkerställa att bedömarna iakttar tystnadsplikt, är opartiska och utför sitt arbete på ett oberoende sätt och med högsta grad av yrkesintegritet,

      iii) har skriftliga förfaranden för att utföra sin verksamhet inom ramen för den ordning som de är auktoriserade för,

   b) inte bedöma eller utfärda europeiska individuella intyg om cybersäkerhetskompetens till sina egna bedömare,

   c) säkerställa, om relevant genom att vidta lämpliga skyddsåtgärder, att deras bedömare kan utföra sitt arbete på ett oberoende sätt, i synnerhet i de fall då dessa individer ingår i deras egen struktur eller är anställda eller studerande i en sådan struktur,

   d) inte delta i någon verksamhet som kan påverka deras bedömares objektivitet eller integritet,

   e) på individens begäran säkerställa att elektroniska intyg för de europeiska individuella intygen om cybersäkerhetskompetens som utfärdas som elektroniska attributsintyg i ett format som kan lagras i europeiska digitala identitetsplånböcker enligt förordning (EU) nr 910/2014.

6. Auktoriserade tillhandahållare av intyg ska omedelbart underrätta Enisa ifall något av de krav som anges i punkterna 3 och 4 eller de skyldigheter som anges i punkt 5 inte längre uppfylls eller om det uppstår tvivel om ifall dessa krav uppfylls, exempelvis beträffande bedömares oberoende.

7. Auktoriserade tillhandahållare av intyg får ta ut en avgift från individer för bedömningen och utfärdandet av europeiska individuella intyg om cybersäkerhetskompetens, med beaktande av den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens i enlighet med artikel 20.4 vilken offentliggjorts på en särskild webbplats i enlighet med artikel 23 d.

8. De sökande och de auktoriserade tillhandahållarna av intyg ska tillåta att Enisa utför utvärderingar som ett led i ansökningsprocessen för eller upprätthållandet av auktorisationen och ska dela med sig av all relevant information för att säkerställa att de krav som anges i punkterna 3 och 4, eller de skyldigheter som anges i punkt 5, är uppfyllda eller fortsätter att uppfyllas i enlighet med artikel 22.2.

Artikel 22

Granskning av ansökningar om att bli auktoriserad tillhandahållare av intyg och upprätthållande av auktorisationer

1. Sökande ska betala en avgift till Enisa för granskningen av deras ansökan. Auktoriserade tillhandahållare av intyg ska betala en avgift till Enisa för upprätthållandet av deras auktorisation.

2. Enisa ska utvärdera om de krav som fastställs i artikel 21.3 och 21.4 och de skyldigheter som fastställs i artikel 21.5 är uppfyllda eller fortsätter att uppfyllas av sökande och auktoriserade tillhandahållare av intyg.

3. Efter granskning av en ansökan mot kraven i artikel 21.3 och 21.4 får Enisa utfärda ett av följande beslut:

   a) Bevilja den sökande status som auktoriserad tillhandahållare av intyg eller förnya denna status.

   b) Avslå ansökan om att bli auktoriserad tillhandahållare av intyg eller besluta att inte förnya denna status.

   c) Avsluta ansökningsprocessen på grund av att den sökande inte har reagerat på en begäran om kompletterande information från Enisa.

   Enisa får ändra, tillfälligt upphäva eller återkalla sådana beslut på grundval av sin utvärdering i enlighet med artikel 22.2 eller i det fall som avses i artikel 21.6.

4. Enisa ska utfärda det beslut som avses i punkt 3 inom tre månader från den dag då ansökningen inkom i enlighet med artikel 21.3. I de fall då Enisa har begärt kompletterande information från den sökande ska byrån utfärda det beslut som avses i punkt 3 inom en månad från den dag då den kompletterande informationen inkom.

5. Det beslut som avses i punkt 3 a ska ha en maximal varaktighet på tre år och avgiften för det årliga upprätthållandet av auktorisationen ska anges.

6. Enisa ska säkerställa att dess verksamhet i samband med utvecklingen och antagandet av ordningar för europeiska individuella intyg om cybersäkerhetskompetens enligt artikel 20 är strikt åtskild från och utförs oberoende av verksamheten i samband med granskning av ansökningar och utvärdering enligt punkterna 2 och 3 i den här artikeln.

Artikel 23
Information till allmänheten

Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande:

a) Den europeiska kompetensramen för cybersäkerhet och dess tidsplan för uppdatering.

b) Ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, deras framsteg och tidsplaner för utvecklingen av dem.

c) De avgifter som är förknippade med varje ordning för europeiska individuella intyg om cybersäkerhetskompetens som antagits i enlighet med artikel 47 i denna förordning.

d) Den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens i enlighet med artikel 20.4.

e) En förteckning över auktoriserade tillhandahållare av intyg.

Kapitel III
Enisas organisation

Artikel 24
Enisas förvaltnings- och ledningsstruktur

Enisas förvaltnings- och ledningsstruktur ska bestå av

a) en styrelse som ska utföra de uppgifter som anges i artikel 28,

b) en direktion som ska utföra de uppgifter som anges i artikel 30,

c) en verkställande direktör med det ansvar som anges i artikel 32,

d) en vice verkställande direktör med det ansvar som anges i artikel 34,

e) Enisas rådgivande grupp,

f) en överklagandenämnd som ska utföra de uppgifter som anges i artiklarna 39–42.

Avsnitt 1
Styrelse

Artikel 25
Styrelsens sammansättning

1. Styrelsen ska bestå av en ledamot per medlemsstat, utsedd av respektive medlemsstat, och två ledamöter som utses av kommissionen. Samtliga ledamöter ska ha rösträtt.

2. Varje ledamot av styrelsen ska ha en suppleant. Suppleanterna ska företräda ledamöterna i deras frånvaro.

3. Varje medlemsstat ska utse chefen för en nationell behörig myndighet som utsetts i enlighet med artikel 8.1 i direktiv (EU) 2022/2555 till styrelseledamot. Om det visar sig att detta inte är genomförbart ska medlemsstaten utse en högnivårepresentant för en nationell behörig myndighet som utsetts i enlighet med artikel 8.1 i direktiv (EU) 2022/2555 till styrelseledamot.

4. De ledamöter som utses av kommissionen och suppleanterna i styrelsen ska utses mot bakgrund av deras kunskaper inom området cybersäkerhet, med hänsyn till relevanta färdigheter i fråga om ledarskap, administration och budget. När det gäller suppleanterna ska kommissionen och medlemsstaterna sträva efter en jämn könsfördelning i styrelsen och bemöda sig om att begränsa omsättningen av suppleanter för att säkerställa kontinuitet i styrelsens arbete.

5. Mandatperioden för de ledamöter som utses av medlemsstaterna ska vara lika lång som den tid de innehar den roll som avses i punkt 3.

6. Mandatperioden för suppleanterna och de ledamöter som utses av kommissionen ska vara fyra år. Mandatperioden får förnyas.

Artikel 26
Styrelsens ordförande

1. Styrelsen ska välja en ordförande och en vice ordförande bland sina röstberättigade ledamöter. Ordföranden och vice ordföranden ska väljas med två tredjedelars majoritet av de röstberättigade styrelseledamöterna.

2. Vice ordföranden ska automatiskt ersätta ordföranden om den senare är förhindrad att fullgöra sina plikter.

3. Ordförandens och vice ordförandens mandatperiod ska vara fyra år och får förnyas en gång. Om deras uppdrag som styrelseledamot upphör någon gång under deras mandatperiod upphör mandatperioden automatiskt vid denna tidpunkt.

Artikel 27
Styrelsens sammanträden

1. Ordföranden ska sammankalla styrelsens sammanträden.

2. Den verkställande direktören ska delta i styrelsens sammanträden utan rösträtt.

3. Styrelsen ska hålla minst två ordinarie sammanträden per år. Dessutom ska styrelsen sammanträda på ordförandens initiativ, på kommissionens begäran eller på begäran av minst en tredjedel av dess ledamöter.

4. En företrädare för Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, som inrättades genom förordning (EU) 2021/887, ska vara permanent observatör utan rösträtt vid styrelsens sammanträden.

5. Styrelsen får bjuda in personer vars synpunkter kan vara av intresse att delta i ett sammanträde, eller en del av ett sammanträde, som en tillfällig observatör utan rösträtt och i enlighet med styrelsens arbetsordning.

6. Styrelseledamöterna och deras suppleanter får, med förbehåll för styrelsens arbetsordning, låta sig biträdas av rådgivare eller experter vid styrelsens sammanträden.

Artikel 28
Styrelsens uppgifter

1. Styrelsen ska göra följande:

   a) Fastställa de allmänna riktlinjerna för Enisas arbete och säkerställa att Enisa agerar i enlighet med de regler och principer som fastställs i denna förordning;

den ska även säkerställa att Enisas arbete överensstämmer med det arbete som utförs av medlemsstaterna och på unionsnivå.

b) Anta Enisas utkast till samlat programdokument som avses i artikel 44 innan det överlämnas till kommissionen för yttrande.

c) Med beaktande av kommissionens yttrande anta Enisas samlade programdokument i enlighet med artikel 29.2 a.

d) Övervaka genomförandet av det fleråriga och årliga program som ingår i det samlade programdokumentet.

e) Anta Enisas årsbudget i enlighet med artikel 29.2 b och utföra andra uppgifter rörande Enisas budget i enlighet med kapitel IV.

f) Bedöma och anta den konsoliderade årliga rapporten om Enisas verksamhet, inklusive räkenskaperna och en beskrivning av hur Enisa har uppnått sina resultatindikatorer, senast den 1 juli följande år sända både den årliga rapporten och bedömningen av denna till Europaparlamentet, rådet, kommissionen och revisionsrätten samt offentliggöra den årliga rapporten.

g) Anta de finansiella regler som ska tillämpas på Enisa i enlighet med artikel 50.

h) Anta en bedrägeribekämpningsstrategi som står i proportion till bedrägeririskerna med beaktande av en kostnads-nyttoanalys av de åtgärder som ska genomföras.

i) Säkerställa lämplig uppföljning av slutsatserna och rekommendationerna från interna eller externa revisionsrapporter och utvärderingar samt från utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och Europeiska åklagarmyndigheten (Eppo).

j) Anta sin arbetsordning, inbegripet regler för preliminära beslut om delegeringen av särskilda uppgifter enligt artikel 30.7.

k) Med avseende på Enisas personal och i enlighet med punkt 2 i denna artikel utöva de befogenheter som i tjänsteföreskrifterna för tjänstemän i Europeiska unionen (*tjänsteföreskrifterna*) och i anställningsvillkoren för övriga anställda i Europeiska unionen (*anställningsvillkoren*), som fastställs i rådets förordning (EEC, Euratom, EKSG) nr 259/68[73], tilldelas tillsättningsmyndigheten och den myndighet som har befogenhet att sluta anställningsavtal (*befogenheter som tillsättningsmyndighet*).

l) Anta genomförandebestämmelser för att ge verkan åt tjänsteföreskrifterna och anställningsvillkoren i enlighet med artikel 110.2 i tjänsteföreskrifterna.

m) Utse den verkställande direktören och, om den beslutar att inrätta funktionen som vice verkställande direktör, utse den vice verkställande direktören samt i förekommande fall förlänga deras mandatperiod eller avsätta dem i enlighet med artikel 31.

n) Utse en räkenskapsförare, som omfattas av tjänsteföreskrifterna och anställningsvillkoren, som ska vara helt oberoende i sin tjänsteutövning.

[73] EGT L 56, 4.3.1968, s. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

o) Fatta alla beslut som rör inrättandet av Enisas interna strukturer och, vid behov, ändringar av dessa interna strukturer, med beaktande av Enisas verksamhetsbehov och en sund budgetförvaltning.

p) Godkänna ingåendet av samarbetsavtal med avseende på artikel 68.

q) Godkänna ingåendet av samarbetsavtal i enlighet med artikel 70.

r) Utse och avsätta överklagandenämndens ledamöter i enlighet med artikel 29.2 d.

s) Anta regler för att förebygga och hantera intressekonflikter bland överklagandenämndens ledamöter.

2. Styrelsen ska, i enlighet med artikel 110.2 i tjänsteföreskrifterna, anta ett beslut grundat på artikel 2.1 i tjänsteföreskrifterna och artikel 6 i anställningsvillkoren om att delegera relevanta befogenheter som tillsättningsmyndighet till den verkställande direktören och fastställa på vilka villkor denna delegering av befogenheter kan dras in. Den verkställande direktören får vidaredelegera dessa befogenheter.

3. Vid exceptionella omständigheter får styrelsen anta ett beslut om att tillfälligt dra in delegeringen till den verkställande direktören av befogenheterna som tillsättningsmyndighet samt de befogenheter som tillsättningsmyndighet som den verkställande direktören vidaredelegerat, och i stället själv utöva dem eller delegera dem till en av sina ledamöter eller till någon annan anställd än den verkställande direktören.

Artikel 29
Omröstningsbestämmelser för styrelsen

1. Styrelsen ska anta sina beslut med absolut majoritet av sina ledamöter med rösträtt, om inte annat föreskrivs i denna förordning.

2. Två tredjedels majoritet av de röstberättigade styrelseledamöterna ska krävas för

a) antagande av det samlade programdokument som avses i artikel 28.1 c,

b) antagande av den årsbudget som avses i artikel 28.1 e,

c) utnämning av, förlängning av mandatperioden för eller avsättning av den verkställande direktören och den vice verkställande direktören som avses i artiklarna 31 och 33,

d) utnämning och avsättning av överklagandenämndens ledamöter i enlighet med artikel 36.

3. Beslut om budget- eller personalfrågor, särskilt frågor som avses i artikel 28.1 c, e, f, g, h, i, k, l, m och n, ska endast antas om kommissionens företrädare avger en positiv röst. Vid antagandet av de beslut som avses i artikel 28.1 c rörande Enisas samlade programdokument ska en positiv röst från kommissionens företrädare krävas endast avseende de delar av beslutet som inte rör Enisas årliga och fleråriga arbetsprogram.

4. Varje röstberättigad styrelseledamot ska ha en röst. I en röstberättigad ledamots frånvaro ska suppleanten ha rätt att utöva ledamotens rösträtt.

5. Styrelsens ordförande ska delta i omröstningen.

6. Den verkställande direktören ska inte delta i omröstningen.

7. Närmare bestämmelser om röstningsförfarandena, i synnerhet på vilka villkor en ledamot får agera på en annan ledamots vägnar, ska fastställas i styrelsens arbetsordning.

Avsnitt 2
Direktion

Artikel 30
Direktion

1. Styrelsen ska bistås av en direktion.

2. Direktionen ska

   a) förbereda beslut som ska antas av styrelsen,

   b) tillsammans med styrelsen säkerställa lämplig uppföljning av slutsatser och rekommendationer från interna eller externa revisionsrapporter och utvärderingar samt från utredningar som utförs av Olaf och Eppo,

   c) utan att det påverkar den verkställande direktörens ansvar enligt artikel 32 bistå och ge råd till den verkställande direktören vid genomförandet av styrelsens beslut, i syfte att förstärka övervakningen av den administrativa och budgetära förvaltningen.

3. Direktionen ska bestå av styrelsens ordförande, kommissionens företrädare i styrelsen och tre andra ledamöter som utses av styrelsen bland dess ledamöter med rösträtt. Styrelsens ordförande ska också vara ordförande i direktionen. Utnämningarna av ledamöter i direktionen ska syfta till att uppnå en jämn könsfördelning i direktionen. Den verkställande direktören ska delta i direktionens sammanträden utan rösträtt.

4. Mandatperioden för ledamöterna i direktionen ska vara fyra år. Mandatperioden får förnyas. Mandatperioden för ledamöterna i direktionen ska löpa ut när uppdraget som styrelseledamot upphör.

5. Direktionen ska hålla minst ett ordinarie sammanträde var tredje månad. Dessutom ska direktionen sammanträda på ordförandens initiativ eller på begäran av ledamöterna.

6. Direktionens arbetsordning ska fastställas av styrelsen.

7. Vid behov får direktionen, i brådskande fall, fatta vissa preliminära beslut på styrelsens vägnar, särskilt i frågor som rör den administrativa ledningen, inklusive om indragning av delegeringen av befogenheterna som tillsättningsmyndighet och budgetfrågor. Sådana preliminära beslut ska utan onödigt dröjsmål meddelas styrelsen. Styrelsen ska besluta huruvida det preliminära beslutet ska godkännas eller avslås senast tre månader efter att beslutet fattades. Direktionen får inte fatta beslut för styrelsens räkning som kräver godkännande av två tredjedels majoritet av styrelsens röstberättigade ledamöter.

Avsnitt 3
Verkställande direktör

Artikel 31

Utnämning, uppsägning och förlängning av mandatperioden

1. Den verkställande direktören ska utses av styrelsen på grundval av meriter och färdigheter från en förteckning över kandidater som föreslagits av kommissionen efter ett öppet och transparent urvalsförfarande.

2. Den kandidat som styrelsen väljer ska före utnämningen ombes att göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

3. Den verkställande direktören ska vara tillfälligt anställd vid Enisa i enlighet med artikel 2 a i anställningsvillkoren.

4. I det avtal som sluts med den verkställande direktören ska Enisa företrädas av styrelsens ordförande.

5. Den verkställande direktörens mandatperiod ska vara fem år. I god tid före utgången av denna period ska kommissionen göra en bedömning på grundval av en utvärdering av den verkställande direktörens arbete och Enisas framtida uppgifter och utmaningar.

6. Styrelsen får på förslag av kommissionen, med beaktande av den bedömning som avses i punkt 5, förlänga den verkställande direktörens mandatperiod en gång med högst fem år.

7. En verkställande direktör vars mandat har förlängts får inte delta i ett annat urvalsförfarande för samma befattning vid slutet av den sammantagna mandatperioden.

8. Styrelsen ska underrätta Europaparlamentet om sin avsikt att förlänga den verkställande direktörens mandatperiod i enlighet med punkt 6. Inom tre månader före en sådan förlängning ska den verkställande direktören på anmodan göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

9. Den verkställande direktören får avsättas endast efter ett beslut av styrelsen på förslag av kommissionen.

Artikel 32

Den verkställande direktörens uppgifter och ansvar

1. Den verkställande direktören ska leda Enisa och ska vara ansvarig inför styrelsen.

2. Den verkställande direktören ska vara oberoende i sin tjänsteutövning och får varken be om eller ta emot instruktioner från någon regering eller något annat organ.

3. Den verkställande direktören ska på uppmaning rapportera till Europaparlamentet om resultatet av sitt arbete. Rådet får uppmana den verkställande direktören att rapportera om resultatet av sitt arbete.

4. Den verkställande direktören ska vara Enisas rättsliga företrädare.

5. Den verkställande direktören ska ansvara för genomförandet av de uppgifter som Enisa tilldelas i denna förordning. Den verkställande direktören ska i synnerhet göra följande:

   a) Säkerställa Enisas dagliga förvaltning.

   b) Genomföra de beslut som antas av styrelsen.

c) Säkerställa efterlevnad av Enisas finansiella regler.

d) Utarbeta utkastet till det samlade programdokumentet och lämna det till styrelsen för godkännande innan det lämnas till kommissionen för ett yttrande.

e) Genomföra det samlade programdokumentet och rapportera till styrelsen om dess genomförande.

f) Utarbeta Enisas konsoliderade årliga verksamhetsrapport, inbegripet genomförandet av Enisas årliga arbetsprogram, och lägga fram den för styrelsen för bedömning och antagande.

g) Utarbeta en handlingsplan för uppföljning av slutsatserna från efterhandsutvärderingarna av Enisa i enlighet med artikel 121 samt rapportera vartannat år till kommissionen om de framsteg som gjorts.

h) Utarbeta en handlingsplan för uppföljning av slutsatserna från interna eller externa revisionsrapporter och utvärderingar, liksom utredningar utförda av Olaf och Eppo, samt rapportera om läget vartannat år till kommissionen och regelbundet till styrelsen.

i) Utarbeta ett utkast till finansiella regler som ska tillämpas på Enisa i den mening som avses i artikel 50.

j) Upprätta Enisas preliminära beräkning av inkomster och utgifter och genomföra dess budget.

k) Skydda unionens finansiella intressen genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, utan att detta påverkar Olafs och Eppos behörighet att göra utredningar, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda belopp samt vid behov genom effektiva, proportionella och avskräckande administrativa och ekonomiska sanktioner.

l) Utarbeta en strategi för bedrägeribekämpning, en strategi för effektivitetsvinster och synergieffekter, en strategi för samarbete med tredjeländer eller internationella organisationer och en strategi för organisatorisk ledning och interna kontrollsystem för Enisa och lägga fram dem för styrelsen för godkännande.

m) Utveckla och underhålla kontakter med näringslivet och konsumentorganisationer för att säkerställa en regelbunden dialog med berörda intressenter.

n) Regelbundet utbyta synpunkter och information med berörda unionsentiteter om deras cybersäkerhetsverksamhet för att säkerställa att unionens policy genomförs på ett enhetligt sätt på det området.

o) Främja mångfald och en jämn könsfördelning vid rekryteringen av Enisas personal.

p) Anta ordningar för europeiska individuella intyg om cybersäkerhetskompetens, som avses i artikel 20.1.

q) Anta beslut med avseende på ansökningar om att bli auktoriserade tillhandahållare av intyg eller om att förnya en auktorisation, i den mening som avses i artikel 22.3.

r) Utföra andra uppgifter som den verkställande direktören tilldelas genom denna förordning.

6. När så är nödvändigt och inom ramen för Enisas mål och uppgifter, får den verkställande direktören inrätta arbetsgrupper bestående av experter, inbegripet experter från medlemsstaternas behöriga myndigheter. Den verkställande direktören ska underrätta styrelsen om detta i förväg. Förfarandena avseende i synnerhet sammansättningen av arbetsgrupperna, den verkställande direktörens tillsättning av arbetsgruppernas experter och arbetsgruppernas arbete ska anges i Enisas interna verksamhetsregler.

7. Där så är nödvändigt för att Enisa ska kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt och grundat på en ändamålsenlig kostnads-nyttoanalys, får den verkställande direktören besluta att inrätta ett eller flera lokala kontor i en eller flera medlemsstater. Innan den verkställande direktören beslutar att inrätta ett lokalt kontor ska han eller hon inhämta ett yttrande från den eller de berörda medlemsstaterna, däribland den medlemsstat där Enisa har sitt säte, och ett förhandsgodkännande från kommissionen och styrelsen. Om oenighet råder under samrådsprocessen mellan den verkställande direktören och de berörda medlemsstaterna ska frågan överlämnas till rådet för diskussion. Det sammanlagda antalet anställda vid alla lokala kontor ska begränsas till ett minimum och inte uppgå till över 40 % av antalet anställda vid Enisa i den medlemsstat där Enisa har sitt säte. Antalet anställda vid varje lokalt kontor ska inte uppgå till över 10 % av antalet anställda vid Enisa i den medlemsstat där Enisa har sitt säte.

8. I beslutet om att inrätta ett lokalt kontor ska man ange omfattningen av den verksamhet som ska bedrivas vid det lokala kontoret på ett sådant sätt att onödiga kostnader och överlappning av Enisas administrativa uppgifter undviks.

Avsnitt 4
Vice verkställande direktör

Artikel 33
Vice verkställande direktör

1. Styrelsen får besluta att inrätta funktionen vice verkställande direktör, med uppgift att bistå den verkställande direktören.

2. Om styrelsen beslutar att inrätta funktionen vice verkställande direktör ska bestämmelserna i artikel 31 vara tillämpliga på den vice verkställande direktören.

Artikel 34
Den vice verkställande direktörens uppgifter och ansvar

Den vice verkställande direktören ska bistå den verkställande direktören i förvaltningen av Enisa och i utförandet av de uppgifter som avses i artikel 32. Om den verkställande direktören är frånvarande eller har förhinder, eller om tjänsten är ledig, ska den vice verkställande direktören agera som ersättare under frånvaron eller till dess att tjänsten är tillsatt.

Avsnitt 5
Enisas rådgivande grupp

Artikel 35
Enisas rådgivande grupp

1. Styrelsen ska, på förslag av den verkställande direktören, på ett transparent sätt inrätta Enisas rådgivande grupp. Enisas rådgivande grupp ska bestå av allmänt erkända experter som företräder berörda intressenter, såsom cybersäkerhetsbranschen, IKT-branschen, små och medelstora företag, entiteter som är verksamma inom de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, tillverkare av produkter med digitala element och förvaltare av programvara med fri och öppen källkod i den mening som avses i förordning (EU) 2024/2847, organ för bedömning av överensstämmelse som anmälts enligt den europeiska ram för cybersäkerhetscertifiering som avses i artikel 93 och förordning (EU) 2024/2847, entiteter som är verksamma inom medel för elektronisk identifiering, konsumentgrupper, akademiska experter på cybersäkerhetsområdet, europeiska standardiseringsorganisationer samt brottsbekämpande myndigheter och tillsynsmyndigheter för dataskydd. Dessa erkända experter ska vara medborgare i medlemsstaterna. Styrelsen ska sträva efter att säkerställa lämplig könsfördelning, geografisk fördelning samt fördelning mellan olika intressentgrupper.

2. Förfaranden för Enisas rådgivande grupp, i synnerhet avseende gruppens sammansättning, det förslag från den verkställande direktören som avses i punkt 1, medlemsantal, utnämning av gruppens medlemmar och den rådgivande gruppens arbete, ska anges i Enisas interna verksamhetsregler och ska offentliggöras.

3. Den verkställande direktören eller en person som han eller hon utser från fall till fall ska vara ordförande för Enisas rådgivande grupp.

4. Mandatperioden för medlemmarna i Enisas rådgivande grupp ska vara två och ett halvt år och kan förnyas en gång. Styrelseledamöter får inte vara medlemmar i Enisas rådgivande grupp. Experter från kommissionen och experter från medlemsstaterna får närvara vid sammanträdena i Enisas rådgivande grupp och delta i dess arbete. Den verkställande direktören får bjuda in företrädare för andra organ som inte är medlemmar av Enisas rådgivande grupp att närvara vid den rådgivande gruppens sammanträden och delta i dess arbete.

5. Enisas rådgivande grupp ska ge Enisa råd med avseende på genomförandet av Enisas verksamhet, med undantag av tillämpningen av avdelningarna III, IV och V i denna förordning. Den ska i synnerhet ge den verkställande direktören råd om utarbetandet av förslaget till Enisas årliga arbetsprogram och om kommunikationen med berörda intressenter om frågor kopplade till det årliga arbetsprogrammet.

6. Enisas rådgivande grupp ska regelbundet informera styrelsen om sin verksamhet.

7. Enisa ska tillhandahålla det logistiska stöd som Enisas rådgivande grupp behöver samt sekretariatshjälp för dess sammanträden.

Avsnitt 6
Överklagandenämnd

Artikel 36
Inrättande och sammansättning av överklagandenämnden

1. Enisa ska inrätta en överklagandenämnd genom ett styrelsebeslut.

2. Överklagandenämnden ska bestå av en ordförande och tre andra ledamöter. Varje ledamot av överklagandenämnden ska ha en suppleant. Suppleanten ska företräda ledamoten i dennas frånvaro.

3. Styrelsen ska utse ordföranden, de övriga ledamöterna och deras suppleanter från en förteckning över kvalificerade sökande som fastställts av kommissionen. Förteckningen över kvalificerade sökande ska vara giltig i fyra år. Styrelsen kan på förslag av kommissionen förlänga förteckningens giltighet med ytterligare fyraårsperioder.

4. Överklagandenämnden får begära att styrelsen utser ytterligare två ledamöter och deras suppleanter från den förteckning som avses i punkt 3 om den anser att ärendet så kräver.

5. Överklagandenämnden ska själv anta och offentliggöra sin arbetsordning.

Artikel 37
Överklagandenämndens ledamöter

1. Mandatperioden för överklagandenämndens ledamöter och suppleanter ska vara fyra år. Styrelsen kan på förslag av kommissionen förnya mandatperioden med ytterligare fyraårsperioder.

2. Överklagandenämndens ledamöter ska vara oberoende och ska inte utföra andra uppgifter inom Enisa. I sitt beslutsfattande får de varken be om eller ta emot instruktioner från någon regering, något annat organ eller någon privat entitet.

3. Under mandatperioden får överklagandenämndens ledamöter inte avsättas eller strykas ur förteckningen över kvalificerade sökande, såvida det inte finns allvarliga skäl till en sådan avsättning eller strykning och styrelsen, på förslag av kommissionen, fattar ett beslut om detta.

Artikel 38
Uteslutning och invändning

1. Överklagandenämndens ledamöter får inte delta i ett överklagandeförfarande om de har personliga intressen i förfarandet, om de tidigare har representerat någon av parterna i förfarandet eller om de varit med om att anta det beslut som överklagas.

2. Om ledamöter av en överklagandenämnd anser att de, av något av de skäl som förtecknas i punkt 1 eller av andra skäl, inte bör delta i ett överklagandeförfarande ska de meddela överklagandenämnden detta.

3. En part i ett överklagandeförfarande får invända mot en ledamot i överklagandenämnden på någon av de grunder som anges i punkt 1, eller om ledamoten misstänks vara partisk. En sådan invändning ska inte godtas om parten har inlett förfarandet med vetskap om att det fanns skäl att invända. Ingen invändning får göras på grund av överklagandenämndsledamöternas nationalitet.

4. Överklagandenämnden ska besluta om vilka åtgärder som ska vidtas i de fall som anges i punkterna 2 och 3 utan att den berörda ledamoten deltar. Vid beslutet ska den berörda ledamoten i överklagandenämnden ersättas av sin suppleant.

Artikel 39
Överklagande av beslut och av underlåtenhet att agera

1. Följande får överklagas till överklagandenämnden:

   a) Beslut som antagits av Enisa i enlighet med artikel 22.3.

   b) Enisas underlåtenhet att agera inom de tillämpliga tidsfrister som anges i artikel 22.4.

2. Ett överklagande enligt punkt 1 ska bli föremål för omprövning i enlighet med artikel 41 innan det läggs fram för överklagandenämnden för prövning.

3. Ett överklagande enligt punkt 1 ska inte ha suspensiv verkan.

Artikel 40
Personer som har rätt att överklaga, tidsfrist och form

1. Sökande i den mening som avses i artikel 21.3 får överklaga

   a) ett beslut av Enisa riktat till dem, i enlighet med artikel 22.3,

   b) Enisas underlåtenhet att agera på en ansökan som de lämnat in till Enisa inom de tillämpliga tidsfrister som anges i artikel 22.4.

2. I det fall som avses i punkt 1 a ska överklagandet, tillsammans med en motivering, lämnas in skriftligen i enlighet med den arbetsordning som avses i artikel 36.5 inom två månader från den dag då beslutet delgavs den berörda sökanden eller, om inget delgivande har skett, den dag då sökanden fick kännedom om beslutet.

3. I det fall som avses i punkt 1 b ska överklagandet lämnas in skriftligen till Enisa i enlighet med den arbetsordning som avses i artikel 36.5 inom två månader från den dag då den tidsfrist som anges i artikel 22.4 löper ut.

Artikel 41
Omprövning

1. Om Enisa anser att överklagandet kan tas upp till prövning och är välgrundat ska byrån ändra beslutet eller avhjälpa den underlåtenhet att agera som avses i artikel 40.1.

2. Om Enisa inte ändrar beslutet inom en månad från mottagandet av överklagandet ska byrån omedelbart besluta om tillämpningen av beslutet ska skjutas upp och hänskjuta överklagandet till överklagandenämnden.

Artikel 42
Prövning av beslut om överklaganden

1. Överklagandenämnden ska, inom tre månader från det att överklagandet lämnats in, besluta att bifalla eller ogilla överklagandet. Vid prövningen av ett överklagande ska överklagandenämnden agera inom de tidsfrister som fastställs i dess arbetsordning. Den ska vid behov anmoda parterna att inom viss tid inkomma med synpunkter på meddelanden från nämnden eller på inlagor från andra parter i överklagandeförfarandet. Parterna i överklagandeförfarandet ska ha rätt att göra muntliga framställningar.

2. Om överklagandenämnden godtar grunderna för överklagandet ska den hänskjuta ärendet till Enisa. När Enisa fattar sitt slutgiltiga beslut ska den rätta sig efter

överklagandenämndens slutsatser och motivera sitt beslut. Enisa ska underrätta parterna i överklagandeförfarandet om det beslutet.

Artikel 43
Talan inför Europeiska unionens domstol

1. Talan om ogiltigförklaring av Enisas beslut som antagits i enlighet med artikel 22.3, eller talan om underlåtenhet att agera inom de tillämpliga tidsfristerna i enlighet med artikel 22.4, får väckas vid Europeiska unionens domstol efter att det överklagandeförfarande inom Enisa som föreskrivs i artiklarna 39–42 har uttömts eller om åtgärder inte har vidtagits inom den tillämpliga tidsfristen i enlighet med artikel 41.2.
2. Enisa ska vidta alla de åtgärder som krävs för att följa Europeiska unionens domstols avgörande.

Avsnitt 7
Verksamhet

Artikel 44
Samlat programdokument

1. Enisa ska genomföra sin verksamhet i enlighet med ett samlat programdokument som innehåller byråns årliga och fleråriga arbetsprogram, vilket ska inbegripa all planerad verksamhet.
2. Den verkställande direktören ska varje år utarbeta ett utkast till samlat programdokument, som avses i punkt 1, med motsvarande planering av ekonomiska resurser och personalresurser i överensstämmelse med artikel 32 i kommissionens delegerade förordning (EU) 2019/715[74] och med hänsyn till kommissionens riktlinjer.
3. Senast den 30 november varje år ska styrelsen anta det samlade programdokument som avses i punkt 1, med beaktande av det yttrande från kommissionen som avses i artikel 32.7 i delegerad förordning (EU) 2019/715. Om styrelsen beslutar att inte beakta vissa aspekter av kommissionens yttrande ska den lämna en utförlig motivering till det beslutet. Styrelsen ska senast den 31 januari följande år översända det samlade programdokumentet, liksom eventuella senare uppdaterade versioner, till Europaparlamentet, rådet och kommissionen.
4. Det samlade programdokumentet ska anses vara slutgiltigt efter det att unionens allmänna budget slutligen har antagits och ska vid behov anpassas i enlighet därmed.
5. Det årliga arbetsprogrammet ska innehålla detaljerade mål och förväntade resultat, inklusive resultatindikatorer. Det ska också innehålla en beskrivning av de åtgärder som ska finansieras och uppgifter om vilka ekonomiska resurser och personalresurser som anslås till varje åtgärd, i enlighet med principerna om verksamhetsbaserad budgetering och förvaltning. Det årliga arbetsprogrammet ska överensstämma med

[74] Kommissionens delegerade förordning (EU) 2019/715 av den 18 december 2018 med rambudgetförordning för de organ som inrättats enligt EUF-fördraget och Euratomfördraget och som avses i artikel 70 i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 (EUT L 122, 10.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

det fleråriga arbetsprogram som avses i punkt 7. I programmet ska det klart anges vilka uppgifter som lagts till, ändrats eller strukits jämfört med föregående räkenskapsår.

6. Styrelsen ska ändra det antagna årliga arbetsprogrammet om Enisa tilldelas en ny uppgift. Varje betydande ändring av det årliga arbetsprogrammet ska antas enligt samma förfarande som det ursprungliga årliga arbetsprogrammet. Styrelsen får delegera befogenheten att göra icke-väsentliga ändringar i det årliga arbetsprogrammet till den verkställande direktören.

7. I det fleråriga arbetsprogrammet ska den övergripande strategiska programplaneringen, inbegripet mål, förväntade resultat och resultatindikatorer, fastställas. Även resursplanering, inklusive flerårig budget och personal, ska fastställas.

8. Resursplaneringen ska uppdateras årligen. Den strategiska programplaneringen ska uppdateras när det är lämpligt, och i synnerhet när det är nödvändigt för att beakta resultatet av den utvärdering som avses i artikel 120.

KAPITEL IV
Upprättande av Enisas budget och budgetens struktur

Artikel 45
Upprättande av Enisas budget

1. Den verkställande direktören ska varje år göra ett preliminärt utkast till beräkning av Enisas inkomster och utgifter för påföljande budgetår, inbegripet tjänsteförteckningen, och översända det till styrelsen.

2. Det preliminära utkastet till beräkning ska baseras på målen i och de förväntade resultaten av det årliga arbetsprogrammet, och i enlighet med principen om sund ekonomisk förvaltning och prestation ska där beaktas vilka ekonomiska resurser som behövs för att uppnå dessa mål och förväntade resultat.

3. På grundval av det preliminära utkastet till beräkning ska styrelsen anta en preliminär beräkning av Enisas inkomster och utgifter för påföljande budgetår och översända den till kommissionen senast den 31 januari varje år.

4. Kommissionen ska översända utkastet till beräkning till budgetmyndigheten tillsammans med förslaget till unionens allmänna budget. Utkastet till beräkning ska också göras tillgängligt för Enisa.

5. På grundval av utkastet till beräkning ska kommissionen ta upp de medel den anser vara nödvändiga för tjänsteförteckningen och det bidrag som ska belasta unionens allmänna budget i det förslag till unionens allmänna budget som kommissionen ska lägga fram för budgetmyndigheten i enlighet med artiklarna 313 och 314 i EUF-fördraget.

6. Budgetmyndigheten ska bevilja anslagen från unionens allmänna budget till Enisa.

7. Budgetmyndigheten ska anta Enisas tjänsteförteckning.

8. Styrelsen ska anta Enisas budget. Budgeten blir slutlig när unionens allmänna budget slutligen antas, och ska vid behov anpassas i enlighet därmed.

9. Alla byggprojekt som kan komma att påverka Enisas budget väsentligt ska omfattas av delegerad förordning (EU) 2019/715.

Artikel 46
Enisas budgets struktur

1. Alla Enisas inkomster och utgifter ska beräknas varje budgetår och redovisas i Enisas budget. Budgetåret ska motsvara kalenderåret.

2. Enisas budget ska vara balanserad i fråga om inkomster och utgifter.

3. Utan att det påverkar andra medel ska Enisas inkomster bestå av

   a) ett bidrag från unionen, vilket tas upp i unionens allmänna budget,

   b) inkomster avsatta för särskilda ändamål i enlighet med Enisas finansiella regler som avses i artikel 50,

   c) unionsfinansiering i form av överenskommelser om medverkan eller ad hoc-bidrag, i enlighet med de finansiella regler för Enisa som avses i artikel 50 och med bestämmelserna i relevanta instrument till stöd för unionens politik,

   d) de avgifter som tas ut av sökande för verksamhet som rör de ordningar för europeiska individuella intyg om cybersäkerhetskompetens som avses i artikel 22.1,

   e) de avgifter som tas ut av organen för bedömning av överensstämmelse för deltagande i och utfärdande av europeiska cybersäkerhetscertifikat inom ramen för en europeisk ordning för cybersäkerhetscertifiering i den mening som avses i artikel 47.2,

   f) de avgifter som tas ut av myndigheter eller privata organ för de testverktyg som avses i artikel 47.3,

   g) eventuella bidrag från tredjeländer som deltar i Enisas arbete i enlighet med artikel 70.4,

   h) eventuella frivilliga bidrag från medlemsstater i pengar eller in natura.

4. Medlemsstater som ger frivilliga bidrag, i den mening som avses i punkt 3 g, får inte göra anspråk på några särskilda rättigheter eller tjänster som en följd av bidragen.

5. Enisas utgifter ska omfatta löner till personalen, kostnader för administration och infrastruktur samt driftskostnader.

Artikel 47
Avgifter

1. För varje verksamhet inom den europeiska certifieringsordning som avses i artikel 22.1 ska avgifter tas ut av sökande i den mening som avses i artikel 21.3 eller av auktoriserade tillhandahållare av intyg, för att bidra till att täcka de totala kostnaderna för Enisas verksamhet, för följande:

   a) Utfärdande av auktorisationer efter granskning av de krav som anges i artikel 21.3 och 21.4, inbegripet genomförande av utvärderingar.

   b) Årligt upprätthållande av auktorisationen.

   c) Förnyande av auktorisationer för tillhandahållare av europeiska individuella intyg om cybersäkerhetskompetens, inbegripet genomförande av utvärderingar.

2. När det gäller certifiering ska följande avgifter tas ut av organen för bedömning av överensstämmelse för upprätthållandet av europeiska ordningar för cybersäkerhetscertifiering enligt vilka europeiska cybersäkerhetscertifikat utfärdas:

   a) En årlig avgift för deltagande i en europeisk ordning för cybersäkerhetscertifiering.

   b) En avgift för utfärdande av europeiska cybersäkerhetscertifikat enligt europeiska ordningar för cybersäkerhetscertifiering.

   De avgifter som avses i led b ska tas ut när organet för bedömning av överensstämmelse lämnar in europeiska cybersäkerhetscertifikat till Enisa för offentliggörande på byråns webbplats i enlighet med artikel 79.

3. När det gäller de testverktyg som avses i artikel 15.1 ska en avgift tas ut av alla myndigheter eller privata organ som använder dem.

4. Alla avgifter ska anges och betalas i euro.

5. Kommissionen ska anta genomförandeakter med närmare regler om fastställande av de avgifter som Enisa ska ta ut, och i synnerhet ange de uppskattade kostnader som kan hänföras till var och en av de tjänster för vilka avgifter enligt punkterna 1, 2 och 3 tas ut, de enskilda avgiftsbelopp som ska tas ut samt hur och på vilka villkor avgifterna bör betalas. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2. Kommissionen ska samråda med Enisa när den utarbetar dessa utkast till genomförandeakter.

6. De avgifter som fastställs genom de genomförandeakter som avses i punkt 5 ska anges i förväg för att stå i proportion till de uppskattade kostnaderna för den verksamhet som utförs eller de tjänster som tillhandahålls, fastställda på ett kostnadseffektivt sätt, och ska vara tillräckliga för att täcka dessa kostnader. Enisas alla utgifter för personal som deltar i verksamhet som avses i punkterna 1, 2 och 3 ska återspeglas i de kostnader som ska täckas. Avgifterna ska fastställas på en sådan nivå att ett underskott eller en betydande ackumulering av överskott i Enisas budget undviks. Budgetöverskott som genereras genom avgifter ska föras över för att finansiera Enisas verksamhet, särskilt framtida avgiftsrelaterad verksamhet, eller kompensera för uppkomna förluster. Om ett betydande positivt saldo i budgeten till följd av verksamhet som omfattas av avgifter blir återkommande, eller om ett betydande negativt saldo uppstår till följd av tillhandahållandet av tjänster som omfattas av avgifter, ska kommissionen ändra de genomförandeakter som avses i punkt 5 för att se över metoden för beräkning av avgifterna i enlighet med artikel 118.2.

   Avgiftsbeloppen för de uppgifter som avses i punkt 1 ska fastställas till en nivå som säkerställer att intäkterna från dessa i tillräcklig utsträckning bidrar till att täcka kostnaderna för verksamhet som rör utveckling och underhåll av ordningar för europeiska individuella intyg, handläggningen av ansökningar och utfärdande och förnyelse av auktorisationer samt vad som behövs för dessa tillsynsåtgärder från Enisas sida.

   Avgiftsbeloppen för de uppgifter som avses i punkt 2 ska fastställas till en nivå som säkerställer att intäkterna från dessa i tillräcklig utsträckning bidrar till att täcka de totala kostnaderna för verksamhet som rör upprätthållandet av de europeiska ordningar för cybersäkerhetscertifiering som avses i artikel 75.

Avgiftsbeloppen för de uppgifter som avses i punkt 3 ska fastställas till en nivå som säkerställer att intäkterna från dessa i tillräcklig utsträckning bidrar till att täcka kostnaderna för verksamhet som rör tillhandahållandet av testverktyg i enlighet med artikel 15.1.

7. Enisa ska tillhandahålla en rapport om de avgifter som tas ut och deras inverkan på byråns budget som en del av det förfarande för redovisning som fastställs i artikel 50.

8. Enisa ska införa en uppsättning indikatorer för att mäta arbetsbördan, ändamålsenligheten och effektiviteten i samband med verksamhet som finansieras genom avgifter. Enisa ska anpassa sin personalplanering och förvaltning av resurser i samband med avgifter i enlighet med detta för att på lämpligt sätt kunna tillgodose en sådan efterfrågan och eventuella fluktuationer i intäkterna från avgifter. Enisa ska dela rapporten med kommissionen, som får använda den som underlag för den utvärdering som avses i artikel 120.1.

Artikel 48
Genomförande av Enisas budget

1. Den verkställande direktören ska ansvara för genomförandet av Enisas budget och ska fungera som utanordnare.

2. Kommissionens internrevisor ska ha samma befogenheter gentemot Enisa som gentemot kommissionens avdelningar.

3. Den verkställande direktören ska varje år till budgetmyndigheten översända all information som rör resultatet av utvärderingsförfaranden.

Artikel 49
Redovisning och förfarande för att bevilja ansvarsfrihet

1. Enisas räkenskapsförare ska översända de preliminära räkenskaperna för räkenskapsåret (år n) till kommissionens räkenskapsförare och till revisionsrätten senast den 1 mars följande räkenskapsår (år n + 1).

2. Senast den 1 mars år n + 1 ska Enisas räkenskapsförare också förse kommissionens räkenskapsförare med de begärda räkenskaperna som ska tjäna som underlag för konsolideringen, på det sätt och i det format som kommissionens räkenskapsförare anger.

3. Senast den 31 mars år n + 1 ska Enisa översända rapporten om budgetförvaltningen och den ekonomiska förvaltningen för år n till Europaparlamentet, rådet, kommissionen och revisionsrätten.

4. När revisionsrättens iakttagelser om Enisas preliminära räkenskaper för år n har inkommit, ska Enisas räkenskapsförare på eget ansvar upprätta Enisas slutliga räkenskaper. Den verkställande direktören ska överlämna dem till styrelsen för ett yttrande.

5. Styrelsen ska avge ett yttrande om Enisas slutliga räkenskaper för år n.

6. Enisas räkenskapsförare ska senast den 1 juli år n + 1 översända de slutliga redovisningarna för år n till Europaparlamentet, rådet, kommissionen och revisionsrätten, tillsammans med styrelsens yttrande.

7. En länk till de webbsidor som innehåller Enisas slutliga räkenskaper ska offentliggöras i *Europeiska unionens officiella tidning* senast den 15 november år n + 1.

8. Senast den 30 september år n + 1 ska den verkställande direktören skicka ett svar till revisionsrätten om de iakttagelser som den framfört i sin årsrapport. Den verkställande direktören ska också skicka detta svar till styrelsen och till kommissionen.

9. Den verkställande direktören ska på Europaparlamentets begäran, i enlighet med artikel 267.3 i Europaparlamentets och rådets förordning (EU, Euratom) 2024/2509, för Europaparlamentet lägga fram alla uppgifter som är nödvändiga för att förfarandet för beviljande av ansvarsfrihet för år n ska kunna tillämpas på ett smidigt sätt.

10. På rekommendation av rådet, som ska fatta sitt beslut med kvalificerad majoritet, ska Europaparlamentet före den 15 maj år n + 2 bevilja den verkställande direktören ansvarsfrihet beträffande budgetens genomförande år n.

Artikel 50
Finansiella regler

1. De finansiella regler som ska tillämpas på Enisa ska antas av styrelsen efter samråd med kommissionen. De får inte avvika från delegerad förordning (EU) 2019/715 såvida inte en sådan avvikelse är specifikt nödvändig för Enisas verksamhet och kommissionen har lämnat sitt samtycke i förväg.

2. Enisa ska upprätta och genomföra sin budget i enlighet med sina finansiella regler och förordning (EU, Euratom) 2024/2509.

Artikel 51
Bedrägeribekämpning

1. Bestämmelserna i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013[75] ska tillämpas fullt ut på Enisas verksamhet i syfte att bekämpa bedrägeri, korruption och andra lagstridiga handlingar.

2. Enisa ska ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 mellan Europaparlamentet, Europeiska unionens råd och Europeiska gemenskapernas kommission om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf)[76] inom sex månader från och med den *[Publikationsbyrån, inför det exakta datum som anges i artikel 127]* och anta lämpliga bestämmelser som ska vara tillämpliga på byråns personal med hjälp av mallen i bilagan till det avtalet.

3. Revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och inspektioner på plats, hos alla stödmottagare, uppdragstagare och underleverantörer som erhållit unionsfinansiering från Enisa.

---

75 Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999 (EUT L 248, 18.9.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

76 EGT L 136, 31.5.1999, s. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

4. Olaf får i enlighet med bestämmelserna och förfarandena i förordning (EU, Euratom) nr 883/2013 och rådets förordning (Euratom, EG) nr 2185/96[77] göra utredningar, inklusive kontroller och inspektioner på plats, i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med bidrag eller avtal som finansierats av Enisa.

5. Utan att det påverkar tillämpningen av punkterna 1–4 ska samarbetsavtal med tredjeländer och internationella organisationer, kontrakt, bidragsavtal och bidragsbeslut från Enisa innehålla bestämmelser som uttryckligen tillerkänner revisionsrätten och Olaf rätten att utföra sådan revision och göra sådana utredningar inom ramen för sina respektive befogenheter.

6. I enlighet med rådets förordning (EU) 2017/1939 får Europeiska åklagarmyndigheten utreda och lagföra bedrägeri och annan olaglig verksamhet som påverkar unionens ekonomiska intressen, i enlighet med Europaparlamentets och rådets direktiv (EU) 2017/1371[78].

Artikel 52
Intresseförklaring

1. Styrelsens ledamöter, den verkställande direktören, den vice verkställande direktören och tjänstemän som är tillfälligt utstationerade av medlemsstaterna ska var och en avge en åtagandeförklaring och en förklaring som anger om det föreligger eller inte föreligger några direkta eller indirekta intressen som skulle kunna anses inverka negativt på deras oberoende. Förklaringarna ska vara korrekta och fullständiga, och de ska avges skriftligen varje år och uppdateras vid behov.

2. Styrelsens ledamöter, den verkställande direktören, den vice verkställande direktören och externa experter som deltar i tillfälliga arbetsgrupper ska var och en senast i inledningen av varje möte korrekt och fullständigt redovisa eventuella intressen som kan påverka deras oberoende i förhållande till frågorna på dagordningen samt avhålla sig från att delta i diskussioner och omröstningar om sådana frågor.

3. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om intresseförklaringar som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 53
Transparens

1. Enisa ska utföra sitt arbete med en hög grad av transparens och i enlighet med artikel 55.

2. Enisa ska säkerställa att allmänheten och eventuella berörda parter får lämplig, objektiv, tillförlitlig och lättillgänglig information, framför allt om resultaten av dess

[77] Rådets förordning (Euratom, EG) nr 2185/96 av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda Europeiska gemenskapernas finansiella intressen mot bedrägerier och andra oegentligheter (EGT L 292, 15.11.1996, s. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

[78] Europaparlamentets och rådets direktiv (EU) 2017/1371 av den 5 juli 2017 om bekämpande genom straffrättsliga bestämmelser av bedrägeri som riktar sig mot unionens finansiella intressen (EUT L 198, 28.7.2017, s. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

arbete. Enisa ska också offentliggöra de intresseförklaringar som avges i enlighet med artikel 52.

3. Styrelsen får, på förslag av den verkställande direktören, ge berörda parter tillstånd att observera delar av Enisas verksamhet.

4. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om transparens som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 54
Konfidentialitet inom Enisa

1. Enisa ska inte för tredje part röja uppgifter som byrån behandlar eller mottar om det i en motiverad ansökan har begärts att uppgifterna ska behandlas konfidentiellt, dock utan att detta påverkar tillämpningen av artikel 55.

2. Ledamöterna i styrelsen, den verkställande direktören, den vice verkställande direktören, medlemmarna i Enisas rådgivande grupp, de externa experter som deltar i olika tillfälliga arbetsgrupper och Enisas personal, inbegripet tjänstemän som är tillfälligt utstationerade av medlemsstaterna, ska omfattas av tystnadsplikt enligt artikel 339 i EUF-fördraget, även efter det att deras uppdrag har upphört.

3. Enisa ska i sina interna verksamhetsregler fastställa hur de regler om konfidentialitet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 55
Tillgång till handlingar

1. Förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos Enisa.

2. Styrelsen ska anta genomförandebestämmelser för förordning (EG) nr 1049/2001.

3. Beslut som fattas av Enisa i enlighet med artikel 8 i förordning (EG) nr 1049/2001 får bli föremål för ett klagomål till Europeiska ombudsmannen enligt artikel 228 i EUF-fördraget eller väckande av talan vid Europeiska unionens domstol enligt artikel 263 i EUF-fördraget.

KAPITEL V
Personal och kontaktpersoner

Artikel 56
Allmänna bestämmelser

1. Tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda samt de bestämmelser som har antagits gemensamt av unionens institutioner för tillämpningen av tjänsteföreskrifterna för tjänstemän och anställningsvillkoren för övriga anställda ska gälla för Enisas personal.

2. Enisas personal, kontaktpersonerna och nationella experter som har utstationerats till Enisa ska genomgå lämplig säkerhetsprövning.

Artikel 57
Privilegier och immunitet

Enisa och dess personal ska omfattas av protokoll nr 7 om Europeiska unionens immunitet och privilegier, fogat till EUF-fördraget.

