Cybersäkerhetsmognadsrapport

Skapad av CyberResilient för Företaget AB, 2025-12-02 14:52

Denna säkerhetsutvärdering har genererats av CyberResilient – en AI-driven plattform utvecklad med stöd från NCC-SE och Myndigheten för samhällsskydd och beredskap (MSB).

Total Cybersäkerhetsmognadsnivå **29%**

Resultatsammanfattning

Organisationens övergripande cybersäkerhetsmognad är **mycket låg** med ett samlat poängvärde om **29/100**. Denna bedömning visar på stora strukturella och operativa gap mot NIS2-kraven, särskilt inom styrning, incidenthantering, kontinuitets- och leverantörskedjehantering. Flera kärnprocesser är endast planerade och saknar implementering eller dokumenterad styrning.

Styrkor finns främst i tekniska och fysiska basåtgärder: ett nästan komplett centralt tillgångsregister, väletablerade rutiner för patchning och säkerhetskopiering samt övergripande fysisk säkerhet (betyg ~75/100). Dessutom visar personalsäkerhet (67/100) att grundläggande HR-kontroller som sekretesssavtal och disciplinära processer till stora delar är infört.

De största och mest kritiska bristerna gäller **ledning och styrning** (13/100), **incidenthantering** (15/100), **kontinuitet** (13/100) och **leverantörskedja** (10/100). Viktiga element som ett implementerat *ledningssystem för informationssäkerhet (LIS)*, formaliserad riskhanteringsmetodik, dokumenterad informationsklassning, fungerande intern rapportering till ledning samt rutiner för rapportering till CSIRT/tillsynsmyndighet saknas eller är ofullständiga. Utbildningsinsatser är i praktiken obefintliga (8/100) vilket försvagar säkerhetskulturen.

Strategiskt behöver organisationen omedelbart prioritera etablering av grundläggande styrning, incident- och kontinuitetsprocesser samt leverantörskontroller för att minska risk för regelöverträdelser och operativa avbrott. Kortfristiga insatser bör fokusera på att

skapa beslutsunderlag och snabbt åtgärda högriskområden, medan ett tvåårigt program krävs för att uppnå NIS2 efterlevnad och hållbar mognadsförbättring.

Innehållsförteckning

- **Ledning och styrning av informationssäkerhetsarbetet**
- **Riskhantering**
- **Tillgångshantering**
- **Utbildning och säkerhetsmedvetenhet**
- **Personalsäkerhet**
- **Skydd av information**
- **Incidenthantering och rapportering**
- **Kontinuitet och krishantering**
- **Leverantörskedjan och tredjepartsrisker**
- **Kontinuerlig förbättring**
- **Fysiskt skydd och åtkomst**

Ledning och styrning av informationssäkerhetsarbetet

13%

Observationer

• Den övergripande mognadsnivån för **ledning och styrning av informationssäkerhetsarbetet** är mycket låg (13/100), vilket indikerar substantiella brister i både styrande processer och rapportering till ledning.

• Det finns en dokumenterad plan för ett **ledningssystem för informationssäkerhet (LIS)**, men den är endast i planeringsfasen och saknar implementering, tydliga ansvarsroller och säkrade resurser.

• Det saknas helt en kontinuerlig och dokumenterad process för **rapportering till ledningen** om status i informationssäkerhetsarbetet, vilket innebär en betydande styrningsrisk och bristande beslutsunderlag för styrelse och högsta ledningen.

• Utifrån NIS2-referenserna framgår att nuläget sannolikt inte uppfyller kraven på **riskhantering**, regelbunden granskning och rapportering till ledningsorgan, eftersom nödvändiga rutiner och dokumentation inte är implementerade.

Rekommendationer:

HÖG PRIORITET

Implementera ledningssystem för informationssäkerhet (LIS)

Starta omgående implementeringen av ett **ledningssystem för informationssäkerhet (LIS)** baserat på tydlig scope-definition och koppling till verksamhetsmål. Ett formellt LIS är en grundläggande förutsättning för att uppfylla NIS2-kraven och möjliggör systematisk riskhantering samt spårbarhet i säkerhetsarbetet.

Genom att formellt tillsätta ägare, definiera roller och säkerställa resurser minskar ni osäkerhet och möjliggör kontinuerlig förbättring. Ett fungerande LIS underlättar även prioritering av investeringar och uppföljning gentemot ledning och styrelse.

- Definiera och dokumentera **omfattning** och **mål** för LIS kopplat till verksamhetens kritiska processer.
- Tillsätt en formell **LIS-ägare** och utse ansvariga för policyer, riskhantering och efterlevnad.
- Upprätta en **implementeringsplan** med tidslinje, milstolpar och tilldelade resurser.
- Samla befintliga säkerhetspolicyer och rutiner i ett styrande dokument och länka dem till operativa mål.
- Genomför en initial **gap-analys** mot NIS2 och prioritera åtgärder i en 90/180-dagarsplan.

HÖG PRIORITET

Etablera kontinuerlig rapportering till ledningen

Inför omgående en enkel men fastställd process för **regelbunden rapportering** till ledningen om informationssäkerhetens status. Rapporteringen bör vara dokumenterad, återkommande och innehålla kärnindikatorer som ger ledningen beslutsunderlag.

En väl definierad rapporteringsprocess förbättrar styrningen, möjliggör snabb eskalering vid incidenter och säkerställer att ledningsorganen kan uppfylla sina uppföljnings- och granskningskrav enligt NIS2.

- Designa en standardiserad **rapportsmall** med nyckelindikatorer (t.ex. incidenter, patchstatus, efterlevnadsmätningar, öppna åtgärder).
- Fastställ rapporteringsfrekvens (månatlig/kvartalsvis) och ansvarig för framställning och presentation.
- Inför en rutin för **eskalering** av högprioriterade incidenter direkt till ledning och styrelse vid behov.
- Presentera rapportstrukturen för ledningen och få formellt godkännande av innehåll och frekvens.

MELLAN PRIORITET

Inför compliance- och granskningsrutiner

Bygg ett program för löpande efterlevnadsövervakning och oberoende granskning som kopplas till LIS. Detta ska inkludera regelbundna policyöversyner, kontrollmätningar och rapportering av resultat till ledningen.

