Checklista NIS2

För dig som själv faller under direktivet,
eller levererar till en NIS2-aktör

Secify

NIS2, som i Sverige kommer döpas till Cybersäkerhetslagen, är ett direktiv för att framtidssäkra samhällsviktiga och digitala tjänster. Syftet med det är att stärka och harmonisera medlemsländernas krav vad gäller cybersäkerheten inom EU. För tillfället råder såväl försening av ikraftträdandet (som tidigast kommer ske efter sommaren 2025) som förvirring över vad som gäller.

Med den här checklistan är vår förhoppning att kunna sprida lite ljus över det som går, och i brist på information åtminstone kunna skicka med en skopa lugn. Vi sitter alla i samma båt, och den bästa förberedelsen är att göra något. Allt är bättre än inget för att förbereda sig, för en sak är säker – informationssäkerhetskraven kommer öka, och ett lugnt och strukturerat förhållningssätt är det bästa över tid.

Vi är flera som sitter i samma båt just nu och undrar vad man behöver göra.
Bland våra kunder har vi spårat upp några funderingar som är genomgående och hittas hos många. Känner du igen dig i något av nedan är du med andra ord inte ensam.

Det råder stor osäkerhet kring om man alls omfattas av direktivet eller ej.

Måste man följa ett direktiv? Vad är status på den svenska lagen? Vad gäller tills den är på plats?

Många upplever det svårt att tolka kraven i direktivet och vad man ska göra åt dem.

De som upplever sig lugnast med att omhänderta kraven har gjort det inom ramen för ett ledningssystem för informationssäkerhet.

Flera känner sig stressade över att organisationen såg efterlevnad av NIS1 som en engångsinsats och nu behöver testa och uppgradera sin efterlevnad.

Många har svårt att se och motivera nyttan med tanken bakom direktivet, dvs att se varför man ska jobba med frågorna utöver att uppfylla lagen.

Många har svårt att tolka NIS2 i relation till andra regelverk. Hur hör de ihop? Gör de ens det? Hur jobbar man med flera samtidigt?

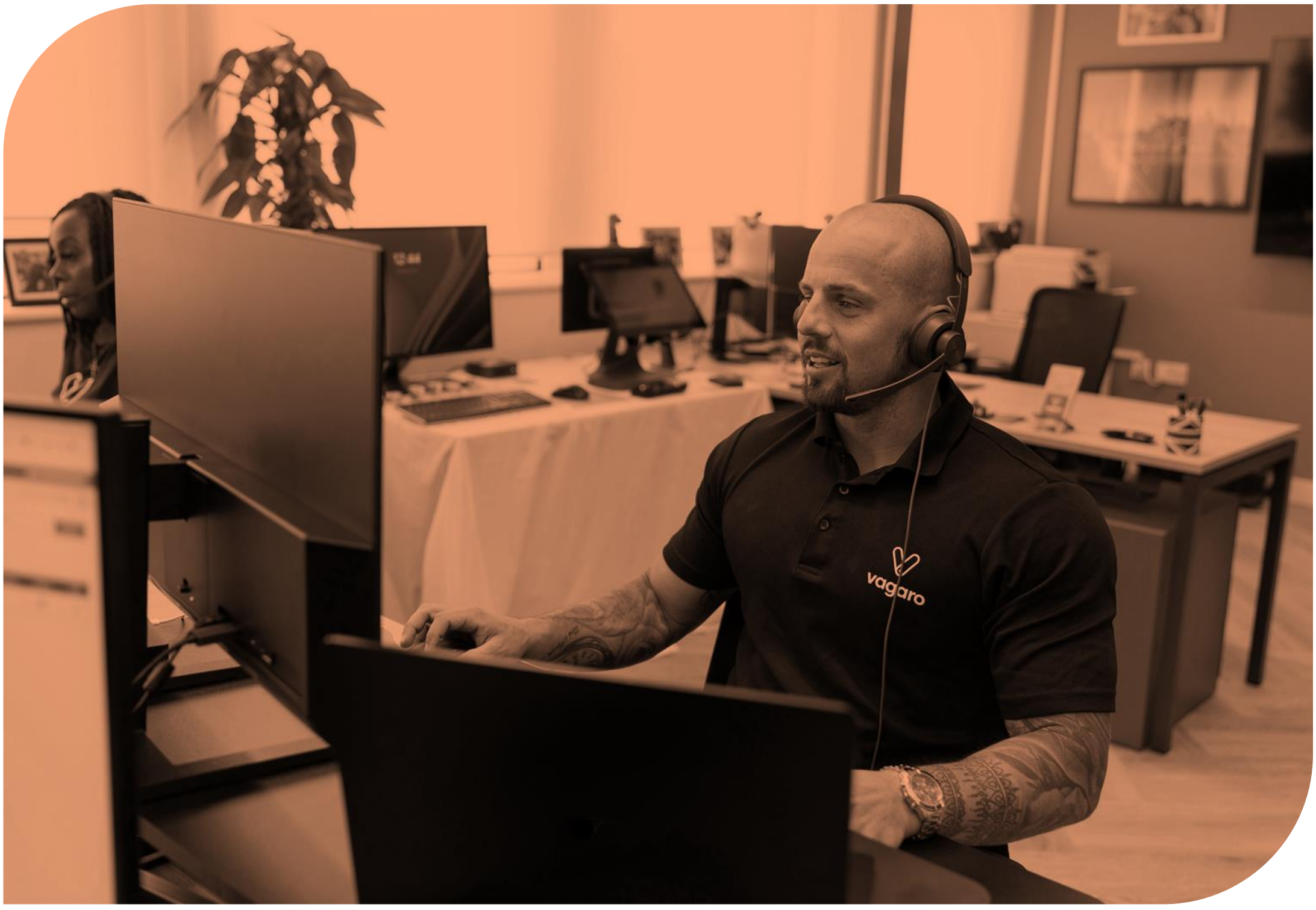
För dig som tror, antar, eller vet att du faller under NIS2 följer här våra bästa råd för att hantera direktivet – idag, och efter ikraftträdandet.