Artikel 58
Kontaktpersoner

1. Varje medlemsstat ska från en nationell behörig myndighet som utsetts i enlighet med artikel 8.1 i direktiv (EU) 2022/2555 utse minst två kontaktpersoner som nationella experter utstationerade till Enisa för att arbeta vid dess säte eller lokala kontor, i enlighet med artikel 59.2. Kommissionen får också utse en kontaktperson.

2. Kontaktpersonerna ska bidra till utförandet av Enisas uppgifter, bland annat genom att underlätta det operativa samarbete och informationsutbyte som avses i artikel 11. Kontaktpersonerna ska också stödja Enisa i dess arbete med att informera relevanta intressenter runtom i unionen om byråns verksamhet, slutsatser och rekommendationer. De ska också fungera som nationella kontaktpunkter för frågor från sina medlemsstater och frågor som rör dessa medlemsstater, antingen genom att svara direkt på frågorna eller genom att ta kontakt med sina nationella förvaltningar.

3. De kontaktpersoner som utsetts av medlemsstater ska ha rätt att begära och ta emot all relevant information från sina medlemsstater i enlighet med denna förordning, samtidigt som de fullt ut ska respektera nationell rätt och medlemsstatens praxis, särskilt när det gäller dataskydd och konfidentialitet.

Artikel 59
Utstationerade nationella experter och annan personal

1. Enisa får använda sig av utstationerade nationella experter och annan personal som inte är anställd av Enisa på alla sina verksamhetsområden. Tjänsteföreskrifterna och anställningsvillkoren ska inte gälla för denna personal.

2. Styrelsen ska anta ett beslut om regler för utstationering av nationella experter, inbegripet kontaktpersoner, till Enisa.

KAPITEL VI
ALLMÄNNA BESTÄMMELSER FÖR ENISA

Artikel 60
Enisas rättsliga ställning

1. Enisa ska vara ett unionsorgan med ställning som juridisk person.

2. Enisa ska i varje medlemsstat ha den mest vittgående rättskapacitet som tillerkänns juridiska personer enligt den medlemsstatens nationella rätt. Enisa får särskilt förvärva eller avyttra lös och fast egendom och föra talan inför domstolar och andra myndigheter.

3. Enisa ska företrädas av den verkställande direktören.

Artikel 61
Säte

Enisa ska ha sitt säte i Aten, Grekland.

Artikel 62
Överenskommelse om säte och villkor för verksamheten

1. De nödvändiga bestämmelserna om de lokaler som ska tillhandahållas för Enisa i värdmedlemsstaten och de anläggningar som ska ställas till Enisas förfogande av den medlemsstaten, tillsammans med de särskilda regler i värdmedlemsstaten som ska tillämpas på den verkställande direktören, styrelseledamöterna, Enisas personal och deras familjemedlemmar, ska fastställas i en överenskommelse om säte mellan Enisa och värdmedlemsstaten, vilken ingås efter att ha godkänts av styrelsen.

2. Enisas värdmedlemsstat ska tillhandahålla bästa möjliga förutsättningar för att säkerställa en väl fungerande byrå, med beaktande av platsens tillgänglighet, adekvata utbildningsmöjligheter för personalens barn samt lämplig tillgång till arbetsmarknad, social trygghet och sjukvård för personalens barn och makar.

Artikel 63
Administrativ kontroll

Enisas verksamhet ska övervakas av Europeiska ombudsmannen i enlighet med artikel 228 i EUF-fördraget.

Artikel 64
Enisas ansvar

1. Enisas avtalsrättsliga ansvar ska regleras av den rätt som är tillämplig på avtalet i fråga.

2. Europeiska unionens domstol ska vara behörig att träffa avgöranden med stöd av en skiljedomsklausul i ett avtal som Enisa ingått.

3. Vad beträffar utomobligatoriskt ansvar ska Enisa enligt de allmänna principer som är gemensamma för medlemsstaternas rättsordningar ersätta skada som vållats av Enisa själv eller dess personal under tjänsteutövning.

4. Europeiska unionens domstol ska vara behörig i tvister om ersättning för sådana skador som avses i punkt 3.

5. Personalens personliga ansvar gentemot Enisa ska regleras av de bestämmelser i tjänsteföreskrifterna eller anställningsvillkoren som är tillämpliga på dem.

Artikel 65
Språkordning

1. Rådets förordning nr 1[79] ska gälla för Enisa. Medlemsstaterna och övriga organ som utsetts av medlemsstaterna kan vända sig till Enisa och har rätt att få svar på det officiella språk vid unionens institutioner som de själva väljer.

[79] Rådets förordning nr 1 om vilka språk som skall användas i Europeiska ekonomiska gemenskapen (EGT 17, 6.10.1958, s. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

2. Översättningstjänster och alla övriga språktjänster som Enisa behöver, med undantag för tolkning, ska tillhandahållas av Översättningscentrum för Europeiska unionens organ.

Artikel 66
Skydd av personuppgifter

1. Enisa ska behandla personuppgifter i enlighet med förordning (EU) 2018/1725.

2. Styrelsen ska anta de genomföranderegler som avses i artikel 45.3 i förordning (EU) 2018/1725. Styrelsen får anta ytterligare åtgärder som behövs för Enisas tillämpning av förordning (EU) 2018/1725.

Artikel 67
Säkerhetsbestämmelser om skydd av säkerhetsskyddsklassificerade uppgifter och känsliga icke-säkerhetsskyddsklassificerade uppgifter

I samförstånd med kommissionen ska Enisa anta säkerhetsbestämmelser som införlivar säkerhetsprinciperna i kommissionens säkerhetsbestämmelser för skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter, i enlighet med beslut (EU, Euratom) 2015/443[80] och 2015/444[81]. Dessa säkerhetsbestämmelser ska omfatta bestämmelser om utbyte, behandling och lagring av sådana uppgifter.

Artikel 68
Samarbete med unionsentiteter och nationella myndigheter

1. För att säkerställa enhetlighet, skapa synergieffekter och hantera frågor av gemensamt intresse ska Enisa i frågor som rör cybersäkerhet samarbeta med CERT-EU och relevanta unionsentiteter, däribland Europol, Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, som inrättats i enlighet med förordning (EU) 2021/887, och Europeiska dataskyddsstyrelsen, som inrättats i enlighet med artikel 68.1 i förordning (EU) 2016/679.

2. Det samarbete som avses i punkt 1 kan säkerställas genom

   a) utbyte av sakkunskap och bästa praxis,

   b) tillhandahållande av råd och utfärdande av riktlinjer om frågor som rör cybersäkerhet,

   c) inrättande av praktiska arrangemang för utförande av särskilda uppgifter, efter samråd med kommissionen.

3. Enisa ska ha ett strukturerat samarbete med CERT-EU, särskilt i frågor som rör kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot.

---

80 Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, s. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

4. Enisa ska samarbeta och utbyta information med relevanta marknadskontroll- och tillsynsmyndigheter som utsetts enligt unionslagstiftningen på cybersäkerhetsområdet, inbegripet förordning (EU) 2024/2847.

Artikel 69
Samarbete med intressenter

1. När det är nödvändigt för att uppnå målen med denna förordning ska Enisa samarbeta med berörda intressenter, såsom cybersäkerhetsbranschen, IKT-branschen, små och medelstora företag, entiteter som är verksamma inom de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, tillverkare, importörer eller distributörer av produkter med digitala element i den mening som avses i förordning (EU) 2024/2847, organ för bedömning av överensstämmelse som anmälts enligt det europeiska ramverket för cybersäkerhetscertifiering och förordning (EU) 2024/2847, entiteter vars verksamhet rör medel för elektronisk identifiering, konsumentgrupper samt akademiska experter på cybersäkerhetsområdet. Enisa får i detta syfte inrätta offentlig-privata partnerskap.

2. Enisa ska i samråd med kommissionen stödja samarbetet mellan anmälda organ för bedömning av överensstämmelse i enlighet med artikel 93. Byrån får i synnerhet inrätta en grupp av anmälda organ för bedömning av överensstämmelse för utbyte av bästa praxis och skapa synergieffekter med annan relevant unionslagstiftning, särskilt förordning (EU) 2024/2847.

Artikel 70
Samarbete med tredjeländer och internationella organisationer

1. I den mån det är nödvändigt för att uppnå målen med denna förordning får Enisa samarbeta med de behöriga myndigheterna i tredjeländer eller med internationella organisationer, eller båda, i linje med unionens prioriteringar. För detta ändamål får Enisa, efter förhandsgodkännande från kommissionen, upprätta samarbetsavtal med myndigheter i tredjeländer och med internationella organisationer. Dessa samarbetsavtal får inte medföra några juridiska förpliktelser för unionen och dess medlemsstater.

2. Styrelsen ska anta en strategi för förbindelserna med tredjeländer och internationella organisationer i de frågor som Enisa har behörighet för och i linje med de prioriteringar som avses i punkt 1. Kommissionen ska säkerställa att Enisa arbetar inom ramen för sitt mandat och den befintliga institutionella ramen genom att ingå lämpliga samarbetsavtal med Enisas verkställande direktör.

3. För att stödja samarbetet med tredjeländer, särskilt länder som är kandidater för anslutning till unionen, får Enisa bidra med sin sakkunskap om kapacitetsuppbyggnad i synnerhet på följande områden:

   a) Bedömning av nivån på cybersäkerhetskapaciteten och cybersäkerhetsresurserna.

   b) Utökning och kompetenshöjning av arbetskraften inom cybersäkerhet, inbegripet genom att främja den europeiska kompetensramen för cybersäkerhet och ordningarna för europeiska intyg om individuell cybersäkerhetskompetens samt genom att tillhandahålla lärande- och utbildningsverksamhet.

   c) Stöd till planeringen och genomförandet av cybersäkerhetsövningar.

4. Enisas verksamhet ska vara öppen för deltagande av tredjeländer som har ingått avtal med unionen i detta syfte. I enlighet med de relevanta bestämmelserna i avtal som har ingåtts mellan tredjeländer och unionen ska det, efter förhandsgodkännande från kommissionen, upprättas samarbetsavtal som särskilt anger i vilken form och utsträckning och på vilket sätt dessa tredjeländer ska delta i Enisas arbete, inklusive bestämmelser om deltagande i Enisas initiativ, om finansiella bidrag och om personal. När det gäller personalfrågor ska dessa samarbetsavtal under alla förhållanden vara förenliga med tjänsteföreskrifterna och anställningsvillkoren.

5. Enisa ska regelbundet rapportera till rådet och kommissionen om genomförandet av de samarbetsavtal som avses i punkterna 1 och 4.

AVDELNING III

EUROPEISKT RAMVERK FÖR CYBERSÄKERHETSCERTIFIERING

KAPITEL I
Mål, tillämpningsområde och förfaranden

Artikel 71

Det europeiska ramverket för cybersäkerhetscertifiering – mål och tillämpningsområde

1. Det europeiska ramverket för cybersäkerhetscertifiering ska inrättas i syfte att skapa en digital inre marknad för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteter. För detta ändamål ska det höja cybersäkerhetsnivån inom unionen och möjliggöra en harmoniserad ansats för europeiska ordningar för cybersäkerhetscertifiering samt med hjälp av certifieringen underlätta efterlevnaden av tillämplig unionslagstiftning.

2. Genom det europeiska ramverket för cybersäkerhetscertifiering ska en mekanism fastställas för att inrätta europeiska ordningar för cybersäkerhetscertifiering och för att intyga följande:

   a) Att de IKT-produkter, IKT-tjänster och IKT-processer som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos lagrade, överförda eller behandlade uppgifter eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, tjänster och processer under hela deras livscykel.

   b) Att utlokaliserade säkerhetstjänster som har utvärderats i enlighet med sådana ordningar uppfyller de angivna säkerhetskraven i syfte att skydda tillgänglighet, autenticitet, integritet och konfidentialitet hos uppgifter som är föremål för åtkomst, behandling, lagring eller överföring i samband med tillhandahållandet av dessa tjänster, och att dessa tjänster tillhandahålls kontinuerligt med erforderlig kompetens, sakkunskap och erfarenhet av personal med tillräcklig och lämplig nivå av relevant teknisk kunskap och yrkesintegritet.

   c) Att cybersäkerhetsstatusen hos en entitet som har utvärderats i enlighet med sådana ordningar uppfyller de angivna cybersäkerhetskraven.

3. Den europeiska cybersäkerhetscertifieringen ska vara frivillig, om inte annat anges i unionsrätten eller nationell rätt.

4. Ett europeiskt cybersäkerhetscertifikat och en EU-försäkran om överensstämmelse som utfärdats enligt det europeiska ramverket för cybersäkerhetscertifiering ska automatiskt erkännas i alla medlemsstater.

Artikel 72
Information till och samråd med allmänheten

1. Minst en gång om året ska kommissionen, med stöd av Enisa, sammankalla en europeisk församling för cybersäkerhetscertifiering dit den bjuder in medlemmar från den europeiska gruppen för cybersäkerhetscertifiering och andra relevanta experter från medlemsstaterna, relevanta experter från unionsentiteter och relevanta intressenter för att diskutera strategiska prioriteringar för harmonisering på området cybersäkerhetscertifiering.

2. Kommissionen ska upprätthålla och regelbundet uppdatera en särskild webbplats med information om följande:

   a) Europeiska ordningar för cybersäkerhetscertifiering avseende vilka utveckling begärts i enlighet med artikel 73.

   b) Strategiska prioriteringar för harmonisering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster, entiteters cybersäkerhetsstatus eller säkerhetskrav i unionslagstiftningen, inbegripet potentiella områden för vilka en europeisk ordning för cybersäkerhetscertifiering kan komma att begäras.

3. Kommissionen ska på den webbplats som avses i punkt 2 i denna artikel offentliggöra information om sin begäran till Enisa om att utarbeta ett förslag till certifieringsordning som avses i artikel 73 och sitt beslut att godta, avslå eller inte gå vidare med ett förslag till certifieringsordning som Enisa lämnat in i enlighet med artikel 74.7.

4. Under Enisas utarbetande av ett förslag till certifieringsordning enligt artikel 74 får Europaparlamentet och rådet begära att kommissionen, i egenskap av ordförande för den europeiska gruppen för cybersäkerhetscertifiering, och Enisa lägger fram relevant information om utkastet till förslag till certifieringsordning. På begäran av Europaparlamentet eller rådet får Enisa, i samförstånd med kommissionen och utan att det påverkar tillämpningen av artikel 54, göra relevanta delar av ett utkast till förslag till certifieringsordning tillgängliga för Europaparlamentet och rådet på ett sätt som är lämpligt med hänsyn till den konfidentialitetsnivå som krävs, och när så är lämpligt på ett begränsat sätt.

5. Europaparlamentet och rådet får uppmana kommissionen och Enisa att diskutera frågor som rör genomförandet av europeiska ordningar för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus.

Artikel 73

Begäranden om en europeisk ordning för cybersäkerhetscertifiering

1. Kommissionen får begära att Enisa utarbetar ett förslag till en europeisk ordning för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus.

2. I vederbörligen motiverade fall får den europeiska gruppen för cybersäkerhetscertifiering föreslå att kommissionen lägger fram en sådan begäran som avses i punkt 1.

3. Den begäran som avses i punkt 1 ska i detalj ange syftet med, omfattningen av och formerna för uppfyllandet av relevanta säkerhetsmål och säkerhetskomponenter som anges i artiklarna 80 och 81. Begäran ska också specificera utvecklingsplanen för förslaget till europeisk ordning för cybersäkerhetscertifiering och relevanta tekniska specifikationer som det ska hänvisas till eller som ska fastställas i certifieringsordningen.

4. När kommissionen utarbetar den begäran som avses i punkt 1 ska den vederbörligen samråda med Enisa och den europeiska gruppen för cybersäkerhetscertifiering samt beakta synpunkterna från alla berörda intressenter och andra unionsentiteter, inbegripet i tillämpliga fall de som är relevanta enligt unionslagstiftning med avseende på vilken en europeisk ordning för cybersäkerhetscertifiering påvisar regelefterlevnad och ger presumtion om överensstämmelse.

Artikel 74

Utarbetande och antagande av europeiska ordningar för cybersäkerhetscertifiering

1. Senast tolv månader efter att ha tagit emot en begäran från kommissionen i enlighet med artikel 73 ska Enisa, om inget annat anges i begäran, utarbeta ett förslag till en europeisk ordning för cybersäkerhetscertifiering som uppfyller kraven i artiklarna 80 och 81.

2. För utarbetandet av varje förslag till certifieringsordning ska Enisa inrätta en tillfällig arbetsgrupp i enlighet med artikel 32.6 i syfte att ge Enisa expertråd.

3. Vid utarbetandet av förslaget till certifieringsordning ska Enisa ha ett nära samarbete med den europeiska gruppen för cybersäkerhetscertifiering. Den europeiska gruppen för cybersäkerhetscertifiering ska ge Enisa bistånd och expertråd vid utarbetandet av förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer.

4. Vid utarbetandet av förslaget till certifieringsordning, i tillämpliga fall inbegripet stödjande tekniska specifikationer, ska Enisa i god tid samråda med intressenter genom en formell, öppen, transparent och inkluderande samrådsprocess. Enisa ska också samarbeta med relevanta myndigheter i medlemsstaterna och med relevanta unionsentiteter för att samla in deras expertråd i samband med utarbetandet av förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer. När Enisa översänder förslaget till certifieringsordning till kommissionen i enlighet med punkt 6 ska byrån beskriva på vilket sätt den har följt denna punkt.

5. Innan Enisa översänder förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer till kommissionen ska byrån begära att medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering lämnar

skriftliga yttranden om förslaget till certifieringsordning. Yttrandena ska lämnas senast 30 dagar efter dagen för begäran. Enisa ska ta största möjliga hänsyn till yttrandena från medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering. Om inga yttranden lämnas ska detta inte hindra Enisa från att översända förslaget till certifieringsordning till kommissionen.

6. Enisa ska översända förslaget till certifieringsordning till kommissionen senast 60 dagar efter dagen för den begäran som avses i punkt 5.

7. När kommissionen mottar förslaget till certifieringsordning ska den utvärdera om certifieringsordningen motsvarar den begäran som gjorts i enlighet med artikel 73. Inom 30 dagar efter det att förslaget till certifieringsordning översändes ska kommissionen vidta någon av följande åtgärder:

   a) Godta förslaget till certifieringsordning.

   b) Återsända förslaget till certifieringsordning till Enisa för översyn tillsammans med en motivering till att det återsänds samt en tidsfrist på högst 90 dagar, inom vilken Enisa ska tillhandahålla ett reviderat förslag till certifieringsordning.

   c) Besluta att inte gå vidare med förslaget till certifieringsordning.

8. Om kommissionen återsänder ett förslag till certifieringsordning till Enisa för översyn i enlighet med punkt 7 b ska punkterna 4, 5 och 7 tillämpas i enlighet med detta.

9. Kommissionen ges befogenhet att, på grundval av det godtagna förslaget till certifieringsordning som utarbetats av Enisa, anta genomförandeakter för en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som uppfyller kraven i artiklarna 80 och 81. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

10. Kommissionen får hänvisa till tekniska specifikationer som utarbetats av Enisa i de genomförandeakter som avses i punkt 9 i denna artikel, i enlighet med artiklarna 18 och 77.

11. Kommissionen får specificera villkoren för internationellt erkännande av europeiska cybersäkerhetscertifikat i de genomförandeakter som avses i punkt 9 i denna artikel, i enlighet med artikel 87.

Artikel 75

Underhåll av en europeisk ordning för cybersäkerhetscertifiering

1. För varje europeisk ordning för cybersäkerhetscertifiering ska det fastställas en underhållsstrategi. Underhållsstrategin ska beskriva förväntningarna när det gäller underhållsverksamhet, särskilt de som rör de standarder eller tekniska specifikationer som det hänvisas till i certifieringsordningen och samspelet med relevanta intressenter.

2. Enisa ska, i samarbete med kommissionen och med stöd av den europeiska gruppen för cybersäkerhetscertifiering och dess relevanta undergrupp för underhåll, säkerställa underhållet av de europeiska ordningarna för cybersäkerhetscertifiering, även med möjligheten att kommissionen kan se över dessa certifieringsordningar i

åtanke. Enisa ska samarbeta och utbyta information med relevanta unionsentiteter och unionsgrupper i samband med underhållsverksamhet.

3. Enisa får organisera den privata sektorns deltagande i underhållet av en certifieringsordning i form av en tillfällig arbetsgrupp i enlighet med den underhållsstrategi som avses i punkt 1.

4. Underhållet av europeiska ordningar för cybersäkerhetscertifiering ska omfatta följande:

   a) Utarbetande, uppdatering och godkännande av tekniska specifikationer och riktlinjer för att stödja en harmoniserad och enhetlig användning av certifieringsordningarna.

   b) Identifiering av standarder eller tekniska specifikationer som är relevanta för certifieringsordningen.

   c) Interaktioner och, när så är relevant, upprättande av kontakter med berörda intressenter, inbegripet europeiska eller internationella standardiseringsorganisationer, även för att lämna eller ta emot tekniska bidrag.

   d) Utfärdande av rekommendationer till kommissionen om nödvändiga förbättringar och uppdateringar av certifieringsordningarna, även med möjligheten att se över certifieringsordningarna i åtanke.

   e) Utbyte av information mellan medlemsstaterna om det praktiska genomförandet av certifieringsordningarna.

   f) Bidrag till mekanismer för inbördes granskning och inbördes bedömning och analyser av resultaten av sådana bedömningar för att förbättra certifieringsordningarnas funktion och stödja en eventuell översyn.

5. Den europeiska gruppen för cybersäkerhetscertifiering får avge ett yttrande om underhållet av europeiska ordningar för cybersäkerhetscertifiering.

Artikel 76

Utvärdering, översyn och återkallande av en europeisk ordning för cybersäkerhetscertifiering

1. Minst vart fjärde år efter det att en europeisk ordning för cybersäkerhetscertifiering har börjat tillämpas ska Enisa utvärdera certifieringsordningens verkningar och effektivitet, i samarbete med den berörda undergruppen för underhåll inom den europeiska gruppen för cybersäkerhetscertifiering samt med beaktande av återkopplingen från intressenterna. Enisa ska genomföra utvärderingen genom att utföra marknadsanalys i enlighet med artikel 8.1.

2. Till följd av den utvärdering som avses i punkt 1 får kommissionen se över eller återkalla genomförandeakter som föreskriver en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 74.9.

3. När kommissionen ser över eller återkallar europeiska ordningar för cybersäkerhetscertifiering ska den samråda med Enisa, den europeiska gruppen för cybersäkerhetscertifiering och dess berörda undergrupp för underhåll samt beakta synpunkter från berörda intressenter och andra unionsentiteter.

4. Den europeiska gruppen för cybersäkerhetscertifiering får avge ett yttrande om översyn eller återkallande av en europeisk ordning för cybersäkerhetscertifiering. Kommissionen ska ta vederbörlig hänsyn till detta när den ser över eller återkallar den europeiska ordningen för cybersäkerhetscertifiering.

Artikel 77

Tekniska specifikationer i europeiska ordningar för cybersäkerhetscertifiering

1. Enisa får utarbeta tekniska specifikationer med sikte på en framtida europeisk ordning för cybersäkerhetscertifiering eller till stöd för underhållet av en europeisk ordning för cybersäkerhetscertifiering.

2. De tekniska specifikationer som avses i punkt 1 i denna artikel ska utarbetas i god tid, med stöd av den europeiska gruppen för cybersäkerhetscertifiering och dess undergrupper för underhåll samt, i tillämpliga fall, motsvarande tillfälliga arbetsgrupp som avses i artikel 75.3. För detta ändamål ska Enisa också inhämta bidrag från relevanta intressentgrupper med beaktande av den underhållsstrategi som avses i artikel 75.1.

3. Om det hänvisas till tekniska specifikationer i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10 ska de göras tillgängliga på den webbplats som avses i artikel 79.

4. I vederbörligen motiverade fall, särskilt om de tekniska specifikationerna innehåller information som skulle kunna äventyra säkerheten för certifierade IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, ska de distribueras endast till de intressenter som berörs av certifieringsordningens krav. Det ska inte hänvisas till sådana tekniska specifikationer i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.

Artikel 78

Underlättande av efterlevnad av unionslagstiftningen

1. Om så föreskrivs i en viss unionsrättsakt ska ett certifikat som utfärdats enligt en europeisk ordning för cybersäkerhetscertifiering påvisa regelefterlevnad och ge presumtion om överensstämmelse med de motsvarande kraven i den rättsakten.

2. Utvärderingsverksamhet inom ramen för en europeisk ordning för cybersäkerhetscertifiering ska vara förenlig med motsvarande unionsrättsakt som föreskriver påvisandet av regelefterlevnad och presumtionen om överensstämmelse. Om ingen sådan utvärderingsverksamhet specificeras i motsvarande unionsrättsakt ska den specificeras i certifieringsordningen. En bedömning av överensstämmelse för certifiering som ger presumtion om överensstämmelse med kraven i unionslagstiftningen ska utföras av ett tredjepartsorgan.

3. I avsaknad av harmoniserad unionslagstiftning får det också i nationell rätt föreskrivas att en europeisk ordning för cybersäkerhetscertifiering får användas för att påvisa regelefterlevnad och fastställa presumtionen om överensstämmelse med de specifika rättsliga krav som anges i nationell rätt.

Artikel 79

Användning av europeiska ordningar för cybersäkerhetscertifiering, Enisas webbplats och offentliggörande av certifikat

1. Enisa ska organisera verksamhet för att främja användningen av antagna europeiska ordningar för cybersäkerhetscertifiering, bland annat genom att underhålla den webbplats som avses i punkt 2 i denna artikel.

2. Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande:

   a) Europeiska ordningar för cybersäkerhetscertifiering.

   b) Avgifterna i samband med underhållet av varje europeisk ordning för cybersäkerhetscertifiering.

   c) Enisas relevanta tekniska specifikationer.

   d) Europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, inbegripet information om sådana certifikat och försäkringar som inte längre är giltiga eller som tillfälligt har upphävts, återkallats eller löpt ut.

   e) Relevant kompletterande cybersäkerhetsinformation som lämnats i enlighet med artikel 84.

   f) Sammanfattningar av inbördes granskningar enligt artikel 89.7.

   g) Tekniska specifikationer som det hänvisas till i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.

3. I tillämpliga fall ska det på den webbplats som avses i punkt 2 också anges vilka nationella ordningar för cybersäkerhetscertifiering som har ersatts av en europeisk ordning för cybersäkerhetscertifiering.

KAPITEL II
Innehåll i europeiska ordningar för cybersäkerhetscertifiering

Artikel 80
Säkerhetsmålen för europeiska ordningar för cybersäkerhetscertifiering

1. En europeisk ordning för cybersäkerhetscertifiering ska, beroende på vad som är tillämpligt, ha följande säkerhetsmål:

   a) Säkerställa att IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster är säkra som standard och har inbyggd säkerhet.

   b) Med lämpliga tekniska medel skydda uppgifter som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten lagring, behandling eller åtkomst eller oavsiktligt eller otillåtet offentliggörande, med beaktande av IKT-produkternas, IKT-tjänsternas eller IKT-processernas hela livscykel.

   c) Skydda integriteten hos lagrade, överförda eller på annat sätt behandlade personuppgifter eller andra uppgifter, kommandon, program och konfigurationer så att de inte manipuleras eller ändras på andra sätt som inte godkänts av användaren, samt rapportera om datadistorsion, med beaktande av IKT-produkternas, IKT-tjänsternas eller IKT-processernas hela livscykel.

   d) Säkerställa skydd mot obehörig åtkomst genom lämpliga kontrollmekanismer, inbegripet men inte begränsat till system för autentiserings-, identitets- eller åtkomsthantering, samt rapportera om eventuell obehörig åtkomst.

   e) Identifiera och dokumentera komponenter och sårbarheter, bland annat genom att när så är lämpligt upprätta en mjukvaruförteckning som åtminstone omfattar beroenden på toppnivå.

f) Tillhandahålla säkerhetsrelaterad information genom att registrera och övervaka relevant intern verksamhet, inbegripet åtkomst till eller ändring av uppgifter, tjänster eller funktioner, i tillämpliga fall med en undantagsmekanism för användaren.

g) Kontrollera att IKT-produkter, IKT-tjänster och IKT-processer inte innehåller några kända sårbarheter som kan utnyttjas.

h) Skydda tillgången till väsentliga och grundläggande funktioner, även efter en incident, inbegripet genom resiliens- och begränsningsåtgärder mot överbelastningsattacker.

i) I händelse av en fysisk eller teknisk incident minimera de negativa effekterna på tillgången till tjänster som tillhandahålls av andra nät och enheter.

j) Säkerställa att IKT-produkter, IKT-tjänster och IKT-processer testas regelbundet och att deras säkerhet ses över.

k) Säkerställa att sårbarheter hanteras och åtgärdas utan dröjsmål, bland annat genom säkerhetsuppdateringar, och att information om åtgärdade sårbarheter delas och offentliggörs, såvida inte riskerna med offentliggörande är större än säkerhetsfördelarna.

l) Säkerställa att det finns en policy för samordnad information om sårbarheter.

m) Underlätta förmedling av information om potentiella sårbarheter i IKT-produkter, IKT-tjänster och IKT-processer.

n) Säkerställa att säkerhetsuppdateringar, när sådana finns tillgängliga för att åtgärda identifierade säkerhetsproblem, sprids utan dröjsmål.

o) Säkerställa att de utlokaliserade säkerhetstjänsterna förses med den kompetens, sakkunskap och erfarenhet som krävs, inbegripet att den personal som fått uppgiften att tillhandahålla dessa tjänster har en tillräcklig och lämplig nivå av teknisk kunskap och kompetens på det specifika området, tillräcklig och lämplig erfarenhet och största möjliga yrkesintegritet.

p) Säkerställa att de IKT-produkter, IKT-tjänster och IKT-processer som används vid tillhandahållandet av de utlokaliserade säkerhetstjänsterna är säkra som standard och har inbyggd säkerhet samt, i tillämpliga fall, inbegriper de senaste säkerhetsuppdateringarna och inte innehåller några kända sårbarheter.

q) Säkerställa att den certifierade entiteten har lämpliga interna förfaranden för att säkerställa att tjänsterna tillhandahålls med en tillräcklig och lämplig kvalitetsnivå.

r) Säkerställa att den certifierade entiteten kan identifiera, skydda sig mot, upptäcka, reagera på och återhämta sig från incidenter.

s) Säkerställa att den certifierade entiteten kan hantera de risker som hotar säkerheten i nätverks- och informationssystem som entiteten använder för sin verksamhet eller för tillhandahållandet av sina tjänster och kan förhindra eller minimera incidenters påverkan på mottagarna av dess tjänster och på andra tjänster.

t) Säkerställa att den certifierade entiteten kan bygga upp, försäkra och se över sin operativa integritet och tillförlitlighet genom att, antingen direkt eller indirekt genom användning av tjänster från tredjepartsleverantörer av IKT-

tjänster, säkerställa att den har hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som entiteten använder och som stöder ett fortlöpande tillhandahållande av tjänsterna och deras kvalitet, inbegripet under avbrott.

u) Säkerställa att den certifierade entiteten kan införa och upprätthålla ett ledningssystem för informationssäkerhet.

v) Motstå händelser som kan undergräva tillgängligheten, autenticiteten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via de nätverks- och informationssystem som entiteten använder samt att säkerställa fortsatt tillhandahållande av tjänster och deras kvalitet, även under avbrott.

w) Säkerställa att entiteten kan säkerställa säkerheten vid behandling av personuppgifter.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 119 för att ändra punkt 1 i den här artikeln genom att lägga till eller ändra säkerhetsmål för att säkerställa att de återspeglar den senaste tekniska utvecklingen och nya relaterade hot samt antagandet av ny unionslagstiftning som fastställer påvisande av regelefterlevnad och presumtion om överensstämmelse genom europeisk cybersäkerhetscertifiering med relevanta cybersäkerhetskrav i den lagstiftningen.

3. En europeisk ordning för cybersäkerhetscertifiering för produkter med digitala element enligt definitionen i artikel 3.1 i förordning (EU) 2024/2847 ska utformas i enlighet med de väsentliga cybersäkerhetskrav som anges i bilaga I till den förordningen och ta hänsyn till tillgängliga harmoniserade standarder.

Artikel 81
Komponenter i europeiska ordningar för cybersäkerhetscertifiering

1. En europeisk ordning för cybersäkerhetscertifiering ska innehålla åtminstone följande:

a) Föremålet och tillämpningsområdet för certifieringsordningen, inbegripet typen eller kategorierna av de IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller entitetens tillgångar, tjänster och funktioner som omfattas av certifieringen.

b) En tydlig beskrivning av certifieringsordningens syfte och, i tillämpliga fall, uppgift om den unionslagstiftning som fastställer krav avseende vilka de europeiska cybersäkerhetscertifikaten påvisar regelefterlevnad och ger presumtion om överensstämmelse.

c) Den underhållsstrategi med specificering av underhållsverksamhet som avses i artikel 75.

d) De specifika cybersäkerhetskrav, utvärderingskriterier och metoder som ska användas för utvärdering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, och hänvisningar till de internationella, europeiska eller nationella standarder som tillämpas vid utvärderingen av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus eller, när sådana standarder inte är tillgängliga eller lämpliga, till tekniska specifikationer

som utarbetats av Enisa i enlighet med artikel 77 eller, om sådana specifikationer inte är tillgängliga, till andra tekniska specifikationer.

e) Längsta giltighetstid för europeiska cybersäkerhetscertifikat som utfärdats enligt certifieringsordningen.

2. En europeisk ordning för cybersäkerhetscertifiering ska åtminstone innehålla regler och villkor om följande:

a) Övervakningen av regelefterlevnaden för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus vad gäller kraven i europeiska cybersäkerhetscertifikat eller EU-försäkringar om överensstämmelse, inklusive mekanismer för att påvisa fortsatt efterlevnad med de angivna cybersäkerhetskraven.

b) Utfärdande, bekräftelse, återkallande och förnyelse av de europeiska cybersäkerhetscertifikaten, utvidgning eller inskränkning av certifieringens omfattning och omcertifiering.

c) Följderna i de fall då IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter som har certifierats, eller för vilka en EU-försäkran om överensstämmelse har utfärdats, inte överensstämmer med kraven i certifieringsordningen.

d) Hur tidigare oupptäckta sårbarheter i fråga om cybersäkerhet hos IKT-produkter, IKT-tjänster och IKT-processer ska rapporteras och hanteras.

e) Innehållet i och formatet på de europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse som ska utfärdas.

f) Den period under vilken tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller ska tillgängliggöra EU-försäkran om överensstämmelse, den tekniska dokumentationen och all annan relevant information som ska göras tillgänglig.

g) Eventuella mekanismer för inbördes bedömning som inrättats inom ramen för certifieringsordningen för myndigheter eller organ som utfärdar europeiska cybersäkerhetscertifikat i enlighet med artikel 85.4, vilka inte ska påverka den inbördes granskning som föreskrivs i artikel 90.

h) Konfidentialiteten för information och data som parterna erhåller när de utför uppgifter och verksamheter i samband med genomförandet av bestämmelserna i denna avdelning.

i) Format och förfaranden som ska följas av tillverkare eller leverantörer av IKT-produkter, IKT-tjänster och IKT-processer när de lämnar och uppdaterar den kompletterande cybersäkerhetsinformationen i enlighet med artikel 84.

j) Kontinuiteten i certifieringsverksamheten under extraordinära krissituationer som är oundvikliga och gör det omöjligt att tillämpa reglerna för certifieringsordningen.

3. En europeisk ordning för cybersäkerhetscertifiering ska, när så är lämpligt, även innehålla följande:

a) En eller flera assuransnivåer och motsvarande utvärderingsnivåer.

b) Skyddsprofiler för att specificera de säkerhetskrav som är tillämpliga på en viss kategori av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster.

c) Tilläggsprofiler för att fastställa ytterligare säkerhetskrav, inbegripet, i tillämpliga fall, säkerhetskrav som fastställs i nationella bestämmelser som införlivar unionsrätten.

d) Klargörande av vilka verksamheter för bedömning av överensstämmelse, såsom kalibrering, testning, certifiering och kontroll, för assuransnivå hög, eller för påvisande av regelefterlevnad och beviljande av presumtion om överensstämmelse, som är tillåtna utanför Europeiska ekonomiska samarbetsområdet (EES).

e) Identifiering av nationella eller internationella ordningar för cybersäkerhetscertifiering som omfattar samma typ eller kategorier av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus.

f) Ytterligare eller specifika krav som gäller för organ för bedömning av överensstämmelse för att garantera deras tekniska kompetens att utvärdera cybersäkerhetskraven.

g) Den information som är nödvändig för certifiering och som en sökande ska lämna till eller på annat sätt göra tillgänglig för organen för bedömning av överensstämmelse.

h) Märken eller etiketter och villkoren för deras användning.

i) Villkor för internationellt erkännande av europeiska cybersäkerhetscertifikat i enlighet med artikel 87.

4. De angivna kraven för den europeiska ordningen för cybersäkerhetscertifiering ska vara förenliga med kraven i unionslagstiftningen.

5. Kommissionen ges befogenhet att anta genomförandeakter för att fastställa gemensamma principer och standardbestämmelser för de komponenter som anges i punkterna 1, 2 och 3 i alla europeiska ordningar för cybersäkerhetscertifiering. En europeisk ordning för cybersäkerhetscertifiering får innehålla hänvisningar till dessa principer och standardbestämmelser när det är lämpligt och sådana finns tillgängliga.

6. De genomförandeakter som avses i punkt 5 ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2. När kommissionen utarbetar eller ser över de gemensamma principerna och standardbestämmelserna för komponenterna i europeiska ordningar för cybersäkerhetscertifiering ska den samråda med Enisa och, när så är lämpligt, beakta synpunkter från den europeiska gruppen för cybersäkerhetscertifiering, berörda intressenter och andra relevanta organ.

Artikel 82
Assuransnivåer och utvärderingsnivåer för europeiska ordningar för cybersäkerhetscertifiering

1. En europeisk ordning för cybersäkerhetscertifiering får ange en eller flera av följande assuransnivåer för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus: ”grundläggande”, ”betydande”

eller ”hög”. Assuransnivåerna ska stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-produkt, IKT-tjänst, IKT-process eller utlokaliserad säkerhetstjänst eller med karaktären av entitet vars cybersäkerhetsstatus certifieringen gäller, samt deras operativa miljö, vad gäller sannolikheten för en incident och den inverkan en sådan skulle ha.

2. Europeiska cybersäkerhetscertifikat ska hänvisa till alla assuransnivåer som anges i den europeiska ordning för cybersäkerhetscertifiering enligt vilken certifikaten utfärdades. EU-försäkringar om överensstämmelse ska hänvisa till assuransnivån ”grundläggande”.

3. De säkerhetskrav som motsvarar varje assuransnivå ska anges i den relevanta europeiska ordningen för cybersäkerhetscertifiering, inbegripet motsvarande säkerhetskontroller och motsvarande utvärdering som IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller entitetens cybersäkerhetsstatus ska genomgå.

4. Det europeiska cybersäkerhetscertifikatet eller EU-försäkran om överensstämmelse ska hänvisa till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, vars syfte är att minska risken för eller förhindra cybersäkerhetsincidenter.

5. Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med assuransnivån ”grundläggande” ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som omfattas av det certifikatet eller den EU-försäkran om överensstämmelse uppfyller motsvarande säkerhetskrav, inbegripet säkerhetskontroller, och att de har utvärderats på en nivå som är avsedd att minimera kända grundläggande risker för incidenter och cyberattacker. Den utvärdering som ska göras ska innefatta åtminstone en granskning av den tekniska dokumentationen. Om en sådan granskning inte är lämplig ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

6. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ”betydande” ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som omfattas av det certifikatet uppfyller motsvarande säkerhetskrav, inbegripet säkerhetskontroller, och att de har utvärderats på en nivå som är avsedd att minimera kända risker för incidenter och cyberattacker och risken för cyberattacker som genomförs av aktörer med begränsade färdigheter och resurser. Den utvärdering som ska göras ska innefatta åtminstone en granskning för att visa att allmänt kända sårbarheter inte föreligger och testning för att visa att IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter på ett korrekt sätt genomför nödvändiga säkerhetskontroller. Om sådana utvärderingar inte är lämpliga ska alternativa utvärderingsinsatser med likvärdig effekt utföras.

7. Ett europeiskt cybersäkerhetscertifikat med assuransnivån ”hög” ska försäkra att IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som omfattas av det certifikatet uppfyller motsvarande säkerhetskrav, inbegripet säkerhetskontroller, och att de har utvärderats på en nivå som är avsedd att minimera kända risker för incidenter och avancerade cyberattacker som genomförs av aktörer med betydande färdigheter och resurser. Den utvärdering som ska göras ska innefatta åtminstone följande:

   a) En granskning för att visa att allmänt kända sårbarheter inte föreligger.

b) Testning för att visa att IKT-produkterna, IKT-tjänsterna, IKT-processerna, de utlokaliserade säkerhetstjänsterna eller entiteterna på ett korrekt sätt genomför nödvändiga säkerhetskontroller, med den senaste tekniken.

c) En bedömning av IKT-produkternas, IKT-tjänsternas, IKT-processernas, de utlokaliserade säkerhetstjänsternas eller entiteternas motståndskraft mot kunniga angripare, med hjälp av penetrationstester när så är relevant.

Om sådana utvärderingar inte är lämpliga får alternativa insatser med likvärdig effekt utföras. All bedömning av överensstämmelse, inbegripet kalibrering, testning, certifiering och inspektion, för assuransnivån ”hög” ska utföras i Europeiska ekonomiska samarbetsområdet, såvida inget annat föreskrivs i en europeisk ordning för cybersäkerhetscertifiering.

8. Om en europeisk ordning för cybersäkerhetscertifiering har utformats för att påvisa regelefterlevnad och ge presumtion om överensstämmelse med en viss unionsrättsakt, ska ett europeiskt cybersäkerhetscertifikat försäkra att certifierade IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller entiteters certifierade cybersäkerhetsstatus uppfyller motsvarande cybersäkerhetskrav i den rättsakten. All bedömning av överensstämmelse, inbegripet kalibrering, testning, certifiering och inspektion, för presumtion om överensstämmelse ska utföras i Europeiska ekonomiska samarbetsområdet, såvida inget annat föreskrivs i en europeisk ordning för cybersäkerhetscertifiering.

9. En europeisk ordning för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer för en viss assuransnivå. Varje utvärderingsnivå ska motsvara en av assuransnivåerna.

Artikel 83
Självbedömning av överensstämmelse

1. En europeisk ordning för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller möjlighet att göra en självbedömning av överensstämmelse på eget ansvar. En självbedömning av överensstämmelse ska endast tillåtas i förhållande till IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som utgör låg risk, motsvarande assuransnivån ”grundläggande”.

2. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller får utfärda en EU-försäkran om överensstämmelse där det anges att det har påvisats att kraven i den europeiska ordningen för cybersäkerhetscertifiering är uppfyllda. Genom att upprätta en sådan försäkran tar tillverkaren, leverantören eller entiteten ansvar för att IKT-produkten, IKT-tjänsten, IKT-processen, den utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen överensstämmer med de krav som anges i den certifieringsordningen.

3. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller ska, under en period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering, ge den nationella myndighet för cybersäkerhetscertifiering som utsetts enligt artikel 89 tillgång till EU-försäkran om

överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas, IKT-tjänsternas, IKT-processernas, de utlokaliserade säkerhetstjänsternas eller cybersäkerhetsstatusens överensstämmelse med certifieringsordningen. En kopia av EU-försäkran om överensstämmelse ska utan onödigt dröjsmål lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

Artikel 84
Kompletterande cybersäkerhetsinformation för certifierade IKT-produkter, IKT-tjänster och IKT-processer

1. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat har utfärdats ska göra följande kompletterande cybersäkerhetsinformation tillgänglig för användaren:

   a) Det avsedda syftet med den berörda IKT-produkten, IKT-tjänsten eller IKT-processen, inbegripet den säkerhetsmiljö som tillhandahålls av tillverkaren eller leverantören.

   b) Vägledning och rekommendationer för att hjälpa användare med säker konfiguration, installation, ibruktagande, användning och underhåll av IKT-produkterna eller IKT-tjänsterna.

   c) Den typ av tekniskt säkerhetsstöd som erbjuds av tillverkaren eller leverantören och slutdatumet för den stödperiod under vilken användarna kan förvänta sig att sårbarheter hanteras och att få säkerhetsuppdateringar.

   d) Om tillverkaren eller leverantören beslutar att göra en programvaruförteckning tillgänglig för användaren, information om var denna finns tillgänglig.

2. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat har utfärdats ska offentliggöra följande kompletterande cybersäkerhetsinformation:

   a) Den gemensamma kontaktpunkt där information om sårbarheter kan rapporteras och tas emot och där tillverkarens policy för samordnad information om sårbarheter kan hittas.

   b) Information om åtgärdade sårbarheter, inbegripet en beskrivning av sårbarheterna, information som gör det möjligt för användarna att identifiera den produkt med digitala element som påverkas, sårbarheternas konsekvenser, deras allvarlighetsgrad och tydlig och tillgänglig information som underlättar för användarna att avhjälpa sårbarheterna. I vederbörligen motiverade fall får tillverkarna, om de anser att säkerhetsriskerna med offentliggörande är större än säkerhetsfördelarna, skjuta upp offentliggörandet av information om en åtgärdad sårbarhet till dess att användarna har fått möjlighet att använda den relevanta programfixen.

3. Den information som avses i punkterna 1 och 2 ska tillgängliggöras i elektroniskt format och finnas tillgänglig och uppdateras vid behov under giltighetsperioden och åtminstone i fem år efter det att motsvarande europeiska cybersäkerhetscertifikat eller EU-försäkran om överensstämmelse löper ut eller återkallas.

4. De skyldigheter som anges i punkterna 1 och 2 ska inte gälla om säkerheten för den berörda IKT-produkten, IKT-tjänsten eller IKT-processen kan äventyras om informationen offentliggörs.

KAPITEL III
Styrning inom det europeiska ramverket för cybersäkerhetscertifiering

Avsnitt 1
Allmänna regler och förvaltning av europeiska ordningar för cybersäkerhetscertifiering

Artikel 85
Utfärdande av europeiska cybersäkerhetscertifikat

1. IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som har certifierats enligt en europeisk ordning för cybersäkerhetscertifiering ska förutsättas överensstämma med kraven i en sådan ordning.
2. De organ för bedömning av överensstämmelse som avses i artikel 91 ska utfärda europeiska cybersäkerhetscertifikat på grundval av de kriterier som ingår i den europeiska ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 74.
3. Genom undantag från punkt 2 får en europeisk ordning för cybersäkerhetscertifiering föreskriva att europeiska cybersäkerhetscertifikat som är ett resultat av den ordningen kan utfärdas endast av ett av följande offentliga organ:
   a) En nationell myndighet för cybersäkerhetscertifiering i den mening som avses i artikel 88 vilken är ackrediterad som ett organ för bedömning av överensstämmelse enligt artikel 91.1.
   b) Ett offentligt organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 91.1.
4. Om en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 74 anger assuransnivån ”hög”, eller om detta särskilt anges för den ordningen, ska det europeiska cybersäkerhetscertifikatet enligt den ordningen utfärdas endast av en nationell myndighet för cybersäkerhetscertifiering i den mening som avses i artikel 88 vilken är ackrediterad som ett organ för bedömning av överensstämmelse enligt artikel 91.1 eller
   a) av ett organ för bedömning av överensstämmelse på grundval av en modell med förhandsgodkännande, eller
   b) av ett organ för bedömning av överensstämmelse på grundval av en modell med allmän delegering.
5. Kommissionen ges befogenhet att anta genomförandeakter som specificerar förfaranden för de modeller med förhandsgodkännande eller allmän delegering som avses i punkt 4 i denna artikel. Vid utarbetandet av dessa genomförandeakter ska kommissionen samråda med den europeiska gruppen för cybersäkerhetscertifiering. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

6. Den fysiska eller juridiska person som lämnar in sina IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för certifiering, eller den entitet som ansöker om certifiering av sin cybersäkerhetsstatus, ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndighet för cybersäkerhetscertifiering som utsetts i enlighet med artikel 89, om denna myndighet är det organ som utfärdar det europeiska cybersäkerhetscertifikatet, eller för det organ för bedömning av överensstämmelse som avses i artikel 91.

7. Organ för bedömning av överensstämmelse och, i tillämpliga fall, nationella myndigheter för cybersäkerhetscertifiering ska utan onödigt dröjsmål informera Enisa om sina beslut som påverkar statusen för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse i enlighet med artikel 94.

8. Innehavaren av ett europeiskt cybersäkerhetscertifikat ska informera det organ för bedömning av överensstämmelse, och i tillämpliga fall den nationella myndighet för cybersäkerhetscertifiering, som avses i punkt 7 om alla sårbarheter eller avvikelser som upptäcks senare när det gäller den certifierade IKT-produkten, IKT-tjänsten, IKT-processen, utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen och som sannolikt påverkar dess överensstämmelse med certifikatet. Detta organ ska utan onödigt dröjsmål vidarebefordra informationen till den berörda nationella myndigheten för cybersäkerhetscertifiering och bedöma inverkan på certifikatet i enlighet med de villkor för certifieringsordningen som avses i artikel 81.2 d.

9. När det gäller certifierade IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster som i sin helhet eller delvis har identifierats som viktiga tillgångar i enlighet med artikel 102 ska innehavaren av ett europeiskt cybersäkerhetscertifikat inte använda, installera eller på annat sätt integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer i de certifierade IKT-produkterna, IKT-tjänsterna, IKT-processerna eller utlokaliserade säkerhetstjänsterna.

10. Ett europeiskt cybersäkerhetscertifikat ska utfärdas för den period som fastställs i den europeiska ordningen för cybersäkerhetscertifiering och får förnyas under förutsättning att de relevanta kraven alltjämt uppfylls.

11. Kommissionen ska samarbeta med medlemsstaterna för att säkerställa tillämpningen av bestämmelserna om utfärdande av europeiska cybersäkerhetscertifikat, även med avseende på tillämpningen av artikel 100.4 b. Organet för bedömning av överensstämmelse och, när så är relevant, den nationella myndigheten för cybersäkerhetscertifiering ska på begäran och utan onödigt dröjsmål förse kommissionen med all information om utfärdandet av de berörda europeiska cybersäkerhetscertifikaten eller EU-försäkringarna om överensstämmelse.

Artikel 86
Nationella ordningar och certifikat för cybersäkerhetscertifiering

1. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus som omfattas av innehållet i och tillämpningsområdet för en europeisk ordning för cybersäkerhetscertifiering, ska upphöra att ha verkan från och med den dag som anges i den genomförandeakt som antagits enligt artikel 74.9. Nationella ordningar för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus som inte omfattas av innehållet i

och tillämpningsområdet för en europeisk ordning för cybersäkerhetscertifiering får fortsätta att användas.

2. Medlemsstaterna får inte införa nya nationella ordningar för cybersäkerhetscertifiering eller därtill hörande förfaranden för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus som redan omfattas av innehållet i och tillämpningsområdet för en europeisk ordning för cybersäkerhetscertifiering.

3. Befintliga certifikat som utfärdats enligt nationella ordningar för cybersäkerhetscertifiering och som omfattas av innehållet i och tillämpningsområdet för en europeisk ordning för cybersäkerhetscertifiering ska förbli giltiga tills de löper ut.

4. Medlemsstaterna ska underrätta kommissionen och den europeiska gruppen för cybersäkerhetscertifiering innan de antar nya nationella ordningar för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus.

5. Kommissionen får föreslå att en medlemsstat återkallar en nationell ordning för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus i de fall då utveckling av en europeisk ordning för cybersäkerhetscertifiering av sådana produkter, tjänster eller processer eller sådan cybersäkerhetsstatus redan har begärts i enlighet med artikel 73, med beaktande av utvecklingsplanen för en sådan ordning.

Artikel 87
Internationellt erkännande av europeiska cybersäkerhetscertifikat

1. Tredjelandscertifikat för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus får, genom en genomförandeakt eller genom ingående av ett avtal mellan unionen och tredjelandet i fråga eller en internationell organisation, erkännas som likvärdiga med europeiska cybersäkerhetscertifikat om kraven i tredjelandets eller den internationella organisationens berörda ordning anses vara likvärdiga med kraven i europeiska ordningar för cybersäkerhetscertifiering. Kommissionen ges befogenhet att anta sådana genomförandeakter. Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

2. De genomförandeakter och avtal som avses i punkt 1 ska baseras på de villkor för internationellt erkännande av europeiska cybersäkerhetscertifikat som fastställts i enlighet med artikel 74.11.

3. Avtal om erkännande av tredjelandscertifikat eller internationella organisationers certifikat i den mening som avses i punkt 1 ska endast ingås om motparten också erkänner europeiska cybersäkerhetscertifikat som likvärdiga med tredjelandscertifikaten.

Artikel 88
Nationella myndigheter för cybersäkerhetscertifiering

1. Varje medlemsstat ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering på sitt territorium eller, efter överenskommelse med en annan medlemsstat, en eller flera nationella myndigheter för

cybersäkerhetscertifiering i denna andra medlemsstat som ansvariga för tillsynsuppgifterna i den utseende medlemsstaten.