Oberoende granskningar och interna kontroller ger underlag för förbättringar och visar på regelefterlevnad gentemot NIS2, samt skapar förutsättningar för dokumenterad uppföljning av åtgärder.

- Definiera en **granskningsplan** med frekvens, omfattning och ansvariga för interna och externa granskningar.
- Utveckla mätbara **efterlevnadskontroller** och KPI:er som inkluderas i ledningsrapporten.
- Planera för och genomför en oberoende **initial granskning** av informationssäkerhetsarbetet inom de första 6 månaderna.
- Integrera granskningsresultat i riskbedömningar och LIS-åtgärdsplaner.

MELLAN PRIORITET

Prioritera snabba styrningsåtgärder och kommunikation

Genomför ett antal snabba styrningsåtgärder för att snabbt höja den operativa kontrollen och synligheten mot ledning. Fokus bör vara på att skapa klarhet i ansvar, dokumentation av pågående initiativ och enkel kommunikation till ledning och nyckelintressenter.

Dessa snabba vinster förbättrar förtroendet för säkerhetsarbetet och skapar momentum för mer omfattande implementeringar av LIS och rapporteringsprocesser.

- Formalisera och kommunicera **roller och ansvar** för informationssäkerhet till berörda chefer och team.
- Starta en minimal **dashboardslösning** eller enklare statusrapport för att visa incidenter och öppna åtgärder.
- Genomför en kort intern informationsinsats för att förankra att ledningsrapportering kommer att initieras och vilka data som krävs.

Riskhantering 31%

Observationer

• Den övergripande mognadsnivån för **riskhantering** är låg (31/100) och visar på betydande brister i formell styrning, beslutsfattande och kontinuitet.

• Organisationen har en **planerad** riskhanteringsmetodik men den är ännu inte beslutad eller etablerad, vilket skapar oklarheter kring roller, ansvar och resurstilldelning.

• Rapportering av riskbedömningar och status för säkerhetsåtgärder till **riskägare och toppledning** sker *delvis*, men saknar fast frekvens, standardiserat innehåll och tydliga uppföljningsmekanismer.

• Det saknas en genomförd **hotbildsanalys** som rapporteras till högsta ledningen. Samtidigt pågår en nätverks- och systemriskanalys, men denna är inte fullständigt dokumenterad eller kopplad till en tydlig åtgärdsplan.

Rekommendationer:

HÖG PRIORITET

Besluta och implementera riskhanteringsmetodik

Organisationen behöver snarast besluta om en formell **riskhanteringsmetodik** som beskriver processer för identifiering, analys, bedömning, behandling och uppföljning av risker. Metodiken bör vara anpassad till verksamhetens storlek och specifika riskbild samt förankras hos högsta ledningen för att säkerställa erforderliga resurser och mandat.

En beslutad metodik ger tydliga roller (t.ex. riskägare), standardiserade bedömningskriterier och en enhetlig grund för prioritering av åtgärder i linje med NIS2-krav.

- Besluta och dokumentera en **riskhanteringsmetodik** baserad på etablerade ramverk (t.ex. ISO 31000) och anpassa den till verksamhetens kontext.
- Formellt utse **riskägare** för huvudområden och definiera ansvar i ett styrdokument.
- Avsätt resurser för implementering och kompetenshöjning, inklusive dedikerad tid för riskarbete i berörda enheter.
- Publicera metodiken i intranätet och håll en formell godkännandeprocess i ledningens agenda.

HÖG PRIORITET

Etablera löpande hotbildsanalys och underrättelseflöde

Avsaknaden av en hotbildsanalys innebär en blind fläck i förmågan att proaktivt hantera förändringar i hotlandskapet. Starta med en grundläggande hotbildsanalys som bygger på öppna källor, CERT-varningar och branschspecifika informationsflöden.

Inför ett kontinuerligt underrättelseflöde som uppdaterar riskbedömningar och informerar både IT- och verksamhetsledning om relevanta hot och sårbarheter.

- Identifiera relevanta källor för hotinformation (t.ex. nationellt CERT, branschorganisationer och betrodda feeds) och prenumerera på dem.
- Utse en ägare för hotbildsanalys som sammanställer en första rapport riktad till högsta ledningen inom 30 dagar.
- Inkludera hotbildsanalysen som input i den ordinarie riskbedömningscykeln och vid exceptionella händelser.
- Skapa en enkel mall för hotbildsrapportering som tydligt visar sannolikhet, påverkan och rekommenderade åtgärder.

MELLAN PRIORITET

Formalisera och schemalägg rapportering till riskägare och högsta ledningen

Den nuvarande ad hoc-rapporteringen behöver ersättas av ett formaliserat rapporteringsupplägg med tydlig frekvens, innehåll och eskaleringsregler. Regelbunden rapportering skapar förutsättningar för styrning, resurstilldelning och kontinuerlig förbättring.

En standardiserad rapportmall och KPI:er gör det enklare att följa status på åtgärder, bedöma kvarstående risker och fatta välgrundade prioriteringsbeslut.

- Inför en kvartalsvis rapporteringscykel till högsta ledningen där resultat från riskbedömningar och status för planerade åtgärder redovisas.
- Utforma en standardiserad rapportmall som innehåller risknivåer, åtgärdsstatus, hinder och föreslagen prioritering.
- Skapa ett enkelt dashboard för ledningen som visar öppna risker och framdrift på högriskåtgärder.
- Definiera en eskaleringsprocedur för risker som överskrider acceptabla nivåer.

MELLAN PRIORITET

Slutför och dokumentera nätverks- och systemriskanalys samt koppla till åtgärdsplan

Den pågående nätverks- och systemriskanalysen bör avslutas, dokumenteras och kopplas till en prioriterad åtgärdsplan med ansvar, tidplan och acceptanskriterier. Involvering från både IT och verksamhet säkerställer att affärspåverkan beaktas i riskbedömningen.

Dokumentation och tydlig uppföljning möjliggör även planering av säkerhetstester och patchhantering i enlighet med identifierade risker.