För samtliga organisationer, oavsett storlek

Hantering av risker i leverantörskedjan
Sätt i system att göra leverantörsbedömningar och se över informationssäkerhetskrav i avtal. Följ upp befintliga leverantörer och tillse en effektiv incidenthantering.

Utbildning och medvetenhet
Medvetenheten internt är viktig och går att göra på flera sätt, bl.a. genom ett utbildningsprogram anpassat efter roller och ansvarsområden (för ledning såväl som för anställda). Löpande utbildningar inom bl.a. phishing, cybersäkerhet, dataskydd (GDPR) och hur man rapporterar incidenter är klokt för alla anställda, och mer avancerade utbildningar för ledning och IT-personal. Phishingtester är ett bra sätt att testa medvetenheten.

Ledningens ansvar och fokus
De som får ledning och styrelse med sig har ett försprång, för att tala klarspråk. Det krävs engagemang och styrning, med tydligt ägandeskap för säkerhetsstrategin. Ledningen behöver ansvara för resurser och budget, samt att tydliga policyer och ramverk finns på plats och kommuniceras. Styrelsen behöver dessutom förstå att en stor skillnad i NIS2 är det personliga ansvaret som faller på personerna i styrelsen och engagera sig i grunden.



För de mindre organisationerna

Grundläggande säkerhetsrutiner
Tillse några grundläggande rutiner såsom patchning av mjukvara och drivrutiner, VPN och kryptering, samt behörighetsstyrning.

Utbildning och medvetenhet
Sätt en rutin för återkommande utbildning, på någon nivå i något format, för ledning och anställda. Försök att bygga en säkerhetskultur som ex. uppmuntrar till att våga anmäla misstänkta phishing-försök eller liknande incidenter.