2. Varje medlemsstat ska underrätta kommissionen om vilka nationella myndigheter för cybersäkerhetscertifiering som utsetts. Om en medlemsstat utser mer än en myndighet ska den också informera kommissionen om vilka uppgifter som var och en av dessa myndigheter tilldelats.

3. Varje nationell myndighet för cybersäkerhetscertifiering ska vara oberoende av de entiteter som den utövar tillsyn över vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande.

4. Den verksamhet som bedrivs av nationella myndigheter för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat enligt denna förordning ska vara strikt avskild från deras tillsynsuppgifter enligt denna artikel och artikel 85.4 a och b och dessa verksamheter ska utföras oberoende av varandra.

5. Medlemsstaterna ska säkerställa att de nationella myndigheterna för cybersäkerhetscertifiering har tillräckliga resurser för att kunna utöva sina befogenheter och kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt.

6. Nationella myndigheter för cybersäkerhetscertifiering ska ha följande uppgifter:

   a) Delta i den europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 90.2.

   b) Övervaka och kontrollera efterlevnaden av reglerna i europeiska ordningar för cybersäkerhetscertifiering enligt artikel 81.2 a för att säkerställa att IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus stämmer överens med kraven i de europeiska cybersäkerhetscertifikat som utfärdats inom deras respektive territorier, i samarbete med berörda marknadskontrollmyndigheter eller tillsynsmyndigheter, inbegripet behöriga myndigheter enligt Europaparlamentets och rådets direktiv (EU) 2022/2555[82] eller förordning (EU) 2024/2847.

   c) I samarbete med berörda marknadskontrollmyndigheter övervaka att tillverkare eller leverantörer av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller entiteter vars cybersäkerhetsstatus har certifierats vilka är etablerade inom deras respektive territorier och vilka utför självbedömning av överensstämmelse inom ramen för motsvarande europeiska ordning för cybersäkerhetscertifiering fullgör sina skyldigheter enligt denna förordning och kontrollera efterlevnaden av dessa skyldigheter.

   d) Utan att det påverkar tillämpningen av artikel 91.3 aktivt bistå och stödja de nationella ackrediteringsorganen eller andra berörda myndigheter med övervakning och tillsyn av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning.

[82] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

e) Samarbeta med kommissionen i de fall då kompetensen hos ett organ för bedömning av överensstämmelse ifrågasätts i enlighet med artikel 94.

f) Övervaka och utöva tillsyn över den verksamhet som bedrivs av de offentliga organ som avses i artikel 85.3.

g) I tillämpliga fall bemyndiga organ för bedömning av överensstämmelse i enlighet med artikel 93, övervaka att organ för bedömning av överensstämmelse fullgör de ytterligare eller specifika krav som fastställs i europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 81.3 f och kontrollera efterlevnaden av dessa krav, och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organ för bedömning av överensstämmelse inte uppfyller kraven i denna förordning.

h) Behandla klagomål från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av nationella myndigheter för cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 85.4, eller avseende EU-försäkringar om överensstämmelse som utfärdats enligt artikel 83, i lämplig utsträckning undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen.

i) Senast den 31 mars [året för ikraftträdande + 12 månader] varje år lämna en årlig rapport om sin huvudsakliga verksamhet till kommissionen, Enisa och den europeiska gruppen för cybersäkerhetscertifiering, samt göra dessa rapporter tillgängliga för den grupp som utför den inbördes granskningen om den nationella myndigheten för cybersäkerhetscertifiering blir föremål för inbördes granskning i enlighet med artikel 89.

j) Samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering, marknadskontrollmyndigheter eller andra myndigheter, inbegripet genom att utbyta information om IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus som eventuellt avviker från kraven i denna förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering.

k) Övervaka relevant utveckling på området cybersäkerhetscertifiering.

7. Varje nationell myndighet för cybersäkerhetscertifiering ska åtminstone ha befogenheter att

a) begära att organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare av EU-försäkringar om överensstämmelse ska lägga fram all information som myndigheten behöver för att kunna fullgöra sina uppgifter,

b) genomföra undersökningar, i form av kontroller, av organ för bedömning av överensstämmelse, innehavare av ett europeiskt cybersäkerhetscertifikat och utfärdare av EU-försäkringar om överensstämmelse, för att kunna verifiera efterlevnad av kraven i denna avdelning,

c) vidta lämpliga åtgärder, i enlighet med nationell rätt, för att säkerställa att organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av EU-försäkringar om

överensstämmelse uppfyller kraven i denna förordning eller en europeisk ordning för cybersäkerhetscertifiering,

d) erhålla tillgång till alla lokaler hos organ för bedömning av överensstämmelse eller innehavare av ett europeiskt cybersäkerhetscertifikat i syfte att genomföra utredningar i enlighet med unionslagstiftningen eller nationell processrätt,

e) i enlighet med nationell rätt, återkalla europeiska cybersäkerhetscertifikat som utfärdats av den nationella myndigheten för cybersäkerhetscertifiering eller av organ för bedömning av överensstämmelse i enlighet med artikel 85.4, om sådana certifikat inte uppfyller kraven i denna förordning eller en europeisk ordning för cybersäkerhetscertifiering,

f) ålägga sanktioner i enlighet med nationell rätt, enligt artikel 97, och kräva att överträdelser av skyldigheterna i denna förordning omedelbart upphör.

8. Nationella myndigheter för cybersäkerhetscertifiering ska samarbeta med varandra och med kommissionen, i synnerhet genom att utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus.

9. Senast den [ikraftträdandet + 6 månader] ska Enisa, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering, utarbeta en mall för den rapport som avses i punkt 6 i i denna artikel.

Artikel 89
Inbördes granskning

1. Nationella myndigheter för cybersäkerhetscertifiering ska vara föremål för inbördes granskning.

2. Den inbördes granskningen ska företas utifrån gedigna och transparenta kriterier och förfaranden för utvärdering, särskilt när det gäller strukturella krav samt krav gällande personal och förfaranden och med hänsyn till konfidentialitet och klagomål.

3. Den inbördes granskningen ska omfatta en bedömning

a) i tillämpliga fall, av om den verksamhet som bedrivs av nationella myndigheter för cybersäkerhetscertifiering i samband med utfärdande av europeiska cybersäkerhetscertifikat i enlighet med denna förordning är strikt åtskilda från deras tillsynsverksamhet enligt artikel 88 och om dessa verksamheter utförs oberoende av varandra,

b) av förfarandena för tillsyn och kontroll av efterlevnaden av reglerna för övervakning av IKT-produkters, IKT-tjänsters, IKT-processers, utlokaliserade säkerhetstjänsters och entiteters cybersäkerhetsstatus överensstämmelse med europeiska cybersäkerhetscertifikat enligt artikel 88.7 a,

c) av förfarandena för övervakning och kontroll av efterlevnaden av de skyldigheter som tillverkare eller tillhandahållare av IKT-produkter, IKT tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter med certifierad cybersäkerhetsstatus har enligt artikel 88.7 b,

d) av förfarandena för övervakning, bemyndigande och översyn av verksamhet som bedrivs av organen för bedömning av överensstämmelse.

4. Den inbördes granskningen ska utföras minst vart femte år av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och av kommissionen. Enisa ska också delta i den inbördes granskningen som observatör. Den grupp som utför den inbördes granskningen ska utarbeta slutrapporten och sammanfattningen av den inbördes granskningen.

5. Enisa ska stödja organisationen av mekanismen för inbördes granskning och de inbördes granskningarna, bland annat genom att utarbeta relevanta vägledningsdokument och mallar, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering.

6. Kommissionen ges befogenhet att anta genomförandeakter om inrättande av en plan för den inbördes granskningen som ska omfatta en period på minst fem år, med kriterier för sammansättningen av den grupp som ska utföra den inbördes granskningen, den metod som ska användas, tidsplanen, frekvensen och andra uppgifter som rör den inbördes granskningen. Vid utarbetandet av genomförandeakterna ska kommissionen samråda med den europeiska gruppen för cybersäkerhetscertifiering och Enisa. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

7. Slutrapporten, inbegripet eventuella riktlinjer eller rekommendationer, och sammanfattningen av den inbördes granskningen ska granskas av den europeiska gruppen för cybersäkerhetscertifiering, som ska godkänna sammanfattningen för offentliggörande på den webbplats som avses i artikel 79.2.

Artikel 90
Den europeiska gruppen för cybersäkerhetscertifiering

1. Den europeiska gruppen för cybersäkerhetscertifiering ska inrättas.

2. Den europeiska gruppen för cybersäkerhetscertifiering ska bestå av företrädare för nationella myndigheter för cybersäkerhetscertifiering eller företrädare för andra berörda nationella myndigheter. En gruppmedlem får inte företräda mer än två medlemsstater.

3. Den europeiska gruppen för cybersäkerhetscertifiering ska ha i uppgift att

   a) ge råd till och bistå kommissionen i dess arbete för att säkerställa ett konsekvent genomförande och en konsekvent tillämpning av denna avdelning, policyfrågor om cybersäkerhetscertifiering och strategisamordning,

   b) ge råd till och bistå kommissionen vid utarbetandet av begäranden om europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 73,

   c) bistå, ge råd till och samarbeta med Enisa när det gäller utarbetande av förslag till en certifieringsordning i enlighet med artikel 74 och tekniska specifikationer i enlighet med artikel 77,

   d) bistå, ge råd till och samarbeta med Enisa och kommissionen när det gäller underhållsverksamhet i enlighet med artikel 75,

   e) bistå, ge råd till och samarbeta med kommissionen när det gäller översyn eller återkallande av befintliga europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 76,

f) föreslå att en begäran lämnas in till kommissionen om utarbetande av ett förslag till en europeisk ordning för cybersäkerhetscertifiering i enlighet med artikel 73.2,

g) anta yttranden riktade till kommissionen rörande underhåll, översyn och återkallande av befintliga europeiska ordningar för cybersäkerhetscertifiering,

h) undersöka den relevanta utvecklingen på området cybersäkerhetscertifiering, även på nationell nivå i enlighet med artikel 86, och utbyta information och god praxis om ordningar för cybersäkerhetscertifiering,

i) underlätta samarbetet mellan nationella myndigheter för cybersäkerhetscertifiering enligt reglerna i denna avdelning genom kapacitetsuppbyggnad och utbyte av information, särskilt när det gäller frågor som rör cybersäkerhetscertifiering,

j) stödja genomförandet av mekanismen för inbördes granskning i enlighet med artikel 89 och mekanismer för inbördes bedömning i enlighet med de regler som fastställts i en europeisk ordning för cybersäkerhetscertifiering enligt artikel 81.2 g,

k) underlätta anpassningen av europeiska ordningar för cybersäkerhetscertifiering till internationellt erkända standarder, också som en del av underhållet av befintliga europeiska ordningar för cybersäkerhetscertifiering och, där så är lämpligt, lämna rekommendationer till Enisa om att samarbeta med relevanta europeiska eller internationella standardiseringsorganisationer för att åtgärda brister eller luckor i de tillgängliga europeiska eller internationellt erkända standarderna.

4. Med stöd från Enisa ska kommissionen vara ordförande i den europeiska gruppen för cybersäkerhetscertifiering och tillhandahålla gruppen ett sekretariat.

5. Kommissionen kan inrätta undergrupper för följande ändamål:

a) Utreda särskilda frågor enligt direktiv från kommissionen.

b) Underhålla och se över de europeiska certifieringsordningarna i enlighet med denna förordning och enligt direktiv från kommissionen.

6. Undergrupperna ska rapportera till den europeiska gruppen för cybersäkerhetscertifiering.

7. Ordförandeskapet i undergrupperna ska innehas gemensamt av kommissionen och Enisa, och undergruppernas sekretariat ska tillhandahållas av Enisa.

8. Den europeiska gruppen för cybersäkerhetscertifiering och dess undergrupper ska anta sin arbetsordning med enkel majoritet, på grundval av ett förslag från och i samförstånd med kommissionen.

Avsnitt 2
Organ för bedömning av överensstämmelse

Artikel 91
Befogenheter för organ för bedömning av överensstämmelse

1. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008. Sådan

ackreditering ska endast utfärdas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i bilaga I till denna förordning.

2. Om ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering i enlighet med denna förordning ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som ett organ för bedömning av överensstämmelse enligt punkt 1.

3. Den ackreditering som avses i punkt 1 ska utfärdas till organen för bedömning av överensstämmelse för en period på högst fem år och får förnyas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i denna artikel. Nationella ackrediteringsorgan ska vidta alla lämpliga åtgärder inom en rimlig tidsram för att begränsa, tillfälligt upphäva eller återkalla ackrediteringen av ett organ för bedömning av överensstämmelse som utfärdats i enlighet med punkt 1 om villkoren för ackrediteringen inte har uppfyllts eller inte längre uppfylls, eller om organet för bedömning av överensstämmelse inte efterlever denna förordning.

4. Vid fastställandet av ytterligare eller specifika ackrediteringskrav för en europeisk ordning för cybersäkerhetscertifiering som omfattar IKT-produkter, i enlighet med artikel 92, ska synergier när så är lämpligt eftersträvas med de krav som rör anmälda organ enligt förordning (EU) 2024/2847 och ackrediteringskraven för ordningar för cybersäkerhetscertifiering som redan har antagits.

5. Om ett organ för bedömning av överensstämmelse har ackrediterats i enlighet med förordning (EU) 2024/2847 får de berörda myndigheterna återanvända resultat från den tidigare ackrediteringsprocessen som bevis avseende eventuella överlappande krav under ackrediteringsprocessen enligt denna förordning.

Artikel 92
Ytterligare harmonisering av befogenheterna för organen för bedömning av överensstämmelse

1. Om en europeisk ordning för cybersäkerhetscertifiering innehåller ytterligare eller specifika krav i enlighet med artikel 81.3 f ska organ för bedömning av överensstämmelse bemyndigas av en nationell myndighet för cybersäkerhetscertifiering som utsetts i enlighet med artikel 88.1 att utföra uppgifter inom ramen för denna ordning. Ett sådant bemyndigande ska utfärdas endast om organet för bedömning av överensstämmelse har ackrediterats och uppfyller de ytterligare eller specifika kraven i den europeiska ordningen för cybersäkerhetscertifiering.

2. Om ett organ för bedömning av överensstämmelse begär bemyndigande enligt denna artikel ska det lämna in sin begäran till den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstat där det är etablerat eller till den nationella myndighet för cybersäkerhetscertifiering som medlemsstaten kan anlita i enlighet med artikel 88.1.

3. Ett organ för bedömning av överensstämmelse kan begära bemyndigande hos en annan nationell myndighet för cybersäkerhetscertifiering än den som avses i punkt 2 i följande situationer:

   a) Om den nationella myndighet för cybersäkerhetscertifiering som avses i punkt 1 inte utför bemyndigande av sådan verksamhet för bedömning av överensstämmelse som bemyndigandet gäller.

b) Om den nationella myndighet för cybersäkerhetscertifiering som avses i punkt 1 inte har genomgått inbördes granskning i enlighet med artikel 89 med avseende på sådan verksamhet för bedömning av överensstämmelse som bemyndigandet gäller.

4. Om en nationell myndighet för cybersäkerhetscertifiering tar emot en begäran enligt punkt 3 ska den informera den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstat där det begärande organet för bedömning av överensstämmelse är etablerat. I sådana fall får den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstaten delta i bemyndigandet som observatör.

5. En nationell myndighet för cybersäkerhetscertifiering får begära att en annan nationell myndighet för cybersäkerhetscertifiering utför delar av bedömningsverksamheten. I sådana fall ska bemyndigandecertifikatet utfärdas av den myndighet som gör denna begäran.

6. Det bemyndigande som avses i punkt 1 ska vara giltigt högst lika länge som ackrediteringen är giltig, och får förnyas under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i punkt 1 och att dess ackreditering också har förnyats.

7. De nationella myndigheterna för cybersäkerhetscertifiering ska inom en rimlig tidsram vidta alla lämpliga åtgärder för att begränsa, tillfälligt upphäva eller återkalla bemyndigandet av ett organ för bedömning av överensstämmelse som utfärdats i enlighet med punkt 1 om villkoren för bemyndigandet inte har uppfyllts eller inte längre uppfylls, eller om organet för bedömning av överensstämmelse inte efterlever denna förordning.

8. Kommissionen ges befogenhet att anta genomförandeakter för att fastställa förfarandena, inbegripet för gränsöverskridande samarbete, för auktorisering av organ för bedömning av överensstämmelse. Vid utarbetandet av dessa genomförandeakter ska kommissionen samråda med Enisa och den europeiska gruppen för cybersäkerhetscertifiering. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

Artikel 93
Anmälan av organ för bedömning av överensstämmelse

1. För varje europeisk ordning för cybersäkerhetscertifiering ska de nationella myndigheterna för cybersäkerhetscertifiering i en medlemsstat till kommissionen och de andra medlemsstaterna anmäla de organ för bedömning av överensstämmelse som har ackrediterats och, i tillämpliga fall, bemyndigats i enlighet med artikel 92.

2. De nationella myndigheterna för cybersäkerhetscertifiering ska göra den anmälan som avses i punkt 1 med hjälp av det elektroniska anmälningsverktyg som utvecklats och förvaltas av kommissionen.

3. Kommissionen ges befogenhet att anta genomförandeakter för att fastställa omständigheter, format och förfaranden för de anmälningar som avses i punkt 1 i denna artikel, inbegripet förfarandet för andra medlemsstaters invändningar under anmälningsprocessen, den unika identifieringen av organ för bedömning av överensstämmelse samt omständigheterna för begränsning, tillfälligt upphävande eller återkallande av anmälan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

Artikel 94

Ifrågasättande av kompetensen hos organen för bedömning av överensstämmelse

1. Kommissionen ska undersöka alla fall i vilka den tvivlar på, eller görs uppmärksam på tvivel på, att ett organ för bedömning av överensstämmelse har kompetens att uppfylla, eller att ett organ för bedömning av överensstämmelse fortsatt uppfyller, de krav och skyldigheter som det omfattas av.

2. Den nationella myndigheten för cybersäkerhetscertifiering ska på begäran ge kommissionen all information om grunderna för anmälan eller om hur kompetensen upprätthålls inom det berörda organet för bedömning av överensstämmelse.

3. Kommissionen ska säkerställa att all känslig information som erhållits i samband med undersökningarna behandlas konfidentiellt.

4. Om kommissionen konstaterar att ett organ för bedömning av överensstämmelse inte uppfyller eller inte längre uppfyller kraven för anmälan ska den meddela detta till den nationella myndigheten för cybersäkerhetscertifiering och begära att den vidtar erforderliga korrigerande åtgärder, såsom att vid behov återta anmälan.

5. Medlemsstaterna ska säkerställa att det finns ett förfarande för överklagande av de anmälda organens beslut.

Artikel 95

Informations- och lagringsskyldighet för organ för bedömning av överensstämmelse

1. Organ för bedömning av överensstämmelse ska informera den nationella myndigheten för cybersäkerhetscertifiering om följande:

   a) Avslag på ansökan om certifikat, eller begränsning, tillfälligt upphävande eller återkallelse av ett certifikat.

   b) Omständigheter som påverkar omfattningen av och villkoren för den anmälan som avses i artikel 93.1.

   c) Eventuella begäranden om information de har tagit emot från marknadskontrollmyndigheterna om bedömningar av överensstämmelse.

   d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. Organ för bedömning av överensstämmelse ska också förse Enisa med den information som avses i punkt 1 a för att underlätta utförandet av dess uppgifter enligt artikel 79.

3. Organ för bedömning av överensstämmelse ska utan onödigt dröjsmål ge de andra organ för bedömning av överensstämmelse, i den mening som avses i denna förordning, som utför liknande bedömningar av överensstämmelse avseende samma IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter vars cybersäkerhetsstatus är certifierad relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

4. Organ för bedömning av överensstämmelse ska upprätthålla ett registersystem som innehåller alla dokument och bevis som tagits fram eller mottagits i samband med varje utvärdering och certifiering som de utför. Registret ska lagras på ett säkert och tillgängligt sätt under den period som krävs för certifieringsändamål och i minst fem

år efter det att det berörda europeiska cybersäkerhetscertifikatet löper ut eller återkallas.

Avsnitt 3
Övriga bestämmelser

Artikel 96
Rätt att lämna in klagomål och rätt till ett effektivt rättsmedel

1. Fysiska och juridiska personer ska ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat eller, när klagomålet rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse som handlar i enlighet med artikel 85.4, till den berörda nationella myndigheten för cybersäkerhetscertifiering.

2. Den myndighet eller det organ till vilket klagomålet har lämnats in ska underrätta den klagande om hur förfarandet fortskrider, vilket beslut som fattats och om den rätt till ett effektivt rättsmedel som avses i punkterna 3 och 4.

3. Utan att det påverkar administrativa rättsmedel eller andra prövningsförfaranden utanför domstol ska fysiska och juridiska personer ha rätt till ett effektivt rättsmedel avseende

   a) beslut fattade av den myndighet eller det organ som avses i punkt 1, i tillämpliga fall även om felaktigt utfärdande, icke-utfärdande eller erkännande av ett europeiskt cybersäkerhetscertifikat som innehas av dessa fysiska och juridiska personer,

   b) underlåtenhet att vidta åtgärder med anledning av ett klagomål som lämnats in till den myndighet eller det organ som avses i punkt 1.

4. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den myndighet eller det organ som rättsmedlet avser ligger.

Artikel 97
Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i denna avdelning och överträdelser av europeiska ordningar för cybersäkerhetscertifiering, och ska vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder utan dröjsmål samt eventuella ändringar som berör dem.

AVDELNING IV
SÄKERHET I IKT-LEVERANSKEDJOR

KAPITEL I
Ramverk för en betrodd IKT-leveranskedja

Artikel 98
Ramverkets omfattning

1. Ramverket för en betrodd IKT-leveranskedja ska fungera som en säkerhetsmekanism på unionsnivå för att hantera icke-tekniska risker i högkritiska sektorer och andra kritiska sektorer som avses i direktiv (EU) 2022/2555. Mekanismen ska identifiera viktiga IKT-tillgångar inom kritiska IKT-leveranskedjor och fastställa lämpliga och proportionella begränsningsåtgärder för entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555.

2. Skyldigheterna i denna avdelning ska inte påverka de skyldigheter som anges i artikel 13 i förordning (EU) 2024/2847 och i nationella bestämmelser som införlivar artikel 21 i direktiv (EU) 2022/2555.

3. Bestämmelserna i detta kapitel hindrar inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå i IKT-leveranskedjor, förutsatt att sådana bestämmelser stämmer överens med deras skyldigheter enligt unionsrätten.

Artikel 99
Säkerhetsriskbedömningar

1. Kommissionen eller en grupp om minst tre medlemsstater får begära att den samarbetsgrupp som inrättats genom artikel 14 i direktiv (EU) 2022/2555 (*samarbetsgruppen för nät- och informationssäkerhet*) genomför samordnade säkerhetsriskbedömningar på unionsnivå i enlighet med artikel 22 i det direktivet. Om en säkerhetsriskbedömning genomförs efter en sådan begäran ska den särskilt omfatta den föreslagna identifieringen av de viktigaste IKT-tillgångarna i respektive IKT-leveranskedja samt de främsta fientliga aktörer, risker och sårbarheter som påverkar dessa tillgångar. Vid de samordnade säkerhetsriskbedömningarna på unionsnivå ska det utarbetas riskscenarier och föreslås åtgärder för att begränsa de identifierade riskerna.

2. De samordnade säkerhetsriskbedömningarna på unionsnivå ska slutföras inom sex månader från den begäran som avses i punkt 1. På begäran av kommissionen kan samarbetsgruppen för nät- och informationssäkerhet samtycka till en kortare period.

3. Om kommissionen har tillräckliga skäl att anta att det föreligger ett betydande cyberhot mot unionens säkerhet i förhållande till en IKT-leveranskedja och att åtgärder krävs för att bevara en väl fungerande inre marknad ska kommissionen utan dröjsmål

   a) samråda med medlemsstaterna om behovet av att vidta en eller flera av de begränsningsåtgärder som avses i artikel 103, och

   b) utföra en säkerhetsriskbedömning, med beaktande av samråd med medlemsstaterna. Säkerhetsriskbedömningen ska omfatta den föreslagna identifieringen av de viktigaste IKT-tillgångarna samt de främsta fientliga aktörer, risker och sårbarheter som påverkar dessa tillgångar. Vid säkerhetsriskbedömningen ska det utarbetas riskscenarier och föreslås åtgärder för att begränsa de identifierade riskerna.

Artikel 100

Utseende av tredjeländer som utgör cybersäkerhetsproblem

1. Om det till följd av den säkerhetsriskbedömning som avses i artikel 99, eller på grundval av andra källor, såsom ett offentligt uttalande på unionens eller en medlemsstats vägnar, framstår som att ett tredjeland utgör en allvarlig och strukturell icke-teknisk risk för IKT-leveranskedjorna, ska kommissionen kontrollera den risk som det landet utgör, med beaktande av följande:

   a) Förekomsten av lagar i tredjelandet som kräver att entiteter inom dess jurisdiktion rapporterar information om sårbarheter i programvara eller maskinvara till myndigheterna i tredjelandet innan det är känt att dessa sårbarheter har utnyttjats.

   b) Befintlig praxis i tredjelandet, styrkt av oberoende källor, som kräver att entiteter inom tredjelandets jurisdiktion rapporterar information om sårbarheter i programvara eller maskinvara till myndigheterna i tredjelandet innan det är känt att dessa sårbarheter har utnyttjats.

   c) Avsaknad av effektiva rättsmedel, och oberoende och demokratiska kontrollmekanismer, som kan avhjälpa de identifierade säkerhetsproblemen, även avseende den befintliga praxis som avses i led b.

   d) Styrkt information om en eller flera incidenter där fientliga aktörer som kontrolleras från det landet och verkar från det landets territorium utför skadlig cyberverksamhet eller skadliga cyberkampanjer, och tredjelandets bristande förmåga eller vilja att samarbeta med kommissionen eller medlemsstaterna för att hantera den risk som härrör från sådana fientliga aktörers verksamhet.

   e) Relevant information som härrör från samordnade säkerhetsriskbedömningar på unionsnivå eller rapporter från medlemsstaterna eller internationella organisationer.

2. När kommissionen efter den kontroll som avses i punkt 1 drar slutsatsen att ett tredjeland utgör allvarliga och strukturella icke-tekniska risker för IKT-leveranskedjorna, får den genom en genomförandeakt beteckna det tredjelandet som ett land som utgör ett cybersäkerhetsproblem för IKT-leveranskedjorna. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

3. Kommissionen ska regelbundet se över de genomförandeakter som antagits i enlighet med punkt 2.

4. Högriskleverantörer ska inte ha rätt att

   a) delta i utarbetandet av, bedömningen av, samråden om eller besluten om de europeiska standarder och europeiska standardiseringsprodukter som avses i artikel 10.1 i förordning (EU) nr 1025/2012 och de gemensamma specifikationer som avses i artikel 27 i förordning (EU) 2024/2847 på cybersäkerhetsområdet,

   b) ansöka om eller inneha ett europeiskt cybersäkerhetscertifikat enligt avdelning III,

   c) bli ett ackrediterat organ för bedömning av överensstämmelse enligt avdelning III,

d) ansöka om att bli auktoriserad tillhandahållare av europeiska individuella intyg om cybersäkerhetskompetens enligt avdelning II avsnitt 4,

e) delta i offentliga upphandlingsförfaranden som anordnas i enlighet med den lagstiftning som införlivar direktiven 2014/24/EU och 2014/25/EU när det gäller tillhandahållande av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka ska användas i viktiga IKT-tillgångar som identifierats i enlighet med artikel 102,

f) delta i verksamhet inom ramen för unionens finansieringsprogram och finansieringsinstrument som genomförs genom direkt och indirekt förvaltning i enlighet med artikel 136 i förordning (EU, Euratom) 2024/2509 och unionens sektorsspecifika regler eller i unionsfinansieringsverksamhet som genomförs genom delad förvaltning när det gäller tillhandahållande av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka ska användas i viktiga IKT-tillgångar som identifierats i enlighet med artikel 102.

De myndigheter som ansvarar för de förfaranden som avses i leden a–f ska genomföra de bedömningar som krävs för tillämpningen av denna punkt. Myndigheterna får för detta ändamål också använda sig av den förteckning som avses i artikel 104.

5. I fall där en högriskleverantör redan har erhållit ett europeiskt cybersäkerhetscertifikat enligt avdelning III ska den behöriga myndigheten återkalla det utan onödigt dröjsmål.

Artikel 101
Allmän säkerhetsmekanism för IKT-leveranskedjan

När samarbetsgruppen för nät- och informationssäkerhet har genomfört en samordnad säkerhetsriskbedömning på unionsnivå i enlighet med artikel 99.1 i denna förordning, eller efter det att förfarandet i händelse av ett betydande cyberhot i enlighet med artikel 99.3 har slutförts för en IKT-leveranskedja, får kommissionen vidta de åtgärder som föreskrivs i artiklarna 102, 103.1 och 103.2.

Artikel 102
Identifiering av viktiga IKT-tillgångar

1. Om den riskbedömning som utförts i enlighet med artikel 99.1 eller 99.3 visar på betydande cybersäkerhetsrisker i förhållande till en IKT-leveranskedja har kommissionen befogenhet att anta genomförandeakter för att identifiera viktiga IKT-tillgångar som används av entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 för tillverkning av produkter eller tillhandahållande av tjänster. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2 i denna förordning.

2. Vid identifiering av de viktiga IKT-tillgångar som avses i punkt 1 ska kommissionen beakta följande:

a) Huruvida dessa tillgångar har väsentliga och känsliga funktioner som behövs för produkter som tillverkas eller tjänster som tillhandahålls av en entitet av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555.

b) Huruvida incidenter, även incidenter som orsakas av utnyttjade sårbarheter som rör dessa tillgångar, kan leda till allvarliga störningar i IKT-leveranskedjorna på den inre marknaden eller leda till exfiltrering av uppgifter.

c) Huruvida det finns ett beroende av ett begränsat antal leverantörer av dessa tillgångar.

d) Resultaten från de riskbedömningar som avses i artikel 99.

Artikel 103
Begränsningsåtgärder i IKT-leveranskedjan

1. Kommissionen ges befogenhet att anta genomförandeakter för att, när så är nödvändigt för att säkerställa en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom unionen, fastställa att vissa typer av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 ska vara förbjudna att i någon form använda, installera eller integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer som identifierats i enlighet med artikel 104 i viktiga IKT-tillgångar som identifierats i enlighet med artikel 102. Sådana genomförandeakter ska föreskriva lämpliga övergångsperioder under vilka kommissionen ska offentliggöra den förteckning över högriskleverantörer som avses i artikel 104 samt ytterligare tidsperioder för utfasning av de berörda IKT-komponenterna och komponenterna som innehåller IKT-komponenter. Sådana genomförandeakter får också specificera dessa IKT-komponenter eller komponenter som innehåller IKT-komponenter.

2. Kommissionen ges befogenhet att anta genomförandeakter för att, när så är nödvändigt för att säkerställa en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom unionen, fastställa att vissa typer av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 ska omfattas av en eller flera av följande begränsningsåtgärder i förhållande till deras IKT-leveranskedja och i synnerhet till viktiga IKT-tillgångar som identifierats i enlighet med artikel 102, för att begränsa risker som identifierats i de säkerhetsriskbedömningar som genomförts i enlighet med artikel 99:

a) Tillämpning av transparenskrav när det gäller tillhandahållande av information till den behöriga myndigheten om leverantörer i IKT-leveranskedjan för viktiga IKT-tillgångar som har utsetts i enlighet med artikel 102.

b) Förbud i samband med överföring av uppgifter till tredjeländer och behandling av uppgifter på distans från ett tredjeland.

c) Tekniska åtgärder som ska granskas av en tredje part, bland annat

i) användning av behandling på enheten,

ii) specifik segmentering av nätverkssystem,

iii) avaktivering av eventuell fjärråtkomst eller fysisk åtkomst till viktiga IKT-tillgångar,

iv) avaktivering av icke-väsentliga funktioner,

v) nätdriftsövervakning,

vi) testning av maskinvara och programvara.

d) Begränsningar som rör operativ kontroll, inbegripet utkontraktering av organisatoriska funktioner till leverantörer av utlokaliserade driftstjänster.

e) Begränsningar som rör entitetens avtalsförbindelser med sina leverantörer.

f) Krav på att tjänsten ska drivas, förvaltas, underhållas eller stödjas av personal som kontrollerats av de relevanta nationella behöriga myndigheterna.

g) Diversifiering av utbudet av IKT-komponenter eller komponenter som ingår i IKT-komponenter.

3. När kommissionen inför de åtgärder som avses i punkt 2 får den fastställa tekniska och metodologiska krav för åtgärderna.

4. Innan kommissionen antar de genomförandeakter som avses i punkterna 1 och 2 ska den bedöma potentiella risker och beroenden, i synnerhet

a) i tillämpliga fall, risknivån i samband med användning, installation eller integrering, i vilken form som helst, av IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer i viktiga IKT-tillgångar,

b) de potentiella ekonomiska och samhälleliga konsekvenser som skyldigheten kan få för entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555,

c) tillgången på alternativa leverantörer till högriskleverantörerna,

d) den potentiella störning av gränsöverskridande ekonomisk och samhällelig verksamhet som orsakas av en incident som påverkar en entitets IKT-leveranskedja.

5. De genomförandeakter som avses i punkterna 1 och 2 i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2 och ska ses över minst var 36:e månad.

6. Under exceptionella omständigheter som motiverar ett ingripande för att bevara en väl fungerande inre marknad och där kommissionen har tillräckliga skäl att anse att användning, installation eller integrering av IKT-komponenter eller komponenter som innehåller IKT-komponenter från en viss entitet som är etablerad i eller kontrolleras av ett tredjeland eller entiteter från ett tredjeland, eller en medborgare i ett tredjeland, utgör en betydande icke-teknisk cybersäkerhetsrisk för ekonomisk eller samhällelig verksamhet i minst tre medlemsstater, ska kommissionen utan dröjsmål samråda med medlemsstaterna om behovet av att vidta åtgärder på unionsnivå.

7. Kommissionen ges befogenhet att anta genomförandeakter för att fastställa att den specifika typ av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 ska förbjudas att använda, installera eller integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från en entitet som avses i punkt 6. I detta syfte ska den samråda med de entiteter av de typer som avses i bilagorna I och II till direktiv (EU) 2022/2555 vilka potentiellt berörs av förbudet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2. När så är relevant ska de inbegripa lämpliga perioder för utfasning av dessa IKT-komponenter eller komponenter som innehåller IKT-komponenter. Sådana genomförandeakter får också specificera dessa IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka omfattas av förbudet. Detta

förbud ska också gälla IKT-komponenter eller komponenter som innehåller IKT-komponenter från alla entiteter som kontrolleras av den specifika entitet som avses i punkt 6.

8. I de genomförandeakter som avses i punkterna 1, 2 och 7 får det också anges att begränsningsåtgärderna endast är tillämpliga på typer av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 av en viss storlek.

9. Artikel 100.4 ska tillämpas på den specifika entitet som är etablerad i eller kontrolleras av ett tredjeland, en entitet från ett tredjeland eller en medborgare i ett tredjeland och som avses i punkt 7.

10. De genomförandeakter som antas i enlighet med punkterna 1, 2 och 7 och som är tillämpliga på den typ av entiteter som avses i punkt 10 i bilaga I till direktiv (EU) 2022/2555 ska i tillämpliga delar tillämpas på EU:s institutioner, organ och byråer.

Artikel 104
Identifiering av högriskleverantörer

1. Kommissionen ska genom genomförandeakter upprätta förteckningar över högriskleverantörer av relevans för de förbud som fastställs i de genomförandeakter som antagits i enlighet med artikel 103.1 eller 103.7 eller det förbud som avses i artikel 111.1.

2. I detta syfte ska kommissionen kartlägga de leverantörer som tillhandahåller IKT-komponenter och komponenter som innehåller IKT-komponenter och som är relevanta för det förbud som avses i punkt 1.

   På grundval av detta ska kommissionen göra en inledande bedömning för att identifiera vilka av de kartlagda leverantörerna som potentiellt är etablerade i ett tredjeland som utsetts i enlighet med artikel 100 eller kontrolleras av ett sådant tredjeland, en entitet etablerad i ett sådant tredjeland eller en medborgare i ett sådant tredjeland. Kommissionen ska också göra en inledande kartläggning av leverantörer som potentiellt kontrolleras av den entitet som avses i artikel 103.6.

3. Kommissionen ska bedöma etableringsorten samt ägar- och kontrollstrukturen för de leverantörer som inledningsvis identifierats i enlighet med punkt 2 andra stycket.

4. För den bedömning som avses i punkt 3 ska kommissionen ha rätt att begära nödvändig information från leverantörerna. Om leverantören inte tillhandahåller den nödvändiga informationen inom den fastställda tidsfristen får kommissionen dra slutsatsen att leverantören är etablerad i ett tredjeland som utsetts i enlighet med artikel 100 eller kontrolleras av ett sådant tredjeland, entiteter från ett sådant tredjeland eller medborgare i ett sådant tredjeland. Om kommissionen genomför en bedömning enligt artikel 103.7 och leverantören inte tillhandahåller den nödvändiga informationen inom den fastställda tidsfristen får kommissionen dra slutsatsen att leverantören kontrolleras av en entitet som har utsetts i enlighet med den artikeln. De behöriga myndigheter som avses i artikel 112 ska också på begäran dela relevant information med kommissionen.

5. Kommissionen ska dela med sig av de preliminära resultaten av bedömningen av etablerings-, kontroll- och ägandestruktur till den berörda leverantören. Kommissionen ska ge leverantören möjlighet att höras angående dessa preliminära resultat.

6. Kommissionen får be en behörig myndighet att göra den inledande bedömningen av en leverantörs etablerings-, ägande- och kontrollstruktur, när detta är motiverat med hänsyn till särdragen för leverantörens verksamhet. En behörig myndighet får erbjuda sig att utföra denna inledande bedömning. Kommissionen ska kontrollera dessa inledande resultat i syfte att besluta om leverantören bör föras upp på förteckningen över högriskleverantörer.

7. Kommissionen ska regelbundet uppdatera förteckningen över högriskleverantörer i syfte att ta bort eller lägga till högriskleverantörer. Högriskleverantörer som ingår i förteckningen får begära att kommissionen gör en ny bedömning av deras etablerings-, kontroll- och ägandestruktur på grundval av bevis att det har skett relevanta ändringar.

8. Om en behörig myndighet får kännedom, till exempel på grundval av information från en entitet av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555, om att en leverantör kan behöva tas upp i en förteckning över högriskleverantörer ska den utan onödigt dröjsmål informera kommissionen.

Artikel 105

Undantag för entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem

1. En entitet som är etablerad i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem och som har utsetts i enlighet med artikel 100 får lämna en motiverad begäran till kommissionen om att undantas

   a) från förbudet för entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 mot att i någon form använda, installera eller integrera sina IKT-komponenter eller komponenter som innehåller de egna IKT-komponenterna i dessa entiteters viktiga IKT-tillgångar genom undantag från artikel 111 eller de genomförandeakter som antagits i enlighet med artikel 103.1,

   b) från förbudet mot att delta i offentliga upphandlingsförfaranden som anordnas i enlighet med den lagstiftning som införlivar direktiv 2014/24/EU och direktiv 2014/25/EU när det gäller tillhandahållande av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka ska användas i viktiga IKT-tillgångar som identifierats i enlighet med artikel 102, genom undantag från artikel 100.4.

2. Den begäran som avses i punkt 1 ska

   a) specificera vilket intresse den entitet som är etablerad i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem och som har utsetts i enlighet med artikel 100 har av att beviljas det undantag som avses i punkt 1 i denna artikel, och

   b) med tydliga bevis påvisa att effektiva begränsningsåtgärder kommer att införas för att hantera icke-tekniska risker och säkerställa att det tredjeland som utsetts i enlighet med artikel 100 inte på något sätt otillbörligen kan blanda sig i tillhandahållandet av IKT-komponenter eller komponenter som innehåller IKT-komponenter för användning, installation eller integrering i viktiga IKT-tillgångar som tillhör en entitet av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555.

3. Kommissionen ges befogenhet att anta genomförandeakter för att ytterligare specificera de villkor som avses i punkt 2 b och för att fastställa närmare regler om de förfaranden som avses i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

4. Kommissionen ska bedöma den begäran som avses i punkt 1 genom ett rättvist och transparent förfarande med beaktande av

   a) de omständigheter och ytterligare faktorer som avses i artikel 100.1 och 100.2 med avseende på det utsedda land som utgör cybersäkerhetsproblem för IKT-leveranskedjor i vilket entiteten är etablerad eller varifrån den kontrolleras,

   b) effektiviteten hos de begränsningsåtgärder som avses i punkt 2 b,

   c) huruvida undantaget för den entitet som är etablerad i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem för IKT-leveranskedjor skulle skada unionens intresse.

5. När kommissionen efter bedömningen i punkt 3 drar slutsatsen att det är motiverat att bevilja ett undantag ska den göra detta genom ett beslut som den ska delge sökanden inom nio månader från mottagandet av begäran.

6. När kommissionen antar ett beslut som avses i punkt 4 får den begränsa undantaget till en viss tidsperiod och får förena undantaget med villkor för entiteten, bland annat i form av

   a) en tidsram för genomförandet av de begränsningsåtgärder som avses i punkt 2 b,

   b) regelbundna tredjepartsgranskningar för att säkerställa ett effektivt genomförande av begränsningsåtgärderna,

   c) rapporteringsskyldigheter när det gäller efterlevnad.

7. När kommissionen efter bedömningen i punkt 3 drar slutsatsen att det inte är motiverat att bevilja ett undantag ska den göra detta genom ett beslut, och ska delge sökandena detta inom nio månader från mottagandet av begäran.

8. Kommissionen får på eget initiativ återkalla eller ändra det beslut som avses i punkt 4 i en eller flera av följande situationer:

   a) Det har skett en väsentlig förändring av de sakförhållanden som låg till grund för beslutet.

   b) Den entitet som begärde undantaget handlar i strid med sina åtaganden.

   c) Undantaget grundades på ofullständig, felaktig eller vilseledande information från den entitet som lämnade in begäran.

Artikel 106
Rätten till försvar

Kommissionen ska säkerställa att den berörda entiteten ges möjlighet att yttra sig innan den antar en genomförandeakt enligt artikel 103.7 eller innan den antar ett beslut om att inte bevilja undantag enligt artikel 105.7 på grundval av att sökanden inte har lämnat vissa uppgifter eller innan den återkallar ett beslut enligt 105.8, med beaktande av behovet av ett skyndsamt förfarande i vissa fall.

Artikel 107
Register

Kommissionen ska föra ett offentligt register över sina beslut enligt artikel 105.5. Registret ska innehålla namnen på de entiteter som omfattas av sådana beslut. Kommissionen ska regelbundet uppdatera registret.

Artikel 108
Konfidentialitet

Information som kommissionen tar emot i enlighet med artiklarna 105 och 106 får endast användas för de ändamål för vilka de inhämtades.

Artikel 109
Avgifter

1. Kommissionen ska ta ut avgifter för begäranden som lämnas in i enlighet med artikel 105.1.
2. Alla avgifter ska anges och betalas i euro.
3. Avgifterna ska stå i proportion till kostnaderna i samband med behandlingen av de begäranden som avses i artikel 105.1, bedömningen av de kriterier och den information som avses i artikel 105.2 samt upprättandet, underhållet och driften av det register som avses i artikel 107. Alla kommissionens utgifter för personal som deltar i denna verksamhet ska ingå i dessa kostnader.
4. Kommissionen ska anta genomförandeakter med närmare regler om avgifterna, där den specificerar avgiftsbeloppen och hur de ska betalas. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.

KAPITEL II
IKT-leveranskedjor i elektroniska kommunikationsnät

Artikel 110
Viktiga IKT-tillgångar för mobila, fasta och satellitbaserade elektroniska kommunikationsnät

1. De viktiga IKT-tillgångarna för mobila, fasta och satellitbaserade elektroniska kommunikationsnät ska vara de som anges i bilaga II.
2. IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka tillhandahålls av högriskleverantörer ska fasas ut från de viktigaste IKT-tillgångarna i mobila, fasta och satellitbaserade elektroniska kommunikationsnät.
3. Tidsperioden för utfasning av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka tillhandahålls av högriskleverantörer med avseende på mobila elektroniska kommunikationsnät får inte överstiga 36 månader från offentliggörandet av den förteckning över högriskleverantörer som avses i artikel 104 och som är relevant för mobila elektroniska kommunikationsnät.
4. Kommissionen ges befogenhet att anta genomförandeakter i enlighet med artikel 118.2 för att specificera tidsperioderna för utfasning av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka tillhandahålls av

högriskleverantörer med avseende på fasta och satellitbaserade elektroniska kommunikationsnät.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 119 för att ändra bilaga II till denna förordning i syfte att anpassa den till den tekniska utvecklingen genom att beakta de faktorer som avses i artikel 103.4.

Artikel 111

Förbud för mobila, fasta och satellitbaserade elektroniska kommunikationsnät

1. Leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät får inte i någon form använda, installera eller integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer vid driften av viktiga IKT-tillgångar som avses i bilaga II.

2. I fall där den behöriga myndighet som utsetts enligt denna förordning i en medlemsstat är en annan myndighet än den behöriga myndigheten enligt förordning (EU) XX/XXXX [förslaget till förordning om digitala nätverk], ska den behöriga myndighet som utsetts enligt den här förordningen utan dröjsmål informera den behöriga myndigheten enligt förordning (EU) XX/XXXX [förslaget till förordning om digitala nätverk] om de åtgärder som åläggs leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät i enlighet med artikel 114. Myndigheterna ska säkerställa ett nära samarbete för en effektiv tillsyn och kontroll av efterlevnaden av dessa åtgärder.

KAPITEL III

Behöriga myndigheter, tillsyn och efterlevnadskontroll, jurisdiktion och rätt till försvar

Artikel 112

Behöriga myndigheter

1. Varje medlemsstat ska utse de behöriga myndigheter som avses i artikel 8 i direktiv (EU) 2022/2555 till myndigheter med ansvar för att vidta de tillsyns- och efterlevnadskontrollåtgärder som avses i artikel 114.

2. De behöriga myndigheterna ska vara strukturellt och funktionellt helt opartiska och fria från all yttre påverkan, oavsett om den är direkt eller indirekt; de ska i synnerhet varken be om eller ta emot instruktioner från någon annan myndighet eller någon privat part.

3. Medlemsstaterna ska säkerställa att deras behöriga myndigheter har lämpliga befogenheter, tillräckliga personalresurser och tekniska resurser och relevant sakkunskap för att effektivt utföra de tillsyns- och efterlevnadskontrollåtgärder som avses i artikel 114.

4. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen namnen på de behöriga myndigheter som utsetts i enlighet med punkt 1, dessa myndigheters respektive uppgifter och eventuella senare ändringar av dessa. Varje medlemsstat ska också offentliggöra namnen på de behöriga myndigheter som utsetts i enlighet med punkt 1.

Artikel 113
Kommissionens samarbets- och stödtjänstnätverk

För att få till stånd en effektiv tillsyn ska kommissionen inrätta ett nätverk för samarbete mellan de behöriga myndigheter i medlemsstaterna som avses i artikel 112 och kommissionen, vilket ska fungera som en plattform för samarbete och informationsutbyte, särskilt när det gäller den bedömning av etablerings-, kontroll- och ägandestruktur som avses i artikel 104. Kommissionen ska ge administrativt stöd till nätverket.

Artikel 114
Tillsyns- och efterlevnadskontrollåtgärder

1. De behöriga myndigheter som avses i artikel 112 har rätt att vidta tillsyns- och efterlevnadskontrollåtgärder avseende entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555. Medlemsstaterna ska säkerställa att ovannämnda åtgärder är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall. Medlemsstaterna ska underrätta kommissionen om de regler som antagits för detta ändamål och om senare ändringar av dessa.

2. När de behöriga myndigheterna utövar sina tillsynsuppgifter avseende de entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 har de rätt att göra dessa entiteter föremål för följande:

   a) Begäranden om en detaljerad och aktuell förteckning över deras relevanta leverantörer och tjänsteleverantörer.

   b) Begäranden om tillgång till uppgifter, handlingar och information som behövs för att kontrollera efterlevnaden av denna förordning.

   c) Inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller som utförs av utbildad personal.

   d) Begäranden om sammansättningen av maskinvaru- eller programvaruprodukter som installeras eller integreras i någon form i nätet eller systemet, inbegripet komponenter och transitiva beroenden, i ett allmänt använt och maskinläsbart format.

3. När de behöriga myndigheterna utövar sina efterlevnadskontrollbefogenheter avseende entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 har de rätt att

   a) utfärda varningar om de berörda entiteternas överträdelser av denna förordning, med angivande av relevanta fakta och rättsliga överväganden,

   b) anta beslut som ålägger de berörda entiteterna att avhjälpa överträdelsen av denna förordning eller de brister som konstaterats vid genomförandet av begränsningsåtgärder,

   c) ålägga de berörda entiteterna att upphöra med verksamhet som utgör en överträdelse av denna förordning och att avstå från att upprepa överträdelserna, och

   d) ålägga sanktioner i enlighet med reglerna om beloppet i artikel 115 eller begära att relevanta organ, domstolar eller tribunaler ålägger sådana sanktioner, i enlighet med nationell rätt.

4. När de behöriga myndigheterna vidtar någon av de efterlevnadskontrollåtgärder som avses i föregående punkt ska de beakta omständigheterna i varje enskilt fall och ta vederbörlig hänsyn till följande faktorer:

   a) Överträdelsens svårighetsgrad och de överträdda bestämmelsernas betydelse.

   b) Överträdelsens varaktighet.

   c) Den berörda entitetens relevanta omsättning.

   d) Eventuella tidigare relevanta överträdelser från den berörda entitetens sida.

   e) I tillämpliga fall, den materiella eller immateriella skada som uppstått till följd av överträdelsen, inbegripet finansiella eller ekonomiska förluster, effekter på andra entiteter och det antal användare som berörs.

   f) Uppsåt eller oaktsamhet från den berörda entitetens sida.

   g) De åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan.

   h) I vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

   Vid tillämpningen av första stycket a ska följande utgöra allvarliga överträdelser:

   i) Upprepade överträdelser.

   j) Underlåtenhet att underrätta om eller avhjälpa betydande incidenter.

   k) Underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter.

5. De behöriga myndigheterna ska underrätta de berörda entiteterna om sina preliminära resultat innan de vidtar efterlevnadskontrollåtgärder. De berörda entiteterna ska ges rimlig tid att lämna synpunkter på de preliminära resultaten. De behöriga myndigheterna ska utförligt motivera sina efterlevnadskontrollåtgärder.

6. De behöriga myndigheterna ska respektera principerna om konfidentialitet, tystnadsplikt och företagshemlighet.

7. De behöriga myndigheterna ska samarbeta med varandra och med kommissionen för tillsyn och efterlevnadskontroll enligt denna avdelning i enlighet med artikel 116.

Artikel 115
Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas.

2. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål eventuella ändringar som berör dem.

3. Sanktioner ska åläggas utöver de åtgärder som avses i artikel 114.3 a, b och c.

4. När beslut fattas om huruvida en sanktion ska åläggas och om avgiftsbeloppet i varje enskilt fall, ska vederbörlig hänsyn tas till åtminstone de faktorer som avses i artikel 114.4 första stycket.

5. Överträdelser av artikel 103.2 a ska i enlighet med punkt 3 i den här artikeln leda till sanktioner på högst 1 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som entiteten tillhör.

6. Överträdelser av artikel 103.2 b–g ska i enlighet med punkt 3 i den här artikeln leda till sanktioner på högst 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som entiteten tillhör.

7. Överträdelser av artiklarna 103.1 och 111 ska i enlighet med punkt 3 i den här artikeln leda till sanktioner på högst 7 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som entiteten tillhör.

Artikel 116
Ömsesidigt bistånd

1. Om en entitet av den typ som avses i bilaga I eller II till direktiv (EU) 2022/2555 tillhandahåller tjänster i fler än en medlemsstat, eller tillhandahåller tjänster i en eller flera medlemsstater och dess viktiga IKT-tjänster är belägna i en eller flera andra medlemsstater, ska de behöriga myndigheterna i de berörda medlemsstaterna samarbeta med varandra och kommissionen och bistå varandra och kommissionen i syfte att säkerställa en ändamålsenlig och effektiv tillämpning av förordningen. I detta syfte ska åtminstone följande regler gälla:

   a) De behöriga myndigheter som tillämpar tillsyns- eller efterlevnadskontrollåtgärder i en medlemsstat ska informera och samråda med de behöriga myndigheterna i övriga berörda medlemsstater om de tillsyns- och efterlevnadskontrollåtgärder som vidtagits.

   b) En behörig myndighet i en medlemsstat får begära att en annan behörig myndighet i en annan medlemsstat vidtar tillsyns- eller efterlevnadskontrollåtgärder.

   c) En behörig myndighet i en medlemsstat ska, efter att ha mottagit en motiverad begäran från en annan behörig myndighet i en annan medlemsstat, göra sitt bästa för att ge den andra behöriga myndigheten ömsesidigt bistånd, så att tillsyns- eller efterlevnadskontrollåtgärderna kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt.