- Slutför befintlig nätverks- och systemriskanalys och dokumentera resultat i en formell rapport.
- Utveckla en riskbehandlingsplan som listar åtgärder, ägare, prioritet och måldatum.
- Schemalägg säkerhetstester och sårbarhetsskanningar baserat på riskbedömningens resultat.
- Inför regelbundna uppdateringar av analysen vid förändringar i system eller verksamhet samt minst årlig översyn.

Tillgångshantering 50%

Observationer

• Organisationen har ett **centralt tillgångsregister** som bedöms vara i det närmaste komplett, vilket återspeglas i delpoängen (75/100).

• Det saknas en genomförd och dokumenterad **klassificering av informationstillgångar**; detta är för närvarande planerat men ej genomfört (25/100).

• Det är oklart i vilken utsträckning registret innehåller alla NIS2-kontrollerade metadata (*unik identifierare, ägare, fysisk plats, klassificering*), vilket utgör en brist mot NIS2:s krav på komplett tillgångsinventering.

• Avsaknaden av klassificering förhindrar en konsekvent tillämpning av skyddsåtgärder, påverkar incidenthantering, patchning och leverantörsbedömningar och skapar därför materiell operativ risk.

Rekommendationer:

HÖG PRIORITET

Genomför och dokumentera en formell tillgångsklassificering

Att klassificera informationstillgångar är en grundförutsättning för att kunna tillämpa lämpliga skyddsåtgärder enligt NIS2. Eftersom klassificeringen endast är planerad måste detta prioriteras för att eliminera nuvarande styrningsbrist.

En tydlig klassificeringsmodell kopplar skyddsnivåer till affärskritikalitet och sekretess, vilket möjliggör konsekvent styrning av tekniska och organisatoriska kontroller.

- Tillsätt en arbetsgrupp bestående av verksamhets-, IT- och informationssäkerhetsrepresentanter för att definiera klassificeringsnivåer.
- Ta fram en klassificeringspolicy som beskriver kriterier för känslighet, kritikalitet och värde, samt hur nivåerna ska dokumenteras i tillgångsregistret.
- Märk och registrera befintliga nyckeltillgångar med klassificeringsnivåer och koppla dessa till rekommenderade säkerhetskontroller.
- Genomför utbildning för relevanta rollinnehavare så att klassificeringsbeslut blir konsekventa och reproducerbara.

MELLAN PRIORITET

Formalisera och stärka det centrala tillgångsregistret

Det befintliga centrala tillgångsregistret är en bra grund men behöver formalisering för att uppfylla NIS2:s krav och för att fungera som en pålitlig källa för styrning.

Genom att standardisera metadatafält och införa rutiner för löpande uppdatering och åtkomststyrning minskar risken för felaktig information och obehörig åtkomst samtidigt som registerdata blir användbara för risk- och incidenthantering.

- Inför en fast mall för tillgångsposter som minst inkluderar **unik identifierare**, **tillgångstyp**, **ägare**, **förvaltare**, **fysisk/plats** och **klassificering**.
- Utse en ansvarig för tillgångsregistret och definiera befattningsspecifika roller för uppdatering och godkännande.
- Etablera en kvartalsvis verifieringsprocess för att säkerställa att registret är aktuellt och fullständigt.
- Implementera åtkomststyrning så att endast behöriga roller kan ändra registerdata, och logga ändringar för revision.

MELLAN PRIORITET

Integrera tillgångsdata med drift- och säkerhetsprocesser

Tillgångsinventariet får maximalt värde först när det används aktivt i drift, förändringshantering, patchhantering, incidenthantering och leverantörsbedömningar.

Genom teknisk integration och arbetsflöden blir registret en levande källa som förbättrar förebyggande skydd och snabbare incidentåterställning.

- Koppla tillgångsregistret till konfigurationshanteringsdatabasen (CMDB) eller motsvarande system för automatiserad upptäckt och synkronisering.
- Definiera regler som automatiskt prioriterar patchning och övervakning baserat på tillgångsklassificering.
- Integrera tillgångsuppgifter i incidenthanteringsrutiner så att berörda ägare och kritikalitetsnivå framgår vid larm.
- Inför regelbundna revisioner som verifierar att kopplingar mellan tillgångsregister och operativa processer fungerar som avsett.

Utbildning och säkerhetsmedvetenhet 8%

Observationer

• Den totala mognadsnivån för **utbildning och säkerhetsmedvetenhet** är mycket låg (8/100) och indikerar att organisationen saknar genomförda, återkommande utbildningar för majoriteten av personalen.

• Det finns en pågående plan för grundläggande utbildning, vilket är en positiv start, men planen är ännu inte operativt implementerad och saknar tydlig periodicitet och rollbaserade inslag.

• Styrelse och högre ledning genomgår för närvarande **ingen regelbunden cybersäkerhetsutbildning**, vilket utgör en strategisk risk eftersom beslutsfattare kan sakna nödvändig förståelse för cyberrisker.

• Det finns inga bevis för återkommande obligatoriska kurser för alla anställda eller dokumenterade utbildningsregister som visar överensstämmelse med *NIS2*-krav.

Rekommendationer:

HÖG PRIORITET

Slutför och formalisera utbildningsplanen

Slutför den pågående planen och omvandla den till en formell **utbildningspolicy** som anger målgrupper, frekvens, innehåll och ansvar. En formaliserad plan skapar förutsägbarhet och gör det möjligt att mäta efterlevnad.

Planen bör kopplas till organisationens **riskbedömning** och definiera både allmänna cybersäkerhetsmoment och rollbaserade moduler för kritiska funktioner.

- Godkänn och publicera en formell utbildningspolicy som beskriver syfte, omfattning och ansvar
- Definiera en årsplan med lämplig periodicitet (minst årlig) och rollbaserade utbildningsspår
- Associera varje utbildningsspår med relevanta risker från organisationens riskbedömning

HÖG PRIORITET

Starta obligatorisk grundutbildning för alla anställda

Implementera en obligatorisk introduktions- och återkommande **grundutbildning** i cybersäkerhet för samtliga anställda. Utbildningen ska omfatta grundläggande cyberhygien, åtkomststyrning, phishing-förebyggande och rapportering av incidenter.

En obligatorisk kurs säkerställer att hela organisationen uppnår en minimumnivå av säkerhetsmedvetenhet och minskar sannolikheten för mänskliga fel som leder till säkerhetsincidenter.