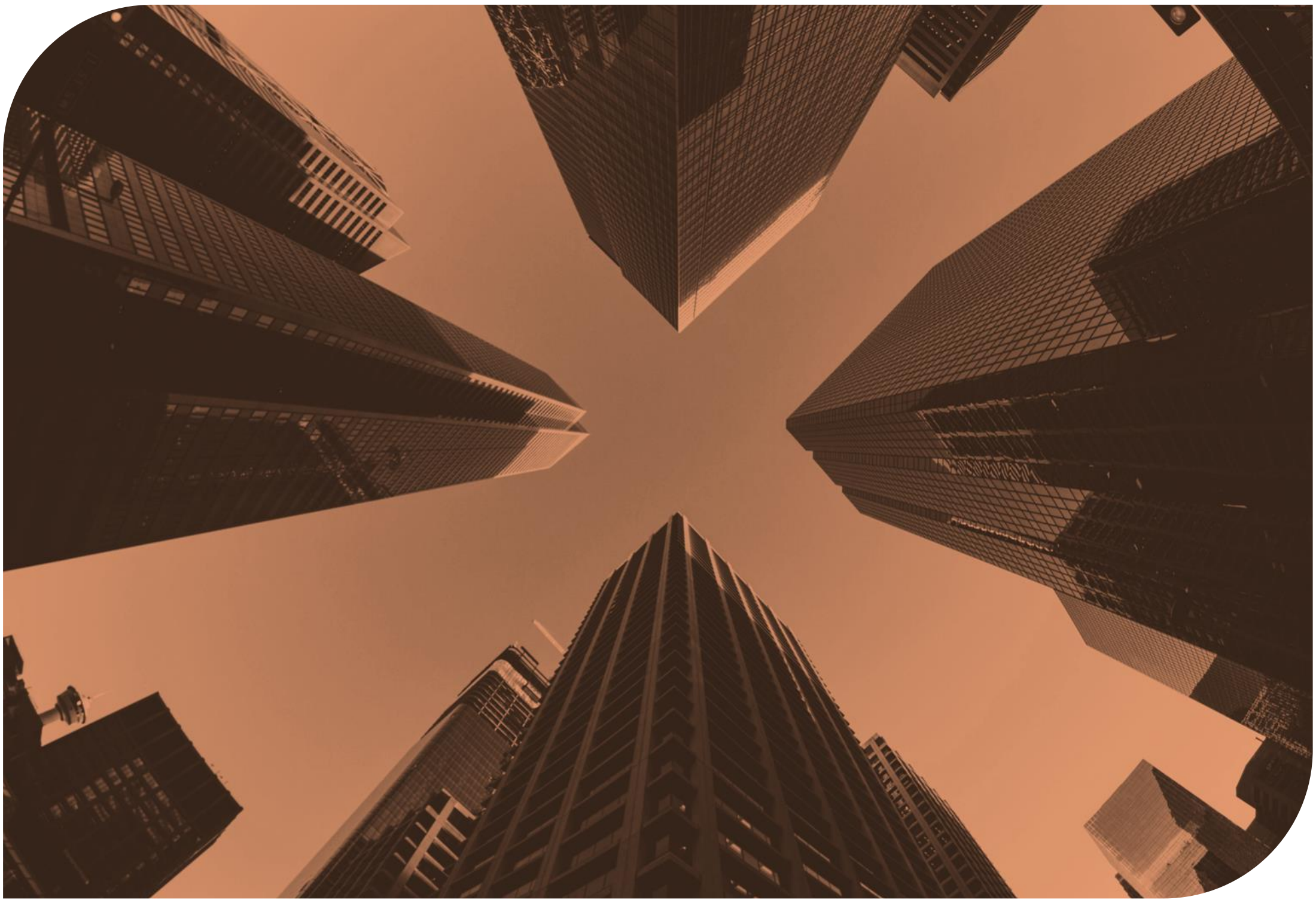
Incidentrapportering
Ta fram en enkel checklista för incidentrapportering, för att hjälpa kollegorna vara beredda när en incident inträffar.

För de medelstora organisationerna

Riskbaserat säkerhetsarbete
Arbeta i enlighet med någon typ av ramverk, ex. ISO27001. Det måste inte innebära att man går hela vägen till certifiering om det inte känns nödvändigt. Genomför också riskanalyser för att identifiera risker och prioritera säkerhetsåtgärder baserat på aktuella hotbilder.

GRC och identifiering av hot och sårbarheter
Governance, risk & compliance (GRC) kan hanteras på olika sätt men det viktiga är att man omsätter strategi i praktisk handling, och tillser efterlevnad av lagar och regler. Det finns tekniska plattformar för att förenkla efterlevnaden. Att utföra löpande sårbarhetsskanningar för att identifiera och klassificera sårbarheter i IT-miljöer och webbsidor rekommenderas.

Incidenthantering och kontinuitetshantering
Sätt upp en intern process för incidenthantering och gör kontinuitetsövningar som hjälper personal att veta hur de ska agera vid en störning i verksamheten.



För de större organisationerna

Heltäckande säkerhetsorganisation
Se till att få strukturer på plats som säkerställer att ni håller fokus på såväl tekniska, organisatoriska som legala säkerhetsåtgärder.

Internationella standarder och certifieringar
Ni kommer förmodligen tjäna på att införa och arbeta enligt någon typ av internationell standard, som ex. ISO27001 eller NIST Cybersecurity Framework. Vilken ni ska välja beror på ambition, förutsättningar, och var någonstans ni bedriver era affärer. Tillse sen regelbundna intern- och externrevisioner för att säkerställa måluppfyllelse med ert säkerhetsarbete.

Ständiga förbättringar
Sätt upp en centraliserad säkerhetsfunktion som kontinuerligt arbetar för att förbättra och anpassa säkerhetsarbetet. Att undvika engångsinsatser och få rull på löpande insatser och ständiga förbättringar är inte sällan skillnaden mellan ett framgångsrikt säkerhetsarbete och ett kostsamt och ineffektivt.

Hjälp, jag är underleverantör till NIS2-aktörer – hur ska jag tänka?

Just NIS2 lägger stor vikt vid säkerheten i hela leveranskedjan, men kraven på leverantörer ökar oaktat om just NIS2 föreligger eller ej. Som leverantör som är en del av kritiska system och tjänster kommer man indirekt att omfattas av högre säkerhetskrav för att garantera att man inte utgör en svag länk. Nedan följer en enkel checklista över de krav och förväntningar rörande informationssäkerhet som man bör vänta sig från sina kunder framgent.