2. Det ömsesidiga bistånd som avses i punkt 1 c får omfatta begäranden om information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får inte avslå begäran om det inte fastställs att myndigheten inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga intressen som rör nationell säkerhet, allmän säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med kommissionen.

3. När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra gemensamma tillsynsåtgärder.

4. Med tanke på skyldigheten att följa de principer om konfidentialitet, tystnadsplikt och företagshemlighet som avses i artikel 114.6 ska all information som utbyts i

samband med en begäran om bistånd och som tillhandahålls i enlighet med den här artikeln endast användas med avseende på det ärende för vilket den begärdes.

Artikel 117
Jurisdiktion och territorialitet

1. Entiteter av en typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 vilka omfattas av denna förordnings tillämpningsområde ska anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller följande:

   a) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, som ska anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster.

   b) Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster och leverantörer av utlokaliserade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, vilka ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

   c) Offentliga förvaltningsentiteter, som ska anses omfattas av jurisdiktionen i den medlemsstat som de tillhör.

   d) Lufttrafikföretag, som ska anses omfattas av jurisdiktionen i den medlemsstat vars behöriga tillståndsmyndighet har beviljat entiteten dess operativa licens i enlighet med Europaparlamentets och rådets förordning (EG) nr 1008/2008[83]; om den operativa licensen eller motsvarande inte har beviljats i enlighet med den förordningen ska de anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

2. Vid tillämpning av denna förordning ska en entitet som avses i punkt 1 b anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där de flesta cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda entiteten har det etableringsställe som har flest anställda i unionen.

3. Om en entitet av en typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om en sådan entitet är en entitet som avses i punkt 1 a ska den anses omfattas av jurisdiktionen i den medlemsstat där den tillhandahåller sina tjänster. Om det inte finns en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av denna förordning.

---

[83] Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen (omarbetning) (EUT L 293, 31.10.2008, s. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj).

4. Det faktum att en entitet som avses i punkt 1 b utsett en företrädare ska inte påverka eventuella rättsliga åtgärder mot entiteten i sig.

5. De medlemsstater som har mottagit en begäran om ömsesidigt bistånd med avseende på en entitet som avses i punkt 1 b får, inom ramen för den begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den berörda entiteten om entiteten tillhandahåller tjänster eller har ett nätverks- och informationssystem inom deras territorium.

AVDELNING VI
SLUTBESTÄMMELSER

Artikel 118
Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Kommittén ska ha två konstellationer. När det gäller avdelningarna II och III ska kommissionen bistås av en kommitté i den första konstellationen, medan kommissionen när det gäller avdelning IV ska biträdas av den andra konstellationen. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 119
Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 80.2 och 110.5 ska ges till kommissionen tills vidare från och med den dag då denna förordning träder i kraft.

3. Den delegering av befogenhet som avses i artiklarna 80.2 och 110.5 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 80.2 och 110.5 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att

invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 120
Utvärdering och granskning

1. Senast den [DD MM ÅÅÅÅ] och därefter vart femte år ska kommissionen beställa en utvärdering som ska genomföras i enlighet med kommissionens riktlinjer.

2. Den utvärdering som avses i punkt 1 ska innefatta en bedömning av följande:

   a) Enisas resultat i förhållande till dess mål, mandat, uppdrag, uppgifter, styrning och lokalisering.

   b) Ändamålsenligheten, effektiviteten och EU-mervärdet hos ordningarna för europeiska individuella intyg om cybersäkerhetskompetens i den mening som avses i avdelning II kapitel II avsnitt 4 i denna förordning.

   c) Effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i denna förordning i fråga om målen att säkerställa en tillräcklig nivå av cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteter i unionen och förbättra den inre marknadens funktion.

   d) Effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning IV i denna förordning i fråga om målen för ramverket för en betrodd IKT-leveranskedja.

3. Den utvärdering som avses i punkt 1 a ska särskilt ta upp eventuella behov av att ändra Enisas mandat samt de finansiella följderna av sådana ändringar.

4. Vid varannan sådan utvärdering som avses i punkt 1 a ska kommissionen bedöma de resultat som uppnåtts av Enisa med hänsyn till dess mål, mandat, uppdrag, styrning och uppgifter, inbegripet en bedömning av huruvida Enisas existens fortsatt är berättigad med avseende på målen, mandatet, uppdraget, styrningen och uppgifterna.

5. Kommissionen ska meddela resultatet av utvärderingen till Europaparlamentet, rådet och styrelsen. Utvärderingens resultat ska offentliggöras.

Artikel 121
Upphävande och fortsatt verksamhet

1. Europaparlamentets och rådets förordning (EU) 2019/881 upphör att gälla med verkan från och med den DDMMÅÅÅÅ.

2. Hänvisningar till förordning (EU) 2019/881, Enisa och europeiska ordningar för cybersäkerhetscertifiering som inrättats genom den förordningen ska anses som hänvisningar till den här förordningen och ska läsas i enlighet med jämförelsetabellen i bilaga III till den här förordningen.

3. Enisa i den form som byrån inrättas genom den här förordningen ska ta över den verksamhet och de aktiviteter som inletts av Enisa i den form som byrån inrättades genom förordning (EU) 2019/881 när det gäller all äganderätt samt alla avtal, rättsliga skyldigheter, anställningsavtal, finansiella åtaganden och ansvarsskyldigheter. Alla beslut som styrelsen och direktionen har fattat i enlighet med förordning (EU) 2019/881 ska fortsätta att gälla, förutsatt att de överensstämmer med den här förordningen.

4. Den verkställande direktör som har utsetts i enlighet med artikel 15.1 n i förordning (EU) 2019/881 ska kvarstå i tjänst och utöva de uppgifter och ha det ansvar som den verkställande direktören har enligt artikel 32 i den här förordningen under den återstående delen av den verkställande direktörens mandatperiod. Övriga villkor i anställningsavtalet ska vara oförändrade.

5. De förslag till certifieringsordning vars utarbetande har begärts i enlighet med artikel 49 i förordning (EU) 2019/881 ska anses ha begärts i enlighet med motsvarande bestämmelser i den här förordningen. Bestämmelserna i avdelning III i denna förordning ska tillämpas på dessa förslag till certifieringsordningar i enlighet med detta.

6. De styrelseledamöter som utsetts av kommissionen och de suppleanter som utsetts i enlighet med artikel 14 i förordning (EU) 2019/881 ska kvarstå i tjänst och utöva de styrelseuppgifter som avses i artikel 27 i den här förordningen under den återstående delen av sina mandatperioder. De styrelseledamöter som utsetts av medlemsstaterna i enlighet med artikel 14 i förordning (EU) 2019/881 ska kvarstå i tjänst och utöva de styrelseuppgifter som avses i artikel 27 i den här förordningen under förutsättning att de innehar de befattningar som avses i artikel 24.3 i den här förordningen.

Artikel 122
Ikraftträdande

Denna förordning träder i kraft den […] dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGS- OCH DIGITALISERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1 Förslagets eller initiativets titel

Förslag till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), om det europeiska ramverket för cybersäkerhetscertifiering och om säkerhet i IKT-leveranskedjan samt om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakt 2)

(Text av betydelse för EES)

Kort rubrik: Andra cybersäkerhetsakten

och

Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till cybersäkerhetsakt 2]

1.2 Berörda politikområden

Politikområde: 09 – Kommunikationsnät, innehåll och teknik

Verksamhet: 09.02 Den digitala inre marknaden

1.3 Mål

1.3.1 Allmänt/allmänna mål

Insatserna har följande huvudmål:

1) Öka kapaciteten och resiliensen på cybersäkerhetsområdet

Bidra till att stärka unionens styrning av cybersäkerheten och hjälpa till att säkerställa att de relevanta institutionerna och myndigheterna samt andra berörda parter är bättre rustade för att förebygga, upptäcka och reagera på cybersäkerhetshot på ett samordnat och effektivt sätt.

2) Förhindra fragmentering på den inre marknaden genom att

stödja utvecklingen, genomförandet och användningen av unionens gemensamma cybersäkerhetsinstrument, såsom certifieringsordningar, samt tillhandahålla harmoniserade ramar som skapar förtroende och interoperabilitet mellan medlemsstaterna.

Dessa allmänna mål motsvarar de centrala utmaningar som konstaterades i problemformuleringen i konsekvensbedömningen av det föreslagna initiativet. De återspeglar det övergripande politiska målet att stärka cybersäkerhetsstyrningen i unionen och stödja utvecklingen av en säker, resilient och konkurrenskraftig digital inre marknad.

1.3.2 Specifikt/specifika mål

Ta itu med den bristande överensstämmelsen mellan EU:s policyram för cybersäkerhet och berörda parters behov:

Specifikt mål nr 1: skapa kapacitet att effektivt genomföra unionens cybersäkerhetspolitik och kontinuerliga operativa samarbete som möjliggör ett mer strukturerat samarbete mellan medlemsstaterna.

Specifikt mål nr 2: utveckla och genomföra medel och mekanismer för att effektivt stödja och tillgodose behoven hos medlemsstaterna, näringslivet och andra berörda parter.

Komma till rätta med den begränsade användningen av och ändamålsenligheten hos det europeiska ramverket för cybersäkerhetscertifiering:

Specifikt mål nr 3: skapa förutsättningar för ett snabbare genomförande av ordningar för cybersäkerhetscertifiering som drivs av marknadsbehov genom att utvidga tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering, säkerställa effektivt underhåll och smidiga förfaranden samt öka öppenheten.

Ta itu med det fragmenterade efterlevnadslandskapet och komplexiteten i övergripande och sektorsspecifika ramar:

Specifikt mål nr 4: skapa mekanismer och villkor för att underlätta efterlevnaden av cybersäkerhetskraven och därigenom göra genomförandet mer samstämmigt och effektivt.

Ta itu med cybersäkerhetsrisker i leveranskedjan:

Specifikt mål nr 5: minska de risker för kritiska IKT-leveranskedjor som orsakas av entiteter som är etablerade i eller kontrolleras av entiteter från länder som utgör cybersäkerhetsproblem (högriskleverantörer) och minska kritiska beroenden genom att utarbeta en samstämmig och ändamålsenlig ram på EU-nivå för att hantera säkerhetsrisker för IKT-leveranskedjan.

1.3.3 Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

De förväntade resultaten är följande:

1) Funktionell reform av Enisa.

2) Reform av det europeiska ramverket för cybersäkerhetscertifiering – utvidgning av tillämpningsområdet, nytt förfarande och reviderad styrning.

3) Ytterligare förenkling av efterlevnaden av den relevanta unionslagstiftningen för cybersäkerhet.

4) En heltäckande och övergripande ram för att hantera cybersäkerhetsrisker för IKT-leveranskedjor.

Övergripande verkan:

Förslaget kommer att få en enorm inverkan på cybersäkerheten i unionen eftersom det berör ett antal olika områden, däribland den nödvändiga förstärkningen av Enisa; det stärker även stödet för genomförandet av EU-lagstiftningen, inför reformer för ett smidigt genomförande av det europeiska ramverket för cybersäkerhetscertifiering, stöder unionens gemensamma förståelse av cyberhoten och begränsar cybersäkerhetsrisker utifrån den geopolitiska verkligheten. Genomförandet av de föreslagna bestämmelserna kommer att säkerställa hög effektivitet och samstämmighet, samtidigt som en alltför stor regelbörda undviks. Paketet är utformat för att stå emot utmaningar i samband med genomförandet och stödja långsiktig politisk samstämmighet i det digitala ekosystemet och cybersäkerhetsekosystemet. Det förbättrar tydligheten, avlägsnar ineffektivitet och anpassar förfarandena inom de rättsliga ramarna, samtidigt som det bidrar till att uppnå en hög cybersäkerhetsnivå i

hela EU. De planerade förenklingsinsatserna motsvarar ett av EU-kommissionens främsta prioriterade mål och kommer att ge betydande ekonomiska fördelar för företag, däribland små och medelstora företag, på över 14,63 miljarder EUR och för myndigheter på 7,5 miljoner EUR.

Bland de specifika resultaten ingår följande:

- Öka medvetenheten och förbättra den operativa samordningen, vilket skulle kunna medföra betydande kostnadsbesparingar kopplade till den snabbare upptäckten och hanteringen av incidenter för företag, myndigheter och allmänheten.
- Förtydliga Enisas räckvidd och befogenheter och samtidigt säkerställa en nödvändig prioritering av dess primära uppgifter.
- Se till att berörda parter får tillräckligt stöd för genomförandet av politiken, den operativa verksamheten och den övergripande samordningen.
- Stödja unionens gemensamma situationsmedvetenhet.
- Fördjupa samarbetet med EU-CyCLONe, CSIRT-nätverket, kommissionen, Europol och CERT-EU samt relevanta unionsentiteter i syfte att utveckla en databas med verifierade, tillförlitliga underrättelser om cyberhot.
- Stödja insatserna för att begränsa attacker med utpressningsprogram.
- Förbättra samordningen med den privata sektorn om cybersäkerhetsrelaterade frågor.
- Sprida information i god tid genom tidiga varningar om betydande eller storskaliga incidenter, eller ett gränsöverskridande cyberhot, i förhållande till de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.
- Främja effektiva synergier med andra EU-organ och EU-byråer.
- Sänka priset på kompetenscertifikat, bland annat genom att öka utbudet på marknaden genom att införa ordningar för europeiska kompetensintyg.
- Bidra till att överbrygga kompetensklyftan i Europa genom individuella intyg om cybersäkerhetskompetens samt hjälpa medlemsstaterna och näringslivet att stärka sin arbetskraft.
- Åtgärda bristen på tydlighet i det europeiska ramverket för cybersäkerhetscertifiering och dess begränsade effekter samt utvidga ramverkets tillämpningsområde och förbättra dess styrningsmodell.
- Öka anseendet hos antagna ordningar genom att inrätta en underhållsstruktur och införa en process för snabb och öppen utveckling.
- Införa avgiftsmekanismer i förhållande till kostnaderna för att utveckla och underhålla ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, för att handlägga ansökningar och bevilja auktorisationer till tillhandahållare samt för att underhålla ordningar som antagits inom det europeiska ramverket för cybersäkerhetscertifiering, vilket kommer att bidra till byråns finansiella stabilitet och generera besparingar inom ramen för EU:s budget.
- Anpassa de europeiska certifieringsordningarna till den befintliga lagstiftningen och därmed bättre stödja genomförandeinsatserna och företagens efterlevnadsbehov.

- Göra det möjligt att anta ordningar som för närvarande är blockerade.
- Främja de europeiska företagens konkurrenskraft genom att underlätta anpassning mellan internationella och europeiska standarder.
- Begränsa fragmenteringen av cybersäkerhetsåtgärder och cybersäkerhetskrav.
- Tillhandahålla rättslig klarhet och avsevärt minska den administrativa bördan, utan att skapa betydande rättsosäkerhet för berörda parter som håller på att anpassa sig till de nya rättsliga ramarna.
- Underlätta efterlevnaden för NIS 2-entiteter, vilket även skulle bidra till ökad efterlevnad överlag, liksom mer meningsfulla cybersäkerhetsåtgärder, samtidigt som myndigheternas tillsynsprocess effektiviseras.

Övrigt

- Små och medelstora företag skulle dra nytta av många fördelar av initiativet med tanke på den ökade konkurrenskraften på EU:s cybersäkerhetsmarknad samt de minskade kostnaderna och administrativa bördorna:

1. *Små och medelstora företag skulle gynnas av ökad cyberresiliens tack vare Enisas förstärkta roll och teknisk vägledning från byrån.*
2. *Små och medelstora företag som har auktoriserats att utfärda intyg inom ramen för ordningen för europeiska kompetensintyg kommer att bli mer synliga, förbättra sitt anseende och locka nya kunder. Dessutom kommer de europeiska individuella intygen om cybersäkerhetskompetens att hjälpa små och medelstora företag att hitta arbetssökande med rätt kompetens.*
3. *Välfungerande europeiska certifieringsordningar kan underlätta valet av tillförlitlig IKT-teknik för små och medelstora företag och bidra till att förbättra deras övergripande cyberresiliens.*
4. *Små och medelstora företag som levererar DNS-tjänster kommer att gynnas av åtgärder kopplade till genomförandet av NIS 2-direktivet tack vare undantag från tillämpningsområdet för leverantörer av DNS-tjänster.*
5. *Små och medelstora företag skulle gynnas av de förtydliganden om tillämpningsområdet som skulle begränsa tillämpningen av skyldigheterna för vissa entiteter i vissa sektorer som förtecknas i NIS 2-direktivet.*
6. *När det gäller säkerhetsåtgärderna för IKT-leveranskedjan skulle små och medelstora företag i allmänhet gynnas av användningen av tillförlitlig teknik. I egenskap av leverantörer som är verksamma inom de sektorer som omfattas av restriktioner skulle de påverkas mer av ersättningar och transaktionskostnader jämfört med större företag. Små och medelstora företag som är betrodda leverantörer kommer dock att dra nytta av nya marknadsmöjligheter.*

- Ingen betydande miljöpåverkan förväntas för något av målen.
- Med avseende på EU-budgeten kan effektivitetsvinster förväntas genom ökat samarbete och samordning av verksamheten mellan EU:s institutioner, byråer och organ. Besparingar förväntas på lång sikt genom införandet av avgiftsmekanismer.

1.3.4 Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

Mål: skapa kapacitet att effektivt genomföra EU:s cybersäkerhetspolitik och regelbundna/kontinuerliga operativa samarbete som möjliggör ett mer strukturerat samarbete mellan medlemsstaterna.

— Antal relevanta bidrag från Enisa till genomförandet av EU:s och medlemsstaternas politik och lagstiftningsinitiativ.

— Positiv återkoppling från berörda parter om de relevanta bidragen från Enisa.

— Ökning med 25 % jämfört med 2023 års referensvärde enligt Enisas årliga verksamhetsrapport (för antalet relevanta bidrag) och enligt Enisas årliga nöjdhetsundersökning (för den positiva återkopplingen).

— Användningsstatistik för EU:s sårbarhetsdatabas.

— Ökning med 25 % av antalet användare jämfört med 2025.

Tillgängligheten av samt säkerheten och funktionen hos plattformen enligt cyberresiliensförordningen.

— Minskning av plattformens driftstopp och antalet incidenter med 25 % jämfört med 2025 års statistik över driftstopp och incidenter på plattformen.

Mål: utveckla och sprida medel och mekanismer för att effektivt stödja och tillgodose behoven hos medlemsstaterna, näringslivet och andra berörda parter.

— Antal berörda parter som stöds av Enisa och kvaliteten på det tillhandahållna stödet.

— Antal åtgärder som vidtagits för att stödja berörda parter.

— Ökning med 10 % av antalet berörda parter som fått stöd och med 10 % av nöjdhetsgraden bland berörda parter som fått stöd jämfört med 2025.

Mål: skapa förutsättningar för ett snabbare genomförande av ordningar för cybersäkerhetscertifiering som drivs av marknadsbehov genom att utvidga tillämpningsområdet för det europeiska ramverket för cybersäkerhetscertifiering, säkerställa effektivt underhåll och smidiga förfaranden samt öka öppenheten.

— Antal antagna ordningar.

— Minskning av den tid det tar att utveckla en ordning med 50 % jämfört med 2025.

— Antal giltiga certifikat som utfärdas årligen.

— Ökning med 25 % jämfört med 2025 års referensvärde.

— Positiv återkoppling från berörda parter om deras deltagande i utvecklingen av ordningar och öppenheten i det europeiska ramverket för cybersäkerhetscertifiering.

— Ökning med 25 % över referensvärdet i Enisas årliga nöjdhetsundersökning jämfört med 2027.

Mål: inrätta mekanismer och villkor för att underlätta efterlevnaden av cybersäkerhetskraven och därigenom göra genomförandet mer samstämmigt och effektivt.

— Andel av de små och medelstora företagens kostnader för efterlevnaden av NIS 2-direktivet och cybersäkerhetsbestämmelser i förhållande till de totala efterlevnadskostnaderna.

— Rapporterad minskning med >70 % av små och medelstora företags efterlevnadskostnader för cybersäkerhet jämfört med 2025.

— Antal attacker med utpressningsprogram och skadebelopp i EUR.

— Minskning av antalet attacker med utpressningsprogram med > 1 % jämfört med 2027.

— Andel gränsöverskridande incidenter under eller efter vilka medlemsstaternas myndigheter använde mekanismer för ömsesidigt bistånd.

— Ökning av andelen fall där ömsesidigt bistånd användes med > 20 procentenheter jämfört med 2025.

Mål: minska kritiska beroenden genom att utarbeta en samstämmig och ändamålsenlig ram på EU-nivå för att hantera säkerhetsrisker för IKT-leveranskedjan.

— Antal vidtagna åtgärder.

— Ökning med 25 % av antalet vidtagna åtgärder och identifierade viktiga tillgångar jämfört med dagen för antagandet + 6 månader.

— Minskning av beroendet av högriskleverantörer avseende viktiga IKT-tillgångar med 25 % jämfört med 2025.

1.4 Förslaget eller initiativet avser

☒ en ny åtgärd *(avdelning IV Leveranskedjan, avdelning V Förenkling)*

☐ en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[84]

☒ en förlängning av en befintlig åtgärd (*avdelning II Enisas mandat och avdelning III Certifiering*)

☐ en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd

1.5 Grunder för förslaget eller initiativet

1.5.1 Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet

I sina politiska riktlinjer[85] efterlyste Europeiska kommissionens ordförande Ursula von der Leyen i juli 2024 förenkling, konsolidering och kodifiering av EU-lagstiftningen för att undanröja eventuella överlappningar och motsägelser och samtidigt upprätthålla höga krav. I uppdragsbeskrivningen till verkställande vice ordförande Henna Virkkunen[86] nämns särskilt en förbättring av processen för antagande av europeiska ordningar för cybersäkerhetscertifiering och behovet av att

84 I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

85 Politiska riktlinjer 2024–2029.

86 Uppdragsbeskrivning till verkställande vice ordförande Henna Virkkunen.

skydda våra industrier, invånare och offentliga förvaltningar mot interna och externa hot. Vidare efterlyses i Niinistö-rapporten från 2024[87] en riskminskning i fråga om oönskade beroenden av kritisk teknik i leveranskedjan. De centrala aspekterna av rapporten om EU:s framtida konkurrenskraft[88] (*Draghi-rapporten*) och högnivårapporten *Much More Than A Market*[89] (*Letta-rapporten*), som båda beställdes av kommissionens ordförande, återspeglar behovet av att den inre marknaden förblir konkurrenskraftig genom förenkling samt av att högsta möjliga säkerhetsnivå och nivå av strategiskt oberoende säkerställs. Mot denna bakgrund utgör översynen av cybersäkerhetsakten en hörnsten i kommissionens säkerhetsarbete och medför en lansering av en ambitiös översyn av det europeiska ekosystemet av cybersäkerhetsregler. Genom förslaget till en andra cybersäkerhetsakt införs mekanismer för att hantera cybersäkerhetsrisker i leveranskedjan samt mekanismer för att minska det fragmenterade efterlevnadslandskapet och komplexiteten i de övergripande och sektorsspecifika ramarna. Enisa förväntas också bli en drivkraft för förenkling av rapporteringsskyldigheterna genom integreringen av en gemensam kontaktpunkt.

Med tanke på antalet sektorsspecifika bestämmelser som infördes efter antagandet av cybersäkerhetsakten 2019 samt den snabbt föränderliga hotbilden på cybersäkerhetsområdet måste Enisas mandat ses över för att man ska kunna fastställa mer målinriktade och förnyade uppgifter, i syfte att effektivt och ändamålsenligt stödja medlemsstaternas, EU-institutionernas och andra berörda parters insatser för att säkerställa en säker cyberrymd i Europeiska unionen. Genom att stärka det europeiska ramverket för cybersäkerhetscertifiering säkerställer förslaget att EU har ett effektivt, modernt och anpassningsbart certifieringssystem så att man kan vidta åtgärder för leveranskedjan och snabbt genomföra cyberresiliensförordningen. Sammanfattningsvis föreslås en avgränsad räckvidd för mandatet, där man stärker de områden där byrån har visat ett tydligt mervärde och lägger till nya områden där stöd behövs mot bakgrund av de nya politiska prioriteringarna och instrumenten och för att stärka det europeiska ramverket för cybersäkerhetscertifiering.

Översynen av cybersäkerhetsakten är därför ett stort steg mot förändring av EU:s cybersäkerhetsstatus och övergripande säkerhet, beredskap och motståndskraft.

1.5.2 Mervärdet av en åtgärd på EU-nivå (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet av en åtgärd på EU-nivå” i detta avsnitt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.

Cybersäkerhetsakten antogs 2019 med rättslig grund i artikel 114 i EUF-fördraget, som ger unionslagstiftarna befogenhet att besluta om åtgärder för harmonisering av nationella lagar och andra författningar som syftar till att upprätta den inre marknaden och få den att fungera.

Det reviderade förslaget till cybersäkerhetsakt syftar till att effektivisera cybersäkerhetslagstiftningen på EU-nivå genom att komplettera och se över den nuvarande cybersäkerhetsakten, som är i kraft sedan 2019 (*den första cybersäkerhetsakten*). Inom ramen för den inledande översynen bibehålls den första

87 Rapport av Sauli Niinistö.
88 Rapporten om EU:s framtida konkurrenskraft.
89 Enrico Letta, *Much more than a market* (april 2024).

cybersäkerhetsaktens mål att ge ett permanent mandat till Enisa, vars syfte är att stödja en hög gemensam cybersäkerhetsnivå i hela EU, samt undvika fragmentering på den inre marknaden när det gäller ordningar för cybersäkerhetscertifiering. Dessa mål, som redan vederbörligen analyserats i förslaget till cybersäkerhetsakt 2017, kan inte i tillräcklig utsträckning uppnås av medlemsstaterna, utan kan endast uppnås på EU-nivå, i enlighet med artikel 5 i fördraget om Europeiska unionen.

Förslaget till översyn av cybersäkerhetsakten har ett tydligt fokus på att effektivisera, prioritera och kodifiera uppgifterna i all cyberrelaterad lagstiftning, vilket endast kan uppnås på EU-nivå, och det finns för närvarande inget sådant initiativ. Det nya förslaget innebär en ytterligare förstärkning av säkerheten i leveranskedjan och cybersäkerhetssektorn inom EU och en förbättring av medlemsstaternas och näringslivets beredskap och motståndskraft. Beroendet av entiteter som är etablerade i eller kontrolleras av entiteter från tredjeländer som utgör cybersäkerhetsproblem (högriskleverantörer) påverkar entiteter i hela unionen, samtidigt som betydande cybersäkerhetsincidenter i leveranskedjan ofta sprids över nationsgränserna. Att enbart ta itu med frågan på nationell nivå kommer sannolikt inte att vara effektivt.

De uppgifter som Enisa nyligen tilldelats är av avgörande betydelse för att uppnå höga nivåer av cybersäkerhet i hela EU. Trots att byrån arbetar i samordning med andra säkerhetsorgan inom EU, såsom Europol och Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, vilket ansvarar för att finansiera genomförandet, är byråns uppdrag och uppgifter unika, och det finns för närvarande inget annat organ med denna typ av ansvar. Inom EU:s cybersäkerhetsekosystem arbetar alla involverade entiteter i nära samverkan och inom ramen för tydliga mandat. Förslaget till en andra cybersäkerhetsakt förstärker därför enbart de delar där det finns ett tydligt mervärde för att se till att det inte finns några tvetydigheter i fråga om dubbelarbete eller innehållet, men även vad gäller finansiering med andra organ inom cybersäkerhetsekosystemet.

Mer information

Enisas mandat har utvidgats genom senare lagstiftning utan att det gjorts någon omfattande översyn av dess huvudsakliga ansvarsområden och resurser. Detta har skapat överlappningar, ineffektivitet och otillräcklig prioritering av centrala uppgifter till stöd för medlemsstaterna.

Flera medlemsstater har genomfört sina egna nationella ordningar för cybersäkerhetscertifiering, som skiljer sig avsevärt åt i fråga om tillämpningsområde och förfaranden för bedömning av överensstämmelse. Detta skapar marknadsfragmentering och dubbelarbete för aktörer och små och medelstora företag som vill certifieras en gång och bedriva verksamhet i hela EU. Det europeiska ramverket för cybersäkerhetscertifiering inrättades genom cybersäkerhetsakten för att åtgärda marknadsfragmenteringen, men genomförandet har varit långsamt och inkonsekvent.

På samma sätt fastställs i flera övergripande och sektorsspecifika rättsakter cybersäkerhetsåtgärder med olika syften och mål, vilket även leder till skillnader i medlemsstaternas metoder för efterlevnadskontroll och tillsyn. Till följd av detta utsätts entiteter, särskilt små och medelstora företag eller företag som är verksamma i flera medlemsstater, för en ytterligare efterlevnadsbörda, vilket har en negativ inverkan på deras konkurrenskraft.

De olika strategierna för säkerhet i IKT-leveranskedjan och de olika åtgärderna från medlemsstaternas sida leder till marknadsfragmentering och skillnader i efterlevnadskraven för entiteter. Eftersom IKT-leveranskedjorna är gränsöverskridande skulle fragmenteringen av efterlevnadskraven på den inre marknaden framför allt undergräva rättssäkerheten för entiteterna. De olika nationella ramarna för begränsningen av högriskleverantörer riskerar att skapa hinder för rörligheten för varor och tjänster över gränserna inom den inre marknaden. Eftersom IKT-leveranskedjor kan involvera kritiska entiteter och infrastrukturer skapar cybersäkerhetsåtgärdernas fragmentering och brister ytterligare säkerhetsrisker för dessa entiteter, oavsett var dessa leverantörer är etablerade.

Förslagen till program inom den fleråriga budgetramen innehåller dessutom en övergripande bestämmelse enligt vilken högriskleverantörer som identifierats enligt EU-lagstiftningen ska uteslutas för att skydda EU-budgetens integritet och säkerställa att unionens utgifter inte används i strid med unionens väsentliga säkerhetsintressen. Cybersäkerhetsaktens ram för leveranskedjan skulle utgöra den mekanism som möjliggör en sådan identifiering på området IKT-leveranskedjor och kan därför endast genomföras på EU-nivå.

Cyberattacker är till sin natur gränsöverskridande, särskilt med tanke på de spridningseffekter som kan uppstå från vad som inledningsvis var en enda berörd ingångspunkt. Hoten mot och riskerna för cybersäkerheten påverkar hela EU, och därför kan en gemensam situationsmedvetenhet avsevärt förbättra cybersäkerhetsnivåerna för entiteterna inom EU. I förslagen inom ramen för Enisas reviderade mandat tas denna fråga upp i syfte att avsevärt öka EU:s cyberresiliens.

Eftersom cybersäkerhetshoten och de därmed sammanhängande utmaningarna sträcker sig utanför de enskilda medlemsstaterna är åtgärder på unionsnivå av avgörande betydelse. Fragmenterade nationella lösningar har visat sig vara otillräckliga för att uppnå marknadsomfattande förtroende och samordning. Det krävs en reviderad rättslig ram för EU för att undanröja hinder, säkerställa ett konsekvent genomförande och stödja medlemsstaterna i en alltmer komplex lagstiftnings- och hotmiljö.

1.5.3 Erfarenheter från tidigare liknande åtgärder

Enisa grundades 2004 med ett tidsbegränsat mandat. År 2019 trädde cybersäkerhetsakten i kraft och Enisa fick genom dess bestämmelser ett permanent mandat och ett mål om att bli Europas centrum för cyberexpertis. I dag är Enisa ett känt namn och en betrodd partner bland intressenterna i EU. Under loppet av 25 år har byråns befogenheter byggts upp gradvis och återspeglar det föränderliga cybersäkerhetsekosystemet.

Enligt artikel 67 i cybersäkerhetsakten ska kommissionen vart femte år utvärdera effekterna av och ändamålsenligheten och effektiviteten hos Enisas arbete samt dess arbetsmetoder, det eventuella behovet av ändringar samt de finansiella följderna av sådana ändringar. Utvärderingen ska även omfatta en bedömning av effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna om det europeiska ramverket för cybersäkerhetscertifiering.

Kommissionen har i enlighet med bestämmelserna gjort en utvärdering av byrån och det europeiska ramverket för cybersäkerhetscertifiering, som omfattade ett offentligt samråd och en oberoende studie. I enlighet med praxis för bättre lagstiftning har kommissionen även inlett ett offentligt samråd specifikt om översynen av

cybersäkerhetsakten samt en inbjudan att lämna synpunkter för att samla in uppgifter från intressentgrupperna. I utvärderingen drogs slutsatsen att Enisa har fullgjort sitt uppdrag genom att uppnå nästan all planerad output. Byråns mål fortsätter att vara relevanta i dag, med output som erkänns av intressenter framför allt i utmanande tider såsom under covid-19-pandemin och Rysslands anfallskrig mot Ukraina. Trots intressenternas allmänt positiva återkoppling om Enisas output framgick det också att det finns betydande utrymme för förbättringar för att konsekvent uppfylla intressenternas förväntningar.

De lärdomar som dragits har visat att Enisa, för att öka effektiviteten, skulle behöva ha en mer strategisk inriktning, prioritera olika uppgifter samt stärka sin kapacitet för att i god tid ge insikter om nya hot och ha strategiska verktyg för att hantera dem. Såsom har uttryckts av ett antal intressenter skulle Enisa dessutom kunna införa mer strukturerade och transparenta metoder för att samarbeta med privata entiteter, med tonvikt på att stödja små och medelstora företag. I alla externa samråd betonades vikten av att öka Enisas finansiering, personal och operativa kapacitet så att byrån kan uppfylla de växande kraven i EU:s cybersäkerhetslandskap. I sin utvärderingsrapport efter studien bedömde kommissionens avdelningar att det finns ett tydligt behov av framtidssäkrad lagstiftning som kan anpassas till den komplexa och snabbt föränderliga cyberhotbilden samt av att förse byrån med de resurser som krävs för att säkerställa stödet för uppnåendet av de högsta möjliga cybersäkerhetsnivåerna i Europa. På grundval av insamlade uppgifter och erfarenheter från genomförandet av cybersäkerhetsakten drogs slutsatsen att samordningen med andra organ bör effektiviseras och att fokus bör ligga på stödet från Enisa för genomförandet av EU-lagstiftningen och stödet till kommissionen på begäran för utarbetande av cybersäkerhetsrelaterad lagstiftning. I förslaget granskas synergieffekter med kommissionens geopolitiska prioriteringar för att hantera risker såsom det ökande beroendet av entiteter som är etablerade i och kontrolleras av länder som utgör cybersäkerhetsproblem (högriskleverantörer) i Europa. I egenskap av expertcentrum är Enisa för närvarande även en viktig källa till information som är avgörande för att skapa en gemensam förståelse av hoten mot och riskerna för entiteterna i EU. Den föreslagna ramen bygger därför på erfarenheterna från den första cybersäkerhetsakten och mobiliserar samordningen av informationsflödena i syfte att sammanställa en helhetsbild av läget.

Utvärderingen av det europeiska ramverket för cybersäkerhetscertifiering utmynnar i flera strategiska rekommendationer. Trots Enisas centrala roll när det gäller att främja samarbete och operativ sammanhållning mellan medlemsstaterna och andra berörda parter har ramverkets effektivitet och ändamålsenlighet tydligt begränsats, främst på grund av de komplexa processerna för antagande av ordningar. Dessa frågor belyste behovet av en omfattande översyn av styrningsstrukturerna för att öka den operativa tydligheten och ansvarsskyldigheten på alla nivåer, vilket berörs i förslaget till översyn av cybersäkerhetsakten. Erfarenheterna av hur det nuvarande ramverket fungerar har visat att det finns ett behov av att modernisera och förtydliga certifieringsramverket och införa underhållsförfaranden för certifieringsordningar så att ordningarna kan motsvara marknadens behov och hotbilden. Slutligen har det ursprungliga ramverket inte tagit hänsyn till icke-tekniska risker, vilka kan ha varit orsaken till att genomförandet av ramverket med avseende på ordningarna för 5G-nät och molntjänster stannade av.

Komplexiteten i EU:s cybersäkerhetsekosystem har ökat mot bakgrund av nya cyberhot. I de skriftliga inlagorna från berörda parter rådde ett starkt samförstånd om

behovet av att minska den administrativa bördan, särskilt för små och medelstora företag, och man efterlyste även förenklade efterlevnadsförfaranden. Även om den främsta förenklingsinsatsen kommer att kanaliseras genom det digitala omnibuspaketet återspeglar förslaget de berörda parternas behov genom att införa ändringar av NIS 2-direktivet för att underlätta genomförandeprocessen.

1.5.4 Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument

Genom den andra cybersäkerhetsakten införs de ändringar som krävs för att förse EU med verktyg och mekanismer för att bemöta cybersäkerhetshoten och uppnå de politiska målen. Den föreslagna förordningen kommer att ytterligare stärka Enisa genom att förse byrån med den kapacitet som krävs för att hjälpa medlemsstaterna att genomföra EU-lagstiftningen och motverka cyberrisker. Med beaktande av de tidigare nämnda Draghi- och Letta-rapporterna sätter förslaget till flerårig budgetram 2028–2034 konkurrenskraft, säkerhet och strategiskt oberoende i centrum.

Genom förslagen inom det övergripande paketet för den fleråriga budgetramen 2028–2034, särskilt förslagen om Europeiska konkurrenskraftsfonden och Horisont Europa, införs därför nya behörighetskriterier som bygger på principen om att högriskleverantörer ska utestängas från möjligheten att ta emot EU-medel. Den andra cybersäkerhetsakten är helt i linje med denna princip och är dessutom ett verktyg för att möjliggöra genomförandet av de nya kraven avseende högriskleverantörer, eftersom den erbjuder en förfaranderam för att utpeka länder som utgör cybersäkerhetsproblem på EU-nivå. I detta avseende är den andra cybersäkerhetsakten ett strategiskt förslag, i linje med kommissionens prioriteringar för att uppnå teknisk suveränitet och öka konkurrenskraften inom Europa.

Den befintliga fragmenteringen kommer att undanröjas genom ytterligare harmonisering på EU:s certifieringsmarknad för att effektivisera den europeiska certifieringsprocessen och göra den mer hållbar.

I förslagen till den fleråriga budgetramen 2028–2034 prioriteras förenkling inom hela ramen. Budgetrubrikerna komprimeras till fyra i stället för sju, och antalet övergripande finansieringsprogram har minskats avsevärt från 52 till 16, vilket ger flexibilitet och anpassningsbarhet till de aktuella behoven. I konsekvensbedömningen för översynen av cybersäkerhetsakten betonades just dessa mål: behovet av att förenkla cybersäkerhetskraven i flera olika lagstiftningsramar samt kodifiera Enisas uppgifter och inrikta dem på de områden som bidrar mest till att öka resiliensen i EU:s cybersäkerhetsekosystem. På grundval av dessa slutsatser syftar de föreslagna bestämmelserna till att öka konkurrenskraften genom förenkling, säkerställa en hög säkerhetsnivå genom ökad samordning och analys av risker och sårbarheter, stödja en högre grad av harmonisering genom att undanröja fragmentering, som är ett resultat av ett antal nationella ordningar. Dessutom är Enisa tänkt att vara den främsta drivkraften för digital förenkling, i och med att byrån kommer att integrera den gemensamma kontaktpunkten för anmälningar, enligt beskrivningen i det digitala omnibuspaketet[90].

En viktig del av paketet för den fleråriga budgetramen 2028–2034 är förslaget om en ny konkurrenskraftsfond, som samlar fler än 16 finansieringsprogram såsom programmet för ett digitalt Europa, programmet EU för hälsa och Europeiska

[90] Ska läggas till när det har offentliggjorts.

försvarsfonden. Horisont Europa kommer att fortsätta att vara ett fristående program, nära förbundet med konkurrenskraftsfonden. Denna nya programplaneringsram kräver en stark samordning och finansiering som motsvarar de aktuella prioriteringarna. I detta sammanhang utgör de föreslagna bestämmelserna i den andra cybersäkerhetsakten grunden för fördjupad samordning mellan Enisa och Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, som ansvarar för programgenomförandet av de cybersäkerhetsrelaterade delarna av programmet för ett digitalt Europa och Horisont Europa. De föreslagna bestämmelserna säkerställer samstämmighet och betonar synergierna mellan Enisa och kompetenscentrumet. Samma strategi har valts för samarbetet med andra byråer och organ, såsom Europol.

En annan aspekt av anpassningen mellan förslaget till en andra cybersäkerhetsakt och den fleråriga budgetramen 2028–2034 utgörs av flexibilitetsprincipen. I och med översynen föreslår kommissionen en avgiftsmekanism som kommer att göra det smidigt för Enisa att delvis finansiera sin verksamhet, mer specifikt med anknytning till utvecklingen och underhållet av ordningar för intyg om cybersäkerhetskompetens, behandlingen och beviljandet av auktorisationer till tillhandahållare samt underhållet av europeiska ordningar för cybersäkerhetscertifiering. Med denna förändring kommer byrån att ha den flexibilitet och skalbarhet som krävs för att tillgodose berörda parters behov och ha hållbara utgifter genom att refinansiera sina tjänster.

1.5.5 Bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning

Sedan den senaste översynen av Enisas mandat 2019 har trenden varit en exponentiell ökning av byråns förväntade bidrag till stödet för genomförandet av EU:s lagstiftning. Detta ledde till begäranden om ökade årliga budget- och personalförstärkningar utöver vad som ursprungligen planerades. Den föreslagna översynen inför viktiga nya uppgifter och samlar de uppgifter inom Enisas mandat som har införts genom andra lagstiftningsakter efter det att den första cybersäkerhetsakten antogs, vilket innebär en utökning av Enisas kapacitet som kräver ytterligare ekonomiska förstärkningar och personalförstärkningar. Förslaget drivs av målet att göra den digitala säkerheten till Europas konkurrensfördel och kräver verkliga effekter inom cybersäkerhetsekosystemet. Detta är endast möjligt med betydande investeringar som motsvarar den önskade effekten och framför allt tillgodoser medlemsstaternas och andra berörda parters behov. De nya uppgifterna omfattar behovet av teknisk och specialiserad personal samt finansiella investeringar (dvs. för verktyg och plattformar), som endast skulle kunna säkras genom ytterligare anslag från EU:s budget.

Med målet om ökad flexibilitet och på samma gång en långsiktig hållbar budget för byrån föreslås en avgiftsmekanism som delvis kommer att finansiera de tjänster som tillhandahålls för underhållet av ramverket för cybersäkerhetscertifiering och i samband med utvecklingen och underhållet av ordningar för europeiska individuella intyg om cybersäkerhetskompetens samt behandlingen och beviljandet av auktorisationer till tillhandahållare.

Alla uppskattningar av ytterligare resurser i översynen av cybersäkerhetsakten görs utifrån Enisas referensbudget för 2025 (driftskostnader och heltidsekvivalenter). Kommissionen har gjort en omfattande analys av möjligheterna till omfördelning inom byrån för att ta hänsyn till de nya uppgifter som planeras inom ramen för det

reviderade mandatet. Det faktum att byrån arbetar till sin maximala kapacitet utan möjlighet att minska antalet uppgifter och att styrelsen redan vidtagit en nedprioriteringsåtgärd 2023 leder tydligt till slutsatsen att det inte finns utrymme för några nya uppgifter inom den aktuella strukturen om inte både budgeten och personalresurserna stärks. Dessutom omfattas många av de nuvarande uppgifterna av överenskommelser om medverkan mellan Enisa och kommissionen. Syftet med förslaget är därför att lägga till dessa uppgifter till Enisas mandat och få en stabil budget för de kommande åren.

Utan att det påverkar förhandlingarna om nästa fleråriga budgetram kommer de anslag som tilldelas byrån från och med 2028 att kompenseras genom omfördelningar från program inom den fleråriga budgetramen 2028–2034. Om en kompenserande minskning blir nödvändig kan de medel som anslås till byrån samt deras finansieringsflöden och finansieringskällor behöva revideras. De åtgärder som införs genom den föreslagna andra cybersäkerhetsakten innebär också att ytterligare uppgifter tilldelas Enisas partnergeneraldirektorat (GD Kommunikationsnät, innehåll och teknik). Det bör särskilt noteras att ramen för IKT-leveranskedjan, inklusive en marknadsanalys som åtföljer riskbedömningarna och utarbetandet av genomförandeakter, kommer att genomföras fullt ut på kommissionsnivå. Kommissionen kommer dessutom att behöva utarbeta och anta ytterligare genomförandeakter om villkoren för avgiftsmekanismerna. Ytterligare tillsyn och stöd på kommissionsnivå kommer att krävas för att säkerställa efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering, utarbeta standardbestämmelser, underhålla cybersäkerhetsordningar, ingå överenskommelser om ömsesidigt erkännande med tredjeländer och utöva tillsyn över Enisa.

1.6 Förslagets eller initiativets varaktighet och budgetkonsekvenser

☐ **begränsad varaktighet**

– ☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ

– ☐ budgetkonsekvenser från och med ÅÅÅÅ till och med ÅÅÅÅ för åtagandebemyndiganden och från och med ÅÅÅÅ till och med ÅÅÅÅ för betalningsbemyndiganden.

☒ **obegränsad varaktighet**

– Efter en inledande period ÅÅÅÅ–ÅÅÅÅ,

– beräknas genomförandetakten nå en stabil nivå.

1.7 Planerad(e) genomförandemetod(er)

☐ **Direkt förvaltning** som sköts av kommissionen

– ☐ via dess avdelningar, vilket också inbegriper personalen vid unionens delegationer;

– ☐ via genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☒ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

– ☐ tredjeländer eller organ som de har utsett

– ☐ internationella organisationer och organ kopplade till dem (ange vilka)

– ☐ Europeiska investeringsbanken och Europeiska investeringsfonden

– ☒ organ som avses i artiklarna 70 och 71 i budgetförordningen

– ☐ offentligrättsliga organ

– ☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de har försetts med tillräckliga ekonomiska garantier

– ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som har försetts med tillräckliga ekonomiska garantier

– ☐ organ eller personer som anförtrotts genomförandet av särskilda åtgärder inom den gemensamma utrikes- och säkerhetspolitiken enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den grundläggande akten

– ☐· organ som är etablerade i en medlemsstat och som omfattas av en medlemsstats privaträtt eller unionsrätten och som i enlighet med sektorsspecifika regler kan anförtros genomförandet av unionsmedel eller budgetgarantier, i den mån sådana organ kontrolleras av offentligrättsliga organ eller privaträttsliga organ som anförtrotts offentliga förvaltningsuppgifter och har tillräckliga finansiella garantier i form av gemensamt och solidariskt ansvar från kontrollorganens sida eller likvärdiga finansiella garantier, som för varje åtgärd kan vara begränsad till det högsta beloppet för unionens stöd.

Anmärkningar

2. FÖRVALTNING

2.1 Regler om uppföljning och rapportering

Uppföljningen och rapporteringen kommer att följa de principer som anges i den nuvarande cybersäkerhetsakten[91] och i budgetförordningen[92] och kommer att vara i linje med den gemensamma ansatsen om decentraliserade organ[93].

Enligt artikel 40 i budgetförordningen ska Enisa varje år till kommissionen, Europaparlamentet och rådet överlämna ett samlat programdokument som innehåller fleråriga och årliga arbetsprogram och resursplanering. Genom kommissionens förslag till ändring av Enisas mandat införs dessutom ett krav på att kommissionen, i egenskap av ledamot av styrelsen, ska rösta för att Enisas styrelse ska anta det samlade programdokumentet i frågor som rör personalresurser och budget. Kommissionen kommer även att avge ett yttrande om utkastet till ett samlat programdokument före omröstningen i styrelsen, som bör ha genomförts innan det samlade programdokumentet antas[94].

Enisa måste lämna in en konsoliderad årlig verksamhetsrapport till styrelsen. Denna rapport innehåller särskilt information om uppnåendet av de mål och resultat som anges i det samlade programdokumentet. Rapporten ska också sändas till kommissionen, Europaparlamentet och rådet. Byråns verkställande direktör bör lägga fram en efterhandsutvärdering av Enisas verksamhet för styrelsen vartannat år. Byrån bör även utarbeta en handlingsplan för uppföljning av de slutsatser som dragits av efterhandsutvärderingarna samt rapportera om framstegen till kommissionen vartannat år. Styrelsen bör bära ansvaret för att övervaka att det sker en lämplig uppföljning av de slutsatserna.

Påstådda missförhållanden i byråns verksamhet kan komma att undersökas av Europeiska ombudsmannen i enlighet med artikel 228 i EUF-fördraget.

Uppgiftskällorna till den planerade övervakningen kommer huvudsakligen att vara Enisa, den europeiska gruppen för cybersäkerhetscertifiering, samarbetsgruppen för nät- och informationssäkerhet, CSIRT-nätverket och medlemsstaternas myndigheter. Utöver uppgifterna i rapporterna (inklusive de årliga verksamhetsrapporterna) från Enisa, den europeiska gruppen för cybersäkerhetscertifiering, samarbetsgruppen för nät- och informationssäkerhet, CSIRT-nätverket och kommissionen kommer särskilda verktyg för uppgiftsinsamling vid behov att användas (t.ex. enkäter till de nationella myndigheterna, Eurobarometern och särskilda studier och rapporter från EU-omfattande övningar).

Kommissionens förslag till en andra cybersäkerhetsakt är en fortsättning på den etablerade praxisen för översyn och utvärdering av byrån. Såsom föreskrivs i artikel 119 i förslaget till en andra cybersäkerhetsakt ska kommissionen beställa en utvärdering av Enisa senast den [DD.MM.ÅÅÅÅ] och därefter vart femte år. Denna utvärdering kommer särskilt att inriktas på huruvida det föreligger ett behov av att ändra Enisas mandat och vilka ekonomiska konsekvenser en sådan ändring kan få.

91 EU:s cybersäkerhetsakt | EUR-Lex.

92 *Financial regulation applicable to the general budget of the Union (recast)* – Europeiska unionens publikationsbyrå.

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.

94 Delegerad förordning - 2019/715 - SV - EUR-Lex.

Vid varannan utvärdering ska en bedömning göras av de resultat som Enisa uppnått med hänsyn till dess mål, mandat, uppdrag, styrning och uppgifter, inklusive en bedömning av huruvida en fortsättning av Enisa är berättigad med avseende på målen, mandatet, uppdraget, styrningen och uppgifterna.

Under utvärderingen ska man även bedöma effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i förordningen i fråga om målen för det europeiska ramverket för cybersäkerhetscertifiering, dvs. att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster och entiteter i unionen och förbättra den inre marknadens funktion.

Utvärderingen ska också omfatta en bedömning av effekterna av och ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning IV i förordningen med avseende på målen för ramen för säkerhet i IKT-leveranskedjan.

Kommissionen ska meddela alla resultat till Europaparlamentet och rådet samt meddela utvärderingsresultaten för avdelning II i förordningen till styrelsen. Utvärderingens resultat ska offentliggöras.

2.2 Förvaltnings- och kontrollsystem

2.2.1 Motivering av den budgetgenomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås

Med tanke på att förslaget påverkar EU:s årliga bidrag till Enisa kommer anslaget från EU-budgeten att genomföras genom indirekt förvaltning.

Enligt principen om sund ekonomisk förvaltning ska Enisas budget genomföras i överensstämmelse med en ändamålsenlig och effektiv intern kontroll. Byrån är därför skyldig att genomföra en lämplig kontrollstrategi som samordnas mellan lämpliga aktörer i kontrollkedjan.

Vad gäller efterhandskontroller är Enisa, i egenskap av en decentraliserad byrå, föremål för följande:

- Intern revision utförd av kommissionens internrevisionstjänst.
- Årliga rapporter från Europeiska revisionsrätten med en revisionsförklaring om årsräkenskapernas tillförlitlighet och de underliggande transaktionernas laglighet och korrekthet.
- Årlig ansvarsfrihet som beviljas av Europaparlamentet.
- Eventuella utredningar som utförs av Olaf för att särskilt säkerställa att de resurser som anslås till byråerna används på ett korrekt sätt.
- I egenskap av partnergeneraldirektorat till Enisa kommer GD Kommunikationsnät, innehåll och teknik att genomföra sin kontrollstrategi för decentraliserade byråer för att säkerställa tillförlitlig rapportering inom ramen för den årliga verksamhetsrapporten. Även om de decentraliserade byråerna har fullt ansvar för genomförandet av sin budget ansvarar GD Kommunikationsnät, innehåll och teknik för regelbundna betalningar av årliga bidrag som fastställs av budgetmyndigheten.
- Slutligen utgör Europeiska ombudsmannen ytterligare en nivå av kontroll och ansvarsskyldighet för Enisa.

På grundval av utvärderingen av byrån och den konsekvensbedömning som utfördes i samband med att förslaget till en andra cybersäkerhetsakt lades fram, konstaterades det att det är av yttersta vikt att säkerställa tillräckliga finansiella resurser för att Enisa ska kunna fullgöra de uppgifter som byrån anförtrotts genom det nya mandatet. En viktig nyhet inom ramen för byråns reviderade mandat kommer att vara införandet av en avgiftsmekanism för att finansiera kostnaderna för underhållet av europeiska ordningar för cybersäkerhetscertifiering, som antas inom det europeiska ramverket för cybersäkerhetscertifiering. Det reviderade ramverket kommer att formalisera underhållsförfarandet. Underhållsverksamheten kommer att ledas av Enisa och delvis finansieras genom avgifter för att ta hänsyn till dess skalbara karaktär (fler ordningar kräver mer personal för att underhålla dem). Byrån kommer också att ha förmågan att tillhandahålla testverktyg för att stödja genomförandet av förfaranden för bedömning av överensstämmelse, både inom ramverket och annan relevant EU-lagstiftning om cybersäkerhet. Villkoren för avgifterna kommer att fastställas i en genomförandeakt som ska antas av kommissionen. Inom översynen planerar man dessutom att utveckla och underhålla ordningar för europeiska individuella intyg samt utfärda beslut om auktorisering av tillhandahållare att utfärda europeiska individuella intyg om cybersäkerhetskompetens.