- Välj eller utveckla en kortfattad obligatorisk e-learningkurs för alla nya och befintliga anställda
- Schemalägg återkommande repetition (minst årligen) och definiera krav på genomförande
- Inför test eller kunskapskontroll för att verifiera deltagande och förståelse

HÖG PRIORITET

Inför skräddarsydd lednings- och styrelseutbildning

Utveckla ett kort, riktat utbildningsprogram för **styrelse och ledning** som fokuserar på strategiska cyberrisker, incidentpåverkan på verksamhetskritiska funktioner och beslutsfattande vid krishantering.

Denna utbildning bör vara interaktiv och upprepas regelbundet för att bibehålla beslutsfattarnas beredskap och säkerställa att cybersäkerhet är integrerat i affärsstrategin.

- Ta fram ett 1–2 timmars utbildningspaket speciellt för styrelse och ledning
- Genomför utbildningen minst årligen och efter större förändringar i riskbilden
- Dokumentera närvaro och följ upp med strategiska scenarier eller bordövningar

MELLAN PRIORITET

Inför loggning av utbildningar och mätbara nyckeltal

Skapa ett system för att dokumentera genomförda utbildningar och deltagande, inklusive resultat av kunskapstester. Dokumentationen är viktig både för intern uppföljning och för att visa efterlevnad vid granskning.

Definiera nyckeltal (KPI:er) såsom genomförandegrad, godkändhetsgrad och tid till genomförande för nya anställda för att mäta effektiviteten i programmet.

- Implementera ett lärplattform (LMS) eller register för att spåra deltagande och resultat
- Definiera och rapportera KPI:er kvartalsvis till ledningen
- Bevara utbildningsregister i enlighet med interna policyer och regulatoriska krav

MELLAN PRIORITET

Integrera utbildning med incidentrapportering och leverantörskommunikation

Se till att utbildningen innehåller tydliga instruktioner om **incidentrapportering** och hur personalen ska använda rapporteringskanaler. Kommunicera även rapporteringsmekanismen till leverantörer och kunder enligt relevanta krav.

Övningar och simuleringar som inkluderar rapportering stärker förmågan att upptäcka, rapportera och hantera incidenter snabbt.

- Inför praktiska övningar och phishingsimuleringar som inkluderar rapporteringsmoment
- Kommunicera incidentrapportering till viktiga leverantörer och kunder samt träna personal i processen
- Utvärdera övningsresultat och uppdatera utbildningsmaterial baserat på lärdomar

Personalsäkerhet 67%

Observationer

• Den sammanlagda bedömningen för personalsäkerhet är **67/100**, vilket indikerar att kärnprinciper är implementerade men att det finns kvarvarande brister som kräver åtgärd.

• Implementeringen av **bakgrundskontroller** är pågående (50/100) och saknar ännu fullständig täckning och dokumentation för konsekvent tillämpning i rekrytering och personalhantering.

• En **disciplinär process** för brott mot informationssäkerhet finns i stor utsträckning (75/100), men det framgår inte om effekt, proportionalitet och återkommande utvärdering säkerställs.

• **Tystnadsavtal** är i stor utsträckning införda (75/100), men det saknas information om rutiner för regelbunden uppdatering och koppling till anställningsförändringar och avslut.

Rekommendationer:

HÖG PRIORITET

Slutför och standardisera bakgrundskontroller

Bakgrundskontroller är kritiska för att minska insiderrisker och för att uppfylla NIS2-krav på säker hantering av personal som har tillgång till känsliga system eller information. Eftersom implementeringen är pågående bör organisationen snabbare gå från ad hoc-processer till en standardiserad, dokumenterad och lagligt förankrad process.

En standardiserad lösning säkerställer konsekvent tillämpning över verksamheten, förbättrar spårbarhet och förenklar revisioner samt ger ett tydligt stöd för rekrytering och behörighetsbeslut.

- Kartlägg och definiera vilka roller och nivåer som omfattas av **bakgrundskontroller** baserat på riskbedömning.
- Utför en **juridisk granskning** för att säkerställa att kontrollerna följer tillämplig arbetsrätt och personuppgiftslagstiftning.
- Inför en formell process för samtycke, genomförande och dokumentation av kontroller i rekryteringskedjan.
- Skapa en årlig granskningsmekanism för att verifiera att kontroller tillämpas konsekvent och uppdateras vid förändrade risker.

MELLAN PRIORITET

Stärk den disciplinära processen och fokusera på förebyggande åtgärder

En väl fungerande disciplinär process är viktig för att upprätthålla efterlevnad av informationssäkerhetspolicys. Eftersom processen är implementerad i stor utsträckning bör fokus ligga på att säkerställa att den är effektiv, proportionerlig och att förebyggande åtgärder minimerar behovet av sanktioner.

Genom att kombinera tydliga rutiner med utbildning och mätetal minskar risken för upprepade avvikelser och stärks säkerhetskulturen i organisationen.

- Genomför en **effektivitetsbedömning** av disciplinära processen inklusive tidslinjer, eskalering och dokumentation.
- Definiera och mät nyckelindikatorer (KPI:er) för incidenter som leder till disciplinära åtgärder och använd dessa för kontinuerlig förbättring.
- Integrera förebyggande åtgärder såsom inledande och uppdaterad **säkerhetsutbildning** för personal i högriskroller.
- Se över och dokumentera proportionaliteten i sanktioner för att säkerställa rättssäker och konsekvent hantering.

MELLAN PRIORITET

Regelbunden översyn av sekretessavtal och hantering vid anställningsförändringar

Sekretessavtal är etablerade men behöver regelbunden uppdatering för att spegla förändringar i verksamhet, legala krav och leverantörskedjor. Dessutom är kopplingen mellan tystnadsavtal och processer för anställningsförändringar/avslut viktig för att säkerställa att åtkomsträttigheter tas bort i tid.

En formaliserad rutin för översyn och koppling till avslutshantering minskar risken för obehörig kvarvarande åtkomst och säkerställer rättslig efterlevnad.