Som underleverantör till en NIS2-aktör kan du räkna med:

Högre säkerhetskrav

Krav på riskhantering

Rapportering av incidenter

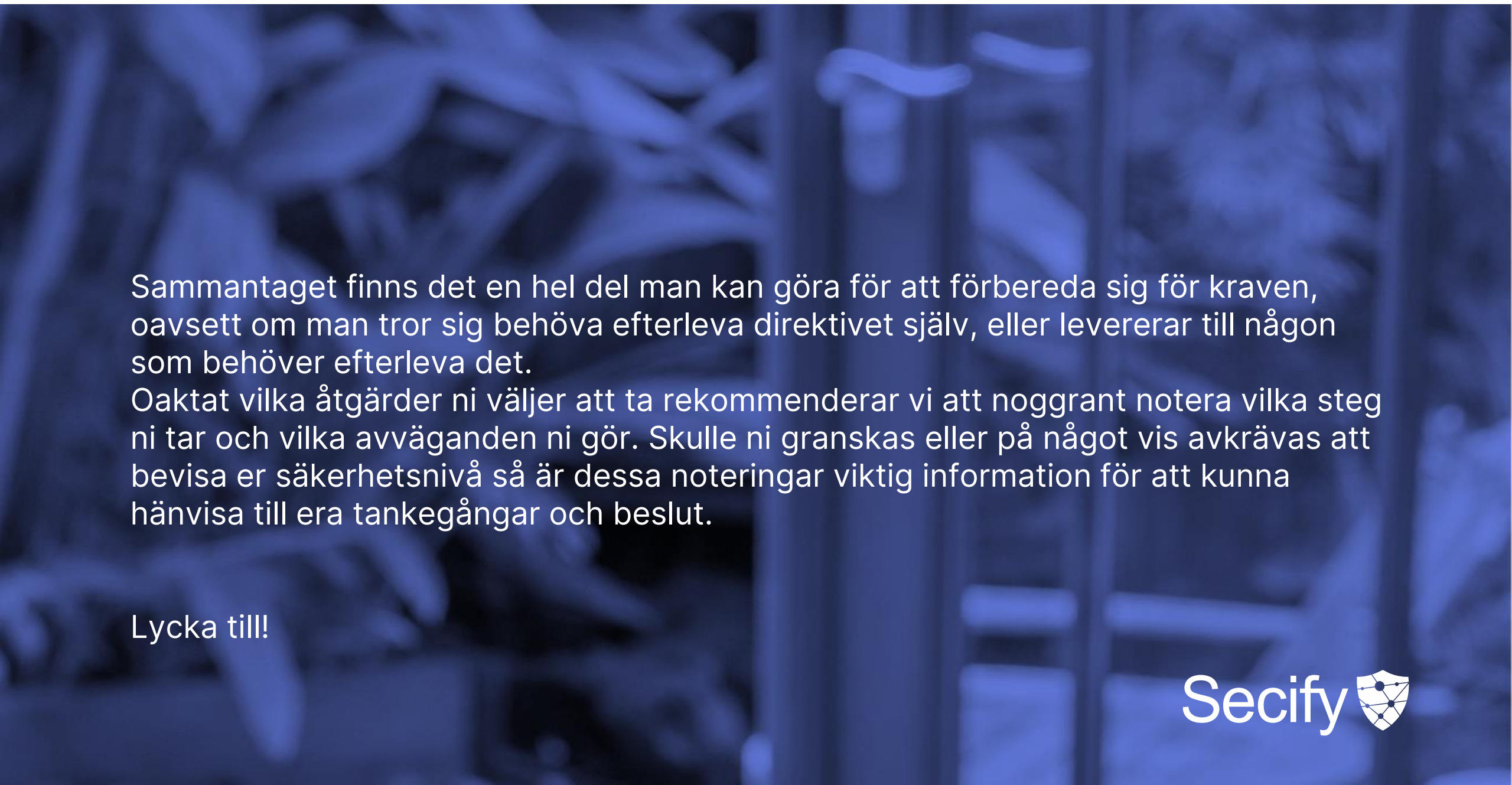
Ökad transparens & dokumentation

Avtal & kontraktskrav – mer omfattande dokumentation

Sanktioner & ansvarsskyldighet

Utbildning & säkerhetsmedvetenhet

Certifieringar och standarder



Sammantaget finns det en hel del man kan göra för att förbereda sig för kraven, oavsett om man tror sig behöva efterleva direktivet själv, eller levererar till någon som behöver efterleva det.
Oaktat vilka åtgärder ni väljer att ta rekommenderar vi att noggrant notera vilka steg ni tar och vilka avväganden ni gör. Skulle ni granskas eller på något vis avkrävas att bevisa er säkerhetsnivå så är dessa noteringar viktig information för att kunna hänvisa till era tankegångar och beslut.

Lycka till!

Secify