2.2.2 Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna

Förslaget till en andra cybersäkerhetsakt syftar till att minska de identifierade riskerna inom Enisas mandat och det europeiska ramverket för cybersäkerhetscertifiering, inklusive ramen för säkerhet i IKT-leveranskedjan och förenklingsbestämmelser. Enisa är ett EU-organ som redan finns, och vid översynen har mandatet ytterligare avgränsats för att stärka de områden där byrån har visat ett tydligt mervärde och lägga till nya områden där stöd behövs med tanke på de nya politiska prioriteringarna och instrumenten, såsom förenkling genom integrering av en gemensam kontaktpunkt för rapportering, stöd till en gemensam europeisk situationsmedvetenhet och operativt samarbete samt ett förstärkt och effektiviserat europeiskt ramverk för cybersäkerhetscertifiering.

En annan identifierad risk som tas upp i förslaget är de överenskommelser om medverkan som kommissionen och byrån har ingått under de senaste åren. På grund av den aktuella geopolitiska situationen och den snabbt föränderliga hotbilden på cybersäkerhetsområdet har kommissionen sedan 2019 ingått överenskommelser om medverkan med byrån för sammanlagt mer än 75 miljoner EUR. Med tanke på att de uppgifter som anförtrotts Enisa genom dessa överenskommelser i dagsläget är permanenta utgör det instabila budgetflödet genom överenskommelserna om medverkan en risk för det långsiktiga uppnåendet av outputen av Enisas verksamhet.

Det aktuella förslaget består därför bland annat av att stärka byråns resurskapacitet, omdefiniera dess uppgifter och åstadkomma effektivitetsvinster. Framför allt kommer möjligheten att ta ut avgifter på lång sikt att främja en hållbar ekonomihanteringsprocess för byrån genom refinansiering av kostnaderna i samband med underhållet av europeiska certifieringsordningar som antagits inom det europeiska ramverket för cybersäkerhetscertifiering, testningen av verktyg samt utvecklingen, underhållet och genomförandet av ordningar för europeiska individuella intyg om cybersäkerhetskompetens. På lång sikt beräknas besparingarna för EU:s budget uppgå till 18,5 miljoner EUR per år. Kommissionen kommer att ansvara för att fastställa villkoren för avgifterna och deras sammansättning genom att anta genomförandeakter.

Utökningen av byråns operativa uppgifter utgör inte någon verklig risk. Dessa uppgifter kommer att komplettera medlemsstaternas åtgärder och stödja dem på begäran. De kommer också att begränsas till fördefinierade tjänster, i analogi med cybersäkerhetsakten (förordning (EU) 2019/881)[95]. De nya komponenterna/uppgifterna i förslaget kommer att tillföra ett mervärde för de europeiska berörda parterna, som skulle gynnas av att Enisa är ett informationsnav som bidrar till informationsutbyte och utfärdar varningar till sina samarbetspartner.

Vidare är den föreslagna modellen för byrån anpassad till kommissionens gemensamma ansats om decentraliserade organ, vilket säkerställer att det finns en tillräcklig kontroll för att se till att Enisa arbetar för att uppnå sina mål. De operativa och finansiella riskerna med de föreslagna ändringarna förefaller vara begränsade, eftersom bestämmelserna består i att minska de nuvarande riskerna. Vissa negativa aspekter kan dock förväntas på lång sikt i fråga om

— ansträngda operativa resurser på grund av ökade operativa behov från medlemsstaternas sida och ständigt föränderliga cyberrisker och hot på cybersäkerhetsområdet,

— en snabbt ökad budget med förväntningar på ett snabbt genomförande,

— otillräckliga ekonomiska resurser och personalresurser för att tillgodose de operativa behoven.

2.2.3 Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)

Kostnaderna för GD Kommunikationsnät, innehåll och teknik för övervakning och tillsyn av anförtrodda enheter, däribland Enisa, uppgår till cirka 5,25 miljoner EUR, vilket framgår av den årliga verksamhetsrapporten för 2024[96]. Detta belopp omfattar främst personalkostnader och utgör 0,50 % av driftsbetalningarna till dessa enheter under 2024. Den totala kontrollkostnaden ökade något till 0,50 % under 2024, från 0,46 % år 2023, men är fortfarande relativt stabil jämfört med tidigare år.

Vad gäller Enisa uppgår kontrollkostnaderna 2024 till 0,32 miljoner EUR eller 0,70 %, jämfört med 0,69 % under 2023 och 1,22 % under 2022. Analysen visar att de högre kontrollkostnaderna främst är förknippade med utarbetandet och övervakningen av överenskommelser om medverkan mellan kommissionen och byrån (i huvudsak personalkostnaderna), som väntas minska avsevärt inom det nya mandatet, och till följd av detta förväntas högre effektivitetsnivåer. När det gäller de totala kostnader som GD Kommunikationsnät, innehåll och teknik ådrar sig för Enisa jämfört med elva andra anförtrodda enheter befinner sig Enisa i mitten.

I förslaget till en andra cybersäkerhetsakt planeras en ökning av personalen vid GD Kommunikationsnät, innehåll och teknik med 50 heltidsekvivalenter, varav ytterligare en heltidsekvivalent kommer att avdelas för uppgifter som rör det generaldirektoratet i egenskap av byråns partnergeneraldirektorat. Denna person kommer att stödja utarbetandet av kommissionens yttrande om Enisas samlade programdokument och övervaka dess genomförande, stödja tillsynen av förberedelserna och genomförandet

95 https://eur-lex.europa.eu/eli/reg/2019/881/oj/.

96 CNECT_AAR_2024_final.

av byråns budget samt bistå byrån med utveckling av verksamheten i enlighet med unionens politik, bland annat genom att delta i relevanta möten. Åtgärden motiveras av de utökade övervakningsuppgifterna för GD Kommunikationsnät, innehåll och teknik, däribland att kommissionen ska rösta för frågor som rör budgeten och personalresurser. Det bör noteras att genomförandet av bestämmelserna om fastställandet av länder som strategiska cybersäkerhetsrisker för högriskleverantörer av specifika viktiga tillgångar kommer att drivas helt av kommissionen. För riskbedömningarna i samband med ovanstående behövs personal på uppskattningsvis 25 heltidsekvivalenter. Åtgärden motiveras av den mängd arbete som genomförandet av den politiska ramen kräver, närmare bestämt stödet till EU:s samordnade riskbedömningar, en ekonomisk analys för varje IKT-produkt eller IKT-tjänst, utarbetandet av respektive genomförandeakter och uppföljningen av genomförandet av ramen samt utförandet av bedömningar av ägar- och kontrollförhållanden. Kommissionens kontrollkostnader för att genomföra ramen för leveranskedjan väntas framför allt påverkas av de olika bedömningar av ägar- och kontrollförhållanden som kommissionen kommer att genomföra. Resultaten av denna uppgift kommer dock i hög grad att bidra till besparingar för medlemsstaterna i deras övervakning av genomförandet av begränsningsåtgärder och fullgörandet av de skyldigheter som NIS 2-entiteterna åläggs genom ramen. Medlemsstaterna kommer att kunna utnyttja resultaten av bedömningarna av ägar- och kontrollförhållanden direkt, snarare än att varje medlemsstat måste lägga resurser på samma bedömningsbehov. Förstärkningen av det europeiska ramverket för cybersäkerhetscertifiering, standardiseringen och genomförandet av relaterad verksamhet samt genomförandet av NIS 2-direktivet (inklusive respektive genomförandebehov, genomförandeakter om avgifter och stöd till underhållet av certifieringsordningar och ordningar för kompetensintyg) har uppskattats till 19 heltidsekvivalenter, medan det operativa samarbetet och politiken för situationsmedvetenhet kräver ytterligare fem heltidsekvivalenter. En fullständig beskrivning av uppgifterna finns i avsnitt 3.2.4.

I sin konsoliderade årliga verksamhetsrapport för 2023[97] drog Enisa en positiv slutsats om bedömningen av sina system för intern kontroll och lämnade in en revisionsförklaring utan reservation. I revisionsrättens årsrapport om EU:s byråer för budgetåret 2023 utfärdade revisionsrätten ett revisionsuttalande utan reservation om räkenskaperna och ett uttalande med reservation om lagligheten och korrektheten i de betalningar som ligger till grund för räkenskaperna (se även avsnitt 2.2.2). GD Kommunikationsnät, innehåll och teknik har noterat rapporten, men dragit slutsatsen att den inte påverkar ändamålsenligheten i generaldirektoratets tillsyn. Enisa rapporterar även regelbundet om de åtgärder som vidtas för att förhindra att resultaten upprepas, och i nuläget finns det inget som tyder på att felprocenten kommer att försämras/överstiga 2 % under de kommande åren.

I artikel 80.2 i Enisas budgetregler[98] föreskrivs dessutom en möjlighet för byrån att dela internrevisionsfunktion med andra unionsorgan som verkar inom samma politikområde om ett unionsorgans internrevisionsfunktion inte är kostnadseffektiv.

Sammanfattningsvis visar analysen på en tillfredsställande kvot för kostnadseffektivitet, med tanke på den föreslagna ökningen av byråns storlek med mer än 100 % jämfört med den relativt begränsade ökningen av kontrollkostnaderna. Sett

97 enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf.

98 MB Decision 2019_8 Financial rules_adopted.pdf.

till alla tillgängliga uppgifter finns det inget som tyder på att den förväntade felprocenten kan överstiga 2 %.

2.3 Åtgärder för att förebygga bedrägeri och oriktigheter

Enisa kommer att tillämpa de högsta möjliga standarderna för att förhindra bedrägeri och oriktigheter.

Betalningar för beställda tjänster eller undersökningar ska kontrolleras av byrån innan utbetalningen görs, med beaktande av villkoren i avtalen, ekonomiska principer samt god ekonomisk och administrativ sed. Åtgärder för bedrägeribekämpning (övervakning, rapporteringskrav osv.) kommer att ingå i alla avtal och kontrakt mellan byrån och dess betalningsmottagare.

Bestämmelserna i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 ska tillämpas fullt ut i syfte att bekämpa bedrägeri, korruption och andra olagliga handlingar.

3. FÖRSLAGETS ELLER INITIATIVETS BERÄKNADE BUDGETKONSEKVENSER

3.1 Berörda rubriker i den fleråriga budgetramen och utgiftsposter i den årliga budgeten

- Befintliga budgetposter

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i den fleråriga budgetramen	Budgetpost	Typ av utgifter	Bidrag			
	Nummer	Diff./Icke-diff.[99]	från Efta-länder[100]	från kandidatländer och potentiella kandidater[101]	från andra tredjeländer	övriga inkomster avsatta för särskilda ändamål
	[XX.YY.YY.YY]	Icke-diff.	JA	NEJ	NEJ	JA/NEJ
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

- Nya budgetposter som föreslås

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd

Rubrik i	Budgetpost	Typ av	Bidrag

99 Differentierade respektive icke-differentierade anslag.

100 Efta: Europeiska frihandelssammanslutningen.

101 Kandidatländer och i förekommande fall potentiella kandidater i västra Balkan.

den fleråriga budgetramen		utgifter				
	Nummer	Diff./Icke-diff.	från Efta-länder	från kandidatländer och potentiella kandidater	från andra tredjeländer	övriga inkomster avsatta för särskilda ändamål
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ
	[XX.YY.YY.YY]	Diff./Icke-diff.	JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

3.2 Förslagets beräknade budgetkonsekvenser för anslagen

3.2.1 Sammanfattning av beräknad inverkan på driftsanslagen

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☒ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

3.2.1.1 Anslag i den antagna budgeten

Miljoner EUR (avrundat till tre decimaler)

Byrå: Enisa	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT Budgetram 2028–2034**
Budgetpost: <…….> / Ytterligare bidrag från EU-budgeten till byrån	20,900€	20,594€	25,338€	26,801€	26,801€	26,301€	26,301€	173,006

Anslag/bidrag från EU-budgeten till byrån kommer att kompenseras genom en minskning av ramanslaget till följande program <…….>/budgetpost: <…….> /under året/åren: <…….> .

			År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT Budgetram 2028–2034**	
TOTALA driftsanslag	Åtaganden	(4)	20,900€	20,594€	25,338€	26,801€	26,801€	26,301€	26,301€	173,006	
	Betalningar	(5)	20,900€	20,594€	25,338€	26,801€	26,801€	26,301€	26,301€	173,006	
TOTALA anslag av administrativ natur som finansieras genom ramanslagen för särskilda program		(6)	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**	
TOTALA anslag för RUBRIK 2	Åtaganden	=4+6	22,265€	21,959€	26,808€	28,586€	28,901€	28,716€	28,926€	186,161	

i den fleråriga budgetramen	Betalningar	=5+6	22,265€	20,890€	24,851€	26,254€	26,254€	25,754€	25,754€	186,161

GD: Kommunikationsnät, innehåll och teknik				År 2028	År 2029	År 2030	År 2031	År 2032	År 2033	År 2034	TOTALT Budgetram 2028–2034
• Personalresurser				3,693	3,693	4,574	5,277	5,980	6,683	7,475	37,375
• Övriga administrativa utgifter				0	0	0	0	0	0	0	0
TOTALT GD Kommunikationsnät, innehåll och teknik	Anslag	3,693	3,693	4,574	5,277	5,980	6,683	7,475			37,375

TOTALA anslag för RUBRIK 4 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	2,328	2,328	3,104	3,492	3,880	4,268	4,850	24,25

Miljoner EUR (avrundat till tre decimaler)

		År 2028	År 2029	År 2030	År 2031	År 2032	År 2033	År 2034	TOTALT Budgetram 2028–2034
TOTALA anslag för RUBRIKERNA 1–4	Åtaganden	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38
i den fleråriga budgetramen	Betalningar	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

3.2.2 Beräknad output som finansierats med driftsanslag (ska inte fyllas i för decentraliserade byråer)

Åtagandebemyndiganden i miljoner EUR (avrundat till tre decimaler)

Ange mål och output ⇩			År **2028**		År **2029**		År **2030**		År **2031**		För in så många år som behövs för att redovisa hur länge resursanvändningen påverkas (jfr avsnitt 1.6)						**TOTALT**	
	OUTPUT																	
	Typ[102]	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Total kostnad
SPECIFIKT MÅL nr 1[103]…																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2…																		
- Output																		
Delsumma för specifikt mål nr 2																		
TOTALT																		

102 Output som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).

103 Mål som redovisats under avsnitt 1.3.2: ”Specifikt/specifika mål”

3.2.3 Sammanfattning av beräknad inverkan på de administrativa anslagen

– ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk

– ☒ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

3.2.3.1 Anslag i den antagna budgeten

(ytterligare)

ANTAGNA ANSLAG	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT 2028–2034**
RUBRIK 4								
Personalresurser	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Övriga administrativa utgifter	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Delsumma för RUBRIK 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Utanför RUBRIK 4								
Personalresurser	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Andra utgifter av administrativ natur	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Delsumma utanför RUBRIK 4	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
TOTALT	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4 Beräknat (ytterligare) personalbehov

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☒ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

3.2.4.1 Finansierat med den antagna budgeten

Beräkningarna ska anges i heltidsekvivalenter[104]

ANTAGNA ANSLAG	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)							
20 01 02 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)	12	12	16	18	20	22	25
20 01 02 03 (EU:s delegationer)	0	0	0	0	0	0	0
(indirekta forskningsåtgärder)	0	0	0	0	0	0	0
(direkta forskningsåtgärder)	0	0	0	0	0	0	0
Andra budgetposter (ange vilka)	0	0	0	0	0	0	0
• Extern personal (heltidsekvivalenter)							
20 02 01 (kontraktsanställda och nationella experter finansierade genom ramanslaget)	0	0	0	0	0	0	0

104 Ange i tabellen nedan hur många heltidsekvivalenter av det angivna antalet som redan är avdelade för förvaltning av åtgärden och/eller kan omfördelas inom ditt GD och vad ditt nettobehov är.

20 02 03 (kontraktsanställda, lokalanställda, nationella experter och unga experter som tjänstgör vid EU:s delegationer)		0	0	0	0	0	0	0
Post för admin. stöd	- vid huvudkontoret	0	0	0	0	0	0	0
[XX.01.YY.YY]	- vid EU:s delegationer	0	0	0	0	0	0	0
(kontraktsanställda och nationella experter – indirekta forskningsåtgärder)		0	0	0	0	0	0	0
(kontraktsanställda och nationella experter – direkta forskningsåtgärder)		0	0	0	0	0	0	0
Andra budgetposter (ange vilka) – rubrik 4		0	0	0	0	0	0	0
Andra budgetposter (ange vilka) – utanför rubrik 4		13	13	14	17	20	23	25
TOTALT		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Personal som behövs för att genomföra förslaget (heltidsekvivalenter):

	Täcks av befintlig personal vid kommissionens avdelningar	**Särskild ytterligare personal**		
		Finansieras genom rubrik 7 eller forskning	**Finansieras genom BA-post**	**Finansieras genom avgifter**
Tjänster i tjänsteförteckningen		25		
Extern personal (kontraktsanställda, nationella experter, vikarier)			25	

Beräknad inverkan på utgifter och personal år 2028 och framåt är vägledande och föregriper inte nästa fleråriga budgetram. Finansieringskällan och omfattningen av unionens ekonomiska åtagande under perioden efter 2027 är fortfarande beroende av utfallet av de interinstitutionella förhandlingarna om den fleråriga budgetramen 2028–2034, det årliga budgetförfarandet och styrmekanismen.

Beskrivning av de uppgifter som ska utföras av sektorns generaldirektorat vid kommissionen:

Tjänstemän och tillfälligt anställda	**Samordning av Enisa (1)**: Företräda kommissionen i byråns styrelse. Utarbeta kommissionens yttrande om Enisas årliga samlade programdokument och övervaka genomförandet av det. Övervaka förberedelserna och genomförandet av byråns budget. Bistå byrån med utveckling av verksamheten i enlighet med unionens politik, bland annat genom att delta i relevanta möten. **Ordningar för kompetensintyg/kompetensakademin (2)**: Det kommer att krävas ytterligare personal från GD Kommunikationsnät, innehåll och teknik för att utarbeta genomförandeakter om fastställande av de avgifter som Enisa kommer att ta ut av dem som ansöker om att bli auktoriserade tillhandahållare. Det rör sig om minst tolv genomförandeakter, en per profil inom den europeiska kompetensramen för cybersäkerhet. **Leveranskedjan (25)**: Stödja utarbetandet av unionens samordnade riskbedömningar. Göra en ekonomisk analys av var och en av de berörda IKT-produkterna och IKT-tjänsterna. Utarbeta respektive genomförandeakter om identifiering av viktiga tillgångar, föreslagna begränsningsåtgärder och fastställande av länder som strategiska cybersäkerhetsrisker för specifika viktiga tillgångar, identifiering av högriskleverantörer, kontroll av begäranden om undantag och utarbetande av kommissionsbeslut. Stödja genomförandet och övervakningen av antagna åtgärder. **Europeiska ramverket för cybersäkerhetscertifiering, standardisering och genomförande av relaterade verksamheter samt genomförande av NIS 2-direktivet (17)**: Genomdrivande av cybersäkerhetsakten, särskilt styrningen av organ för bedömning av överensstämmelse (ifrågasättande av ansvarsområden) Deltagande av berörda parter (och församlingen) Ömsesidigt erkännande med tredjeländer Utarbetande av standardiserade genomförandeakter (detaljerade begäranden som är föremål för samråd och utarbetande av standardbestämmelser) Underhåll av ordningar, rättslig prövning, kommittéförfarande Samordning med samarbetsgruppen för nät- och informationssäkerhet och underhåll av ordningar Genomförandeakter enligt NIS 2-direktivet Anpassning av organ för bedömning av överensstämmelse till cybersäkerhetsakten, presumtion om överensstämmelse + standardisering Samordning mellan marknadskontroll och nationella myndigheter för cybersäkerhetscertifiering Teknisk anpassning mellan cyberresiliensförordningen och certifieringsordningar **Operativ samordning och situationsmedvetenhet (5)**: Sektorsexpertis och expertis om fientliga aktörer för att bidra till situationsmedvetenheten på EU-nivå med avseende på hot mot kritisk infrastruktur, bland annat genom ny teknik Samordning med Enisa och andra entiteter och nätverk på EU-nivå för förberedelser inför betydande och storskaliga cyberincidenter

Extern personal	Samma som ovan

Beskrivning av ytterligare uppgifter som ska utföras av Enisa:

Tjänstemän och tillfälligt anställda	Förvaltning av EU-cybersäkerhetsreserven (landsansvariga och stöd för genomförandet, medan de faktiska driftskostnaderna för reserven täcks i enlighet med cybersolidaritetsakten) (10) Förvaltning enligt cyberresiliensförordningen av den gemensamma rapporteringsplattformen (drift) (9) Sårbarhetstjänster kopplade till den gemensamma rapporteringsplattformen (4) Utökning av den gemensamma rapporteringsplattformen till en gemensam kontaktpunkt (utveckling och drift) (8) Utarbetande av teknisk vägledning, produktsäkerhetsexpertis och marknadsanalys till stöd för genomförandet av cyberresiliensförordningen (7) Standardisering till stöd för genomförandet av cyberresiliensförordningen/certifiering/NIS 2-direktivet (4) Stöd till marknadskontroll inom ramen för cyberresiliensförordningen (4) Stöd till provning av överensstämmelse och säkerhetsutvärdering av produkter (4) Stöd till medlemsstaterna i fråga om ömsesidigt bistånd (3) Tillhandahållande av sårbarhetshanteringstjänster, underhåll av den europeiska sårbarhetsdatabasen och tillhandahållande av rådgivnings- och berikningsfunktioner (samordnad information om sårbarheter) (15) Operativt samarbete och situationsmedvetenhet – begränsnings- och stödplattformar såsom CSIRT-nätverket/CyCLONe, stöd till uppgifter i samband med varningar, stöd till den förbättrade samordningen med andra relevanta entiteter för att utveckla databaser över verifierade, tillförlitliga underrättelser om cyberhot (artikel 11.1a i den andra cybersäkerhetsakten) (5) Stöd till resiliensen i kritiska sektorer (inklusive genomförandet av handlingsplanen för cybersäkerhet inom hälso- och sjukvården) (4) Utveckling av ordningar för kompetensintyg (2) Underhåll och tillsyn av ordningar för kompetensintyg (6) Administration (revisor för avgifterna/personalresurser/it) (8) Underhåll av certifieringsordningar (11) Övergripande uppgifter – ökat deltagande av berörda parter, utarbetande av tekniska specifikationer och delaktighet i standardiseringsverksamhet till stöd för ordningar (1)
Extern personal	Samma som ovan Två obligatoriska nationella experter per medlemsstat för att stödja byråns verksamhet; de ska fungera som nationella kontaktpersoner, med fokus på operativt samarbete och samordnad information om sårbarheter (13) De övriga 27 nationella experterna planeras vara kostnadsfria och har därför inga budgetkonsekvenser

Ytterligare driftskostnader per år för Enisa under 2028–2034:

Kostn.	Budget	Tidsplan	Förklaring
Webbplats för cybersäkerhetskompetens	750 000 EUR	50 % 2029 50 % 2030	För att säkerställa i förfarandena inn förslaget krav på att ska upprätthålla webbplats med p inom den euro kompetensramen cybersäkerhet, intygsordningar, information om avgi varje o rekommenderade a för varje intyg o förteckning auktoriserade tillhandahållare av in
Samordnad information om sårbarheter	1 miljon EUR	Från och med 2028	Säkerheten för pro och tjänster som anv vår kritiska infrastru i hög grad beroende information om upp sårbarheter begränsningen av delas i god tid
Underrättelser om cybersäkerhetshot	3 miljoner EUR	Från och med 2028	Enisa och kommis ska tillsammans ska lägesbild
Gemensam kontaktpunkt	8 miljoner EUR	6 miljoner EUR under 2028 500 000 under 2029 500 000 under 2030 500 000 under 2031 500 000 under 2032	För att kunna gen kommissionens försl ett digitalt omnibusp syfte att fö efterlevnaden rapporteringsskyldigh avseende cybersäk och uppgiftsincident man utveckla upprätthålla en gem kontaktpunkt
Underhåll enligt cyberresiliensförordningen av den gemensamma rapporteringsplattformen m.m.	3 miljoner EUR	Från och med 2028	Den gemen rapporteringsplattfor har införts medlagstiftarna är största it-system någonsin utveckla Enisas historia och u

			hörnsten cyberresiliensförordn Etableringen finansie närvarande genom överenskommelse medverkan, men dagliga förvalt kommer att heltidsekvivalenter ovan) samt driftskost Enisa har en viktig spela när det gäll säkerställa att unione för produktsäkerhet cyberresiliensförordn blir framgångsrik.
Säker kommunikation och Enisas cybersäkerhetsmognad	Över 2 miljoner EUR	Investeringar på 1,1 miljoner EUR 2028 (CyCLONe/CSIRT-plattformar + säker kommunikation) 1 miljon EUR per år för underhåll från och med 2029 1,5 miljoner EUR för cybermognad	Säkerställa cybersäkerhet kommunikationsverk
Underhåll av cybersäkerhetscertifiering	1 400 000 miljoner EUR	2028: 600 000 2029: 1 000 000 2030: 1 200 000 2031: 1 400 000 2032: 1 400 000 2033: 1 400 000 2034: 1 400 000	Täcks av avgifter (h hållet från och med 2
Ordningar för cybersäkerhetsintyg	212 920 EUR	Från och med 2030 täcks 50 % av EU:s budget	Täcks helt av avgift och med 2033

3.2.5 Översikt över beräknad inverkan på it-relaterade investeringar

Obligatoriskt: bästa skattning av de it-relaterade investeringar som förslaget/initiativet medför ska anges i tabellen nedan.

När så krävs för genomförandet av förslaget/initiativet ska i undantagsfall anslag under rubrik 4 anges på därför avsedd rad.

Anslagen under rubrikerna 1–3 ska redovisas som ”It-utgifter inom operativa program som inte omfattas av kommissionens administrativa självständighet och institutionella befogenheter”. Dessa utgifter avser den driftsbudget som tas i anspråk för att återanvända/köpa in/utveckla it-plattformar och it-verktyg med direkt koppling till initiativets genomförande, med tillhörande investeringar (t.ex. licenser, undersökningar och datalagring). Uppgifterna i den här tabellen bör vara förenliga med uppgifterna i avsnitt 4 ”Digitala inslag”.

TOTALT Anslag för digital teknik och it	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT Budgetram 2028–2034**
RUBRIK 4								
It-utgifter (centralt)	0	0	0	0	0	0	0	**0**
Delsumma för RUBRIK 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Utanför RUBRIK 4								
It-utgifter inom operativa program som inte omfattas av kommissionens administrativa självständighet och institutionella befogenheter	0	0	0	0	0	0	0	**0**
Delsumma utanför RUBRIK 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTALT	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6 Förenlighet med den gällande fleråriga budgetramen

Förslaget/initiativet

– ☒ kan finansieras fullständigt genom omfördelningar inom den berörda rubriken i den fleråriga budgetramen

Utan att det påverkar förhandlingarna om nästa fleråriga budgetram kommer de anslag som tilldelas byrån från och med 2028 att kompenseras genom omfördelningar från program inom den fleråriga budgetramen 2028–2034. Om en

kompenserande minskning blir nödvändig kan de medel som anslås till byrån samt deras finansieringsflöden och finansieringskällor behöva revideras.

– ☐ kräver användning av den outnyttjade marginalen under den relevanta rubriken i den fleråriga budgetramen och/eller användning av särskilda instrument enligt definitionen i förordningen om den fleråriga budgetramen

– ☐ kräver en översyn av den fleråriga budgetramen

3.2.7 Bidrag från tredje part

Förslaget/initiativet

– ☒ innehåller inga bestämmelser om samfinansiering från tredje parter

– ☐ innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner EUR (avrundat till tre decimaler)

	År **2028**	År **2029**	År **2030**	År **2031**	Totalt
Ange vilket organ som deltar i samfinansieringen					
TOTALA anslag som tillförs genom samfinansiering					

3.2.8 Beräknat personalbehov och beräknad användning av anslag vid ett decentraliserat organ

Ytterligare personalbehov (heltidsekvivalenter)

Byrå: Enisa	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**
Tillfälligt anställda (AD-tjänster)	5	11	17	19	19	19	19
Tillfälligt anställda (AST-tjänster)	4	7	11	12	12	12	12
Delsumma tillfälligt anställda (AD + AST)	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Kontraktsanställda	22	44	66	74	74	74	74
Utsända nationella experter	4	8	11	13	13	13	13
Delsumma kontraktsanställda och utsända nationella experter	26	52	77	87	87	87	87
TOTAL personal	35	70	105	118	118	118	118

Anslag som täcks av bidraget från EU-budgeten i miljoner euro (avrundat till tre decimaler)

Byrå: Enisa	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT 2028–2034**

Rubrik 1: Personalutgifter	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Rubrik 2: Infrastruktur och driftsutgifter								
Rubrik 3: Driftsutgifter	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
TOTALA anslag som täcks av EU-budgeten	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Anslag som täcks av eventuella avgifter i miljoner euro (avrundat till tre decimaler)

Byrå: Enisa	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT 2028–2034**
Rubrik 1: Personalutgifter		0,510	1,043	1,539	4,604	5,176	5,650	**18,522**
Rubrik 2: Infrastruktur och driftsutgifter								**0,000**
Rubrik 3: Driftsutgifter								**0,000**
TOTALA anslag som täcks av avgifter	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Översikt/sammanfattning av personal och anslag (i miljoner euro) som krävs för förslaget/initiativet vid decentraliserade byråer

Byrå: Enisa	År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**	**TOTALT 2028–2034**
Tillfälligt anställda (AD + AST)	9	18	28	31	31	31	31	*31*
Kontraktsanställda	22	44	66	74	74	74	74	74
Utsända nationella experter	4	8	11	13	13	13	13	13
Total personal	35	70	105	118	118	118	118	**118**
Anslag som täcks av EU-budgeten	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Anslag som täcks av avgifter (i tillämpliga fall)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**
Anslag från medfinansiering (i tillämpliga fall)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**

TOTALA anslag	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3 Beräknad inverkan på inkomsterna

– ☒ Förslaget/initiativet påverkar inte inkomsterna.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på andra inkomster

– ☐ Ange om inkomsterna är avsatta för särskilda utgiftsposter

Miljoner EUR (avrundat till tre decimaler)

Inkomstposter i den årliga budgeten:	Belopp som förts in för det innevarande budgetåret	Förslagets/initiativets inverkan på inkomsterna[105]						
		År **2028**	År **2029**	År **2030**	År **2031**	År **2032**	År **2033**	År **2034**
Artikel …….								

För inkomster avsatta för särskilda ändamål, ange vilka utgiftsposter i budgeten som berörs.

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

Avgiftsmekanismerna rör tre av Enisas verksamhetsområden:

- Avgifter kopplade till auktorisering av tillhandahållare enligt ordningarna för europeiska individuella intyg om cybersäkerhetskompetens.

Avgifterna i samband med denna verksamhet kommer att fastställas i en genomförandeakt efter det att den reviderade cybersäkerhetsakten har antagits. För att kunna uppskatta de investeringar som krävs samt kostnaderna gjordes dock beräkningar med hjälp av en befintlig modell i en EU-medlemsstat[106]. I modellen ingår en engångsbetalning och en årlig avgift.

Fasta kostnader: 8,540 EUR

Årsavgift: 800 EUR

Avgifterna är avsedda att refinansiera kostnaderna för denna specifika verksamhet. Kostnaderna har uppskattats till 1 064 600 EUR under en femårsperiod. De särskilda kostnaderna för den verksamhet som ingår i denna siffra hör samman med utvecklingen och underhållet av ordningar, inbegripet utgifter för medlemmarna i en tillfällig arbetsgrupp som skulle hjälpa Enisa att utveckla ordningarna (ersättning för utgifter och betalning till rapportörer),

105 Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.

106 *Decision RR – 02: Price list of SNAS services*: https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf.

revisionsuppdrag på plats hos tillhandahållare och utbildning av bedömare för att se till att ordningarna tillämpas enhetligt:

A) Den tillfälliga arbetsgruppen skulle kosta 800 000 EUR.

B) Utbildningen av två bedömare per medlemsstat skulle kosta 129 600 EUR.

C) Revisionen av en entitet per medlemsstat skulle kosta 135 000 EUR.

(A+B+C)/5=212 920 EUR per år

I förslaget planeras en övergångsperiod och nyinvesteringar under de tre första åren. Under övergångsperioden kommer kostnaderna att täckas av EU:s budget, och under åren 4 och 5 kommer täckningen att vara 50 %; under åren 6 och 7 kommer avgifterna att tillämpas fullt ut.

År	Avgifter
2028	0
2029	0
2030	0
2031	106 460 (intäkter)
2032	106 460 (intäkter)
2033	212 920 (intäkter)
2034	212 920 (intäkter)

- Avgifter för att täcka kostnaderna för att underhålla en ordning för cybersäkerhetscertifiering som antagits inom det europeiska ramverket för cybersäkerhetscertifiering.

Avgifterna i samband med denna verksamhet kommer att fastställas i en genomförandeakt efter det att den reviderade cybersäkerhetsakten har antagits. Uppskattningarna av kostnaderna för att underhålla en ordning bygger på de marknadsanalyser som ingår i konsekvensbedömningen av förslaget till översyn av cybersäkerhetsakten. De totala kostnaderna för verksamheten under en femårsperiod beräknas uppgå till 5 600 000 EUR för driftskostnader och 7 100 000 EUR för heltidsekvivalenter.

Den årliga kostnaden för underhållet beräknas utifrån nuvarande erfarenheter till 200 000 EUR per år för underhåll av en ordning[107] och två heltidsekvivalenter för sådan verksamhet (med en årlig kostnad på 125 887 EUR per heltidsekvivalent), med beaktande av det planerade året för antagande av sådana ordningar. Förväntningarna är att intäkterna från dessa avgifter ska öka i takt med varje ny ordnings antagande och gradvisa utnyttjande. Hittills har en ordning antagits (EUCC, den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering) inom det europeiska ramverket för

[107] Mer specifikt omfattar underhållet två personliga möten med experter per år (100 000 EUR), kostnader för uppdragstagare som stöder utarbetandet och granskningen av styrkande handlingar för ordningen, spridningen av certifieringsordningar, stöd till inbördes granskningar och genomförandet av bedömningar av överensstämmelse (4x15 000=60 000 EUR). I kostnaden ingår även den operativa delen av FSE-plattformen och Enisas certifieringswebbplats (40 000 EUR).

cybersäkerhetscertifiering, och de första intäkterna från underhållet av den ordningen förväntas under 2029. Enligt förväntningarna kommer kostnaderna att täckas senast 2032.

De uppskattade intäkterna har beräknats utifrån specifika antaganden för varje potentiell ordning med beaktande av följande aspekter: den förväntade spridningen (antal certifikat som ska utfärdas), giltighetstiden för varje certifikat och antalet aktiva organ för bedömning av överensstämmelse. Betydande intäkter förväntas till följd av spridningen av en framtida ordning för cybersäkerhetsstatus.

År Intäkter (andel kostnader som täcks/betalas genom EU:s budget)

2028 0

2029 250 000 (11 %/ - 1 350 000 EUR) – en ordning (EUCC)

2030 783 000 (29 %/ - 2 000 000 EUR) – tre ordningar (EUCC, den europeiska digitala identitetsplånboken, utlokaliserade säkerhetstjänster)

2031 783 000 (25 %/ - 1 930 000 EUR) – tre ordningar (EUCC, den europeiska digitala identitetsplånboken, utlokaliserade säkerhetstjänster)

2032 3 850 000 (122 %/ - 2 400 000 EUR) – fem ordningar (EUCC, den europeiska digitala identitetsplånboken, utlokaliserade säkerhetstjänster, cybersäkerhetscertifiering av molntjänster, cybersäkerhetscertifiering av 5G-nät)

2033 4 000 000 (126 %/+685 000 EUR) – sex ordningar (EUCC, den europeiska digitala identitetsplånboken, utlokaliserade säkerhetstjänster, cybersäkerhetscertifiering av molntjänster, cybersäkerhetscertifiering av 5G-nät, cybersäkerhetsstatus)

2034 4 500 000 (141 %/+825 000 EUR) – sju ordningar

Avgifter för testverktyg till stöd för förfaranden för bedömning av överensstämmelse.

Avgifterna i samband med denna verksamhet kommer att fastställas i en genomförandeakt efter det att den reviderade cybersäkerhetsakten har antagits. För att ange uppskattade kostnader och förväntade intäkter gjordes dock beräkningar på grundval av uppskattningar från Enisa; dessa inkluderades i konsekvensbedömningen av förslaget till översyn av cybersäkerhetsakten. Följande kostnader uppskattas för stöd till testning och utvärdering:

Heltidsekvivalenter: 4 per år

Driftskostnader: 800 000 EUR per år

Totala kostnader: 6 500 000 EUR (5 år), per år: 1 300 000 EUR

För Enisa förväntas engångsinvesteringar för det första året, följt av underhållskostnader. Dessa kostnader skulle gradvis täckas av intäkter från avgifter.

År Intäkter

2028 0

2029 260 000

2030 260 000

2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIGITALA INSLAG

4.1 Krav med digital relevans

Beskriv på ett övergripande sätt kraven med digital relevans och relevanta kategorier (data, processdigitalisering och processautomatisering, digitala lösningar och/eller digitala offentliga tjänster)

Hänvisning till kravet	**Beskrivning av kravet**	**Aktörer som påverkas eller berörs av kravet**	**Övergripande processer**	**Kategorier**
Artikel 5.1 a Stöd för genomförandet av EU-lagstiftning	a) Hjälpa medlemsstaterna att genomföra unionens politik och lagstiftning på cybersäkerhetsområdet på ett konsekvent sätt, bland annat genom att **utfärda teknisk vägledning och rapporter, tillhandahålla rådgivning och bästa praxis och främja ett utbyte av bästa praxis mellan behöriga myndigheter i detta syfte**.	Enisa Medlemsstaterna	Behandla data för att utfärda teknisk vägledning och rapporter, tillhandahålla rådgivning och utbyta bästa praxis samt underlätta utbyte av bästa praxis mellan behöriga myndigheter Underlätta utbyte av bästa praxis	Databehandling Dataflöde
Artikel 5.1 b Stöd för genomförandet av EU-lagstiftning	b) Stödja **informationsutbyte inom och mellan sektorer, i synnerhet när det gäller de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555** och produkter med digitala element som omfattas av förordning (EU) 2024/2847, **genom att tillhandahålla bästa praxis och vägledning om tillgängliga verktyg och förfaranden**.	Enisa Sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 Berörda parter som påverkas av förordning (EU) 2024/2847	Tillhandahålla bästa praxis och vägledning om tillgängliga verktyg och förfaranden för informationsutbyte	Databehandling Dataflöde

Artikel 5.1 c Stöd för genomförandet av EU-lagstiftning	c) På begäran av kommissionen bistå medlemsstaterna genom att tillhandahålla stöd, såsom **teknisk vägledning – däribland om riskhanteringsåtgärder för cybersäkerhet, verktyg för mognadsbedömning av cybersäkerheten och strategilistor för hantering av cyberincidenter** – som är särskilt anpassat till de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555, för att främja en förbättring av cybersäkerhetens mognadsgrad och efterlevnaden av unionens cybersäkerhetslagstiftning.	EU-kommissionen Enisa Sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555	Tillhandahålla teknisk vägledning	Databehandling Dataflöde
Artikel 5.1 e	e) Hjälpa medlemsstaterna och relevanta unionsentiteter att **utveckla och främja politik på cybersäkerhetsområdet** som rör upprätthållandet av den allmänna tillgängligheten till och integriteten för den offentliga kärnan av det öppna internet.	Enisa Medlemsstaterna EU-entiteter	Bistå i utvecklingen och främjandet av politik på cybersäkerhetsområdet	Databehandling Dataflöde
Artikel 5.1 f Stöd för genomförandet av EU-lagstiftning	f) I enlighet med förordning (EU) 2024/2847 **tillhandahålla teknisk rådgivning och tekniskt stöd** när det gäller frågor som rör genomförandet av den förordningen.	Enisa Berörda parter som påverkas av förordning (EU) 2024/2847	För att tillhandahålla teknisk rådgivning och tekniskt stöd krävs behandling och utbyte av information om lagstadgade krav, utmaningar i samband med genomförandet och vägledning om efterlevnad	Databehandling Dataflöde
Artikel 5.1 h	h) På begäran av Europeiska dataskyddsstyrelsen tillhandahålla råd om genomförandet av specifika cybersäkerhetsaspekter av unionens politik och lagstiftning som rör dataskydd och integritet.	Enisa EDPB	Tillhandahålla rådgivning på begäran	Databehandling Dataflöde

Artikel 5.2 Bidrag till bedömningar på unionsnivå av cybersäkerhetsrisker	Enisa ska bidra till samordnade cybersäkerhetsriskbedömningar på unionsnivå, inbegripet de som utförs i enlighet med artikel 22 i direktiv (EU) 2022/2555.	Enisa Medlemsstaterna Allmänheten	Bidra till samordnade riskbedömningar, vilket kräver databehandling och dataflöde	Databehandling Dataflöde
Artikel 5.3 Enisa ska utfärda riktlinjer	Enisa ska **utfärda riktlinjer** om interoperabiliteten för nätverks- och informationssystem som används för informationsutbyte, även med avseende på gränsöverskridande cybernav enligt artikel 6.3 i förordning (EU) 2025/38.	Enisa Medlemsstaterna	Enisa ska utfärda riktlinjer	Databehandling Dataflöde
Artikel 5.5 Stöd till kommissionen	På **begäran av kommissionen** ska Enisa **tillhandahålla expertis, teknisk rådgivning, information eller analys eller utföra förberedande arbete** i specifika frågor som rör cybersäkerhet, som kan användas som underlag för kommissionens beslutsfattande och övervakning av genomförandet av unionslagstiftningen.	EU-kommissionen Enisa	Förbereda och skicka information till kommissionen	Databehandling Dataflöde

Artikel 6 Kapacitetsuppbyggnad	Enisa ska bistå genom att tillhandahålla kunskap och expertis, bästa praxis osv.	Enisa Medlemsstaterna EU-entiteter Offentliga och privata berörda parter Marknadskontrollmyndigheter Medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning	Tillhandahålla kunskap och expertis	Databehandling Dataflöde
Artikel 7 Medvetandehöjande åtgärder och talangreserv	Enisa ska bistå medlemsstaterna i deras insatser för att öka medvetenheten om unionens politik och lagstiftning på cybersäkerhetsområdet och främja politikens och lagstiftningens synlighet **genom att utveckla vägledning och konkreta verktyg som kan användas**. Enisa ska stödja initiativ som syftar till att öka den europeiska talangreserven på cybersäkerhetsområdet, i synnerhet genom att samordna uttagningsprov.	Enisa Medlemsstaterna	Utveckla användbara verktyg och utarbeta vägledning	Databehandling
Artikel 8.1 Marknadskännedom och marknadsanalyser	Enisa ska **utföra och sprida analyser** av de viktigaste marknadstrenderna på cybersäkerhetsmarknaden på både efterfråge- och utbudssidan, i synnerhet när det gäller områden där det existerar eller planeras europeiska ordningar för cybersäkerhetscertifiering, sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och produktkategorier som omfattas av förordning (EU) 2024/2847, inklusive bilagorna III och IV till den	Enisa Sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 Produktkategorier som omfattas av förordning (EU) 2024/2847	Utföra och sprida analyser	Databehandling Dataflöde

	förordningen.			
Artikel 8.2 Marknadskännedom och marknadsanalyser	Enisa ska **utföra och sprida analyser** av tekniska cybersäkerhetstrender, i synnerhet när det gäller verksamheter och entiteter som omfattas av direktiv (EU) 2022/2555 och produkter med digitala element som omfattas av förordning (EU) 2024/2847.	Enisa Allmänheten, intressenter i den mening som avses i direktiv (EU) 2022/2555 och förordning (EU) 2024/2847	Utföra och sprida analyser	Databehandling Dataflöde
Artikel 8.3 Marknadskännedom och stöd för ekosystem	Enisa ska bygga upp kunskap och **sprida tekniska råd och analyser** om de senaste cybersäkerhetsverktygen, ramar för standarder samt bästa praxis.	Enisa Allmänheten	Sprida teknisk rådgivning och analyser av de senaste cybersäkerhetsverktygen, ramstandarder och bästa praxis	Databehandling Dataflöde
Artikel 9 Internationellt samarbete	Enisa ska bidra genom att analysera och rapportera till styrelsen om resultatet av internationella övningar, underlätta utbytet av bästa praxis och tillhandahålla kommissionen expertis och rådgivning.	Internationell publik Enisa Enisas styrelse EU-kommissionen	Analysera och rapportera, tillhandahålla rådgivning m.m.	Databehandling Dataflöde

Artikel 10.2 och 10.3 Operativt samarbete	2. Enisa ska vara medlem i det nätverk av nationella CSIRT-enheter som inrättats i enlighet med artikel 15.1 i direktiv (EU) 2022/2555 och ska **tillhandahålla CSIRT-nätverkets sekretariat** i enlighet med artikel 15.2 i direktiv (EU) 2022/2555. 3. Enisa ska **tillhandahålla sekretariatet** för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) i enlighet med artikel 16.2 andra stycket i direktiv (EU) 2022/2555.	Enisa CSIRT-enheter (artikel 15.1 i direktiv (EU) 2022/2555) EU-CyCLONe (artikel 16.2 i direktiv (EU) 2022/2555)	Underlätta informationsutbyte och ta sig an uppgifter i egenskap av nätverkssekretariat	Dataflöde Digital lösning Digital offentlig tjänst
Artikel 11.1 b Situationsmedvetenhet Artikel 12 Tidiga varningar	**Utfärda tidiga varningar** i enlighet med artikel 12.	EU-kommissionen Enisa Europol EU-CyCLONe CSIRT-nätverket CERT-EU Entiteter som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555	Utfärda tidiga varningar	Databehandling Dataflöde Digital offentlig tjänst
Artikel 10.4 b Operativt samarbete	b) På begäran av en eller flera medlemsstater **tillhandahålla råd och bedömningar med avseende på specifika potentiella eller pågående incidenter eller cyberhot**, däribland genom att tillhandahålla expertis och **underlätta den tekniska hanteringen av sådana incidenter**, och genom att **stödja frivilligt utbyte av relevant**	Enisa Medlemsstaterna	Tillhandahålla rådgivning och bedömningar i samband med en specifik potentiell eller pågående incident eller ett specifikt potentiellt eller pågående cyberhot Underlätta den tekniska hanteringen av sådana incidenter	Databehandling Dataflöde Digitala offentliga tjänster

	information och tekniska lösningar mellan medlemsstaterna.		Stödja det frivilliga utbytet av relevant information och relevanta tekniska lösningar mellan medlemsstaterna	
Artikel 10.4 c Operativt samarbete	c) Analysera sårbarheter, hot och incidenter.	Enisa Medlemsstaterna	Samla in data från offentliga källor och utbyta data med medlemsstaterna	Databehandling Dataflöde
Artikel 10.4 d Operativt samarbete	d) På **begäran av en eller flera medlemsstater, ge stöd** till tekniska efterhandsundersökningar av betydande incidenter i den mening som avses i direktiv (EU) 2022/2555.	Enisa Medlemsstaterna	Tillhandahålla analys och stöd i samband med tekniska undersökningar av incidenter	Databehandling Dataflöde
Artikel 10.4 e Operativt samarbete	e) Bidra till att stödja den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå, i synnerhet genom att **bistå EU-CyCLONe i arbetet med att utarbeta rapporter för den politiska nivån och genom att främja ett snabbt informationsutbyte mellan CSIRT-nätverket och EU-CyCLONe**.	Enisa EU-CyCLONe CSIRT-nätverket	Analysera data till stöd för utarbetandet av rapporter samt underlätta informationsutbyte i god tid mellan olika nätverk	Databehandling Dataflöde Digital offentlig tjänst
Artikel 10.5 Operativt samarbete	På **begäran av en medlemsstat** eller en unionsentitet ska Enisa i samarbete med CERT-EU stödja konsekvent kommunikation till allmänheten om en incident eller ett cyberhot.	Enisa Medlemsstaterna	Ta emot begäran och kommunicera vid behov	Dataflöde

Artikel 10.6 Operativt samarbete	Enisa ska **stödja** samarbete mellan medlemsstaterna och genom CERT-EU mellan unionsentiteter när det gäller **införandet av säkra kommunikationsverktyg**. Enisa ska inom CSIRT-nätverket och EU-CyCLONe använda säkra kommunikationsverktyg som tillhandahålls av juridiska enheter som inte är etablerade i eller kontrolleras av tredjeländer eller medborgare i tredjeländer.	Enisa EU-kommissionen Medlemsstaterna EU-entiteter CSIRT-nätverket EU-CyCLONe	Stödja införandet av säkra kommunikationsverktyg och använda sådana verktyg inom CSIRT-nätverket och EU-CyCLONe	Digital lösning Digital offentlig tjänst
Artikel 11.1 a Gemensam situationsmedvetenhet på cybersäkerhetsområdet	a) I samarbete med EU-CyCLONe, CSIRT-nätverket, kommissionen, CERT-EU, Europol och andra relevanta unionsentiteter **utveckla databaser** med verifierad och tillförlitlig underrättelseinformation om cyberhot, inbegripet trender i fråga om incidenter, taktik, teknik och förfaranden.	EU-kommissionen Enisa EU-CyCLONe CSIRT-nätverket Europol EU-entiteter CERT-EU	Utveckla databaser	Digitalt flöde Digital lösning Digital offentlig tjänst
Artikel 11.1 c–g Gemensam situationsmedvetenhet på cybersäkerhetsområdet	Tillhandahålla ad hoc-analyser i god tid (ibland på begäran), tillhandahålla analyser och teknisk rådgivning, utarbeta tekniska lägesrapporter i samarbete med andra entiteter samt övervaka och informera om trender	Enisa Medlemsstaterna EU-kommissionen EU-entiteter EU-CyCLONe CSIRT-nätverket	Dataanalys, informationsutbyte och tillhandahållande av rapporter (ibland på begäran)	Databehandling Dataflöde

Artikel 11.2 a Gemensam situationsmedvetenhet på cybersäkerhetsområdet	Enisa ska **utföra analyser** av cyberhot, incidenter, trender, framväxande teknik och konsekvenserna av dessa, inklusive en regelbunden **analys** av sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555 och relevanta produktkategorier som omfattas av förordning (EU) 2024/2847.	Enisa Allmänheten	Analysera data för att tillhandahålla information som är viktig för cybersäkerheten samt rapportera regelbundet	Databehandling Dataflöde
Artikel 11.2 b Gemensam situationsmedvetenhet på cybersäkerhetsområdet	Enisa ska, **i samarbete med kommissionen och, när så är lämpligt, CSIRT-nätverket, utfärda råd, vägledning och bästa praxis** avseende säkerheten i nätverks- och informationssystem, i synnerhet säkerheten för infrastrukturer som stöder de sektorer som förtecknas i bilagorna I och II till direktiv (EU) 2022/2555.	EU-kommissionen CERT-EU CSIRT-nätverket Allmänheten	Utfärda råd, vägledning och bästa praxis	Databehandling Dataflöde
Artikel 11.2 c Gemensam situationsmedvetenhet på cybersäkerhetsområdet	Enisa ska göra **långsiktiga strategiska analyser av cyberhot** och cybersäkerhetsincidenter i syfte att **identifiera** framväxande trender och bidra till att förebygga incidenter.	Enisa Allmänheten	Analysera data och identifiera nya hot	Databehandling
Artikel 11.3 Gemensam situationsmedvetenhet på cybersäkerhetsområdet	Enisa får **offentliggöra analyser**, råd, vägledning, bästa praxis och rapporter som avses i punkt 2, i samförstånd med de bidragande entiteter som avses i punkt 2.	Enisa Allmänheten	Offentliggöra information	Dataflöde Digital offentlig tjänst