- Planera och genomför en årlig **juridisk översyn** av sekretessavtal och mallar för att säkerställa regelefterlevnad.
- Inför en checklista för **avslutshantering** som inkluderar återkallelse av åtkomsträttigheter, återlämning av utrustning och uppdatering av behörighetslistor.
- Dokumentera kopplingen mellan sekretessavtal, rollbaserade åtkomsträttigheter och HR-processer för anställningsförändringar.
- Genomför regelbundna stickprov eller revisioner för att verifiera att avtal och avslutsrutiner tillämpas i praktiken.

Skydd av information 42%

Observationer

• Den övergripande mognadsnivån för **Skydd av information** är ojämn: rutiner för patchning och säkerhetskopiering är **väl etablerade** (75/100), medan viktiga organisatoriska processer som **säker systemutveckling** saknas helt (0/100).

• Flera tekniska kontroller är under införande eller pågående arbete (50/100), vilket indikerar att grundläggande försvar finns men inte är konsekvent dokumenterade eller fullt implementerade.

• Åtkomst- och identitetshantering visar tydliga brister: unika användaridentiteter, registrerings-/avregistreringsrutiner och åtkomstuppföljning är endast delvis genomförda eller planerade (25–50/100), vilket utgör en betydande efterlevnads- och säkerhetsrisk.

• Kryptering och nyckelhantering är på planeringsstadiet eller delvis implementerat, särskilt för överföring av känslig information (25–50/100), vilket skapar osäkerheter kring konfidentialitet och integritet vid både lagring och kommunikation.

• Loggning och central övervakning är under uppbyggnad men behöver definiera tydliga användningsfall och rutiner för att stödja incidenthantering och revision (50/100).

Rekommendationer:

HÖG PRIORITET

Inför policy för säker systemutveckling och säkra upphandlingar

Det saknas en formell process för **säker systemutveckling** vid upphandling och underhåll. En tydlig policy minskar risken för införande av sårbara system och säkerställer att säkerhetskrav beaktas redan i kravställningen.

Genom att införa krav på säkerhetskrav i upphandlingsdokument, kodgranskningar och säkerhetstester i utvecklingslivscykeln uppfyller organisationen NIS2-krav kring säker utveckling och leverantörsbedömning.

- Upprätta en **policy för säker systemutveckling** som beskriver säkerhetskrav i kravspecifikationer och upphandlingar
- Inför ett krav på **säkerhetsgranskning** (kodgranskning eller statisk analys) för alla nyanskaffningar och större förändringar
- Redovisa roller och ansvar för säkerhetskrav i upphandlingar och avtalsvillkor gentemot leverantörer
- Planera och genomför regelbundna säkerhetstester (penetrationstest eller sårbarhetsskanning) innan produktionssättning

HÖG PRIORITET

Stärk identitets- och åtkomsthantering (IAM) inklusive privilegierad åtkomst

Delvisa rutiner för identifiering och användarregistrering indikerar bristande kontroll över vem som har tillgång till kritiska system. Enhetlig IAM säkerställer spårbarhet och minimerar risken för obehörig åtkomst.

Implementera livscykelhantering för användarkonton, rollbaserad åtkomstkontroll och separata processer för privilegierade konton. Regelbundna åtkomstgranskningar och automatisering via HR-system minskar mänskliga fel.

- Inför en formell **åtkomstpolicy** som täcker identifiering, autentisering och auktorisation
- Automatisera användarlivscykeln genom integration mellan HR och IAM/AD för onboarding och offboarding
- Identifiera och dokumentera alla privilegierade konton och inför särskilda godkännande- och granskningsprocesser
- Genomför kvartalsvisa åtkomstrevisioner och avvikelsehantering

HÖG PRIORITET

Rulla ut flerfaktorsautentisering (MFA) för kritiska system

Flerfaktorsautentisering är planerat men ej genomfört för kritiska system. Implementering av **flerfaktorsautentisering** är en kostnadseffektiv åtgärd för att kraftigt minska risken för kontoövertagande.

Prioritera kritiska åtkomster (administratörskonton, fjärråtkomst, molntjänster) och välj robusta tekniska lösningar med stöd för mobil appar eller hårdvarunycklar. Kombinera införandet med användarutbildning och undantagshantering.

- Kartlägg kritiska system och användarkategorier som ska omfattas av **flerfaktorsautentisering**
- Välj och implementera en MFA-lösning (appbaserad eller hårdvarutoken) med tydliga återhämtningsprocedurer
- Skapa kommunikations- och utbildningsmaterial för slutanvändare inför utrullning
- Övervaka och verifiera adoption samt dokumentera undantag och risker

HÖG PRIORITET

Etablera krypteringspolicy och robust nyckelhantering

Kryptering för lagring är delvis infört, medan kryptering för överföring och nyckelhantering fortfarande är planerade. En formell **krypteringspolicy** och nyckelhanteringsprocess är nödvändig för att säkerställa konfidentialitet och långsiktig hantering av kryptografiska nycklar.

Policy ska ange när och var kryptering krävs, godkända algoritmer, nyckellivscykel och roller för nyckelansvar. Integrera teknisk lösning med säker hårdvara eller HSM för kritiska nycklar och definiera rutiner för nyckelbackup och destruktion.

- Utveckla en **krypterings- och nyckelhanteringspolicy** med krav på algoritmer, nyckellängder och livscykelhantering
- Implementera en central nyckelhanteringslösning eller HSM för kritiska nycklar
- Tillämpa kryptering för alla känsliga data i vila och i transit enligt policy
- Genomför test av återställning av krypterade data och nyckelåterställning

MELLAN PRIORITET

Förbättra nätverkssegmentering och skydd mot skadlig kod

Nätverkssegmentering och antivirusskydd är delvis implementerade men behöver konsolideras genom dokumentation, testning och återkommande granskning. Segmentering bör baseras på riskanalys och tillämpa principet om **least privilege** och zonindelning.

Komplettera med uppdaterade malwaredetekteringsverktyg, konfigurationsstyrning och regelbundna sårbarhetsskanningar för att upptäcka och åtgärda brister i försvarslagren.