Artikel 13.2 Stöd till incidenthantering	2. På begäran av kommissionen eller EU-CyCLONe ska Enisa, med stöd av CSIRT-nätverket och med de berörda medlemsstaternas godkännande, **granska och analysera betydande cybersäkerhetsincidenter** eller storskaliga cybersäkerhetsincidenter i enlighet med artikel 21 i förordning (EU) 2025/38.	EU-kommissionen Enisa EU-CyCLONe CSIRT-nätverket Medlemsstaterna	Utvärdera och analysera betydande cybersäkerhetsincidenter	Databehandling
Artikel 14.2 Cybersäkerhetsövningar på unionsnivå	2. Enisa ska **upprätthålla en databas** över lärdomar från de övningar som avses i punkt 1 och ge medlemsstaterna och, när så är relevant, unionsentiteterna rekommendationer om hur dessa lärdomar ska omsättas i handling på ett ändamålsenligt och effektivt sätt.	Enisa Medlemsstaterna EU-entiteter	Underhålla en databas	Databehandling Digital lösning Digital offentlig tjänst
Artikel 14 Cybersäkerhetsövningar på unionsnivå	Enisa ska, på begäran av EU-CyCLONe, kommissionen, medlemsstaterna eller CERT-EU, anordna eller bidra till anordnandet av cybersäkerhetsövningar. Enisa ska hjälpa kommissionen att sammanställa ett årligt rullande program för cybersäkerhetsövningar på unionsnivå.	Enisa Kommissionen Medlemsstaterna EU-entiteter CERT-EU	Ta emot begäranden om att anordna eller bidra till anordnandet av övningar	Dataflöde Databehandling

Artikel 15 Tillhandahållande av verktyg och plattformar	1. **Enisa ska inrätta, tillhandahålla, driva, underhålla och uppdatera, såsom nödvändigt, operativa tekniska verktyg, inbegripet plattformar** för cybersäkerhet på unionsnivå, i synnerhet den gemensamma rapporteringsplattform för incidentrapportering som inrättats i enlighet med artikel 16.1 i förordning (EU) 2024/2847 [och den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555], och testverktyg till stöd för genomförandet av förfaranden för bedömning av överensstämmelse i enlighet med relevant unionslagstiftning. 2. När så är lämpligt för tillämpningen av punkt 1 **ska Enisa samarbeta och utbyta information** med CSIRT-nätverket och, i tillämpliga fall, marknadskontrollmyndigheter.	Enisa CSIRT-nätverket Allmänheten Marknadskontrollmyndigheter	Enisa ska, beroende på vad som är tillämpligt, inrätta, tillhandahålla, driva, underhålla och uppdatera operativa tekniska verktyg, såsom plattformar	Digital lösning Digital offentlig tjänst Dataflöde
Artikel 16.2 Sårbarhetshanteringstjänster	a) underhålla den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555, b) förse **intressenterna** med sårbarhetshanteringstjänster, på grundval av den europeiska sårbarhetsdatabasen och med utnyttjande av den relevanta information som Enisa har tillgång till, c) när så är lämpligt, ingå strukturerat samarbete med **organisationer** som tillhandahåller program, register eller databaser som liknar den europeiska sårbarhetsdatabasen, d) aktivt stödja **CSIRT-enheter** som utsetts till samordnare i enlighet med	Enisa Nationella CSIRT-enheter CSIRT-nätverket Nationella behöriga myndigheter Näringslivet Forskarsamhället Allmänheten Internationella aktörer som tillhandahåller program, register eller databaser	Tillhandahålla sårbarhetshanteringstjänster, vid behov inleda strukturerade samarbeten samt samarbeta med berörda parter	Digital lösning Digital offentlig tjänst Dataflöde

	artikel 12.1 i direktiv (EU) 2022/2555 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat, e) utveckla och underhålla metoder och styrningsmekanismer för identifiering av sårbarheter och samordnad information om sådana, **i samarbete med nationella behöriga myndigheter, CSIRT-enheter, branschen och forskarsamhället**.			
Artikel 17 Cybersäkerhetscertifiering Artikel 18 Standardisering, tekniska specifikationer och vägledning	Artikel 17.1 a) **Utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordningar*)** för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus och tekniska specifikationer i enlighet med artikel 74. b) **Underhålla antagna europeiska ordningar för cybersäkerhetscertifiering** i enlighet med artikel 75, bland annat med sikte på en eventuell översyn av de antagna europeiska ordningarna för cybersäkerhetscertifiering i enlighet med artikel 76. c) Främja användningen av antagna ordningar och underhålla en särskild webbplats med information om och offentliggörande av europeiska ordningar för cybersäkerhetscertifiering, europeiska cybersäkerhetscertifikat och EU-intyg om överensstämmelse i enlighet med artikel 79.	Enisa Allmänheten	Analysera data och utbyta dataflöden med kommissionen och andra berörda parter, utarbeta förslag till certifieringsordningar samt underhålla Enisas webbplats	Databehandling Dataflöden Digital offentlig tjänst

	Artikel 17.2 e) **Utarbetandet** av standardbestämmelser som det kan hänvisas till i de europeiska ordningarna för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus i enlighet med artikel 81.5. Artikel 18 1. Enisa ska utarbeta tekniska specifikationer och vägledning till stöd för genomförandet av unionslagstiftningen på cybersäkerhetsområdet. 2. Enisa ska **övervaka, delta i och leda arbetet med att utveckla standardiseringen** på unionsnivå och, i enlighet med artikel 9, på internationell nivå. 3. Enisa ska stödja utvecklingen och utvärderingen av krypteringsalgoritmer. Vid ett positivt utfall av utvärderingen av en krypteringsalgoritm ska Enisa samarbeta, i enlighet med förordning (EU) nr 1025/2012, med europeiska standardiseringsorgan för att stödja dess standardisering. 4. Enisa ska ge kommissionen och den europeiska gruppen för cybersäkerhetscertifiering **teknisk sakkunskap** om lämpliga standarder eller tekniska specifikationer till stöd för unionens cybersäkerhetspolitik, i synnerhet förordning (EU) 2024/2847, inbegripet för harmoniserad unionslagstiftning på			

	cybersäkerhetsområdet och europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 81.1 d. 5. Enisa ska bistå kommissionen i bedömningen av förslag till harmoniserade standarder för att stödja genomförandet av harmoniserad unionslagstiftning på cybersäkerhetsområdet.			
Artikel 19 – Den europeiska kompetensramen för cybersäkerhet	Enisa **ska utarbeta och offentliggöra en europeisk kompetensram för cybersäkerhet (*kompetensramen*)**. Innan kompetensramen offentliggörs eller uppdateras i enlighet med punkt 4 ska Enisa **samråda med kommissionen**. Användningen av kompetensramen ska vara **frivillig för offentliga och privata entiteter**. Enisa får **samråda med intressenter** vid utvecklingen och spridningen av kompetensramen.	Enisa Kommissionen Allmänheten Medlemsstaterna EU-entiteter Offentliga och privata berörda parter	Upprätthålla den europeiska kompetensramen för cybersäkerhet, samråda med berörda parter samt främja spridningen av den europeiska kompetensramen för cybersäkerhet	Databehandling Dataflöde Digital lösning
Artiklarna 20–23 – Ordningar för europeiska individuella intyg om cybersäkerhetskompetens	Enisa ska **utveckla, anta och underhålla ordningar för europeiska individuella intyg om cybersäkerhetskompetens**. Användningen av ordningar för europeiska individuella intyg om cybersäkerhetskompetens ska vara **frivillig för nationella offentliga organ och privata entiteter**, om inte annat anges i nationell lagstiftning. Innan en ny ordning för europeiska individuella intyg om cybersäkerhetskompetens inleds ska Enisa **samråda med kommissionen**. Enisa får endast anta en sådan ordning om **kommissionen avgett ett positivt yttrande**.	Enisa Kommissionen Allmänheten Medlemsstaterna EU-entiteter Offentliga och privata berörda parter (som bidrar till utvecklingen av en intygsordning, sökande och tillhandahållare av europeiska individuella intyg om cybersäkerhetskompetens, inklusive bedömare)	Utveckla och underhålla ordningar, samråda med berörda parter, handlägga ansökningar, utfärda beslut samt underhålla en webbplats	Databehandling Dataflöde Digital lösning Digital offentlig tjänst

	Vid utarbetandet av en ordning för europeiska individuella intyg om cybersäkerhetskompetens får Enisa **konsultera relevanta intressenter**. Enisa ska säkerställa ett **nära samarbete med medlemsstaterna** under hela arbetet med att utarbeta ordningar för europeiska individuella intyg om cybersäkerhetskompetens. Auktoriserade tillhandahållare av intyg ska **bedöma om individer uppfyller kraven** i en ordning för europeiska individuella intyg om cybersäkerhetskompetens och ska om dessa krav uppfylls utfärda europeiska individuella intyg om cybersäkerhetskompetens. Enisa ska tillhandahålla **vägledning för och genomföra obligatorisk utbildning av bedömare** med avseende på de krav och bedömningsmetoder som ingår i ordningen för europeiska individuella intyg om cybersäkerhetskompetens enligt artikel 20.3 b. Entiteter som önskar bli auktoriserade tillhandahållare av intyg eller som önskar förnya sin auktorisation **(*sökande*) ska lämna en ansökan** till Enisa. Auktoriserade tillhandahållare av intyg ska **på individens begäran** säkerställa att elektroniska intyg för de europeiska individuella intygen om cybersäkerhetskompetens som utfärdas som elektroniska attributsintyg i ett format som kan lagras i europeiska digitala identitetsplånböcker enligt förordning (EU) nr 910/2014.			

	De sökande och de auktoriserade tillhandahållarna av intyg ska tillåta att **Enisa utför utvärderingar** som ett led i den inledande ansökningsprocessen, upprätthållandet av auktorisationen eller förnyelsen av den och ska dela med sig av all relevant information för att säkerställa att de krav som anges i punkterna 3 och 4 och de skyldigheter som anges i punkt 5 är uppfyllda eller fortsätter att uppfyllas i enlighet med artikel 22.2. Auktoriserade tillhandahållare av intyg ska omedelbart **underrätta Enisa** ifall något av de krav som anges i punkt 3 inte längre uppfylls eller om det uppstår tvivel om ifall dessa krav uppfylls, exempelvis beträffande bedömares oberoende. Sökande ska **betala en avgift till Enisa** för granskningen av deras ansökan. Auktoriserade tillhandahållare av intyg ska **betala en avgift till Enisa** för upprätthållandet av deras auktorisation. **Enisa ska utvärdera** om de krav som fastställs i artikel 21.3 och 21.4 och de skyldigheter som fastställs i artikel 21.5 är uppfyllda eller fortsätter att uppfyllas av sökande och auktoriserade tillhandahållare av intyg. Efter granskning av en ansökan mot kraven i artikel 21.3 och 21.4 **får Enisa utfärda ett beslut**. **Enisa får ändra, tillfälligt upphäva eller återkalla sådana beslut**.			

	Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande: a) Den europeiska kompetensramen för cybersäkerhet och dess tidsplan för uppdatering. b) Ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, deras framsteg och tidsplaner för utvecklingen av dem. c) De avgifter som är förknippade med varje ordning för europeiska individuella intyg om cybersäkerhetskompetens som antagits i enlighet med artikel 47 i denna förordning. d) Den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens i enlighet med artikel 20.4. e) En förteckning över auktoriserade tillhandahållare av intyg.			

Artikel 25 Styrelsens sammansättning	**Utse ledamöter** till Enisas styrelse.	Enisa EU-kommissionen Medlemsstaterna	Utse ledamöter	Dataflöde Databehandling
Artikel 28.1 Styrelsens uppgifter Artikel 30 Direktion	b. Anta Enisas utkast till samlat programdokument som avses i artikel 44 innan det **överlämnas till kommissionen för yttrande**. f) **Bedöma** och anta den konsoliderade årliga rapporten om Enisas verksamhet, inklusive räkenskaperna och en beskrivning av hur Enisa har uppnått sina resultatindikatorer, senast den 1 juli följande år **sända både den årliga rapporten och bedömningen** av denna till Europaparlamentet, rådet, kommissionen och revisionsrätten samt offentliggöra den årliga rapporten. i) Säkerställa lämplig **uppföljning av slutsatserna** och rekommendationerna från interna eller externa revisionsrapporter och utvärderingar samt från utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och Europeiska åklagarmyndigheten (Eppo).	Enisa EU-kommissionen Europaparlamentet Rådet Revisionsrätten Medlemsstaterna Allmänheten	Lämna in det samlade programdokumentet till kommissionen för yttrande. Bedöma och anta den konsoliderade årliga rapporten om Enisas verksamhet, inklusive räkenskaperna och en beskrivning av hur Enisa har uppnått sina resultatindikatorer samt skicka in både den årliga rapporten och bedömningen. Följa upp resultaten.	Dataflöde Databehandling

Artikel 31.8 Utnämning, uppsägning och förlängning av mandatperioden	**Styrelsen ska underrätta Europaparlamentet** om sin avsikt att förlänga den verkställande direktörens mandatperiod i enlighet med punkt 6. Inom tre månader före en sådan förlängning ska den verkställande direktören på anmodan göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.	Enisa Enisas styrelse Europaparlamentet	Styrelsen ska informera Europaparlamentet	Dataflöde
Artikel 32.3 Den verkställande direktörens uppgifter och ansvar Artikel 32.5	3. Den **verkställande direktören ska** på uppmaning **rapportera till Europaparlamentet** om resultatet av sitt arbete. Rådet får uppmana den verkställande direktören att rapportera om resultatet av sitt arbete. Utarbeta förslag till strategier för budgetplaner och strategiska dokument.	Enisas verkställande direktör Europaparlamentet	Rapportera om resultaten	Dataflöde Databehandling
Artikel 35.5 och 35.6 Enisas rådgivande grupp	5. Enisas rådgivande grupp **ska ge Enisa råd** med avseende på genomförandet av Enisas verksamhet, med undantag av tillämpningen av avdelningarna III, IV och V i denna förordning. Den ska i synnerhet ge den verkställande direktören råd om utarbetandet av förslaget till Enisas årliga arbetsprogram och om kommunikationen med berörda intressenter om frågor kopplade till det årliga arbetsprogrammet. 6. Enisas rådgivande grupp ska regelbundet **informera styrelsen** om sin verksamhet.	Enisa Medlemmarna i Enisas rådgivande grupp Enisas styrelse Enisas verkställande direktör	Tillhandahålla rådgivning och information om dess verksamhet	Databehandling Dataflöde

Artiklarna 36–43 Överklagandenämnd	Enisa ska **inrätta en överklagandenämnd** genom ett styrelsebeslut. Överklagandenämnden ska bestå av en ordförande och tre andra ledamöter. Varje ledamot av överklagandenämnden ska ha en suppleant. Suppleanten ska företräda ledamoten i dennas frånvaro. Styrelsen ska **utse ordföranden, de övriga ledamöterna och deras suppleanter** från en **förteckning över kvalificerade sökande som fastställts av kommissionen**. Förteckningen över kvalificerade sökande ska vara giltig i fyra år. Styrelsen kan på förslag av kommissionen förlänga förteckningens giltighet med ytterligare fyraårsperioder. Överklagandenämnden får begära att **styrelsen utser ytterligare två ledamöter och deras suppleanter** från den förteckning som avses i punkt 3 om den anser att ärendet så kräver. Överklagandenämnden ska själv anta och **offentliggöra sin arbetsordning**. Om ledamöter av en överklagandenämnd anser att de, av något av de skäl som förtecknas i punkt 1 eller av andra skäl, inte bör delta i ett överklagandeförfarande **ska de meddela överklagandenämnden detta**. Överklagandenämnden ska **besluta om vilka åtgärder som ska vidtas** i de fall som anges i punkterna 2 och 3 utan att den berörda ledamoten deltar. Vid beslutet ska den berörda ledamoten i överklagandenämnden ersättas av sin suppleant. Ett överklagande enligt punkt 1 ska bli föremål för omprövning i	Enisa Enisas styrelse Kommissionen Överklagandenämnden i den mening som avses i artikel 36 i förslaget till en andra cybersäkerhetsakt Sökande (juridiska personer som vill bli auktoriserade tillhandahållare av intyg eller behålla eller förnya sin auktorisation)	Utfärda beslut på grundval av överklaganden Handlägga överklagandena Utarbeta och offentliggöra arbetsordningen Informationsflöden	Databehandling Dataflöde Digital offentlig tjänst

	enlighet med artikel 41 innan det läggs fram för överklagandenämnden för prövning. Sökande i den mening som avses i artikel 21.3 får **överklaga ett beslut av Enisa** riktat till dem, i enlighet med artikel 22.3, Enisas underlåtenhet att agera på en ansökan som de lämnat in till Enisa inom de tillämpliga tidsfrister som anges i artikel 22.4. I det fall som avses i punkt 1 a ska överklagandet, tillsammans med en motivering, **lämnas in skriftligen** i enlighet med den arbetsordning som avses i artikel 36.5 inom två månader från den dag då beslutet delgavs den berörda sökanden eller, om inget delgivande har skett, den dag då sökanden fick kännedom om beslutet. I det fall som avses i punkt 1 b ska överklagandet **lämnas in skriftligen till Enisa** i enlighet med den arbetsordning som avses i artikel 36.5 inom två månader från den dag då den tidsfrist som anges i artikel 22.4 löper ut. Om Enisa anser att överklagandet kan tas upp till prövning och är välgrundat ska byrån **ändra beslutet eller avhjälpa den underlåtenhet att agera** som avses i artikel 40.1. Om Enisa inte ändrar beslutet inom en månad från mottagandet av överklagandet ska byrån omedelbart **besluta om tillämpningen av beslutet ska skjutas upp och hänskjuta överklagandet till överklagandenämnden**. **Överklagandenämnden** ska, inom tre månader från det att överklagandet lämnats in,			

	besluta att bifalla eller ogilla överklagandet. Vid prövningen av ett överklagande ska överklagandenämnden agera inom de tidsfrister som fastställs i dess arbetsordning. Den ska vid behov **anmoda parterna att inom viss tid inkomma med synpunkter på meddelanden från nämnden eller på inlagor från andra parter i överklagandeförfarandet**. Parterna i överklagandeförfarandet ska ha rätt att göra **muntliga framställningar**. Om överklagandenämnden godtar grunderna för överklagandet ska **den hänskjuta ärendet till Enisa**. När Enisa **fattar sitt slutgiltiga beslut** ska den rätta sig efter överklagandenämndens slutsatser och **motivera sitt beslut**. Enisa ska **underrätta parterna** i överklagandeförfarandet om det beslutet. Talan om ogiltigförklaring av Enisas beslut som antagits i enlighet med artikel 22.3, eller talan om underlåtenhet att agera inom de tillämpliga tidsfristerna i enlighet med artikel 22.4, får **väckas vid Europeiska unionens domstol** efter att det överklagandeförfarande inom Enisa som föreskrivs i artiklarna 39–42 har uttömts eller om åtgärder inte har vidtagits inom den tillämpliga tidsfristen i enlighet med artikel 41.2. Enisa ska **vidta alla de åtgärder som krävs för att följa** Europeiska unionens domstols avgörande.			

Artikel 44 Samlat programdokument	2. Den verkställande direktören ska varje år utarbeta ett utkast till samlat programdokument, som avses i punkt 1, med motsvarande planering av ekonomiska resurser och personalresurser i överensstämmelse med artikel 32 i kommissionens delegerade förordning (EU) 2019/715 och med hänsyn till kommissionens riktlinjer. 3. Senast den 30 november varje år ska styrelsen anta det samlade programdokument som avses i punkt 1, med beaktande av det yttrande från kommissionen som avses i artikel 32.7 i delegerad förordning (EU) 2019/715. Om styrelsen beslutar att inte beakta vissa aspekter av kommissionens yttrande ska den lämna en utförlig motivering till det beslutet. Styrelsen ska senast den 31 januari följande år översända det samlade programdokumentet, liksom eventuella senare uppdaterade versioner, till Europaparlamentet, rådet och kommissionen.	Enisas verkställande direktör Enisas styrelse EU-kommissionen Europaparlamentet Rådet	Utarbeta, anta och översända ett samlat programdokument varje år	Dataflöde
Artikel 45 Upprättande av Enisas budget	4. **Kommissionen ska översända utkastet till beräkning till budgetmyndigheten** tillsammans med förslaget till unionens allmänna budget. Utkastet till beräkning ska också göras tillgängligt för Enisa.	Enisa EU-kommissionen	Utbyta information	Dataflöde

Artikel 47 Avgifter	För verksamhet inom de ordningar för europeiska individuella intyg som avses i artikel 22.1 ska **avgifter tas ut** av sökande i den mening som avses i artikel 21.3 eller av auktoriserade tillhandahållare av intyg, för att bidra till att täcka de totala kostnaderna för Enisas verksamhet, för följande: a. Utfärdande av auktorisationer efter granskning av de krav som anges i artikel 21.3 och 21.4, inbegripet genomförande av utvärderingar. b. Årligt upprätthållande av auktorisationen. c. Förnyande av auktorisationer för tillhandahållare av europeiska individuella intyg om cybersäkerhetskompetens, inbegripet genomförande av utvärderingar. När det gäller certifiering ska **följande avgifter tas ut av organen för bedömning av överensstämmelse** för upprätthållandet av europeiska ordningar för cybersäkerhetscertifiering enligt vilka europeiska cybersäkerhetscertifikat utfärdas: En årlig avgift för deltagande i en europeisk ordning för cybersäkerhetscertifiering. En avgift för utfärdande av europeiska cybersäkerhetscertifikat enligt europeiska ordningar för cybersäkerhetscertifiering. De avgifter som avses i led b ska tas ut när organet för bedömning av överensstämmelse lämnar in europeiska cybersäkerhetscertifikat till Enisa för offentliggörande på byråns webbplats i enlighet med artikel 79.	Kommissionen Enisa Tillhandahållare av intyg Organ för bedömning av överensstämmelse	Behandla information, betala avgifter och rapportera om avgifter	Databehandling Dataflöde

	Kommissionen ska anta genomförandeakter med närmare regler om fastställande av de avgifter som Enisa ska ta ut. Enisa ska inkludera en **rapport om de avgifter som tas ut och deras inverkan på byråns budget** som en del av förfarandet för redovisning.			
Artikel 48 Artikel 49 Budgetkonsekvenser	Artikel 48 3. Den verkställande direktören ska varje år **till budgetmyndigheten översända all information** som rör resultatet av utvärderingsförfaranden. Artikel 49 1. Enisas räkenskapsförare ska **översända de preliminära räkenskaperna för räkenskapsåret** (år n) till kommissionens räkenskapsförare och till revisionsrätten senast den 1 mars följande räkenskapsår (år n + 1). 2. Senast den 1 mars år n + 1 ska Enisas räkenskapsförare också **förse kommissionens räkenskapsförare med de begärda räkenskaperna som ska tjäna som underlag för konsolideringen**, på det sätt och i det format som kommissionens räkenskapsförare anger. 3. Senast den 31 mars år n + 1 **ska Enisa översända rapporten om budgetförvaltningen och den ekonomiska förvaltningen för år n till Europaparlamentet, rådet, kommissionen** och revisionsrätten. 4. **När revisionsrättens iakttagelser om Enisas preliminära räkenskaper för år**	Enisa Enisas styrelse EU-kommissionen Rådet Europaparlamentet	Behandla och utbyta information om Enisas budget	Databehandling Dataflöde

	n har inkommit, ska byråns räkenskapsförare upprätta Enisas slutliga räkenskaper. 5. **Styrelsen ska avge ett yttrande** om Enisas slutliga räkenskaper för år n. **Enisas räkenskapsförare ska upprätta byråns slutliga räkenskaper på eget ansvar. Den verkställande direktören ska överlämna dem till styrelsen för ett yttrande.**			
Artikel 52 Intresseförklaring	Parterna ska **avge en åtagandeförklaring och en förklaring som anger om det föreligger eller inte föreligger** några direkta eller indirekta intressen som skulle kunna anses inverka negativt på deras oberoende.	Enisas ledning (verkställande direktör, vice verkställande direktör) Styrelsen Utsända nationella experter	Behandla och utbyta data om intresseförklaringar	Databehandling Dataflöde
Artikel 58 Kontaktpersoner	1. **Varje medlemsstat ska utse minst två kontaktpersoner** [från deras nationella cybersäkerhetsmyndighet] som nationella experter utstationerade till Enisa för att arbeta vid dess säte eller lokala kontor, i enlighet med artikel 59.2. Kommissionen får också utse en kontaktperson. 2. De kontaktpersoner som utsetts av medlemsstater ska ha rätt att **begära och ta emot all relevant information från sina medlemsstater** i enlighet med denna	Enisa Medlemsstaterna	Utse kontaktpersoner och utbyta information	Databehandling Dataflöde

	förordning, samtidigt som de fullt ut ska respektera nationell rätt och medlemsstatens praxis, särskilt när det gäller dataskydd och regler om konfidentialitet.			
Artikel 67 Hantera säkerhetsskyddsklassificerade uppgifter	**Efter samråd med kommissionen** ska Enisa anta säkerhetsbestämmelser som införlivar säkerhetsprinciperna i kommissionens säkerhetsbestämmelser för skydd av känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter, i enlighet med beslut (EU, Euratom) 2015/443 och 2015/444. Enisas säkerhetsbestämmelser ska omfatta **bestämmelser om utbyte, behandling och lagring av sådana uppgifter**.	Enisa Styrelsen Kommissionen	Hantera säkerhetsskyddsklassificerade uppgifter	Databehandling Dataflöde
Artiklarna 68, 69 och 70 Samarbete med unionsentiteter och nationella myndigheter Samarbete med intressenter Samarbete med tredjeländer	Enisa ska samarbeta och utbyta information i frågor som rör cybersäkerhet med relevanta unionsenheter, marknadstillsynsmyndigheter och tillsynsmyndigheter samt relevanta berörda parter, behöriga myndigheter från tredjeländer eller internationella organisationer.	Enisa Europol Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning Europeiska dataskyddsstyrelsen Allmänheten Rådet	Utbyta information	Dataflöde
Artikel 72 om information till och samråd med allmänheten om europeiska ordningar för cybersäkerhetscertifiering	2. Kommissionen ska upprätthålla och regelbundet uppdatera en särskild webbplats med information om följande: a) Europeiska ordningar för cybersäkerhetscertifiering avseende vilka utveckling begärts. b) Strategiska prioriteringar för	EU-kommissionen Allmänheten Enisa	Underhålla en webbplats för information. Detta innebär att kommissionen ska tillhandahålla information på en allmänt tillgänglig webbplats och löpande sköta den relaterade datahanteringen.	Digital offentlig tjänst Digital lösning

	harmonisering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller säkerhetskrav i unionslagstiftningen, inbegripet potentiella områden för vilka en europeisk ordning för cybersäkerhetscertifiering kan komma att begäras. 3. Kommissionen ska på den webbplats som avses i punkt 2 i denna artikel offentliggöra information om sin begäran till Enisa om att utarbeta ett förslag till certifieringsordning som avses i artikel 73 och sitt beslut att godta, avslå eller inte gå vidare med ett förslag till certifieringsordning som Enisa lämnat in i enlighet med artikel 74.7.			
Artikel 72 om information till och samråd med allmänheten om europeiska ordningar för cybersäkerhetscertifiering	Under Enisas utarbetande av ett förslag till certifieringsordning enligt artikel 74 får **Europaparlamentet och rådet begära att kommissionen**, i egenskap av ordförande för den europeiska gruppen för cybersäkerhetscertifiering, och Enisa lägger fram relevant information om utkastet till förslag till certifieringsordning. **På begäran av Europaparlamentet eller rådet får Enisa, i samförstånd med kommissionen** och utan att det påverkar tillämpningen av artikel 54, **göra relevanta delar av ett utkast till förslag till certifieringsordning tillgängliga för Europaparlamentet och rådet** på ett sätt som är lämpligt med hänsyn till den konfidentialitetsnivå som krävs, och när så är lämpligt på ett begränsat sätt. **Europaparlamentet och rådet får uppmana kommissionen och Enisa att diskutera**	Enisa Rådet Europaparlamentet	Begära och skicka information om ett utkast till förslag till certifieringsordning som utarbetats av Enisa	Dataflöden

	frågor som rör genomförandet av europeiska ordningar för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus.			
Artikel 73 Begäranden om en europeisk ordning för cybersäkerhetscertifiering Artikel 74 Utarbetande och antagande av europeiska ordningar för cybersäkerhetscertifiering **(omfattas av artikel 17)**	**Artikel 73** **1. Kommissionen får begära att Enisa utarbetar ett förslag till en europeisk ordning för cybersäkerhetscertifiering** för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus. I vederbörligen motiverade fall får den europeiska gruppen för cybersäkerhetscertifiering föreslå att kommissionen lägger fram en sådan begäran som avses i punkt 1. 4. När **kommissionen** utarbetar den begäran som avses i punkt 1 ska den vederbörligen samråda med Enisa och den europeiska gruppen för cybersäkerhetscertifiering samt beakta synpunkterna från alla **berörda intressenter** och andra unionsentiteter, inbegripet i tillämpliga fall de som är relevanta enligt unionslagstiftning med avseende på vilken en europeisk ordning för cybersäkerhetscertifiering ger presumtion om överensstämmelse. Artikel 74 3. Vid utarbetandet av förslaget till	EU-kommissionen Enisa Den europeiska gruppen för cybersäkerhetscertifiering Sakkunniga berörda parter	Utarbeta en begäran och en certifieringsordning samt genomföra ett relaterat samråd med berörda parter	Databehandling Dataflöden Digital offentlig tjänst (omfattas av artikel 17)

	certifieringsordning ska Enisa ha ett **nära samarbete med den europeiska gruppen för cybersäkerhetscertifiering**. **Den europeiska gruppen för cybersäkerhetscertifiering ska ge Enisa bistånd** och expertråd vid utarbetandet av förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer. **Enisa ska begära att medlemmarna i den europeiska gruppen för cybersäkerhetscertifiering lämnar skriftliga yttranden om förslaget till certifieringsordning.** 4. **Enisa ska** i god tid **samråda med intressenter** genom en formell, öppen, transparent och inkluderande samrådsprocess. **Enisa ska också samarbeta med relevanta myndigheter i medlemsstaterna och med relevanta unionsentiteter för att samla in deras expertråd** i samband med utarbetandet av förslaget till certifieringsordning och, i tillämpliga fall, stödjande tekniska specifikationer. 6. **Enisa ska översända förslaget till certifieringsordning** till kommissionen senast 60 dagar efter dagen för den begäran som avses i punkt 5. 7. När kommissionen mottar förslaget till **certifieringsordning** ska den **utvärdera** om certifieringsordningen motsvarar den begäran som gjorts i enlighet med artikel 73. 8. Om kommissionen återsänder ett förslag till certifieringsordning till Enisa för översyn i enlighet med punkt 7 b ska			

	punkterna 4, 5 och 7 tillämpas i enlighet med detta.			
Artikel 75 Underhåll av en europeisk ordning för cybersäkerhetscertifiering	2. Enisa ska, i samarbete med kommissionen och med stöd av den europeiska gruppen för cybersäkerhetscertifiering och dess relevanta undergrupp för underhåll, säkerställa underhållet av de europeiska ordningarna för cybersäkerhetscertifiering, även med möjligheten att kommissionen kan se över dessa certifieringsordningar i åtanke. Enisa ska samarbeta och utbyta information med relevanta unionsentiteter och unionsgrupper i samband med underhållsverksamhet. 5. Den europeiska gruppen för cybersäkerhetscertifiering får avge ett yttrande om underhållet av europeiska ordningar för cybersäkerhetscertifiering.	EU-kommissionen Enisa Den europeiska gruppen för cybersäkerhetscertifiering Organ för bedömning av överensstämmelse	Enisa ska säkerställa underhållet. Detta inbegriper regelbundna hybridmöten eller onlinemöten, insamling av information, analys och utbyte (i förhållande till en europeisk ordning för cybersäkerhetscertifiering).	Databehandling Dataflöde
Artikel 76 Utvärdering, översyn och återkallande av en europeisk ordning för cybersäkerhetscertifiering	1. Minst vart fjärde år efter det att en europeisk ordning för cybersäkerhetscertifiering har börjat tillämpas ska Enisa utvärdera certifieringsordningens verkningar och effektivitet, i samarbete med den berörda undergruppen för underhåll inom den europeiska gruppen för cybersäkerhetscertifiering samt med beaktande av återkopplingen från intressenterna. Enisa ska genomföra utvärderingen genom att utföra nödvändig marknadsanalys i enlighet med artikel 8.1. 3. När kommissionen ser över eller återkallar europeiska ordningar för cybersäkerhetscertifiering ska den samråda med Enisa, den europeiska gruppen för	EU-kommissionen Enisa Den europeiska gruppen för cybersäkerhetscertifiering	Kommissionen ska se över ordningarna och samtidigt samråda med berörda parter	Databehandling Dataflöde

	cybersäkerhetscertifiering och dess berörda undergrupp för underhåll samt beakta synpunkter från berörda intressenter och andra unionsentiteter. 4. Den europeiska gruppen för cybersäkerhetscertifiering får avge ett yttrande om översyn eller återkallande av en europeisk ordning för cybersäkerhetscertifiering. Kommissionen ska ta vederbörlig hänsyn till detta när den ser över eller återkallar den europeiska ordningen för cybersäkerhetscertifiering.			
Artikel 77 Tekniska specifikationer i europeiska ordningar för cybersäkerhetscertifiering	3. Om det hänvisas till tekniska specifikationer i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10 ska de göras tillgängliga på den webbplats som avses i artikel 79. 4. I vederbörligen motiverade fall, särskilt om de tekniska specifikationerna innehåller information som skulle kunna äventyra säkerheten för certifierade IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus, ska de distribueras endast till de intressenter som berörs av certifieringsordningens krav. Det ska inte hänvisas till sådana ordningar i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.	Enisa Medlemsstaterna Organ för bedömning av överensstämmelse	Offentliggöra information på Enisas certifieringswebbplats	Dataflöde Digital offentlig tjänst
Artikel 79 Webbplats om europeiska ordningar för cybersäkerhetscertifiering	1. Enisa ska organisera verksamhet för att främja användningen av antagna europeiska ordningar för cybersäkerhetscertifiering, bland annat genom att underhålla den webbplats som	Enisa Medlemsstaterna Organ för bedömning av överensstämmelse	Inom ramen för underhållet av webbplatsen för information ska Enisa samla in, bearbeta och upprätthålla omfattande databaser	Digital offentlig tjänst Digital lösning Databehandling

	avses i punkt 2 i denna artikel. 2. Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande: a) Europeiska ordningar för cybersäkerhetscertifiering. b) Avgifterna i samband med underhållet av varje europeisk ordning för cybersäkerhetscertifiering. c) Enisas relevanta tekniska specifikationer. d) Europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, inbegripet information om sådana certifikat och försäkringar som inte längre är giltiga eller som tillfälligt har upphävts, återkallats eller löpt ut. e) Relevant kompletterande cybersäkerhetsinformation som lämnats i enlighet med artikel 84.2. f) Sammanfattningar av inbördes granskningar enligt artikel 89.7. g) Tekniska specifikationer som det hänvisas till i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10. 3. I tillämpliga fall ska det på den **webbplats som avses i punkt 2 också anges** vilka nationella ordningar för cybersäkerhetscertifiering som har ersatts av en europeisk ordning för cybersäkerhetscertifiering.		med certifieringsinformation, vilket kräver löpande datahantering	Dataflöde
Artikel 81 Komponenter i europeiska ordningar för	5. Kommissionen ges befogenhet att anta genomförandeakter för att fastställa gemensamma principer och	Enisa Allmänheten Medlemsstaternas myndigheter	Samråda med relevanta berörda parter, vilket kräver dataflöden och databehandling	Dataflöde Databehandling

cybersäkerhetscertifiering	standardbestämmelser för de komponenter som anges i punkterna 1, 2 och 3 i alla europeiska ordningar för cybersäkerhetscertifiering. En europeisk ordning för cybersäkerhetscertifiering får innehålla hänvisningar till dessa principer och standardbestämmelser när det är lämpligt och sådana finns tillgängliga. De genomförandeakter som avses i punkt 5 ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2. **När kommissionen utarbetar eller ser över de gemensamma principerna och standardbestämmelserna för komponenterna i europeiska ordningar för cybersäkerhetscertifiering ska den samråda med Enisa och, när så är lämpligt, beakta synpunkter från den europeiska gruppen för cybersäkerhetscertifiering, berörda intressenter och andra relevanta organ.**			
Artikel 83 Självbedömning av överensstämmelse	3. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller den entitet vars cybersäkerhetsstatus certifieringen gäller ska, under en period som fastställs i den motsvarande europeiska ordningen för cybersäkerhetscertifiering, ge den nationella myndighet för cybersäkerhetscertifiering som utsetts enligt artikel 89 tillgång till EU-försäkran om överensstämmelse, teknisk dokumentation och all annan relevant information avseende IKT-produkternas, IKT-tjänsternas, IKT-processernas, de	Enisa Allmänheten Medlemsstaternas myndigheter	Tillhandahålla information och utbyta data. De data som utbyts måste behandlas av Enisa och medlemsstaternas myndigheter.	Dataflöde Databehandling

	utlokaliserade säkerhetstjänsternas eller cybersäkerhetsstatusens överensstämmelse med certifieringsordningen. **En kopia av EU-försäkran om överensstämmelse ska utan onödigt dröjsmål lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.**			
Artikel 84 Kompletterande cybersäkerhetsinformation för certifierade IKT-produkter, IKT-tjänster och IKT-processer	1. Tillverkaren eller leverantören av IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat har utfärdats **ska offentliggöra följande kompletterande cybersäkerhetsinformation**:	Tillverkare eller leverantör av IKT-produkter, IKT-tjänster eller IKT-processer Allmänheten Organ för bedömning av överensstämmelse	Offentliggöra information i elektronisk form	Dataflöde
Artikel 85 Utfärdande av europeiska cybersäkerhetscertifikat	2. De organ för bedömning av överensstämmelse som avses i artikel 91 ska utfärda europeiska cybersäkerhetscertifikat på grundval av de kriterier som ingår i den europeiska ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 74. 6. Den fysiska eller juridiska person som lämnar in sina IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster för certifiering, eller den entitet som ansöker om certifiering av sin cybersäkerhetsstatus, **ska göra all information som krävs för att genomföra certifieringen tillgänglig för den nationella myndighet för cybersäkerhetscertifiering** som utsetts i enlighet med artikel 89, om denna myndighet är det organ som utfärdar det europeiska cybersäkerhetscertifikatet, eller för det organ för bedömning av överensstämmelse	Enisa Allmänheten Medlemsstaternas myndigheter Organ för bedömning av överensstämmelse	Utbyta information som är relevant för certifieringsprocesser	Dataflöde Databehandling

	som avses i artikel 91. 7. Organ för bedömning av överensstämmelse och, i tillämpliga fall, nationella myndigheter för cybersäkerhetscertifiering ska utan onödigt dröjsmål **informera Enisa** om sina beslut som påverkar statusen för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse i enlighet med artikel 94. 8. **Innehavaren av ett europeiskt cybersäkerhetscertifikat ska informera det organ för bedömning av överensstämmelse**, och i tillämpliga fall den nationella myndighet för cybersäkerhetscertifiering, som avses i punkt 7 om alla sårbarheter eller avvikelser som upptäcks senare när det gäller den certifierade IKT-produkten, IKT-tjänsten, IKT-processen, utlokaliserade säkerhetstjänsten eller cybersäkerhetsstatusen och som sannolikt påverkar dess överensstämmelse med certifikatet. **Detta organ ska utan onödigt dröjsmål vidarebefordra informationen** till den berörda nationella myndigheten för cybersäkerhetscertifiering och bedöma inverkan på certifikatet i enlighet med de villkor för certifieringsordningen som avses i artikel 81 f.			
Artikel 86 Nationella ordningar för cybersäkerhetscertifiering	4. **Medlemsstaterna ska underrätta kommissionen och den europeiska gruppen för cybersäkerhetscertifiering innan de antar nya nationella ordningar för cybersäkerhetscertifiering** för IKT-produkter, IKT-tjänster, IKT-processer,	Enisa Medlemsstaterna EU-kommissionen	Utbyta information	Dataflöde

	utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus.			
Artikel 88 Nationella myndigheter för cybersäkerhetscertifiering	2. Varje medlemsstat ska **underrätta kommissionen om vilka nationella myndigheter för cybersäkerhetscertifiering som utsetts**. Om en medlemsstat utser mer än en myndighet ska den också informera kommissionen om vilka uppgifter som var och en av dessa myndigheter tilldelats. 6. Nationella myndigheter för cybersäkerhetscertifiering ska ha följande uppgifter: c) **I samarbete med berörda marknadskontrollmyndigheter övervaka att tillverkare eller leverantörer** av IKT-produkter, IKT-tjänster, IKT-processer eller utlokaliserade säkerhetstjänster eller entiteter vars cybersäkerhetsstatus har certifierats vilka är etablerade inom deras respektive territorier och vilka utför självbedömning av överensstämmelse inom ramen för motsvarande europeiska ordning för cybersäkerhetscertifiering **fullgör sina skyldigheter** enligt denna förordning och **kontrollera efterlevnaden av**. **dessa skyldigheter**. d) Utan att det påverkar tillämpningen av artikel 91.3 **aktivt bistå och stödja de nationella ackrediteringsorganen eller andra berörda myndigheter med övervakning och tillsyn** av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning.	Enisa Medlemsstaternas myndigheter EU-kommissionen Allmänheten Organ för bedömning av överensstämmelse	Medlemsstaten ska informera kommissionen om de nationella myndigheter för cybersäkerhetscertifiering som utsetts. Medlemsstaternas myndigheter ska utföra olika uppgifter bestående av övervakning, tillsyn och samarbete som kräver dataflöden och databehandling.	Dataflöde Databehandling

	e) Samarbeta med Europeiska kommissionen i de fall då kompetensen hos ett organ för bedömning av överensstämmelse ifrågasätts i enlighet med artikel 94. f) **Övervaka och utöva tillsyn över den verksamhet** som bedrivs av de offentliga organ som avses i artikel 85.3. g) I tillämpliga fall bemyndiga organ för bedömning av överensstämmelse i enlighet med artikel 93, övervaka att organ för bedömning av överensstämmelse fullgör de specifika eller ytterligare krav som fastställs i europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 81.3 f och kontrollera efterlevnaden av dessa krav, och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om organ för bedömning av överensstämmelse inte uppfyller kraven i denna förordning. h) **Behandla klagomål** från fysiska eller juridiska personer avseende europeiska cybersäkerhetscertifikat som utfärdats av nationella myndigheter för cybersäkerhetscertifiering eller europeiska cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 85.4, eller avseende EU-försäkringar om överensstämmelse som utfärdats enligt artikel 83, i lämplig utsträckning undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen. i) Senast den 31 mars [året för			

	ikraftträdande + 12 månader] varje år lämna en årlig rapport om sin huvudsakliga verksamhet till kommissionen, Enisa och den europeiska gruppen för cybersäkerhetscertifiering, samt göra dessa rapporter tillgängliga för den grupp som utför den inbördes granskningen om den nationella myndigheten för cybersäkerhetscertifiering blir föremål för inbördes granskning i enlighet med artikel 89. j) **Samarbeta med andra nationella myndigheter för cybersäkerhetscertifiering**, marknadskontrollmyndigheter eller andra myndigheter, inbegripet genom att utbyta information om IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus som eventuellt avviker från kraven i denna förordning eller från kraven i särskilda europeiska ordningar för cybersäkerhetscertifiering. k) **Övervaka relevant utveckling på området cybersäkerhetscertifiering**. 8. Nationella myndigheter för cybersäkerhetscertifiering ska samarbeta med varandra och med kommissionen, i synnerhet genom att **utbyta information, erfarenheter och god praxis** när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus.			

	9. Senast den [ikraftträdandet + 6 månader] ska Enisa, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering, utarbeta en mall för den rapport som avses i punkt 6 i i denna artikel.			
Artikel 89 Inbördes granskning	5. **Enisa ska stödja** organisationen av mekanismen för inbördes granskning och de inbördes granskningarna, bland annat genom att **utarbeta relevanta vägledningsdokument och mallar**, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering. 7. **Slutrapporten, inbegripet eventuella** riktlinjer eller rekommendationer, och sammanfattningen av den inbördes granskningen ska granskas av den europeiska gruppen för cybersäkerhetscertifiering, som ska godkänna sammanfattningen för offentliggörande på den webbplats som avses i artikel 79.2.	EU Enisa Den europeiska gruppen för cybersäkerhetscertifiering	Göra data tillgängliga på nätet	Dataflöde Databehandling
Artikel 90 Den europeiska gruppen för cybersäkerhetscertifiering	3. Den europeiska gruppen för cybersäkerhetscertifiering ska ha i uppgift att [hänvisning till andra artiklar] h) undersöka den relevanta utvecklingen på området cybersäkerhetscertifiering, även på nationell nivå i enlighet med artikel 86, och utbyta information och god praxis om ordningar för cybersäkerhetscertifiering, i) underlätta samarbetet mellan nationella myndigheter för cybersäkerhetscertifiering enligt reglerna i	Medlemsstaterna Enisa EU-kommissionen	Analys, informationsutbyte och samarbete mellan medlemsstaternas myndigheter och internationella organisationer rörande europeisk cybersäkerhetscertifiering	Databehandling Dataflöde

	denna avdelning genom kapacitetsuppbyggnad och utbyte av information, särskilt när det gäller frågor som rör cybersäkerhetscertifiering, [hänvisning till andra artiklar] k) underlätta anpassningen av europeiska ordningar för cybersäkerhetscertifiering till internationellt erkända standarder, också som en del av underhållet av befintliga europeiska ordningar för cybersäkerhetscertifiering och, där så är lämpligt, lämna rekommendationer till Enisa om att samarbeta med relevanta europeiska eller internationella standardiseringsorganisationer för att åtgärda brister eller luckor i de tillgängliga europeiska eller internationellt erkända standarderna.			
Artikel 92 Ytterligare harmonisering av befogenheterna för organen för bedömning av överensstämmelse	4. Om en nationell myndighet för cybersäkerhetscertifiering tar emot en begäran enligt punkt 3 ska den **informera den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstat där det begärande organet för bedömning av överensstämmelse är etablerat**. I sådana fall får den nationella myndigheten för cybersäkerhetscertifiering i den medlemsstaten delta i bemyndigandet som observatör.	Medlemsstaternas myndigheter Organ för bedömning av överensstämmelse	Utbyta och lagra information	Dataflöde Databehandling
Artikel 93 Anmälan av organ för bedömning av överensstämmelse	1. För varje europeisk ordning för cybersäkerhetscertifiering ska de nationella **myndigheterna för cybersäkerhetscertifiering i en medlemsstat till kommissionen och de andra medlemsstaterna anmäla** de organ för bedömning av överensstämmelse som har	Enisa Medlemsstaterna EU-kommissionen Organ för bedömning av överensstämmelse	Anmäla ackrediterade och auktoriserade organ för bedömning av överensstämmelse	Dataflöden Databehandling

	ackrediterats och, i tillämpliga fall, bemyndigats i enlighet med artikel 92. 2. **De nationella myndigheterna för cybersäkerhetscertifiering ska göra den anmälan som avses i punkt 1** med hjälp av det elektroniska anmälningsverktyg som utvecklats och förvaltas av kommissionen.			
Artikel 94 Ifrågasättande av kompetensen hos organen för bedömning av överensstämmelse	1. 1. **Kommissionen ska undersöka** alla fall i vilka den tvivlar på, eller görs uppmärksam på tvivel på, att ett organ för bedömning av överensstämmelse har kompetens att uppfylla, eller att ett organ för bedömning av överensstämmelse fortsatt uppfyller, de krav och skyldigheter som det omfattas av. 2. **Den nationella myndigheten för cybersäkerhetscertifiering ska på begäran ge kommissionen** all information om grunderna för anmälan eller om hur kompetensen upprätthålls inom det berörda organet för bedömning av överensstämmelse. 3. **Kommissionen ska säkerställa att all känslig information som erhållits i samband med undersökningarna behandlas konfidentiellt.** 4. Om kommissionen konstaterar att ett organ för bedömning av överensstämmelse inte uppfyller eller inte längre uppfyller kraven för anmälan ska den **meddela detta till den nationella myndigheten för cybersäkerhetscertifiering** och begära att den vidtar erforderliga korrigerande åtgärder, såsom att vid behov återta anmälan.	Kommissionen Medlemsstaterna Enisa	Ifrågasättande av kompetensen hos organen för bedömning av överensstämmelse	Dataflöde Databehandling Digital offentlig tjänst
Artikel 95	1. Organ för bedömning av överensstämmelse	Medlemsstaternas myndigheter	Ta emot information från organ	Dataflöde

Informations- och lagringsskyldighet för organ för bedömning av överensstämmelse	**ska informera den nationella myndigheten för cybersäkerhetscertifiering** om följande: a) Avslag på ansökan om certifikat, eller begränsning, tillfälligt upphävande eller återkallelse av ett certifikat. b) Omständigheter som påverkar omfattningen av och villkoren för den anmälan som avses i artikel 93.1. c) Eventuella begäranden om information de har tagit emot från marknadskontrollmyndigheterna om bedömningar av överensstämmelse. d) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad. 2. **Organ för bedömning av överensstämmelse ska också förse Enisa med den information** som avses i punkt 1 a för att underlätta utförandet av dess uppgifter enligt artikel 79. 3. **Organ för bedömning av överensstämmelse ska utan onödigt dröjsmål ge de andra organ för bedömning av överensstämmelse**, i den mening som avses i denna förordning, som utför liknande bedömningar av överensstämmelse avseende samma IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteter vars cybersäkerhetsstatus är	Organ för bedömning av överensstämmelse	för bedömning av överensstämmelse	Databehandling

	certifierad **relevant information** om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse. 4. **Organ för bedömning av överensstämmelse ska upprätthålla ett registersystem** som innehåller alla dokument och bevis som tagits fram eller mottagits i samband med varje utvärdering och certifiering som de utför. Registret ska lagras på ett säkert och tillgängligt sätt under den period som krävs för certifieringsändamål och i minst fem år efter det att det berörda europeiska cybersäkerhetscertifikatet löper ut eller återkallas.			
Artikel 96 Rätt att lämna in klagomål och rätt till ett effektivt rättsmedel	2. Den myndighet eller det organ till vilket klagomålet har lämnats in **ska underrätta den klagande om hur förfarandet fortskrider**, vilket beslut som fattats och om den rätt till ett effektivt rättsmedel som avses i punkterna 3 och 4. 4. Förfaranden enligt denna artikel ska inledas vid domstolarna i den medlemsstat där den myndighet eller det organ som rättsmedlet avser ligger.	Medlemsstaternas myndigheter EU-kommissionen Allmänheten Innehavare av certifikat	Informationsflöde mellan myndigheter och allmänheten om klagomål Förfaranden vid medlemsstatens domstol	Dataflöde
Artikel 97 Sanktioner	**Medlemsstaterna ska till kommissionen anmäla** dessa regler och åtgärder utan dröjsmål samt eventuella ändringar som berör dem.	Medlemsstaternas myndigheter EU-kommissionen	Informationsflöde i samband med medlemsstaternas anmälan till kommissionen om sanktioner	Dataflöde

Artikel 99 Säkerhetsriskbedömningar	Kommissionen eller minst tre medlemsstater får begära att samarbetsgruppen för nät- och informationssäkerhet utför samordnade riskbedömningar inom sex månader. Kommissionen får begära kortare tidsfrister. I riskbedömningarna ska riskscenarier tas fram, och riskbedömningarna ska bygga på dataanalyser. Utarbetande av samordnade säkerhetsriskbedömningar I fall där ett omedelbart ingripande är motiverat ska kommissionen utan dröjsmål samråda med medlemsstaterna och göra en riskbedömning. Beslut om att genomföra riskbedömningar (databehandling/dataanalys).	EU-kommissionen Medlemsstaterna Samarbetsgruppen för nät- och informationssäkerhet Enisa	Begära och ta emot information samt utföra dataanalyser för samordnade riskbedömningar Samråda med medlemsstaterna och göra en riskbedömning	Databehandling Dataflöde
Artikel 100.1 och 100.2 Utseende av tredjeländer som utgör cybersäkerhetsproblem	1. Om det till följd av den säkerhetsriskbedömning som avses i artikel 99, eller på grundval av andra källor, såsom ett offentligt uttalande på unionens eller en medlemsstats vägnar, framstår som att ett tredjeland utgör allvarliga och strukturella icke-tekniska risker för IKT-leveranskedjorna, ska kommissionen kontrollera det hot som det landet utgör, med beaktande av ett antal element, vilket leder till	Medlemsstaterna EU-kommissionen	Ta emot, analysera och utbyta information	Dataflöden Databehandling

	databehandling/dataanalys. 2. När kommissionen efter den kontroll som avses i punkt 1 drar slutsatsen att ett tredjeland utgör allvarliga och strukturella icke-tekniska risker för IKT-leveranskedjorna, får den genom en genomförandeakt besluta att beteckna det tredjelandet som ett land som utgör cybersäkerhetsproblem för IKT-leveranskedjorna, vilket leder till databehandling/dataanalys.			
Artikel 101 Allmän mekanism för IKT-leveranskedjan Artikel 102 Identifiering av viktiga IKT-tillgångar	1. När samarbetsgruppen för nät- och informationssäkerhet har genomfört en samordnad säkerhetsriskbedömning på unionsnivå i enlighet med artikel 99.1 och 99.2 i denna förordning, eller efter det att förfarandet i händelse av ett betydande cyberhot i enlighet med artikel 99.3 har slutförts, får kommissionen vidta de åtgärder som föreskrivs i artiklarna 102 och 103. Kommissionen ges befogenhet att anta genomförandeakter, i vilka viktiga IKT-tillgångar och begränsningsåtgärder kommer att fastställas, inklusive begränsningar och förbud för IKT-leveranskedjor (se avsnitt 4.5 nedan). Under förberedelserna för denna process	EU-kommissionen Samarbetsgruppen för nät- och informationssäkerhet Relevanta berörda parter	Analysera/behandla data samt samråda med relevanta berörda parter	Databehandling Dataflöde

Artikel 103 Begränsningsåtgärder i IKT-leveranskedjan	ska kommissionen beakta flera aspekter som kräver **databehandling/dataanalys och i vissa fall dataflöde**: Artikel 102 a–f Artikel 103.4 a–d Artikel 103.6			
Artikel 104 Identifiering av högriskleverantörer	Kommissionen ska genom genomförandeakter upprätta förteckningar över högriskleverantörer av relevans för de förbud som fastställs i de genomförandeakter som antagits i enlighet med artikel 103.1 eller det förbud som avses i artikel 111.1. Kommissionen ska kartlägga leverantörer av IKT-komponenter och komponenter som innehåller IKT-komponenter samt göra en inledande bedömning av huruvida leverantörerna potentiellt är etablerade i eller kontrolleras av tredjeländer som fastställts i enlighet med artikel 100. Kommissionen ska bedöma etableringsorten samt ägar- och kontrollstrukturen. Kommissionen ska ha rätt att begära nödvändig information från leverantörerna och ska dela med sig av de preliminära slutsatserna om bedömningen av etableringen samt ägar- och	EU-kommissionen Behöriga myndigheter Leverantörer	Analysera/behandla data samt samråda med behöriga myndigheter och leverantörer	Databehandling Dataflöde

	kontrollstrukturen till de berörda leverantörerna och ge dem tillfälle att bli hörda. Kommissionen får be en behörig myndighet att göra den inledande bedömningen av en leverantörs etablerings-, ägande- och kontrollstruktur, när detta är motiverat med hänsyn till särdragen för leverantörens verksamhet. En behörig myndighet får erbjuda sig att utföra denna inledande bedömning. Kommissionen ska kontrollera dessa inledande resultat i syfte att besluta om leverantören bör föras upp på förteckningen över högriskleverantörer. Kommissionen ska regelbundet uppdatera förteckningarna över högriskleverantörer i syfte att ta bort eller lägga till högriskleverantörer. Högriskleverantörer som ingår i förteckningen får begära att kommissionen gör en ny bedömning av deras etablerings-, kontroll- och ägandestruktur på grundval av bevis att det har skett relevanta ändringar.			