- Dokumentera nätverksarkitektur och flöden samt definiera zoner och regler för **nätverkssegmentering**
- Utför regelbundna penetrationstester och sårbarhetsskanningar mot segmentgränser
- Inför och underhåll uppdaterade malwaredetekterings- och reparationslösningar
- Granska och uppdatera brandväggsregler, åtkomstlistor och segmenteringsregler minst årligen eller vid större förändringar

MELLAN PRIORITET

Konsolidera logghantering, övervakning och återställningstester

Centralt logghanteringssystem är under uppbyggnad men behöver definierade användningsfall, retentionpolicyer och korrelation för incidenthantering. Synkroniserade tidskällor och skyddade loggarkiv är grundläggande för spårbarhet och utredning.

Backuprutiner är i stort på plats men kräver regelbundna återställningstester och dokumenterade återställningstider för att uppfylla kontinuitetskrav.

- Definiera tydliga användningsfall för loggning (incidenthantering, revision, efterlevnad) och säkerställ central lagring med åtkomstkontroll
- Säkerställ att alla system har synkroniserade tidskällor för korrekt korrelation av loggar
- Etablera regelbundna testscheman för återställning av säkerhetskopior och dokumentera RTO/RPO
- Utbilda drift- och säkerhetsteam i användning av loggverktyg och incidentkorrelation

Incidenthantering och rapportering 15%

Observationer

• Det övergripande mognadsvärdet är mycket lågt (**15/100**), vilket indikerar betydande brister i både organisatoriska och tekniska aspekter av incidenthantering.

• Organisationen har en pågående process för incidenthantering men den är ofullständig och saknar tydlig dokumentation för roller, kategorisering och triage.

• Intern incidentrapportering är endast planerad och saknar genomförande, vilket innebär att personalen sannolikt inte vet hur och när rapportering ska ske.

• Viktiga krav enligt NIS2 saknas: ingen etablerad rutin för rapportering till CSIRT/tillsynsmyndighet, ingen process för att snabbt informera drabbade användare och inga regelbundna incidentövningar.

Rekommendationer:

HÖG PRIORITET

Etablera och dokumentera en incidenthanteringspolicy

Upprätta en formell **incidenthanteringspolicy** som tydligt beskriver syfte, omfattning, roller och ansvar, incidentkategorisering samt kriterier för triage och eskalering. En väl definierad policy är grundläggande för att uppfylla NIS2-krav och för att kunna agera snabbt och konsekvent vid incidenter.

Policy ska vara lättillgänglig för all relevant personal och kopplas till befintliga processer för riskhantering, kontinuitetsplanering och leverantörsstyrning för att säkerställa att lärdomar blir bestående förbättringar.

- Utforma ett första utkast till incidenthanteringspolicy som inkluderar **roller, ansvar, incidentkategorier och triagekriterier**.
- Gör en formell godkännandeprocess genom ledningen och publicera policyn i centrala intranätet eller dokumenthanteringssystemet.
- Kommunicera policyn till samtliga berörda funktioner och inkludera i onboarding för ny personal.
- Integrera policyn med befintlig riskhantering och krisledning.

HÖG PRIORITET

Implementera intern incidentrapportering och kommunikationskanaler

Inför dokumenterade rutiner och tydliga kontaktvägar för intern incidentrapportering så att incidenter kan rapporteras snabbt och korrekt dygnet runt. Intern rapportering är avgörande för snabb eskalering och för att minimera påverkan.

Säkerställ att kommunikationen omfattar teknisk personal, ledning, kommunikation/PR och juriststöd för att hantera både åtgärder och extern kommunikation.

- Definiera och publicera en kontaktlista med primära och sekundära kontaktpersoner för incidentrapportering.
- Inför ett enkelt och tillgängligt rapporteringsformulär (t.ex. intern webblankett eller e-postadress med SLA) och kommunicera hur och när det ska användas.
- Skapa eskaleringsregler och notifieringskedjor som inkluderar ledning och relevanta stödfunktioner.
- Genomför intern utbildning så att alla anställda vet hur de ska rapportera misstänkta incidenter, även utanför kontorstid.

HÖG PRIORITET

Inför rutiner för rapportering till CSIRT och tillsynsmyndigheter

Utveckla en formell process för att identifiera vilka incidenter som enligt lag eller tillsynsmyndighet måste rapporteras, inklusive tidsfrister, innehåll och kontaktvägar. Avsaknad av denna process medför risk för regelöverträdelser och sanktioner under NIS2.

Processen bör innehålla färdiga rapportmallar, ansvarig rapporteringsfunktion samt regelbundna övningar för att säkerställa att rapportering kan ske korrekt och inom kravställda tidsramar.

- Sätt upp en checklista för incidenttyper som utlöser rapporteringsskyldighet enligt NIS2 och nationell lagstiftning.
- Samla och upprätthåll kontaktuppgifter till aktuell CSIRT och tillsynsmyndighet och skapa färdiga rapportmallar.
- Definiera ansvarig funktion som gör den formella rapporteringen och säkerställ rättsligt stöd för innehåll i rapporter.
- Genomför en övning som simulerar rapportering till CSIRT för att verifiera process och tidsramar.

MELLAN PRIORITET

Upprätta process för att informera drabbade användare och kunder

Definiera hur och när användare och kunder ska informeras vid incidenter som påverkar tjänster och tillgång till data. Snabb och tydlig användarinformation minskar osäkerhet och gör det möjligt för kunder att vidta egna riskreducerande åtgärder.

Bestäm vilka kommunikationskanaler som ska användas, utarbeta mallar och koppla processen till incidentkategorisering så att informationsutskick sker proportionerligt och korrekt.

- Identifiera kommunikationskanaler (e-post, SMS, statuswebb, kundportal) och ansvariga för varje kanal.
- Skapa mallar för användarinformation med tydlig fakta, rekommenderade åtgärder och kontaktvägar för support.
- Definiera tröskelvärden för när kunder ska informeras och vem som godkänner utskick.
- Testa informationskanaler i samband med incidentövningar för att säkerställa leverans och tydlighet.

MELLAN PRIORITET

Inför regelbundna incidentövningar och simuleringar

Börja med enkla **skrivbordsövningar (tabletopövningar)** för att träna nyckelroller och processer, och utveckla därefter mer avancerade simuleringar som involverar teknisk återställning och kommunikation. Övningar identifierar brister, förbättrar beslutsfattande och minskar återställningstid vid verkliga incidenter.

Dokumentera alltid resultat och uppföljande åtgärder så att övningarna leder till konkreta förbättringar i incidenthantering och kontinuitetsplaner.

- Planera en serie skrivborsdövningar som täcker olika incidenttyper (t.ex. dataintrång, tjänsteavbrott, ransomware).
- Utse en övningsledare och deltagare från IT, säkerhet, kommunikation och ledning.
- Efter varje övning, genomför en efterhandsanalys och dokumentera minst tre konkreta förbättringsåtgärder.
- Inför en årlig övningsplan med ökande komplexitet och inkludera leverantörer vid behov.

MELLAN PRIORITET

Formalisera efterhandsanalyser och lärandeprocess

Inför strukturerade **post-incident reviews** som identifierar rotorsak, bedömer åtgärdernas effektivitet och beskriver korrigerande åtgärder. Lärdomar måste återföras till riskhantering, policies och tekniska motåtgärder för att minska sannolikhet och påverkan av framtida incidenter.

Säkra att alla större incidenter resulterar i en handlingsplan med ansvariga, tidsfrister och uppföljning.

- Skapa en mall för efterhandsanalys som täcker rotorsaksanalys, påverkansomfattning och rekommenderade åtgärder.
- Se till att rekommenderade åtgärder prioriteras i riskhanteringsplanen och får ägare och tidsplan.
- Rapportera sammanställda lärdomar till ledningen och inkludera dem i regelbundna revisioner av säkerhetspolicys.
- Mät och rapportera nyckelindikatorer (t.ex. MTTR, antal rapporterade incidenter, tid till rapportering till myndighet) för att följa förbättringar över tid.

Kontinuitet och krishantering 13%

Observationer

- Den sammanlagda bedömningen är **mycket låg** med ett poängvärde på 13/100, vilket indikerar att organisationen fortfarande befinner sig i ett tidigt planeringsskede för centrala kontinuitets- och krishanteringsåtgärder.
- Tre nyckelkomponenter—kartläggning av beroenden, kontinuitetsplan och återställningsprocesser—är markerade som **planerade**, men saknar implementering och dokumenterad styrning.
- Väsentliga element för incident- och krishantering är **inte implementerade**: det finns ingen fungerande krisorganisation, inga regelbundna tester av planer och inga säkra alternativa kommunikationskanaler.
- Den nuvarande bristen på testning och säker kommunikation skapar en förhöjd risk att återställningstagningar och samordning vid allvarliga cyberincidenter eller leverantörsavbrott blir fördröjda eller ineffektiva.

Rekommendationer:

HÖG PRIORITET

Genomför en komplett tillgångs- och beroendekartläggning

Starta med en systematisk identifiering och dokumentation av alla tillgångar som stödjer kritiska affärsprocesser, inklusive informationstillgångar, system och leverantörer. En tydlig dokumentation är förutsättning för att prioritera kontinuitetsåtgärder och uppfylla NIS2 krav.

Varför: Utan en uppdaterad inventarie och beroendekarta kan verksamheten inte bedöma vilken påverkan avbrott får eller vilka resurser som kräver redundans och snabb återställning.

- Definiera kriterier för vad som räknas som **kritiskt** (affärspåverkan, säkerhetspåverkan, regulatoriska krav).
- Upprätta ett centraliserat **tillgångsregister** med unik identifierare, ägare, plats och klassificering enligt NIS2.
- Kartlägg externa beroenden och leverantörer inklusive SLA, kontaktuppgifter och alternativa leverantörer.
- Genomför en initial **affärspåverkansanalys (BIA)** för att kvantifiera konsekvenser och prioritera återställningsmål.

HÖG PRIORITET

Utveckla och implementera kontinuitets- och återställningsplaner

Basera kontinuitetsplanen på resultaten från tillgångs- och BIA-arbetet. Planen ska beskriva hur verksamheten ska fortsätta vid olika typer av avbrott (tekniska fel, cyberattacker, leverantörsavbrott) samt ange tydliga återställningsmål (RTO, RPO).

Varför: En dokumenterad och implementerad plan minskar både återställningstid och affärspåverkan och uppfyller NIS2 krav på business continuity och disaster recovery.

- Formulera en **kontinuitetsplan (BCP)** som täcker scenarier för tekniska fel, cyberincidenter och leverantörsstörningar.
- Definiera konkreta **RTO och RPO** för varje kritisk tjänst och inför övervakning mot dessa mål.
- Inför säkrade och testade **säkerhetskopior** med kryptering och geografisk redundans.
- Implementera redundans för kritiska nätverks- och systemkomponenter enligt prioriterad lista.

HÖG PRIORITET

Etablera en formell krisorganisation och kommunikationsplan

Utse en krisledningsgrupp med tydliga roller, ansvar och beslutsvägar. Ta fram en kommunikationsplan som beskriver intern och extern kommunikation vid incidenter, inklusive eskalering till CSIRT och ansvariga myndigheter enligt NIS2.

Varför: En etablerad krisorganisation säkerställer snabbare beslutstagande, tydlig ansvarsfördelning och korrekt rapportering under pressade förhållanden.

- Definiera **krisorganisationens** sammansättning, roller och befogenheter i en krismanual.
- Skapa en **kontaktlista** och eskaleringskedja med primära och sekundära kontaktvägar.
- Inkludera rutiner för rapportering till **CSIRT** och ansvariga myndigheter i enlighet med regelverket.
- Utbilda ledning och nyckelpersoner i roller och beslutspunkter vid kris.

MELLAN PRIORITET

Inför regelbundna tester och övningar för planer och återställning

Utveckla en teststrategi som omfattar både bordövningar och praktiska återställningstester. Dokumentera resultat, identifiera brister och integrera lärdomar i planerna. Testfrekvens och typ bör bestämmas utifrån riskbedömning och affärskritikalitet.

Varför: Endast genom regelbunden testning kan organisationen verifiera att backuprutiner, återställningsprocesser och krisledning fungerar i praktiken.