Artikel 105 Undantag för entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem Artikel 108 Konfidentialitet	1) En entitet som är etablerad i eller kontrolleras av ett tredjeland som fastställts utgöra cybersäkerhetsproblem **kan lämna en motiverad ansökan** till kommissionen. 3) Kommissionen ska bedöma och anta ett beslut **med beaktande av flera aspekter** som leder till dataanalys (artikel 105.3 och 105.4). Information som kommissionen tar emot får endast användas för de ändamål för vilka de inhämtades.	EU-kommissionen Entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som fastställts utgöra cybersäkerhetsproblem	Kommissionen tar emot ansökan och analyserar data	Dataflöde Databehandling
Artikel 107 Register	Kommissionen ska föra ett offentligt register över sina beslut enligt artikel 105. Registret ska innehålla namnen på de entiteter som omfattas av besluten.	EU-kommissionen Entiteter som är etablerade i eller kontrolleras av ett tredjeland som fastställts utgöra cybersäkerhetsproblem	Kommissionen för ett offentligt register	Digital lösning
Artikel 111 Förbud för mobila, fasta och satellitbaserade elektroniska kommunikationsnät	Den behöriga myndighet som utsetts enligt den här förordningen ska utan dröjsmål **informera** den behöriga myndigheten enligt förordning (EU) XX/XXXX [förslaget till förordning om digitala nätverk] om de åtgärder som åläggs leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät.	Behörig myndighet i den mening som avses i artikel 9 eller 20 i förordning (EU) XXXX/XX [förslaget till rättsakt om digitala nät] Leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät	Informationsflöde från behöriga myndigheter till entiteter vad gäller auktorisationer	Dataflöde

Artikel 112.1 och 112.4 Behöriga myndigheter	1) **Varje medlemsstat ska utse** en eller flera behöriga myndigheter med ansvar för att vidta de tillsyns- och efterlevnadskontrollåtgärder som avses i artikel 114. 4) Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen namnen på de behöriga myndigheter som utsetts i enlighet med punkt 1, dessa myndigheters respektive uppgifter och eventuella senare ändringar av dessa. Varje medlemsstat ska också offentliggöra namnen på de behöriga myndigheter som utsetts i enlighet med punkt 1.	Medlemsstaterna EU-kommissionen Allmänheten	Medlemsstaterna utser behöriga myndigheter och underrättar kommissionen	Dataflöde
Artikel 113 Kommissionens samarbets- och stödtjänstnätverk	1. Kommissionen ska inrätta ett nätverk för samarbete mellan de behöriga myndigheterna i medlemsstaterna och kommissionen, vilket ska fungera som en plattform för samarbete och informationsutbyte. Kommissionen ska ge administrativt stöd till nätverket. 2. För att hjälpa medlemsstaterna med deras tillsynsuppgifter ska kommissionen bedöma huruvida leverantörer som kan påverkas av särskilda förbud är etablerade i eller kontrolleras av tredjeländer som har fastställts utgöra cybersäkerhetsproblem i enlighet med artikel 100. För detta	Kommissionen Behöriga myndigheter Entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555	Kommissionen bedömer leverantörerna och delar med sig av resultaten till de behöriga myndigheterna som i sin tur delar dem med entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555. Kommissionen begär information från leverantörerna. De behöriga myndigheterna underrättar kommissionen.	Databehandling Dataflöden

	ändamål ska den behöriga myndigheten utbyta relevant information med kommissionen. 3. Inom ramen för bedömningen ska kommissionen ha rätt att begära nödvändig information från leverantörer som kan påverkas av särskilda förbud och som är etablerade i eller kontrolleras av tredjeländer som fastställts i enlighet med artikel 100. 4. När en bedömning har slutförts ska kommissionen dela resultaten med de behöriga myndigheterna inom det nätverk som inrättats i enlighet med punkt 1. De behöriga myndigheterna ska i god tid informera de berörda entiteterna av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555 om resultaten. 5. Om en behörig myndighet får kännedom om en leverantör som kan påverkas av särskilda förbud och som är etablerad i eller kontrolleras av ett tredjeland som utgör cybersäkerhetsproblem och om den leverantören inte har genomgått en bedömning, ska den behöriga myndigheten utan onödigt dröjsmål underrätta kommissionen.			

Artikel 114 Tillsyns- och efterlevnadskontrollåtgärder	Krav på medlemsstaterna som kommer att säkerställa informationsflödet med de entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555. Innan de behöriga myndigheterna antar åtgärder ska de underrätta de berörda entiteterna om sina preliminära slutsatser. De behöriga myndigheterna ska samarbeta med varandra och med kommissionen.	Medlemsstaterna EU-kommissionen Entiteter inom ramen för bilagorna I och II till direktiv (EU) 2022/2555	Krav som säkerställer informationsflödet	Dataflöde Databehandling
Artikel 115 Sanktioner	Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder samt utan dröjsmål eventuella ändringar som berör dem.	EU-kommissionen Medlemsstaterna	Medlemsstaterna underrättar kommissionen	Dataflöde
Artikel 116 Ömsesidigt bistånd	Om en entitet som avses i bilaga I eller II till direktiv (EU) 2022/2555 tillhandahåller tjänster i fler än en medlemsstat, eller tillhandahåller tjänster i en eller flera medlemsstater och dess viktiga IKT-tjänster är belägna i en eller flera andra medlemsstater, **ska de behöriga myndigheterna i de berörda medlemsstaterna vid behov samarbeta med varandra och bistå varandra**. Det ömsesidiga bistånd som avses i första stycket c får omfatta begäranden om	Medlemsstaterna	Ömsesidigt bistånd vid tillsynsåtgärder	Dataflöde Databehandling

	information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får inte avslå begäran om det inte fastställs att myndigheten inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga intressen som rör nationell säkerhet, allmän säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med kommissionen. När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra gemensamma tillsynsåtgärder.			

Artikel 1.8 i direktivet Rapportering av attacker med utpressningsprogram (artikel 27.13 i NIS 2-direktivet)	I artikel 23 ska följande punkter läggas till som punkterna 12 och 13: ”13. Medlemsstaterna ska säkerställa att de berörda entiteterna, i händelse av en betydande incident som orsakas av en attack med utpressningsprogram, på begäran av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten via en kommunikationskanal som tillhandahålls av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten, lämnar in följande information Huruvida entiteten har mottagit ett krav på lösensumma och, i förekommande fall, av vem. Huruvida en lösensumma betalades och om ja, vilket belopp, vilket betalningssätt och till vilken mottagare eller mottagande sida, inbegripet leverantören av kryptotillgångar och leverantören av kryptotillgångstjänster, i förekommande fall.”	Medlemsstaterna Väsentliga och viktiga entiteter	Rapportering	Dataflöde
Artikel 1.10 i direktivet Förteckning över entiteter och register (artikel 27.1 i NIS 2-direktivet)	**Enisa ska skapa och upprätthålla ett register över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 2**.	Enisa Medlemsstaterna (väsentliga och viktiga entiteter enligt NIS 2-direktivet samt entiteter som tillhandahåller domännamnsregistreringstjänster)	Enisa ska skapa och upprätthålla ett register	Digital lösning Digital offentlig tjänst

Artikel 1.11 i direktivet Förteckning över entiteter och register (artikel 27.4 i NIS 2-direktivet)	**”4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i artikel 3.4, ska den utan dröjsmål vidarebefordra den informationen till Enisa.”**	Enisa Medlemsstaterna	Medlemsstaterna utbyter information med Enisa	Dataflöde
Artikel 1.12 i direktivet Ömsesidigt bistånd (artikel 37a.1, 37a.2 och 37a.3 i NIS 2-direktivet)	**1. Enisa ska hjälpa medlemsstaterna** att genomföra ömsesidigt bistånd i den mening som avses i artikel 37 och **hjälpa till att främja sådana samarbetsförfaranden** för väsentliga och viktiga entiteter [...]. 2. Enisa [ska] **genomföra en heltäckande analys** [...] **Enisa [ska], i samarbete med** kommissionen och samarbetsgruppen, utarbeta en metod. Rapporten ska uppdateras varje år. 3. Enisa [ska] vid behov rekommendera [...] utarbeta riktlinjer [...] bistå [...]	Enisa Medlemsstaterna Viktiga och väsentliga entiteter i den mening som avses i NIS 2-direktivet EU-kommissionen	Enisa ska bistå medlemsstaterna och underlätta samarbetet samt utföra analyser och utarbeta riktlinjer, metoder och rapporter	Databehandling Dataflöde
Artikel 1.12 i direktivet Ömsesidigt bistånd (artikel 37a i NIS 2-direktivet [4])	4. Vid tillämpning av punkt 4 e i denna artikel ska de behöriga myndigheterna i de **berörda medlemsstaterna i förekommande fall förse Enisa med** [följande]. 5. Om en medlemsstat erhåller ömsesidigt bistånd enligt artikel 37.1 första stycket c, ska den **gemensamma kontaktpunkten informera Enisa** om att ömsesidigt bistånd ägde rum.	Enisa Medlemsstaterna	Informationsutbyte	Dataflöde
Artikel 119 Utövande av delegeringen	3. Så snart kommissionen antar en delegerad akt ska den **samtidigt delge** Europaparlamentet och rådet denna.	EU-kommissionen Europaparlamentet Rådet	Information skickas till Europaparlamentet och rådet	Dataflöde
Artikel 120 Utvärdering och granskning	1. Senast den [DD MM ÅÅÅÅ] och därefter vart femte år ska kommissionen beställa en utvärdering av Enisas resultat i	Enisa Kommissionen Allmänheten	Samla in och analysera data samt offentliggöra information	Databehandling Dataflöde

	förhållande till dess mål, mandat, uppdrag, uppgifter, styrning och lokalisering i enlighet med kommissionens riktlinjer. 5. Kommissionen ska meddela resultatet av utvärderingen till Europaparlamentet, rådet och styrelsen. Utvärderingens resultat ska offentliggöras.			

4.2 Data

Beskrivning (övergripande nivå) av data som omfattas och eventuella tillhörande standarder/specifikationer

Typ av data	**Hänvisning/hänvisningar till kravet**	**Standard och/eller specifikation (i tillämpliga fall)**
Data kopplade till analyser/rapporter av betydelse för cybersäkerhetsresiliensen och samhället	**Artikel 5.1 a, b, c, e, f och h** **Artikel 5.2, 5.3 och 5.4** **Artikel 6** **Artikel 7** **Artikel 8** **Artikel 9** **Artikel 10** **Artikel 11.2 b och c** **Artikel 12.4** **Artikel 15** **Artikel 1.7 i direktivet**	Vid utförandet av de uppgifter som anges i artiklarna 11.1 a–e och 11.2 ska Enisa använda sina egna analyser och, när så är lämpligt, information som byrån fått i samband med utförandet av sina uppgifter, däribland följande: a) Information från allmänt tillgängliga källor, inklusive allmänt kända sårbarheter i IKT-produkter eller IKT-tjänster som finns tillgängliga i den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555. b) Information som förmedlats av medlemsstater, unionsentiteter, CERT-EU, partner inom privat sektor eller icke-statliga partner samt tredjelandsorganisationer och internationella organisationer, med förbehåll för eventuella

		begränsningar av vidarespridningen av informationen som anges med en synlig märkning. Enisa ska utfärda riktlinjer om interoperabiliteten för nätverks- och informationssystem som används för informationsutbyte, även med avseende på gränsöverskridande cybernav enligt artikel 6.3 i förordning (EU) 2025/38.
Data av betydelse för det operativa samarbetet och situationsmedvetenheten	**Artikel 10.4 a–g** **Artikel 10.6** **Artikel 11.1 a–g** **Artikel 11.2 a, b och c** **Artikel 11.3** **Artikel 11.4** **Artikel 13.2** **Artikel 15** **Artikel 16.2 e**	**Standarder för konfidentialitet och hantering av känslig information** Vid utförandet av de uppgifter som anges i artiklarna 11.1 a–e och 11.2 ska Enisa använda sina egna analyser och, när så är lämpligt, information som byrån fått i samband med utförandet av sina uppgifter, däribland följande: a) Information från allmänt tillgängliga källor, inklusive allmänt kända sårbarheter i IKT-produkter eller IKT-tjänster som finns tillgängliga i den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555. b) Information som förmedlats av medlemsstater, unionsentiteter, CERT-EU, partner inom privat sektor eller icke-statliga partner samt tredjelandsorganisationer och internationella organisationer, med förbehåll för eventuella begränsningar av vidarespridningen av informationen som anges med en synlig märkning.
Data av betydelse för ordningarna för europeiska individuella intyg om cybersäkerhetskompetens och auktorisering av tillhandahållare **Data av betydelse för målen och syftet med samt**	**Artikel 17** **Artikel 18** **Artiklarna 19–23** **Artiklarna 72, 73, 74, 75, 76, 77, 79, 81, 83 och 84**	En ordning för europeiska individuella intyg om cybersäkerhetskompetens ska omfatta [...] Regler om hur auktoriserade tillhandahållare av intyg ska bevara uppgifter. Auktoriserade tillhandahållare ska på individens begäran säkerställa att elektroniska intyg för de europeiska individuella intygen om cybersäkerhetskompetens som utfärdas som elektroniska attributsintyg i ett format som kan lagras i europeiska digitala identitetsplånböcker enligt förordning (EU)

innehållet i europeiska ordningar för cybersäkerhetscertifiering		nr 910/2014. . Kommissionen och Enisa bör följa relevanta bestämmelser i unionslagstiftningen när de inrättar en europeisk ordning för cybersäkerhetscertifiering när det gäller data.
Data om styrningen av det europeiska ramverket för cybersäkerhetscertifiering	**Artiklarna 85, 86, 88, 89, 90, 92, 93, 94, 95, 96 och 97**	Enisa, organen för bedömning av överensstämmelse och de nationella myndigheterna för cybersäkerhetscertifiering bör säkerställa datakonfidentialiteten och följa bestämmelserna för en relevant ordning samtidigt som de hänvisar till internationella standarder som specificerar kraven.
Data av betydelse för Enisas interna funktioner (budgeten, det samlade programdokumentet, interna strategier)	**Artikel 25** **Artikel 28.1** **Artikel 30** **Artikel 31.8** **Artikel 32.3 och 32.5** **Artikel 35.5 och 35.6** **Artiklarna 36–43** **Artikel 44** **Artikel 45** **Artikel 47.10** **Artiklarna 48–49** **Artiklarna 52 och 58**	**Mallar och riktlinjer enligt budgetförordningen samt interna riktlinjer**
Personuppgifter	**Artikel 22** **Avdelning II kapitel III avsnitt 6** **Överklagandenämnd** **Artikel 66** **Artikel 80.1 c och x** **Artikel 81.2** **Artikel 88.6 h**	**Förordning (EU) 2018/1725** **Förordning (EU) 2016/679**

	Artikel 95 **Artikel 96**	
Data som samlas in och analyseras i samband med samordnade riskbedömningar, utarbetandet av riskscenarier och identifieringen av viktiga IKT-tillgångar	**Artikel 98** **Artikel 99** **Artikel 102** **Artikel 103** **Artikel 105**	Utan att det påverkar tillämpningen av artikel 13 i förordning (EU) 2024/2847 och artikel 21 i direktiv (EU) 2022/2555.
Data om tredjeländer/entiteter i tredjeländer	**Artikel 100.1, 100.3 och 100.4** **Artikel 104** **Artikel 105** **Artikel 107** **Artikel 113**	Ej tillämpligt
Data om nationella myndigheter	**Artikel 112** **Artikel 114** **Artikel 116**	Ej tillämpligt
Data av betydelse för riskbedömningarna	**Artikel 5.2**	**Standarder för konfidentialitet och hantering av känslig information**
Ömsesidigt bistånd mellan medlemsstaterna	**Artikel 5.1 g i förordningen och artikel 1.12 i direktivet**	**/**

Överensstämmelse med EU:s datastrategi

Förklara hur kravet/kraven har anpassats till EU:s datastrategi

Kraven i förslaget till en andra cybersäkerhetsakt har anpassats utan någon särskild inverkan på EU-strategin för data så här långt.

Överensstämmelse med engångsprincipen

Förklara hur engångsprincipen har övervägts och hur möjligheten att återanvända befintliga data har undersökts

Ett av målen med förslaget är att maximera kommissionens förenklingsinsatser och minska den administrativa bördan för medlemsstaterna och berörda parter. Under de senaste åren har Enisa blivit ett informationsnav, med information från olika källor. I detta avseende är många av Enisas uppgifter förknippade med återanvändning och återvinning av information för olika analyser. Det handlar till exempel om att för vissa ändamål återanvända information som meddelats i enlighet med artiklarna 23 och 30 i direktiv (EU) 2022/2555 samt information som anmälts, delats eller analyserats i enlighet med artiklarna 14.1–14.3, 15, 17.1 och 17.3 i förordning (EU) 2024/2847. Bestämmelserna i ramen för leveranskedjan förutsätter att genomförandet stöds av de uppgifter som mottagits genom artikel 22 i direktiv (EU) 2022/2555, som visar på återanvändning av information och samordning.

Förklara hur nyskapade data är sökbara, tillgängliga, interoperabla och återanvändbara samt uppfyller högkvalitativa standarder

I lagstiftningsförslaget anges uttryckligen när data bör göras tillgängliga för allmänheten. I förslaget beaktas arten av bestämmelserna med strikta säkerhets- och konfidentialitetsaspekter, och alla data som skapas inom ramen för översynen av cybersäkerhetsakten kommer därför inte att vara avsedda för allmänheten. Anpassningen till den europeiska digitala identitetsplånboken har säkerställts för de nödvändiga bestämmelserna. Enisa har i uppgift att erbjuda tidiga varningar i ett maskinläsbart format.

Dataflöden

Beskrivning (övergripande nivå) av data som omfattas och eventuella tillhörande standarder/specifikationer

Typ av data	Förklara dataflödet	Hänvisningar
Enisa tillhandahåller rapporter och analyser, teknisk vägledning och bästa praxis	Detta är ett dataflöde som riktar sig till Enisas intressenter och stöder genomförandet av EU:s politik och lagstiftning. I dessa dataflöden samlar Enisa in information, oftast genom offentliga källor, samt analyserar den och delar resultaten med sina intressenter. Enisa utför även vissa uppgifter på begäran av kommissionen.	Artikel 5.1 a, b, c, e, f och h Artikel 5.2, 5.3 och 5.5 Artikel 6 Artikel 7 Artikel 8 Artikel 9 Artikel 10 Artikel 11.2 Artikel 11.4 Artikel 14
Dataflöden mellan kommissionen, Enisa, medlemsstaterna och andra berörda aktörer inom EU:s cybersäkerhetsekosystem, inom ramen för det operativa samarbetet	Denna typ av dataflöden upprättas för operativt samarbete och situationsmedvetenhet. Informationsutbytet sker i båda riktningarna, dvs. både in och ut. Utbytet avser operativa data.	Artikel 10.4 a–g Artikel 11.1 b–g Artikel 11.2 a och b Artikel 11.3 Artikel 15 Artikel 16.2 e
Dataflöden som upprättas för att stödja den europeiska kompetensramen för cybersäkerhet och ordningarna för europeiska individuella intyg om cybersäkerhetskompetens samt deras genomförande	Dessa dataflöden stöder utbyten in och ut för — underhåll och spridning av den europeiska kompetensramen för cybersäkerhet, med flöden mellan Enisa och medlemmarna i dess tillfälliga arbetsgrupp samt mellan Enisa och kommissionen, — utveckling och underhåll av ordningar för europeiska individuella intyg om cybersäkerhetskompetens, med flöden mellan Enisa och medlemmarna i dess tillfälliga arbetsgrupp samt mellan Enisa, kommissionen och medlemsstaterna,	Artiklarna 19–23 Artiklarna 36–43

	— genomförande av ordningar för europeiska individuella intyg om cybersäkerhetskompetens med dataflöden mellan de sökande och Enisa, — dataflöden mellan överklagandenämnden, Enisa, kommissionen och de sökande.	
Data av betydelse för målen och syftet med samt innehållet i europeiska ordningar för cybersäkerhetscertifiering	Denna typ av dataflöden är relevant för begäran om samt planering, utveckling, antagande och underhåll (inklusive en eventuell översyn) av europeiska ordningar för cybersäkerhetscertifiering. Den är särskilt relaterad till deltagande av och expertrådgivning från berörda parter, Enisa och medlemsstaternas myndigheter genom den europeiska gruppen för cybersäkerhetscertifiering i olika skeden av förfarandet. Ytterligare dataflöden har dessutom anknytning till tillhandahållandet av relevant information till allmänheten genom kommissionens och Enisas särskilda webbplatser. Slutligen planeras att allmänheten ska få tillgång till kompletterande cybersäkerhetsinformation från tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer för vilka en EU-försäkran om överensstämmelse eller ett europeiskt cybersäkerhetscertifikat har utfärdats på tillverkarens eller leverantörens eget initiativ.	Artikel 18 Artikel 19 Artiklarna 72, 73, 74, 75, 76, 77, 79, 81, 83 och 84
Data om styrningen av det europeiska ramverket för cybersäkerhetscertifiering	Dessa dataflöden stöder utbyten in och ut för — samordning och förvaltning av europeiska ordningar för cybersäkerhetscertifiering, — ackreditering och auktorisering av organ för bedömning av överensstämmelse samt efterföljande anmälningar av dessa genom den relevanta plattformen och de relaterade förfarandena, — förfaranden för rättslig prövning, såsom rätten att lämna in klagomål, rättsmedel eller överklagande- och ändringsförfaranden.	Artiklarna 85, 86, 88, 89, 90, 92, 93, 94, 95 och 96

Dataflöden i förhållande till byråns administrativa verksamhet	Flöden mellan Enisa, styrelsen, medlemsstaterna och kommissionen. Informationen gäller byråns administrativa verksamhet, och utbytet sker i båda riktningarna. I vissa fall skickas även information till Europaparlamentet (dataflödet i detta avseende presenteras nedan).	Artikel 25 Artikel 28.1 Artikel 30 Artikel 31.8 Artikel 32.3 och 32.5 Artikel 35.5 och 35.6 Artiklarna 36–43 Artikel 44 Artikel 45
Data som skickas till Europaparlamentet	Flöden till Europaparlamentet vad gäller Enisas verksamhet och utförande av uppgifter, budgetförvaltningen och den ekonomiska förvaltningen, samarbetet med tredjeländer och internationella organisationer, utfrågningen av kandidaten till posten som verkställande direktör samt frågor som rör europeisk cybersäkerhetscertifiering.	Artiklarna 28.1 f, 31.8, 32.3, 44.3, 49.6, 49.9, 70.5, 72.4 och 72.5 samt artikel 119.3 Utövande av delegeringen och artikel 120 Utvärdering och granskning
Data som skickas till rådet	Flöden till Europaparlamentet vad gäller Enisas verksamhet och utförande av uppgifter, budgetförvaltningen och den ekonomiska förvaltningen, samarbetet med tredjeländer och internationella organisationer, utfrågningen av kandidaten till posten som verkställande direktör samt förslag till certifieringsordning som håller på att utarbetas i enlighet med det europeiska ramverket för cybersäkerhetscertifiering.	Artikel 28.1 f, artikel 31.8, artikel 32.3 och 32.7, artikel 49.6 och 49.9, artikel 70.5, artikel 72.4 och 72.5, artikel 119.3 Utövande av delegeringen samt artikel 120 Utvärdering och granskning
Dataflöden i samband med inlämning av klagomål	Behandling av klagomål från fysiska eller juridiska personer i samband med europeiska cybersäkerhetscertifikat som utfärdats av nationella myndigheter för cybersäkerhetscertifiering eller europeiska	Artikel 55.3, artikel 88.7 f, Artikel 96

	cybersäkerhetscertifikat som utfärdats av organ för bedömning av överensstämmelse i enlighet med artikel 84.4 eller i samband med EU-försäkringar om överensstämmelse. Fysiska och juridiska personer ska ha rätt att lämna in klagomål till utfärdaren av ett europeiskt cybersäkerhetscertifikat och klagomål som rör ett europeiskt cybersäkerhetscertifikat som utfärdats av ett organ för bedömning av överensstämmelse.	
Dataflöden rörande attacker med utpressningsprogram	Rapportering av viss information vid attacker med utpressningsprogram.	Artikel 1.8 i direktivet

Typ av data	**Hänvisning/hänvisningar till kravet/kraven**	**Aktör som tillhandahåller data**	**Aktör som tar emot data**	**Utlösande faktor för datautbyte**	**Frekvens (i tillämpliga fall)**
Dataflöden mellan kommissionen och medlemsstaterna i samband med samordnade säkerhetsriskbedömningar på unionsnivå	Artikel 99 Säkerhetsriskbedömningar	Kommissionen och medlemsstaterna	Medlemsstaterna (samarbetsgruppen för nät- och informationssäkerhet)	Artikel 99 Säkerhetsriskbedömningar	Ej tillämpligt
Dataflöden mellan kommissionen och rådet i samband med fastställandet av	Artikel 100 Utseende av tredjeländer som utgör	Kommissionen	Rådet	Artikel 100 Kommissionens verifiering av hotet från	

Typ av data	Hänvisning/hänvisningar till kravet/kraven	Aktör som tillhandahåller data	Aktör som tar emot data	Utlösande faktor för datautbyte	Frekvens (i tillämpliga fall)
tredjeländer som cybersäkerhetsproblem	cybersäkerhetsproblem			tredjelandet	
Dataflöden mellan kommissionen och medlemsstaterna i samband med begränsningsåtgärder vid exceptionella omständigheter	Artikel 103.6 Begränsningsåtgärder i IKT-leveranskedjan	Kommissionen	Medlemsstaterna	Exceptionella omständigheter	Ej tillämpligt
Dataflöden mellan kommissionen och leverantörer samt mellan kommissionen och de behöriga myndigheterna vad gäller bedömningen av leverantörernas etablering samt ägar- och kontrollförhållanden	Artikel 104.4, 104.5 och 104.6 Identifiering av högriskleverantörer	Leverantörer Kommissionen Behöriga myndigheter	Behöriga myndigheter Leverantörer Kommissionen	Genomförandeakter som antagits i enlighet med artikel 103.1 och med avseende på det förbud som avses i artikel 111.1	Ej tillämpligt
Dataflöde mellan kommissionen och medlemsstaterna när det gäller tillsynsbefogenheter i samband med	Artikel 112.1 och 112.4 Behöriga myndigheter Artikel 114 Tillsyns- och efterlevnadskontrollåtgärde	Medlemsstaterna	Kommissionen	Artikel 112.1 och 112.4 Behöriga myndigheter Artikel 114 Tillsyns- och verkställighetsåtgärder	Ej tillämpligt

Typ av data	Hänvisning/hänvisningar till kravet/kraven	Aktör som tillhandahåller data	Aktör som tar emot data	Utlösande faktor för datautbyte	Frekvens (i tillämpliga fall)
genomförandet av ramen för säkerhet i den tillförlitliga IKT-leveranskedjan	r			(kommissionen ska i samarbete med medlemsstaterna utfärda en förteckning över entiteter som är anknutna till högriskleverantörer)	
Dataflöde mellan kommissionen och tredje parter för undantag	Artikel 105 Undantag för entiteter som är etablerade i eller kontrolleras av ett tredjeland som fastställts utgöra cybersäkerhetsproblem	Tredje parter (entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem, i den mening som avses i artikel 100, när de lämnar in en begäran om undantag) EU-kommissionen (när den utfärdar beslut)	EU-kommissionen (när den mottar en begäran om undantag) Tredje parter (entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som utgör cybersäkerhetsproblem, i den mening som avses i artikel 100, när de mottar kommissionens beslut)	Beslut enligt artikel 100 Utseende av tredjeländer som utgör cybersäkerhetsproblem	Ej tillämpligt
Dataflöde mellan medlemsstaterna och tredje parter i samband med förbud för	Artikel 111 Förbud för mobila, fasta och satellitbaserade elektroniska	Medlemsstaterna (behöriga myndigheter)	Tredje parter (leverantörer av mobila, fasta och satellitbaserade	Den behöriga myndighet som utsetts i enlighet med denna förordning ska utan dröjsmål informera den	Ej tillämpligt

Typ av data	Hänvisning/hänvisningar till kravet/kraven	Aktör som tillhandahåller data	Aktör som tar emot data	Utlösande faktor för datautbyte	Frekvens (i tillämpliga fall)
elektroniska kommunikationsnät	kommunikationsnät		elektroniska kommunikationsnät)	behöriga myndigheten i enlighet med förordning (EU) XXXX/XX [förslaget till rättsakt om digitala nät] om de åtgärder som införts för leverantörer av mobila, fasta och satellitbaserade elektroniska kommunikationsnät	
Dataflöde mellan kommissionen och medlemsstaterna inom ramen för nätverket för samarbete och stödtjänster	Artikel 113 Kommissionens samarbets- och stödtjänstnätverk	Kommissionen Medlemsstaterna (behöriga myndigheter)	Kommissionen Medlemsstaterna (behöriga myndigheter)	Utseende av tredjeländer som utgör cybersäkerhetsproblem	
Dataflöde mellan medlemsstaterna och tredje parter i samband med tillsyns- och verkställighetsåtgärder	Artikel 114 Tillsyns- och efterlevnadskontrollåtgärder	Tredje parter (entiteter av den typ som avses i bilagorna I och II till direktiv (EU) 2022/2555)	Medlemsstaterna (behöriga myndigheter)	Genomförande av de åtgärder som avses i avdelning IV	
Dataflöde mellan medlemsstaterna för ömsesidigt bistånd	Artikel 116 Ömsesidigt bistånd	Medlemsstaterna	Medlemsstaterna	Om en entitet enligt vad som avses i bilaga I eller II till direktiv (EU)	Ej tillämpligt

Typ av data	Hänvisning/hänvisningar till kravet/kraven	Aktör som tillhandahåller data	Aktör som tar emot data	Utlösande faktor för datautbyte	Frekvens (i tillämpliga fall)
				2022/2555 tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess viktiga IKT-tillgångar är belägna i en eller flera andra medlemsstater ska de behöriga myndigheterna i de berörda medlemsstaterna vid behov samarbeta med och bistå varandra	

4.3 Digitala lösningar

Övergripande beskrivning av digitala lösningar

Förklara, för varje digital lösning, hur den digitala lösningen uppfyller tillämplig digital politik och lagstiftning.

Digital lösning	Hänvisning/hänvisningar till kravet/kraven	Huvudsakliga föreskrivna funktioner	Ansvarigt organ	Hur tillgodoses tillgängligheten?	Hur övervägs möjligheten till återanvändning?	Användning av AI-teknik (i tillämpliga fall)
Enisa ska, i egenskap av						

sekretariatet för CSIRT-nätverket och EU-CyCLONe, inom CSIRT-nätverket och EU-CyCLONe införa **säkra kommunikationsverktyg** som tillhandahålls av juridiska personer som inte är etablerade i eller kontrolleras av tredjeländer eller av medborgare i tredjeländer.	Artikel 10.2, 10.3 och 10.5	Icke-offentlig information	Enisa	Icke-offentlig information	Icke-offentlig information	Icke-offentlig information
I samarbete med EU-CyCLONe, CSIRT-nätverket, kommissionen, Europol och CERT-EU samt relevanta unionsentiteter utveckla **databaser med verifierad och tillförlitlig underrättelseinformation om cyberhot**, inbegripet trender i fråga om incidenter, taktik, metoder och förfaranden.	Artikel 11.1 a	Verifierade, tillförlitliga underrättelser om cyberhot, inbegripet trender i fråga om incidenter, taktik, metoder och förfaranden	Enisa EU-CyCLONe, CSIRT-nätverket, kommissionen, Europol och CERT-EU samt relevanta unionsentiteter	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Enisa ska **upprätthålla en databas över lärdomar**.	Artikel 14.2	Enisa ska upprätthålla en databas över lärdomar från övningar och ge medlemsstaterna och, när så är relevant, unionsentiteterna rekommendationer om hur dessa lärdomar ska omsättas i handling på ett ändamålsenligt och effektivt sätt.	Enisa	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt

Enisa ska inrätta, tillhandahålla, driva, underhålla och uppdatera, såsom nödvändigt, operativa tekniska verktyg, såsom **plattformar** för cybersäkerhet på unionsnivå, i synnerhet den gemensamma rapporteringsplattform som inrättats i enlighet med artikel 16.1 i förordning (EU) 2024/2847 [och den gemensamma kontaktpunkt för incidentrapportering som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555], eller testverktyg till stöd för genomförandet av förfaranden för bedömning av överensstämmelse i enlighet med relevant unionslagstiftning.	Artikel 15	Den gemensamma rapporteringsplattformen Artikel 16.1 i förordning (EU) 2024/2847 [den gemensamma kontaktpunkten artikel 23a i direktiv (EU) 2022/2555]	Enisa	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Upprätthålla den europeiska sårbarhetsdatabasen, som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555, och **tillhandahålla sårbarhetshanteringstjänster**.	Artikel 16.2	Artikel 12.2 i direktiv (EU) 2022/2555 Upprätthålla databasen och tillhandahålla sårbarhetshanteringstjänster	Enisa	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt
Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med	Artiklarna 19–23	Underhålla och regelbundet uppdatera en särskild	Enisa	Ej tillämpligt	Ej tillämpligt	Ej tillämpligt

offentlig information.		webbplats med offentlig information om den europeiska kompetensramen för cybersäkerhet, inbegripet ramverket och tidsplanen för uppdatering. Ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, deras framsteg och tidsplaner för utvecklingen av dem. De avgifter som är förknippade med varje ordning för europeiska individuella intyg om cybersäkerhetskompetens. Den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens. En förteckning över auktoriserade tillhandahållare av intyg.				
Kommissionen ska upprätthålla och regelbundet uppdatera en särskild offentlig webbplats.	Artikel 72	Följande information: a) Europeiska ordningar för cybersäkerhetscertifiering avseende vilka utveckling begärts. b) Strategiska prioriteringar för harmonisering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller	EU-kommissionen	Efterlevnad av riktlinjerna	Efterlevnad av riktlinjerna	Ej tillämpligt

		säkerhetskrav i unionslagstiftningen, inbegripet potentiella områden för vilka en europeisk ordning för cybersäkerhetscertifiering kan komma att begäras.				
Enisa ska underhålla en särskild certifieringswebbplats	Artikel 79	Tillhandahålla information om a) Europeiska ordningar för cybersäkerhetscertifiering. b) Avgifterna i samband med underhållet av varje europeisk ordning för cybersäkerhetscertifiering. c) Enisas relevanta tekniska specifikationer. d) Europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, inbegripet information om sådana certifikat och försäkringar som inte längre är giltiga eller som tillfälligt har upphävts, återkallats eller löpt ut. e) Relevant kompletterande cybersäkerhetsinformation som lämnats i enlighet med artikel 84.2.	Enisa	Efterlevnad av riktlinjerna	Efterlevnad av riktlinjerna	Ej tillämpligt

		f) Sammanfattningar av inbördes granskningar enligt artikel 89.7. g) Tekniska specifikationer som det hänvisas till i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.				
Register (över undantag för entiteter som är etablerade i eller kontrolleras av entiteter från ett tredjeland som fastställts utgöra cybersäkerhetsproblem)	Artikel 107 Register	Kommissionen ska föra ett offentligt register över sina beslut enligt artikel 105.4. Registret ska innehålla namnen på de entiteter som omfattas av besluten. Kommissionen ska regelbundet uppdatera registret.	Kommissionen	”Kommissionen ska föra ett offentligt register”	Ej tillämpligt	Ej tillämpligt
Plattform (för samarbete och informationsutbyte mellan kommissionen och behöriga myndigheter)	Artikel 113	Kommissionen ska inrätta ett nätverk för samarbete mellan de behöriga myndigheterna i medlemsstaterna och	Kommissionen	Ej offentlig, endast för de behöriga myndigheterna	Ej tillämpligt	Ej tillämpligt

		kommissionen, vilket ska fungera som en plattform för samarbete och informationsutbyte. Kommissionen ska ge administrativt stöd till nätverket.				
Enisa ska skapa och upprätthålla ett register över väsentliga och viktiga entiteter, liksom entiteter som tillhandahåller domännamnsregistreringstjänster.	Artikel 1.11 i direktivet	Register över väsentliga och viktiga entiteter, liksom entiteter som tillhandahåller domännamnsregistreringstjänster.	Enisa	Ej tillämpligt	På grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 2 (artikel 27 i NIS 2-direktivet)	Ej tillämpligt

Digitala lösningar som ingår i tabellen ovan

Digital och/eller sektoriell politik (i tillämpliga fall)	**Beskrivning av överensstämmelse**
Förordningen om artificiell intelligens	Ej tillämpligt

EU:s cybersäkerhetsram	Ej tillämpligt
eIDA	Ej tillämpligt
Den gemensamma digitala ingången och IMI	Ej tillämpligt
Övriga	Ej tillämpligt

Övergripande beskrivning av den digitala offentliga tjänst/de digitala offentliga tjänster som påverkas av kravet

Digital offentlig tjänst eller kategori av digitala offentliga tjänster	**Beskrivning**	**Hänvisning/hänvisningar till kravet/kraven**	**Lösning/lösningar för ett interoperabelt Europa (EJ TILLÄMPLIGT)**	**Andra interoperabilitetslösningar**
Enisa som nätverkssekretariat och införande av säkra kommunikationsverktyg	Enisa ska tillhandahålla CSIRT-nätverkets sekretariat i enlighet med artikel 15.2 i direktiv (EU) 2022/2555. Enisa ska tillhandahålla EU-CyCLONes sekretariat i enlighet med artikel 16.2 i direktiv (EU) 2022/2555 [och den gemensamma kontaktpunkt för incidentrapportering som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555] samt testverktyg för att stödja genomförandet av förfaranden för bedömning av överensstämmelse i enlighet med relevant unionslagstiftning. Enisa ska inom CSIRT-nätverket och EU-CyCLONe införa säkra	Artikel 11	//	Ej tillämpligt

	kommunikationsverktyg som tillhandahålls av juridiska personer som inte är etablerade i eller kontrolleras av tredjeländer eller av medborgare i tredjeländer.			
Tidiga varningar	Utfärda tidiga varningar.	Artikel 11 Artikel 12		
Stöd med avseende på specifika potentiella eller pågående incidenter eller cyberhot	På begäran av en eller flera medlemsstater tillhandahålla råd och bedömningar med avseende på specifika potentiella eller pågående incidenter eller cyberhot, däribland genom att tillhandahålla expertis och underlätta den tekniska hanteringen av sådana incidenter, och genom att stödja frivilligt utbyte av relevant information och tekniska lösningar mellan medlemsstaterna.	Artikel 10		
Stöd till den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå	Bidra till att stödja den samordnade hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå, i synnerhet genom att bistå EU-CyCLONe i arbetet med att utarbeta rapporter för den politiska nivån och genom att främja ett snabbt informationsutbyte mellan CSIRT-nätverket och EU-CyCLONe.	Artikel 10		
Databaser med verifierad och tillförlitlig underrättelseinformation om cyberhot	I samarbete med EU-CyCLONe, CSIRT-nätverket, kommissionen, Europol och CERT-EU och relevanta unionsentiteter utveckla databaser med verifierad och tillförlitlig underrättelseinformation om cyberhot, inbegripet trender i	Artikel 11		

	fråga om incidenter, taktik, teknik och förfaranden.			
Databas över lärdomar	Enisa ska upprätthålla en databas över lärdomar från dessa övningar och ge medlemsstaterna och, när så är relevant, unionsentiteterna rekommendationer om hur dessa lärdomar ska omsättas i handling på ett ändamålsenligt och effektivt sätt.	Artikel 14		
Enisa ska inrätta, tillhandahålla, driva, underhålla och uppdatera, såsom nödvändigt, operativa tekniska verktyg, såsom plattformar	Enisa ska inrätta, tillhandahålla, driva, underhålla och uppdatera, såsom nödvändigt, operativa tekniska verktyg, såsom plattformar för cybersäkerhet på unionsnivå, i synnerhet den gemensamma rapporteringsplattform som inrättats i enlighet med artikel 16.1 i förordning (EU) 2024/2847 [och den gemensamma kontaktpunkt för incidentrapportering som inrättats i enlighet med artikel 23a i direktiv (EU) 2022/2555], och testverktyg till stöd för genomförandet av förfaranden för bedömning av överensstämmelse i enlighet med relevant unionslagstiftning.	Artikel 15		
Underhålla den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555	Underhålla den europeiska sårbarhetsdatabas som inrättats i enlighet med artikel 12.2 i direktiv (EU) 2022/2555. Förse intressenterna med sårbarhetshanteringstjänster, på grundval av den europeiska sårbarhetsdatabasen och med utnyttjande av den relevanta information som Enisa har tillgång till.	Artikel 16		

	Ingå strukturerat samarbete med organisationer som tillhandahåller program, register eller databaser som liknar den europeiska sårbarhetsdatabasen. Aktivt stödja CSIRT-enheter som utsetts till samordnare i enlighet med artikel 12.1 i direktiv (EU) 2022/2555 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat. Utveckla och underhålla metoder och styrningsmekanismer för identifiering av sårbarheter och samordnad information om sådana, i samarbete med nationella behöriga myndigheter, CSIRT-enheter, branschen och forskarsamhället.			
Utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordningar*)	Utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (*förslag till certifieringsordningar*) för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus och relaterade tekniska specifikationer i enlighet med artikel 74. Underhålla antagna europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 75, bland annat med sikte på en eventuell översyn av de antagna europeiska ordningarna för cybersäkerhetscertifiering i enlighet	Artikel 17		

	med artikel 76.			
Enisa ska utveckla och underhålla ordningar för europeiska individuella intyg om cybersäkerhetskompetens	Enisa ska utveckla och underhålla ordningar för europeiska individuella intyg om cybersäkerhetskompetens. Enisa ska utfärda ett motiverat beslut antingen om att bevilja en sökande auktorisation att utfärda europeiska individuella intyg för genomförande och underhåll av ordningar och av auktorisationen, om att inte bevilja en sådan auktorisation eller om att avsluta handläggningen av ansökan på grund av att sökanden inte har lämnat in tillräcklig information eller inte har agerat efter att ha mottagit en framställning om ytterligare information.	Artiklarna 20–22		
Enisa ska underhålla och regelbundet uppdatera en särskild webbplats.	Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande: a) Den europeiska kompetensramen för cybersäkerhet och dess tidsplan för uppdatering. b) Ordningarna för europeiska individuella intyg om cybersäkerhetskompetens, deras framsteg och tidsplaner för utvecklingen av dem. c) De avgifter som är förknippade med varje ordning för europeiska individuella intyg om cybersäkerhetskompetens som	Artikel 23		

	antagits i enlighet med artikel 47 i denna förordning. d) Den indikativa kostnaden för ett europeiskt individuellt intyg om cybersäkerhetskompetens i enlighet med artikel 20.4. e) En förteckning över auktoriserade tillhandahållare av intyg.			
Kommissionen ska upprätthålla och regelbundet uppdatera en särskild offentlig webbplats.	Kommissionen ska upprätthålla och regelbundet uppdatera en särskild webbplats med information om följande: a) Europeiska ordningar för cybersäkerhetscertifiering avseende vilka utveckling begärts. b) Strategiska prioriteringar för harmonisering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller säkerhetskrav i unionslagstiftningen, inbegripet potentiella områden för vilka en europeisk ordning för cybersäkerhetscertifiering kan komma att begäras.	Artikel 72		
Enisa ska underhålla en särskild certifieringswebbplats	Enisa ska underhålla och regelbundet uppdatera en särskild webbplats med offentlig information om följande: a) Europeiska ordningar för cybersäkerhetscertifiering. b) Avgifterna i samband med underhållet av varje europeisk ordning för cybersäkerhetscertifiering. c) Enisas relevanta tekniska specifikationer. d) Europeiska	Artikel 79		

	cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse, inbegripet information om sådana certifikat och försäkringar som inte längre är giltiga eller som tillfälligt har upphävts, återkallats eller löpt ut. e) Relevant kompletterande cybersäkerhetsinformation som lämnats i enlighet med artikel 84.2. f) Sammanfattningar av inbördes granskningar enligt artikel 89.7. g) Tekniska specifikationer som det hänvisas till i en europeisk ordning för cybersäkerhetscertifiering på det sätt som avses i artikel 74.10.			
Undersökningar	Kommissionen ska undersöka alla fall i vilka den tvivlar på, eller görs uppmärksam på tvivel på, att ett organ för bedömning av överensstämmelse har kompetens att uppfylla, eller att ett organ för bedömning av överensstämmelse fortsatt uppfyller, de krav och skyldigheter som det omfattas av. Kommissionen ska säkerställa att all känslig information som erhållits i samband med undersökningarna behandlas konfidentiellt.	Artikel 94		
Enisa ska skapa och upprätthålla ett register över väsentliga och viktiga entiteter, liksom entiteter som tillhandahåller domännamnsregistreringstjänster.	Register över väsentliga och viktiga entiteter, liksom entiteter som tillhandahåller domännamnsregistreringstjänster. Enisa ska på begäran ge de behöriga myndigheterna tillgång till information om leverantörer av DNS-tjänster, registreringsenheter	Artikel 1.11 i direktivet		

	för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster samt leverantörer av marknadsplatser online, av onlinesökmotorer och av plattformar för sociala nätverkstjänster som lagras i det registret, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.			

4.4 Interoperabilitetsbedömning

Kravets/kravens inverkan på gränsöverskridande interoperabilitet vad gäller digitala offentliga tjänster

Databaser/plattformar/tidiga varningar/sekretariat/operativt samarbete/databas för samordnad information om sårbarheter

Bedömning	**Åtgärder**	**Potentiella återstående hinder**
Bedöm överensstämmelsen med befintlig digital och sektoriell politik **Ange tillämplig digital och sektoriell politik som identifierats**	*Cybersäkerhet*	*Inga kända hinder*
Bedöm de organisatoriska åtgärderna för att smidigt tillhandahålla digitala offentliga tjänster över gränserna **Ange planerade förvaltningsåtgärder**	*Enisas styrelse* *CSIRT-nätverket* *EU-CyCLONe* *Samarbetsgruppen för nät- och informationssäkerhet*	*Ej tillämpligt*

	Alla dessa är forum där frågor kan tas upp.	
Bedöm de åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**	*Ej tillämpligt*	*Ej tillämpligt*
Bedöm användningen av gemensamt överenskomna öppna tekniska specifikationer och standarder **Ange dessa åtgärder**	*Ej tillämpligt*	*Ej tillämpligt*

Ordningar för europeiska individuella intyg om cybersäkerhetskompetens

Bedömning	**Åtgärder**	**Potentiella återstående hinder**
Bedöm överensstämmelsen med befintlig digital och sektoriell politik **Ange tillämplig digital och sektoriell politik som identifierats**	*Förslaget bygger på COM(2023) 207 final (EU-akademin för cyberkompetens) där det står att ”Enisa [kommer] att utveckla ett pilotprojekt för att undersöka möjligheterna att inrätta ett europeiskt certifieringssystem för cybersäkerhetskompetens”.* *Förslaget utgår från förordning (EU) 2024/1183 (den europeiska digitala identitetsplånboken) genom att fastställa att Enisa och auktoriserade tillhandahållare av intyg ska säkerställa att de elektroniska europeiska individuella intygen om cybersäkerhetskompetens utfärdas till de europeiska digitala identitetsplånböckerna.* *Cybersäkerhet* *Allmänna dataskyddsförordningen (tillhandahållares bevarande av uppgifter)*	*Inga kända hinder*
Bedöm de organisatoriska åtgärderna för att smidigt tillhandahålla digitala offentliga tjänster över gränserna	*Samråd med berörda parter vid utarbetandet av en ordning för europeiska individuella intyg om cybersäkerhetskompetens*	*Det ska fortsätta att vara frivilligt för offentliga och privata entiteter att använda och erkänna ordningar för*

Ange planerade förvaltningsåtgärder	*Separation av verksamheten inom Enisa för att säkerställa ett oberoende utförande av densamma* *Överklagandenämnd*	*europeiska individuella intyg om cybersäkerhetskompetens.*
Bedöm de åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**	*Utveckla ordningar som bland annat omfattar bestämmelser om intygens innehåll och format. Auktoriserade tillhandahållare ska på begäran av en enskild person säkerställa att elektroniska europeiska individuella intyg om cybersäkerhetskompetens utfärdas som elektroniska attributsintyg i ett format som kan lagras i de europeiska digitala identitetsplånböckerna. Enisa ska tillhandahålla vägledning till och genomföra obligatorisk utbildning av bedömare om de krav och bedömningsmetoder som ingår i ordningen för europeiska individuella intyg om cybersäkerhetskompetens.* *Tillhandahålla offentlig information på en webbplats.* *Genomförandeakter om avgifter.*	*Ordningarna bör vara så detaljerade som möjligt för att säkerställa en gemensam förståelse och underlätta genomförandet, och Enisa kommer att tillhandahålla vägledning till och genomföra obligatorisk utbildning av bedömare för att säkerställa ett konsekvent genomförande av ordningarna; trots detta kan oförutsedda aspekter uppkomma om de auktoriserade tillhandahållarna av intyg behöver interagera med Enisa, andra tillhandahållare eller bedömarna.*
Bedöm användningen av gemensamt överenskomna öppna tekniska specifikationer och standarder **Ange dessa åtgärder**	*Ordningar för europeiska individuella intyg om cybersäkerhetskompetens utvecklas med stöd av berörda parter*	*Ej tillämpligt*

Utarbeta förslag till europeiska ordningar för cybersäkerhetscertifiering (förslag till certifieringsordning)/tilldela nummer till organ för bedömning av överensstämmelse

Bedömning	**Åtgärder**	**Potentiella återstående hinder**

Bedöm överensstämmelsen med befintlig digital och sektoriell politik **Ange tillämplig digital och sektoriell politik som identifierats**	*Förslaget syftar till att anpassa styrningen till den nya lagstiftningsramen, särskilt när det gäller förordning (EG) nr 765/2008[26].* *Syftet är också att underlätta efterlevnaden av relevant sektorslagstiftning för cybersäkerhet genom att utveckla särskilda europeiska ordningar för cybersäkerhetscertifiering.*	*Inga kända hinder*
Bedöm de organisatoriska åtgärderna för att smidigt tillhandahålla digitala offentliga tjänster över gränserna **Ange planerade förvaltningsåtgärder**	*Den europeiska gruppen för cybersäkerhetscertifiering* *Enisa* *Tillfälliga arbetsgrupper* *Europeiska församlingen för cybersäkerhetscertifiering* *Samråd med berörda parter på begäran samt utveckling och antagande av europeiska ordningar för cybersäkerhetscertifiering* *Kommittéförfaranden för planerade genomförandeakter med anknytning till europeiska ordningar för cybersäkerhetscertifiering*	*Användningen av europeisk cybersäkerhetscertifiering ska vara frivillig om inte annat anges i EU-lagstiftningen.*
Bedöm de åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**	*Genomförandeakter i enlighet med avsnitt 4.5.*	*Användningen av europeisk cybersäkerhetscertifiering ska vara frivillig om inte annat anges i EU-lagstiftningen.*
Bedöm användningen av gemensamt överenskomna öppna tekniska specifikationer och standarder **Ange dessa åtgärder**	*Genomförandeakter i enlighet med avsnitt 4.5.* *De angivna kraven för den europeiska ordningen för cybersäkerhetscertifiering ska vara förenliga med kraven i unionslagstiftningen.* *Europeiska ordningar för cybersäkerhetscertifiering ska utnyttja och hänvisa till de internationella, europeiska eller nationella standarder som tillämpas vid*	*Ej tillämpligt*

	utvärderingen eller, om sådana standarder inte finns tillgängliga eller är olämpliga, tekniska specifikationer som utarbetats av Enisa.	

Allmänt tillgängliga webbplatser

Bedömning	**Åtgärder**	**Potentiella återstående hinder**
Bedöm överensstämmelsen med befintlig digital och sektoriell politik **Ange tillämplig digital och sektoriell politik som identifierats**	*Det europeiska tillgänglighetsdirektivet och direktivet om webbtillgänglighet* *Cybersäkerhet*	*Inga kända hinder*
Bedöm de organisatoriska åtgärderna för att smidigt tillhandahålla digitala offentliga tjänster över gränserna **Ange planerade förvaltningsåtgärder**	*Ej tillämpligt*	*Ej tillämpligt*
Bedöm de åtgärder som vidtagits för att säkerställa en samstämmig förståelse av data **Ange dessa åtgärder**		*Ej tillämpligt*
Bedöm användningen av gemensamt överenskomna öppna tekniska specifikationer och standarder **Ange dessa åtgärder**		*Ej tillämpligt*

4.5 Åtgärder till stöd för digitalt genomförande

Övergripande beskrivning av åtgärder till stöd för digitalt genomförande

Beskrivning av åtgärden	**Hänvisning/hänvisningar till kravet/kraven**	**Kommissionens roll** (i tillämpliga fall)	**Aktörer som ska involveras** (i tillämpliga fall)	**Förväntad tidsplan** (i tillämpliga fall)
Kommissionen ges befogenhet att, på	Artikel 75.9	Kommissionen ges		Ej tillämpligt

grundval av det godtagna förslaget till certifieringsordning som utarbetats av Enisa, anta genomförandeakter för en europeisk ordning för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster eller entiteters cybersäkerhetsstatus som uppfyller kraven i artiklarna 80 och 81. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.		befogenhet att anta genomförandeakter		
Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 119 för att ändra punkt 1 i den här artikeln genom att lägga till eller ändra säkerhetsmål för att säkerställa att de återspeglar den senaste tekniska utvecklingen och nya relaterade hot samt antagandet av ny unionslagstiftning som fastställer presumtion om överensstämmelse genom europeisk cybersäkerhetscertifiering med relevanta cybersäkerhetskrav i den lagstiftningen.	Artikel 80.2	Kommissionen ges befogenhet att anta delegerade akter		Ej tillämpligt
Kommissionen ges befogenhet att anta genomförandeakter för att fastställa gemensamma principer och standardbestämmelser för de komponenter som anges i punkterna 1,	Artikel 81.5	Kommissionen ges befogenhet att anta genomförandeakter	Enisa Den europeiska gruppen för cybersäkerhetscertifiering	Ej tillämpligt

2 och 3 i alla europeiska ordningar för cybersäkerhetscertifiering. En europeisk ordning för cybersäkerhetscertifiering får innehålla hänvisningar till dessa principer och standardbestämmelser när det är lämpligt och sådana finns tillgängliga. De genomförandeakter som avses i första stycket ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2. När kommissionen utarbetar eller ser över de gemensamma principerna och standardbestämmelserna för komponenterna i europeiska ordningar för cybersäkerhetscertifiering ska den samråda med Enisa och, när så är lämpligt, beakta synpunkter från den europeiska gruppen för cybersäkerhetscertifiering, berörda intressenter och andra relevanta organ.				
Kommissionen ges befogenhet att anta genomförandeakter som specificerar förfaranden för de modeller med förhandsgodkännande eller allmän delegering som avses i punkt 4 i denna artikel. Vid utarbetandet av dessa genomförandeakter ska kommissionen samråda med den europeiska gruppen för cybersäkerhetscertifiering. Dessa genomförandeakter ska antas i enlighet	Artikel 85.5	Kommissionen ges befogenhet att anta genomförandeakter	Den europeiska gruppen för cybersäkerhetscertifiering	Ej tillämpligt

med det granskningsförfarande som avses i artikel 118.2.				
Tredjelandscertifikat för IKT-produkter, IKT-tjänster, IKT-processer, utlokaliserade säkerhetstjänster och entiteters cybersäkerhetsstatus får, genom en genomförandeakt eller genom ingående av ett avtal mellan unionen och tredjelandet i fråga eller en internationell organisation, erkännas som likvärdiga med europeiska cybersäkerhetscertifikat om kraven i tredjelandets eller den internationella organisationens berörda ordning anses vara likvärdiga med kraven i europeiska ordningar för cybersäkerhetscertifiering. Kommissionen ges befogenhet att anta sådana genomförandeakter. Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.	Artikel 87.1	Kommissionen ges befogenhet att anta genomförandeakter		Ej tillämpligt
Kommissionen ges befogenhet att anta genomförandeakter om inrättande av en plan för den inbördes granskningen som ska omfatta en period på minst fem år, med kriterier för sammansättningen av den grupp som ska utföra den inbördes granskningen, den metod som ska användas, tidsplanen, frekvensen och andra	Artikel 89.6	Kommissionen ges befogenhet att anta genomförandeakter		Ej tillämpligt

uppgifter som rör den inbördes granskningen. Vid utarbetandet av genomförandeakterna ska kommissionen samråda med den europeiska gruppen för cybersäkerhetscertifiering och Enisa. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.				
Kommissionen ges befogenhet att anta genomförandeakter för att fastställa förfarandena, inbegripet för gränsöverskridande samarbete, för auktorisering av organ för bedömning av överensstämmelse. Vid utarbetandet av dessa genomförandeakter ska kommissionen samråda med Enisa och den europeiska gruppen för cybersäkerhetscertifiering. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.	Artikel 92.8	Kommissionen ges befogenhet att anta genomförandeakter	Enisa Den europeiska gruppen för cybersäkerhetscertifiering	Ej tillämpligt
Kommissionen ges befogenhet att anta genomförandeakter för att fastställa omständigheter, format och förfaranden för de anmälningar som avses i punkt 1 i denna artikel, inbegripet förfarandet för andra medlemsstaters invändningar under anmälningsprocessen, den unika identifieringen av organ för bedömning	Artikel 93.3	Kommissionen ges befogenhet att anta genomförandeakter		Ej tillämpligt

av överensstämmelse samt omständigheterna för begränsning, tillfälligt upphävande eller återkallande av anmälan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 118.2.				
Kommissionen får anta genomförandeakter i enlighet med artikel 100 för att fastställa att ett tredjeland utgör cybersäkerhetsproblem för IKT-leveranskedjor.	Artikel 100.2 Utseende av tredjeländer som utgör cybersäkerhetsproblem	Anta genomförandeakter		Ej tillämpligt Ingen tidsplan, men genomförandeakterna bör ses över regelbundet
Kommissionen får anta genomförandeakter för att föreskriva en eller flera av de begränsningsåtgärder som avses i artikel 103.2.	Artikel 103.2 Begränsningsåtgärder i IKT-leveranskedjan	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt Ingen tidsplan, men situationen ska ses över var 36:e månad (i enlighet med det granskningsförfarande som avses i artikel 118.2)
Kommissionen får anta genomförandeakter i enlighet med artikel 102 för att identifiera viktiga IKT-tillgångar som används av de typer av entiteter som avses i bilagorna I och II till direktiv (EU) 2022/2555 för att tillverka produkter eller tillhandahålla tjänster.	Artikel 102.1 Identifiering av viktiga IKT-tillgångar	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt

Kommissionen får anta genomförandeakter om förbud av användning och installation av eller integrering i alla former av IKT-komponenter eller komponenter som innehåller IKT-komponenter från högriskleverantörer som fastställts i enlighet med artikel 100.2 i viktiga IKT-tillgångar som identifierats i enlighet med artikel 102.	Artikel 103.1 Begränsningsåtgärder i IKT-leveranskedjan	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt
Kommissionen får anta genomförandeakter för att fastställa att det är förbjudet för entiteter av de typer som avses i bilagorna I och II till direktiv (EU) 2022/2555 att använda, installera eller integrera IKT-komponenter eller komponenter som innehåller IKT-komponenter från en viss entitet.	Artikel 103.7	Anta genomförandeakter	Samråd med medlemsstaterna och de berörda entiteterna	Ej tillämpligt
Kommissionen ska genom genomförandeakter upprätta förteckningar över högriskleverantörer av relevans för de förbud som fastställs i de genomförandeakter som antagits i enlighet med artikel 103.1 eller det förbud som avses i artikel 1110.1.	Artikel 104.1	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt
Kommissionen får anta genomförandeakter för att ytterligare specificera de villkor som avses i artikel 105.2 b och för att fastställa	Artikel 105 Undantag för entiteter som är etablerade i eller kontrolleras av	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt

närmare bestämmelser om de förfaranden som avses i artikel 105.	entiteter från ett tredjeland som utgör cybersäkerhetsproblem			
Kommissionen får anta genomförandeakter med närmare regler om avgifterna, där den specificerar avgiftsbeloppen och hur de ska betalas.	Artikel 109 Avgifter	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt
Kommissionen ska anta genomförandeakter för att specificera tidsperioderna för utfasning av IKT-komponenter eller komponenter som innehåller IKT-komponenter vilka tillhandahålls av högriskleverantörer med avseende på fasta och satellitbaserade elektroniska kommunikationsnät.	Artikel 110.4 Viktiga IKT-tillgångar för mobila, fasta och satellitbaserade elektroniska kommunikationsnät	Anta genomförandeakter	Ej tillämpligt	Ej tillämpligt
Kommissionen får anta delegerade akter i enlighet med artikel 119 för att ändra bilaga II i syfte att anpassa den till den tekniska utvecklingen genom att beakta de faktorer som avses i artikel 103.3.	Artikel 110.5	Anta delegerade akter	Ej tillämpligt	Ej tillämpligt
7. Artikel 21.5 ska ändras på följande sätt: a) Andra stycket ska ersättas med följande: ”Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på	Artikel 1.7 i direktivet Maximal harmonisering	Kommissionen får anta genomförandeakter		Ej tillämpligt

andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt. Kommissionen ska regelbundet bedöma huruvida de genomförandeakter som avses i detta stycke ska antas för specifika sektorer eller typer av entiteter för att förbättra den inre marknadens funktion. På grundval av resultatet av dessa bedömningar får kommissionen föreslå sådana genomförandeakter för de identifierade sektorerna eller typerna av entiteter. När kommissionen utarbetar sådana bedömningar ska den särskilt fokusera på sektorers eller entitetstypers gränsöverskridande karaktär och genomföra en öppen, transparent och inkluderande samrådsprocess med de berörda parterna och medlemsstaterna.” b) Följande stycke ska läggas till efter fjärde stycket: ”Om kommissionen antar sådana genomförandeakter som avses i första och andra stycket i denna punkt, får medlemsstaterna inte införa några ytterligare tekniska krav eller metodologiska krav för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 för de entiteter som omfattas av de genomförandeakterna.”				

EUROPEISKA
KOMMISSIONEN

Strasbourg den 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslag till cybersäkerhetsakt 2]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Text av betydelse för EES)

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Detta förslag ingår i ett åtgärdspaket som syftar till att anpassa unionens cybersäkerhetsram till berörda parters behov mot bakgrund av en alltmer sofistikerad cyberhotbild och komplex geopolitisk verklighet. Väsentliga och viktiga entiteter från kritiska sektorer utsätts i allt högre grad för cyberattacker[1], medan statliga fientliga aktörer utnyttjar ny teknik såsom artificiell intelligens (AI) för att ytterligare skala upp och optimera sina attacker. I detta sammanhang erkänns den kritiska infrastrukturens motståndskraft mot cyberhot som en strategisk pelare för våra demokratier och unionens ekonomiska säkerhet. Både EU:s strategi för en beredskapsunion[2] och EU:s strategi för inre säkerhet (ProtectEU)[3] har satt cybersäkerhet i centrum för unionens agenda för resiliens. På samma sätt anges i meddelandet om att stärka EU:s ekonomiska säkerhet[4] att förhindra tillgång till känslig information och känsliga uppgifter som skulle kunna undergräva unionens ekonomiska säkerhet och förebygga och mildra störningar av unionens kritiska infrastruktur som påverkar unionens ekonomi är prioriterade mål, där effektiva cybersäkerhetsåtgärder spelar en avgörande roll. I Draghi-rapporten betonades dessutom behovet av att öka säkerheten och minska beroendet som ett viktigt åtgärdsområde i unionen[5]. I kommissionens meddelande om ett enklare och snabbare Europa[6] tillkännagav kommissionen sitt stöd för ett ambitiöst program för att främja framåtblickande och innovativ politik som stärker unionens konkurrenskraft och minskar regelbördan för allmänheten, företag och förvaltningar samtidigt som höga standarder upprätthålls i fråga om att främja EU:s värden.

Mot den bakgrunden syftar detta förslag till direktiv om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslaget till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), den europeiska ramen för cybersäkerhetscertifiering och säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881 (cybersäkerhetsakten 2)] till att gripa sig an problemet med komplexiteten och mångfalden i den cybersäkerhetsrelaterade politik som påverkar unionens cybersäkerhetsstatus, särskilt genom att införa förtydliganden och underlätta efterlevnaden för de reglerade entiteterna.

Syftet med detta direktiv bör betraktas som en del av de övergripande målen för paketet för översyn av cybersäkerhetsakten som inbegriper förslaget till Europaparlamentets och rådets förordning om Europeiska unionens cybersäkerhetsbyrå (Enisa), den europeiska ramen för cybersäkerhetscertifiering och säkerhet i IKT-leveranskedjan och om upphävande av förordning (EU) 2019/881. Förslaget till förordning syftar till att åtgärda följande: i) Den bristande överensstämmelsen mellan unionens policyram för cybersäkerhet och intressenternas behov i en alltmer fientlig hotbild. ii) Det avstannade genomförandet av det europeiska ramverket för cybersäkerhetscertifiering (ECCF). iii) Komplexiteten och

---

1 ENISA, ENISA Threat Landscape 2025.
2 JOIN/2025/130 final.
3 COM/2025/148 final.
4 JOIN(2025) 977 final.
5 Europeiska kommissionen, *Rapport om EU:s framtida konkurrenskraft*, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 final.

mångfalden hos den cybersäkerhetsrelaterade politiken som påverkar unionens cybersäkerhetsstatus. iv) öka säkerhetsriskerna i IKT-leveranskedjorna. När det gäller komplexiteten och mångfalden i den cybersäkerhetsrelaterade politik som påverkar unionens cybersäkerhetsstatus föreslås i översynspaketet för cybersäkerhetsakten – som en del av en reform av den europeiska ramen för cybersäkerhetscertifiering – att man ska främja certifiering som ett efterlevnadsverktyg för företag och göra det möjligt att utveckla ett system för entiteters cybersäkerhetsstatus för att minska efterlevnadskostnaderna för entiteter som omfattas av NIS 2-direktivet och annan relevant unionslagstiftning om cybersäkerhet. Detta tillvägagångssätt kommer att avsevärt förenkla de lagstadgade skyldigheterna för enheter som omfattas av flera efterlevnadskrav och säkerställa en effektivare resursanvändning av alla nationella myndigheter.

I motiveringen till förslaget till förordning om cybersäkerhetsakt 2 beskrivs de viktigaste frågor som ligger till grund för förslaget samt de specifika målen för att hantera dem. Förslaget till direktiv kommer att behandla det särskilda målet nr 4 i konsekvensbedömningen för översynen av cybersäkerhetsakten, nämligen att fastställa mekanismer och villkor för att underlätta efterlevnaden av cybersäkerhetskraven och därigenom göra genomförandet av dem mer konsekvent och effektivt. Riktade ändringar av NIS 2-direktivet syftar till att förenkla efterlevnaden av och säkerställa ett anpassat och enhetligt genomförande av specifika aspekter av cybersäkerhetsramen, bland annat när det gäller tillämpningsområde, definitioner, rapportering av utpressningsprogram och tillsyn över entiteter som tillhandahåller gränsöverskridande tjänster.

Förslaget till direktiv om ändring av direktiv (EU) 2022/2555 om förenklingsåtgärder och anpassning till [cybersäkerhetsakten 2] omfattas av programmet om lagstiftningens ändamålsenlighet och resultat (Refit-programmet). Tillsammans med översynen av cybersäkerhetsakten bidrar det i hög grad till att förbättra tydligheten, minska ineffektiviteten och anpassa förfarandena mellan olika rättsliga ramar. Det bidrar till en väl fungerande inre marknad och säkerställer samtidigt unionens säkerhet och strategiska oberoende.

- **Förenlighet med befintliga bestämmelser inom området**

Unionen har utökat sina rättsliga och politiska verktyg genom att anta ett antal rättsliga instrument och politiska åtgärder: i) NIS 2-direktivet som syftar till att stärka cybersäkerheten för kritisk infrastruktur. ii) Fysiska säkerhetsåtgärder, såsom definieras i dess systerdirektiv, direktivet om kritiska entiteters motståndskraft (CER-direktivet). iii) Cyberresiliensförordningen som förbättrar cybersäkerheten för produkter. iv) Cybersolidaritetsakten som bygger upp EU-omfattande insatskapacitet. v) EU:s cyberplan[7] som stöder krishanteringssamarbete på EU-nivå. vi) EU:s verktygslåda för 5G-säkerhet som stöder cybersäkerhet i 5G-nät. vii) Den europeiska handlingsplanen för cybersäkerhet för sjukhus och vårdgivare[8], som bidrar till att förbättra deras cybersäkerhet. och viii) EU-akademin för cyberkompetens[9] som behandlar den ökande kompetensbristen på cybersäkerhetsområdet.

Ovannämnda rättsliga ramverk för cybersäkerhet kompletterades med sektorsspecifik lagstiftning, nämligen förordningen om digital operativ motståndskraft (DORA-förordningen) för finanssektorn, nätföreskriften om sektorsspecifika regler för cybersäkerhetsaspekter av

7 COM/2025/66 final.
8 COM(2025) 10 final.
9 COM(2023) 207 final.

gränsöverskridande elflöden (NCCS) för delsektorn för elektricitet, informationssäkerhetsregler (Del-IS[10]) för delsektorn för lufttransporter.

Detta förslag till direktiv är, i likhet med det förslag till förordning som det åtföljer, en del av en bredare uppsättning rättsliga och politiska initiativ som antagits av unionen för att förbättra entiteternas motståndskraft mot säkerhets- och cyberhot. Det är inriktat på riktade ändringar av NIS 2-direktivet som bland annat syftar till att klargöra vissa aspekter när det gäller tillämpningsområde, definitioner och behörighetsregler, minska bördan vid tillsynen av väsentliga och viktiga entiteter och underlätta tillsynen av gränsöverskridande entiteter genom att stärka Enisas roll i stödet till operativt samarbete. Tillsammans med förslaget till förordning skapar detta förslag dessutom en stark synergi som härrör från utvecklingen av certifiering av cybersäkerhetsstatus för NIS 2-direktivet samt potentiellt för att underlätta efterlevnaden av andra relevanta unionsrättsakter, såsom den allmänna dataskyddsförordningen, utan att det påverkar deras särskilda certifieringskrav. Dessa förenklingsåtgärder bör frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter i unionens kritiska sektorer.

- **Förenlighet med unionens politik inom andra områden**

Detta förslag skärper säkerhetskraven för de entiteter som tillhandahåller företagsplånböcker i enlighet med förslaget till Europaparlamentets och rådets förordning om inrättande av europeiska företagsplånböcker.[11] Dessutom kommer kommissionen att säkerställa överensstämmelse med kommande initiativ, såsom rättsakten om digitala nätverk. Detta förslag är i linje med förslaget till förordning om förenkling av den digitala lagstiftningen (det digitala omnibuspaketet), som bland annat innehåller ändringar av NIS 2-direktivet, tillsammans med andra unionsrättsakter. I det digitala omnibuspaketet föreslås att efterlevnaden av rapporteringskraven för cybersäkerhet ska ändras, bland annat enligt NIS 2-direktivet, genom rapportering via en gemensam kontaktpunkt för incidentrapportering, som ska utvecklas och underhållas av Enisa. Dessutom är detta förslag i linje med förslaget till Europaparlamentets och rådets förordning om säkerhet, resiliens och hållbarhet i rymdverksamhet i unionen[12].

Dessutom är förslaget i linje med Mario Draghis rapport om den europeiska konkurrenskraftens framtid, såsom framhålls ovan.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Den rättsliga grunden för detta förslag är artikel 114 i fördraget om Europeiska unionens funktionssätt, vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. Genom detta förslag ändras direktiv (EU) 2022/2555, som antogs i enlighet med artikel 114 i EUF-fördraget.

[10] Kommissionens genomförandeförordning (EU) 2023/203 och kommissionens delegerade förordning (EU) 2022/1645.

[11] COM/2025/838 final.

[12] COM/2025/335 final.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Subsidiaritetsprincipen kräver att det görs en bedömning av nödvändigheten och mervärdet av en åtgärd på unionsnivå. Förenligheten med subsidiaritetsprincipen på detta område erkändes redan vid antagandet av direktiv (EU) 2022/2555, som ändras genom detta förslag.

Detta förslag underlättar efterlevnaden av unionens cybersäkerhetslagstiftning, minskar efterlevnadskostnaderna och den rättsliga osäkerheten för berörda entiteter samt underlättar och förbättrar efterlevnaden av cybersäkerhetskraven. Det bidrar också till att skapa lika villkor när det gäller metoder för tillsyn och efterlevnadskontroller i medlemsstaterna.

- **Proportionalitet**

De regler som föreslås i detta direktiv går inte utöver vad som är nödvändigt för att i tillräckligt hög grad uppnå de särskilda målen. Den planerade anpassningen och rationaliseringen av tillämpningsområde, säkerhetsåtgärder och rapporteringsskyldigheter har samband med medlemsstaternas och företagens önskemål om en förbättring av den nuvarande ramen.

- **Val av instrument**

Förslaget kommer att ändra det befintliga NIS 2-direktivet och ytterligare rationalisera de skyldigheter som åläggs företag, och därmed säkerställa en högre harmoniseringsnivå i hela unionen. Valet av rättsligt instrument för detta förslag är förenligt med valet av den rättsakt som det ändrar, dvs. NIS 2-direktivet. Detta förslag bygger på syftet med NIS 2-direktivet att ge medlemsstaterna den flexibilitet som krävs för att ta hänsyn till nationella särdrag.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

- **Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Samråd med berörda parter**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Insamling och användning av sakkunnigutlåtanden**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Konsekvensbedömning**

Se motiveringen och den konsekvensbedömning som åtföljer [förslag till cybersäkerhetsakt 2].

- **Lagstiftningens ändamålsenlighet och förenkling**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

- **Grundläggande rättigheter**

Se motiveringen till [förslag till cybersäkerhetsakt 2].

4. BUDGETKONSEKVENSER

Se lagstiftnings- och finansieringsöversikten i [förslag till cybersäkerhetsakt 2].

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Enligt artikel 40 i NIS 2-direktivet ska kommissionen se över hur direktivet fungerar och rapportera resultatet till Europaparlamentet och rådet var 36:e månad.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Förslaget syftar till att underlätta efterlevnaden av cybersäkerhetsskyldigheter och frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos entiteter inom unionens kritiska sektorer.

Genom förslaget införs riktade ändringar av NIS 2-direktivet för att förenkla specifika aspekter av cybersäkerhetsramen, öka rättssäkerheten och harmonisera genomförandet.

För att göra det lättare för entiteter och leverantörer att visa efterlevnad av NIS 2-direktivet, i linje med det förslag till förordning som detta förslag åtföljer, kommer entiteter som regleras av NIS 2-direktivet att kunna erhålla certifikat inom ramen för organisatoriska system för cybersäkerhetscertifiering som utvecklats inom det europeiska ramverket för cybersäkerhetscertifiering.

För att ytterligare underlätta efterlevnaden av riskhanteringsåtgärder för cybersäkerhet för entiteter som omfattar flera länder och som står under tillsyn av behöriga myndigheter från flera medlemsstater har Enisa fått en ny roll som stöder medlemsstaterna i tillsynen av dessa entiteter, underlättar ömsesidigt bistånd och skapar en bättre överblick över de entiteter som omfattas av NIS 2-direktivet.

Enligt förslaget ska kommissionen dessutom anta riktlinjer för tillämpningen av de säkerhetskrav i leveranskedjan som entiteter som omfattas av NIS 2-direktivet överför till sina leverantörer, i syfte att säkerställa rättssäkerhet och förhindra otillbörlig övervältring av skyldigheter på entiteter som inte omfattas av NIS 2-direktivet.

Andra riktade ändringar av NIS 2-direktivet är följande:

- Förtydligande av tillämpningsområde och definitioner.
- Strykning av leverantörer av DNS-tjänster som är mikroföretag eller små företag från tillämpningsområdet.
- Införande av maximal harmonisering för genomförandeakter enligt artikel 21.5 (som specificerar riskhanteringsåtgärder för cybersäkerhet) för att underlätta entiteternas efterlevnad och myndigheternas tillsyn.
- Införande av en ny kategori av små midcapföretag, i linje med 2025 års kommissionsrekommendation om definition av små midcapföretag[18]. Enheter som klassificeras som små midcapföretag ska betecknas som viktiga entiteter, vilket minskar deras efterlevnadsbörda och tillsynsbördan för de behöriga myndigheterna.
- Kravet på att medlemsstaterna ska anta strategier för migrering till postkvantkryptografi (PQC) som en del av sin nationella strategi för cybersäkerhet.
- Införande av en harmoniserad insamling av uppgifter om attacker med utpressningsprogram.

2026/0012 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om ändring av direktiv (EU) 2022/2555 vad gäller förenklingsåtgärder och anpassning till [förslag till cybersäkerhetsakt 2]

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

med beaktande av Regionkommitténs yttrande[2],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I Europaparlamentets och rådets direktiv (EU) 2022/2555[3] fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Sedan direktiv (EU) 2022/2555 trädde i kraft har framsteg gjorts med att öka unionens nivå av cyberresiliens. Samtidigt har vissa utmaningar uppstått under medlemsstaternas genomförande, bland annat när det gäller direktivets tillämpningsområde, genomförandet av riskhanterings- och incidentrapporteringsskyldigheterna för cybersäkerhet och tillsynen över gränsöverskridande entiteter. Med utgångspunkt i [förslag till cybersäkerhetsakt 2] bör riktade ändringar göras av direktiv (EU) 2022/2555 för att möta dessa utmaningar, genom att förenkla specifika aspekter i syfte att öka rättssäkerheten och säkerställa ett enhetligt genomförande av direktiv (EU) 2022/2555.

(2) För att minska efterlevnadsbördan för entiterna och tillsynsbördan för de behöriga myndigheterna bör en ny kategori av små midcapföretag införas i direktiv (EU) 2022/2555, i linje med kommissionens rekommendation (EU) 2025/1099[4]. Entiteter av den typ som avses i bilaga I till direktiv (EU) 2022/2555, som klassificeras som små midcapföretag enligt den rekommendationen, bör som huvudregel betecknas viktiga

---

1 EUT C [...], [...], s. [...].

2 EUT C [...], [...], s. [...].

3 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

4 Kommissionens rekommendation (EU) 2025/1099 av den 21 maj 2025 om definition av små midcapföretag (EUT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

entiteter. För att stödja kommissionens mål att minska de administrativa kostnaderna med totalt 25 % och med 35 % för de små och medelstora företagen bör dessutom den allmänna storleksbegränsningsregel som föreskrivs i direktiv (EU) 2022/2555, enligt vilken alla enheter som räknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG[5], eller överskrider de tak för medelstora företag som föreskrivs i punkt 1 i den artikeln, omfattas av direktiv (EU) 2022/2555, tillämpas på leverantörer av domännamnssystemtjänster.

(3) Under genomförandet av direktiv (EU) 2022/2555 har det förekommit utmaningar när det gäller tolkningen av bestämmelserna om dess tillämpningsområde. Därför bör vissa tillämpningsrelaterade bestämmelser som avser vårdgivare, elproducenter, vätgasföretag och entiteter inom den kemiska sektorn förtydligas för att säkerställa rättssäkerheten och minska efterlevnadsbördan för både entiteterna och de nationella myndigheterna.

(4) För att säkerställa proportionaliteten i fråga om elproducenter enligt artikel 2.38 i Europaparlamentets och rådets direktiv (EU) 2019/944[6] bör endast de elproducenter som har en total produktionskapacitet på mer än 1 MW anses vara väsentliga eller viktiga entiteter enligt direktiv (EU) 2022/2555, förutsatt att de uppfyller storleksbegränsningsregeln. Detta bör omfatta elproducenter med en enda elproduktionsanläggning som överstiger 1 MW och elproducenter som driver flera produktionsanläggningar som tillsammans har en produktionskapacitet som överstiger 1 MW. Ett sådant tillvägagångssätt möjliggör en balans mellan behovet av att fånga upp de enheter där störningar i deras nätverks- och informationssystem skulle kunna medföra en förlust, okontrollerbarhet eller extern kontroll av produktionskapaciteten som i sig är relevant för elnätets säkerhet och stabilitet, och behovet av att inte lägga en oproportionerlig administrativ börda på företag enligt direktiv (EU) 2022/2555.

(5) De europeiska digitala identitetsplånböckerna, som föreskrivs i Europaparlamentets och rådets förordning (EU) nr 910/2014[7], är en väsentlig del av unionens digitala infrastruktur och möjliggör säker identifiering och autentisering samt utbyte av elektroniska dokument, inbegripet elektroniska attributsintyg. Med tanke på deras avgörande roll för allmänheten och för tillhandahållandet av offentliga och privata tjänster skulle alla cybersäkerhetsincidenter som påverkar dessa plånböcker kunna ha en bred inverkan. För att tillhandahållandet av de tjänster som tillhandahållarna av europeiska digitala identitetsplånböcker tillhandahåller ska säkerställas bör de vara skyldiga att genomföra lämpliga tekniska, operativa och organisatoriska åtgärder för att hantera cybersäkerhetsrisker, förebygga och hantera incidenter och samarbeta med behöriga myndigheter i enlighet med direktiv (EU) 2022/2555. De bör därför ingå bland de entiteter som omfattas av det direktivet oavsett deras storlek och klassificeras som väsentliga entiteter. De europeiska företagsplånböckerna erbjuder liknande funktioner och tjänster som är anpassade till de ekonomiska aktörernas och de

---

5 Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

offentliga myndigheternas behov, med utgångspunkt i EU:s ramverk för digital identitet, och är lika kritiska för den digitala ekonomins säkerhet och integritet. Följaktligen bör tillhandahållarna av europeiska företagsplånböcker, som inrättas i enlighet med[förslag till förordning om inrättande av europeiska företagsplånböcker][8], omfattas av samma cybersäkerhetskrav och cybersäkerhetsskyldigheter som tillhandahållarna av europeiska digitala identitetsplånböcker, för att säkerställa en konsekvent och hög säkerhetsnivå i hela ekosystemet för digital identitet.

(6) Infrastruktur för dataöverföring under vatten omfattar inte bara kablar utan även infrastruktur som hänför sig till driften av dem. Sådan infrastruktur omfattar markstationer och undervattenskabelns anslutningsdelar ovan mark (till exempel landvägar från inspektionsbrunnen på stranden till en markstation, datacentral eller ”point of presence”). Infrastruktur för dataöverföring under vatten drivs vanligtvis av enheter som redan omfattas av direktiv (EU) 2022/2555, inbegripet leverantörer av allmänna elektroniska kommunikationsnät och kommunikationstjänster eller leverantörer av molntjänster. Infrastrukturen för dataöverföring under vatten kan dock också drivas av andra typer av entiteter som för närvarande inte omfattas av direktiv (EU) 2022/2555, såsom infrastruktur för dataöverföring under vatten som drivs av leverantörer av elektroniska kommunikationsnät som inte är allmänna, eller av entiteter som leasar driften av infrastruktur för dataöverföring under vatten antingen helt eller delvis till leverantörer av allmänna elektroniska kommunikationsnät. Med tanke på de ökande riskerna för infrastruktur för dataöverföring under vatten och den därav följande höga kritikaliteten är det nödvändigt att säkerställa att alla typer av operatörer av infrastruktur för dataöverföring under vatten omfattas av direktiv (EU) 2022/2555. Annan havsbaserad kritisk infrastruktur, såsom elkablar under vattnet samt gas-, vätgas- och oljeledningar, omfattas normalt redan av direktiv (EU) 2022/2555, eftersom de drivs av systemansvariga för överföringssystem inom delsektorerna el, gas, vätgas och olja.

(7) För att göra det möjligt för de entiteter som tillhandahåller tjänster i flera medlemsstater att dra nytta av mer enhetliga och mindre betungande tillsynsmetoder på hela den inre marknaden bör de entiteterna kunna visa att de uppfyller specifika eller samtliga skyldigheter avseende hantering av cybersäkerhetsrisker som fastställs i direktiv (EU) 2022/2555 genom att beviljas ett certifikat om cybersäkerhetsstatus inom ramen för en europeisk ordning för cybersäkerhetscertifiering. Utvecklingen av en sådan ordning kommer att gynnas av antagandet av genomförandeakter om tekniska och metodologiska krav samt de sektorsspecifika krav avseende riskhanteringsåtgärder för cybersäkerhet som föreskrivs i direktiv (EU) 2022/2555 och som bygger på maximal harmonisering.

(8) Med tanke på vårt samhälles och vår ekonomis ständigt ökande beroende av digital teknik är det nödvändigt att vidta begränsningsåtgärder mot kvanthotet. Möjligheten av ”lagra nu, dekryptera senare”-attacker (*harvest now - decrypt later*), som sannolikt pågår redan i dag, och den framtida risken för kvantattacker till följd av förfalskning av namnteckningar, liksom den avskrivning av vissa bestämda algoritmtillämpningar och det fullständiga borttagande av aktuella krypteringsalgoritmer med öppna nycklar som planeras, gör behovet av att inleda åtgärder för att migrera till postkvantkryptografi (PQC) desto mer brådskande. Medlemsstaterna bör därför vara skyldiga att anta strategier för att migrera till PQC som en del av sina nationella

[8] COM(2025) 838 final.

strategier för cybersäkerhet. De strategierna bör göra det lättare att påskynda strategisk planering och att skapa stödåtgärder och verktyg för att bedöma krypteringsresursers exponering för de risker som kvantdatorerna medför. De bör dessutom bidra till att skapa en migrationsplan och testa införandet av PQC i digitala tillämpningar och nätverk, och samtidigt främja framväxten och användningen av formellt verifierade och utvärderade europeiska PQC-lösningar som följer efterlevnadsramverket för produkter och tjänster. De strategierna bör anpassas till de delmål som fastställs i unionens rättsakter och politik och till de dokument som antagits av samarbetsgruppen för nät- och informationssäkerhet, särskilt den samordnade färdplanen för genomförandet av övergången till PQC, som antogs av samarbetsgruppen för nät- och informationssäkerhet i juni 2025, som på så sätt fullbordar migrationen till PC senast 2030 för kritiska användningsfall, och senast 2035 för användningsfall med medelhög och låg nivå.

(9) Enligt artikel 21.2 d i direktiv (EU) 2022/2555 ska de väsentliga och viktiga entiteterna säkerställa en lämplig säkerhetsnivå i sin leveranskedja. I praktiken har denna skyldighet lett till att många enheter har begärt omfattande information från sina leverantörer med hjälp av heterogena frågeformulär, format och processer. Även om sådana begäranden syftar till att stödja tillbörlig aktsamhet och riskhantering kan de skapa en betydande administrativ börda för leverantörer till väsentliga och viktiga entiteter, särskilt när liknande information måste tillhandahållas upprepade gånger i olika former. För att minska denna börda och främja en konsekvent, proportionell och effektiv strategi för säkerhetsbedömningar i leveranskedjan bör kommissionen utarbeta riktlinjer för att rekommendera passande detaljnivå, struktur och format för sådana begäranden om information. Riktlinjerna bör underlätta harmonisering, minska onödigt dubbelarbete och hjälpa både entiteter och deras leverantörer att effektivt fullgöra sina skyldigheter enligt direktiv (EU) 2022/2555.

(10) Attacker med utpressningsprogram i vilka sabotageprogram krypterar uppgifter och system och kräver en lösensumma för frigörande är fortfarande ett av de främsta hoten mot väsentliga och viktiga entiteter. En harmonisering och förbättring av insamlingen av uppgifter om attacker med utpressningsprogram från de berörda väsentliga och viktiga entiteter skulle ge enheterna för hantering av it-säkerhetsincidenter (CSIRT-enheterna) och de nationella myndigheterna insikter som gör att de kan säkerställa att framtida ingripanden avseende utpressningsprogram är lämpliga och effektiva, hjälpa entiteter att öka sin motståndskraft och förhindra framtida attacker, och sammanställa de underrättelser och bevis som de brottsbekämpande organen behöver för att störa och upplösa gäng med utpressningsprogram och bestraffa sina anställda. Med tanke på den potentiellt känsliga karaktären hos den information som ska utbytas om attacker med utpressningsprogram, särskilt huruvida en enhet har betalat en lösensumma, och i så fall vilket belopp och till vem, bör sådan information endast lämnas till CSIRT-enheter eller, i tillämpliga fall, behöriga myndigheter på deras begäran. För sådant informationsutbyte uppmuntras väsentliga och viktiga entiteter att utse en person som fungerar som kontaktpunkt och säkerställer informationsutbytets konfidentialitet och tillförlitlighet. Inom ramen för det internationella initiativet för att motverka utpressningsprogram har unionen godkänt en icke-bindande internationell policyförklaring enligt vilken relevanta institutioner under de deltagande nationella regeringarnas överinseende inte bör betala det belopp som krävs av utpressningsprogram.

(11) Fullgörandet av skyldigheterna att rapportera relevant information om incidenter med utpressningsprogram bör inte leda till införandet av några ytterligare skyldigheter

enligt direktiv (EU) 2022/2555 som entiteten inte skulle ha varit föremål för om den inte hade rapporterat informationen. I detta syfte bör medlemsstaterna, inom ramen för sin nationella rättsordning, hantera eventuella risker som uppstår till följd av ökat ansvar i samband med rapportering av relevant information om incidenter med utpressningsprogram.

(12) Med tanke på den gränsöverskridande dimensionen hos många väsentliga och viktiga entiteter på hela den inre marknaden och behovet av att säkerställa samstämmighet och främja konvergens och effektivitet när det gäller tillsynsmetoder, bör Enisa stödja medlemsstaterna i genomförandet av ömsesidigt bistånd för väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater. För detta bör medlemsstaterna lämna in ytterligare information till Enisas register över entiteter. På grundval av informationen i registret över väsentliga och viktiga entiteter bör Enisa genomföra en omfattande analys av gränsöverskridande cybersäkerhetsrisker som rör väsentliga och viktiga entiteter. Analysen bör baseras på en metod som utvecklats tillsammans med kommissionen och samarbetsgruppen för nät- och informationssäkerhet. Denna metod skulle kunna ta hänsyn till i vilken utsträckning väsentliga och viktiga entiteter använder sina tjänster över gränserna, är beroende av gränsöverskridande tjänster, är utsatta för en koncentrationsrisk i leveranskedjan, kan identifieras som en källa till koncentrationsrisk i leveranskedjan, är utsatta för incidenter som skulle kunna ha betydande störande effekter på gränsöverskridande tjänster eller är beroende av nätverks- och informationssystem för tillhandahållandet av sina tjänster som är belägna i olika medlemsstater och utanför unionen. På grundval av riskanalysrapporten bör Enisa rekommendera de relevanta behöriga myndigheterna att inrätta gemensamma undersökningsgrupper för att stödja tillsynen av entiteter med en högre risknivå för en väl fungerande inre marknad i händelse av incidenter och bistå de behöriga myndigheterna i genomförandet av gemensamma tillsynsåtgärder på deras begäran.

(13) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.

(14) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42 i Europaparlamentets och rådets förordning[9] (EU) 2018/1725 och avgav ett gemensamt yttrande den 31 mars 2021.

[9] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HÄRIGENOM F<ÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av direktiv (EU) 2022/2555

Direktiv (EU) 2022/2555 ska ändras på följande sätt:

(1) Artikel 2 ska ändras på följande sätt:

(a) I punkt 2 ska led a ändras på följande sätt:

i) Led iii ska ersättas med följande:

”iii) registreringsenheter för toppdomäner,”

ii) Följande led ska läggas till som leden iv och v:

”tillhandahållare av europeiska digitala identitetsplånböcker i enlighet med förordning (EU) nr 910/2014,”

v) tillhandahållare av europeiska företagsplånböcker som inrättats i enlighet med förordning (EU) [...]*.

_____

* ”Förordning (EU) [...] [förslag till förordning om inrättande av europeiska företagsplånböcker].”

(b) Följande punkt ska införas som punkt 3a:

”3a. Detta direktiv är tillämpligt på entiteter som identifieras som ägare, förvaltare och operatörer av strategisk infrastruktur med dubbla användningsområden enligt förordning (EU) [...] **, oavsett storlek.

_____

** ”[...] förordning (EU) [...] [Förslag till Europaparlamentets och rådets förordning om inrättande av en åtgärdsram för att underlätta transport av militär utrustning, militära varor och militär personal i hela unionen].”

(2) Artikel 3 ska ändras på följande sätt:

(a) Punkt 1 ska ändras på följande sätt:

i) Leden a och b ska ersättas med följande:

”a) Entiteter av en typ som avses i bilaga I som överstiger trösklarna för små midcapföretag.

b) Kvalificerade tillhandahållare av betrodda tjänster, tillhandahållare av europeiska digitala identitetsplånböcker, tillhandahållare av europeiska företagsplånböcker och registreringsenheter för toppdomäner, oavsett storlek.”.

Följande led ska läggas till som led h:

”h) Entiteter som identifieras som ägare, förvaltare och operatörer av strategisk infrastruktur med dubbla användningsområden enligt förordning (EU) [...] [Förslag till Europaparlamentets och rådets förordning om inrättande av en åtgärdsram för att underlätta transport av militär utrustning, militära varor och militär personal i hela unionen].”

(b) I punkt 4 ska första stycket ersättas med följande:

”Vid upprättandet av den förteckning som avses i punkt 3 ska medlemsstaterna ålägga de entiteter som avses i den punkten att lämna minst följande information till de behöriga myndigheterna:

a) Entitetens namn.

b) Den relevanta sektorn och delsektorn samt typen av entitet enligt bilaga I eller II i tillämpliga fall.

c) Entitetens adress eller, i tillämpliga fall, adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 26.3.

d) Entitetens aktuella kontaktuppgifter, inklusive e-postadresser, telefonnummer, och den unika identifikationskoden och de digitala adresserna för entitetens europeiska företagsplånbok, i tillämpliga fall, och entitetens företrädare som utsetts i enlighet med artikel 26.3, i tillämpliga fall.

e) De medlemsstater där entiteten tillhandahåller tjänster.

f) Entitetens IP-adressintervall.

(3) Artikel 5 ska ersättas med följande:

”*Artikel 5*

Minimiharmonisering

Utan att tillämpningen av artikel 21.5 femte stycket påverkas hindrar detta direktiv inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.”

(4) I artikel 6

ska följande punkter läggas till som punkterna 42 och 43:

”42. *små midcapföretag*: små midcapföretag enligt definitionen i bilagan till kommissionens rekommendation (EU) 2025/1099***.

43. *infrastruktur för dataöverföring under vatten*: undervattenskablar som överför data, tillhörande infrastruktur och andra anläggningar eller element som är kopplade till dataöverföring.

_____

*** Kommissionens rekommendation (EU) 2025/1099 av den 21 maj 2025 om definition av små midcapföretag (EUT L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).”

(5) I artikel 7.2 ska följande led läggas till som led k:

”k) Riktlinjer för övergången till postkvantkryptografi, med beaktande av de tidsramar för övergången och relevanta krav som fastställs i unionens tillämpliga rättsakter och politik.”

(6) I artikel 15.2 ska den första meningen ersättas med följande:

”CSIRT-nätverket ska bestå av företrädare för de CSIRT-enheter som utsetts eller inrättats i enlighet med artikel 10, incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU) och Enisa.”

(7) Artikel 21.5 ska ändras på följande sätt:

(a) Andra stycket ska ersättas med följande:

”Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt. Kommissionen ska regelbundet bedöma huruvida de genomförandeakter som avses i detta stycke ska antas för specifika sektorer eller typer av entiteter för att förbättra den inre marknadens funktion. När kommissionen utarbetar sådana bedömningar ska den särskilt fokusera på sektorers eller entitetstypers gränsöverskridande karaktär och genomföra en öppen, transparent och inkluderande samrådsprocess med de berörda parterna och medlemsstaterna.”

(b) Följande stycke ska läggas till som femte stycke:

”Om kommissionen antar sådana genomförandeakter som avses i första och andra stycket i denna punkt, får medlemsstaterna inte införa några ytterligare tekniska krav, metodologiska krav eller sektorskrav för de åtgärder som avses i artikel 21.2 i direktiv (EU) 2022/2555 för de entiteter som omfattas av de genomförandeakterna.”

(8) I artikel 23 ska följande punkter läggas till som punkterna 12 och 13:

”12. När kommissionen antar en genomförandeakt i enlighet med punkt 11 första stycket ska den inkludera krav på att följande information avseende attacker med utpressningsprogram lämnas in i enlighet med punkt 1:

(a) Huruvida entiteten upptäckte en attack med utpressningsprogram.

(b) Attackvektorn för attacken med utpressningsprogram.

(c) Huruvida begränsningsåtgärder har vidtagits.

13. Medlemsstaterna ska säkerställa att de berörda entiteterna, i händelse av en betydande incident som orsakas av en attack med utpressningsprogram, på begäran av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten via en kommunikationskanal som tillhandahålls av CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten, lämnar in följande information:

(a) Huruvida entiteten har mottagit ett krav på lösensumma och, om så är fallet, från vem.

(b) Huruvida en lösensumma betalades och om så är fallet, vilket belopp, vilket betalningssätt och till vilken mottagare eller mottagande sida, inbegripet leverantören av kryptotillgångar och leverantören av kryptotillgångstjänster, i förekommande fall.”

(9) I artikel 24 ska följande punkter läggas till som punkterna 4, 5 och 6:

”4. För att visa efterlevnad av artikel 21 får medlemsstaterna kräva att väsentliga och viktiga entiteter erhåller ett certifikat om cybersäkerhetsstatus enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 75 i förordning (EU) XXX/XXX * * * * [förslag till CSA2].

5. Om en väsentlig eller viktig entitets cybersäkerhetsstatus är certifierad enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med artikel 74 i förordning (EU) XXX/XXX * * * * * [förslag till CSA2] och om certifikatet visar att de krav som fastställs i en genomförandeakt som antagits i enlighet med artikel 21.5 i detta direktiv eller nationell rätt som införlivar artikel 21.1 och 21.2 i detta direktiv efterlevs, får de behöriga myndigheterna inte underställa entiteten ytterligare åtgärder i enlighet med artikel 32.2 b eller artikel 33.2 b, beroende på vad som är tillämpligt med avseende på de krav som omfattas av certifikatet.

6. En certifiering enligt punkt 4 ska inte påverka den väsentliga eller viktiga entitetens ansvar för att efterleva detta direktiv.

_____

* * * * förordning (EU) XXX/XXX [förslag till CSA2].”

(10) Artikel 26 ska ändras på följande sätt:

(a) I punkt 1 ska följande led läggas till som led d:

”d) Lufttrafikföretag, som ska anses omfattas av jurisdiktionen i den medlemsstat vars behöriga tillståndsmyndighet utfärdade den operativa licensen för verksamhetsutövaren i enlighet med Europaparlamentets och rådets förordning (EG) nr 1008/2008 * * * * *, eller, om den operativa licensen eller motsvarande inte har utfärdats i enlighet med den förordningen, som ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

_____

***** Europaparlamentets och rådets förordning (EG) nr 1008/2008 av den 24 september 2008 om gemensamma regler för tillhandahållande av lufttrafik i gemenskapen (EUT L 293, 31.10.2008, s. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj).”

(b) Punkt 3 ska ersättas med följande:

”3. Om en väsentliga eller viktig entitet inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om en sådan entitet är en entitet som avses i punkt 1 a, ska den anses omfattas av jurisdiktionen i den medlemsstat där den tillhandahåller sina tjänster. Om det inte finns en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av detta direktiv.”

(11) Artikel 27 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”1. Enisa ska skapa och upprätthålla ett register över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 4. Enisa ska på begäran ge de behöriga myndigheterna tillgång till information om leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller

domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, av internetbaserade sökmotorer och av plattformar för sociala nätverkstjänster och lufttrafikföretag som lagras i det registret, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.”

(b) Punkt 2 ska utgå.

(c) Punkterna 3, 4 och 5 ska ersättas med följande:

”3. Medlemsstaterna ska säkerställa att de väsentliga och viktiga entiteterna underrättar den behöriga myndigheten om alla ändringar av de uppgifter som de lämnat enligt artikel 3.4 utan dröjsmål och under alla omständigheter inom två veckor från dagen för ändringen.

4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i artikel 3.4, ska den utan dröjsmål vidarebefordra den informationen till Enisa.

5. Den information som avses i artikel 3.4 första stycket ska, i tillämpliga fall, lämnas genom den nationella mekanism som avses i artikel 3.4 fjärde stycket.”

(12) Följande artikel ska införas som artikel 37a:

”Artikel 37a

Enisas roll i det ömsesidiga biståndet

1. Enisa ska bistå medlemsstaterna vid tillhandahållandet av ömsesidigt bistånd i den mening som avses i artikel 37 och bidra till att underlätta sådana samarbetsprocesser för väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater.

2. För tillämpningen av punkt 1 ska Enisa senast den... [15 månader efter denna förordnings ikraftträdande] genomföra en heltäckande analys av gränsöverskridande cybersäkerhetsrisker som rör väsentliga och viktiga entiteter som tillhandahåller tjänster i mer än en medlemsstat eller som tillhandahåller tjänster i en eller flera medlemsstater och vars nätverks- och informationssystem är belägna i en eller flera andra medlemsstater. I analysen ska en utvärdering göras av omfattningen av möjliga gränsöverskridande konsekvenser, och konsekvenser för den inre marknaden, av incidenter som påverkar sådana väsentliga och viktiga entiteter. Vid denna analys ska Enisa, i samarbete med kommissionen och samarbetsgruppen, utarbeta en metod. På grundval av analysen ska Enisa utarbeta en rapport om den övergripande bedömningen av gränsöverskridande cybersäkerhetsrisker, som ska uppdateras årligen.

3. På grundval av rapporten om den övergripande bedömningen av gränsöverskridande cybersäkerhetsrisker ska Enisa

(a) vid behov rekommendera de relevanta behöriga myndigheterna att inrätta gemensamma undersökningsgrupper för att stödja tillsynen av specifika enheter,

(b) utarbeta riktlinjer för gemensamma tillsynsåtgärder,

(c) på begäran av de behöriga myndigheterna i de berörda medlemsstaterna fastställa praktiska arrangemang för genomförandet av gemensamma tillsynsåtgärder,

(d) på begäran av de behöriga myndigheterna i de berörda medlemsstaterna och med förbehåll för och i proportion till sina egna resurser, delta i gemensamma tillsynsåtgärder,

(e) på begäran av de berörda medlemsstaternas behöriga myndigheter bistå vid bedömningen av en väsentlig eller viktig entitets grad av genomförande av de riskhanteringsåtgärder för cybersäkerhet som fastställs i artikel 21.

4. Vid tillämpning av punkt 3 e i denna artikel ska de behöriga myndigheterna i de berörda medlemsstaterna i förekommande fall förse Enisa med en förteckning över de riskhanteringsåtgärder för cybersäkerhet som vidtagits av den väsentliga eller viktiga entiteten i enlighet med artikel 21, en förteckning över de tillsyns- eller efterlevnadskontrollåtgärder som vidtagits samt relevant dokumentation, inbegripet bevis på genomförande av cybersäkerhetspolicyer, såsom resultaten av säkerhetsrevisioner, som de behöriga myndigheterna har gjort i enlighet med artiklarna 32 och 33 med avseende på den entiteten.

5. Om en medlemsstat erhåller ömsesidigt bistånd enligt artikel 37.1 första stycket c, ska den gemensamma kontaktpunkten informera Enisa om att ömsesidigt bistånd ägde rum. I tillämpliga fall ska den gemensamma kontaktpunkten ange vilken gränsöverskridande incident enligt artikel 23.6 som var kopplad till fallet av ömsesidigt bistånd.”

(13) Bilagorna I och II ska ändras i enlighet med bilagan till detta direktiv.

Artikel 2
Införlivande

1. Senast den … [12 månader efter detta direktivs ikraftträdande] ska medlemsstaterna anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den ... [en dag efter den dag som avses i första stycket].

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 3
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 4

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*
[...]	*[...]*