- Upprätta ett **testprogram** med ansvar, frekvens och testtyper (bordövning, återställningstest, fullskalig övning).
- Genomför regelbundna **återställningstester** av backupkopior för kritiska system och dokumentera resultat.
- Genomför årliga **skrivbordövningar** för krisorganisationen med realistiska scenarier.
- Uppdatera kontinuitets- och incidentplaner baserat på testresultat och lessons learned.

MELLAN PRIORITET

Säkra alternativa kommunikationskanaler och teknisk utrustning

Skaffa och validera säkra alternativa kommunikationslösningar som fungerar även vid primära systemavbrott. Lösningarna bör inkludera krypterade kommunikationsverktyg, offlinekontaktlistor och fysiska alternativ där så behövs.

Varför: Förmågan att kommunicera säkert och snabbt är avgörande för koordination under kriser och för att säkerställa korrekt incidentrapportering.

- Inventera befintliga kommunikationsresurser och identifiera svagheter vid avbrott.
- Implementera åtminstone två alternativa kommunikationskanaler (t.ex. krypterad chatt, mobiltelefonkedjor, satellitlösning).
- Säkra åtkomstkontroller och nyckelhantering för de alternativa kanalerna.
- Testa kommunikationskanalerna i samband med övningar och inkludera användarmanualer för nyckelpersoner.

Leverantörskedjan och tredjepartsrisker 10%

Observationer

• Organisationens sammantagna mognad för leverantörskedja och tredjepartsrisker är mycket låg med ett totalt poängläge på **10/100**, vilket indikerar betydande efterlevnadsgap mot NIS2.

• Identifiering av informationssystem och dokumentation av leverantörskedjor är enbart **planerad** och saknar fortfarande genomförd och uppdaterad registerföring av kritiska beroenden.

• Det finns **ingen genomförd leverantörsriskbedömning** och inga specificerade säkerhetsåtgärder baserade på informationsklassificering, vilket medför osäkerhet kring skyddsnivån hos externa leverantörer.

• Avtal som ska reglera cybersäkerhetskrav är endast **planerade** och saknar tydlig implementering, och det finns **inga rutiner för regelbunden uppföljning** eller hantering av avvikanden från leverantörer.

• Flera relevanta NIS2-krav pekar på behov av dokumentation, klassificering, kontraktskrav och uppföljning; dessa områden är i dagsläget otillräckligt adresserade i organisationens svar.

Rekommendationer:

HÖG PRIORITET

Etablera ett leverantörsregister och identifiera kritiska beroenden

För att uppfylla NIS2:s krav måste organisationen ha en aktuell och fullständig inventering av direkta leverantörer och de informations- och systemberoenden som är nödvändiga för att tillhandahålla kritiska tjänster.

En centraliserad **leverantörsregister** tillsammans med dokumentation av kritiska informationssystem skapar förutsättningar för systematisk riskbedömning, kontraktstyrning och uppföljning.

- Samla in leverantörsdata från samtliga affärsenheter och skapa ett centralt **leverantörsregister** som innehåller kontaktinformation, tjänstebeskrivning och leveranskritikalitet.
- Inventera och dokumentera alla informationssystem som stödjer kritiska processer och koppla dem till respektive leverantör.
- Prioritera leverantörer efter kritikalitet för att fokusera följande åtgärder på högst riskexponering.

HÖG PRIORITET

Genomför en leverantörsriskbedömning och klassificera leverantörer

Organisationen saknar en genomförd leverantörsriskbedömning. Detta är en central komponent i NIS2:s riskhanteringsramverk och behövs för att kunna ställa differentierade krav och prioritera uppföljning.

En pragmatisk, stegvis metod som börjar med de mest kritiska leverantörerna möjliggör snabb riskreduktion och ger beslutsunderlag för kontraktskrav och tekniska kontroller.

- Utforma en enkel riskmatris som bedömer leverantörer utifrån påverkan på tjänst, informationskänslighet och leverantörens säkerhetshistorik.
- Genomför riskbedömningar för de högst prioriterade leverantörerna och dokumentera resultat samt rekommenderade åtgärder.
- Integrera leverantörsriskresultat i beslutsunderlag för upphandlingar och kontraktsförnyelser.

HÖG PRIORITET

Inför tydliga cybersäkerhetskrav i leverantörsavtal och SLA

Avtalen är i nuläget endast planerade och måste kompletteras med tydliga tekniska och organisatoriska krav samt sanktioner för bristande efterlevnad.

Kontraktskrav bör omfatta informationsklassificering, åtkomststyrning, kryptering, loggning, incidentrapportering och rätt till revision eller tredjepartskontroll för att säkerställa spårbarhet och ansvar.

- Utforma och inför standardiserade klausuler för cybersäkerhetskrav att användas i upphandlingar och befintliga avtal.
- Specificera servicenivåer (SLA) kopplade till säkerhetsprestanda och incidentrapporteringstider.
- Inkludera rätt till säkerhetsrevision eller oberoende granskning i avtal med kritiska leverantörer.

HÖG PRIORITET

Etablera uppföljnings- och avvikelsehanteringsprocesser för leverantörer

Det finns i nuläget inga rutiner för regelbunden uppföljning eller hantering av avvikelser från leverantörer, vilket ökar risken för outredda brister och obevakade förändringar i leverantörers säkerhetspraxis.

Genom att införa strukturerade uppföljningsmekanismer, som årliga revisioner, kontinuerliga rapporter och riskbaserad kontrollfrekvens, kan organisationen snabbt agera vid säkerhetsbrister och dokumentera efterlevnad över tid.

- Definiera en uppföljningsplan som anger frekvens (t.ex. årlig, halvårlig) och ansvar för leverantörsgranskningar baserat på leverantörens risknivå.
- Skapa en checklista för uppföljning som inkluderar tekniska kontroller, incidentrapportering och efterlevnad av kontraktsklausuler.
- Bibliotekför avvikelseärenden och genomför åtgärdsplaner med tydliga tidsfrister och ansvarsfördelning.

MELLAN PRIORITET

Inför informationsklassificering och koppla säkerhetsåtgärder till värde

Organisationen saknar specificerade säkerhetsåtgärder baserade på informationens värde. Utan klassificering är det svårt att ställa adekvata krav på leverantörernas skyddsnivå.

Genom att klassificera information och definiera skyddsnivåer kan ni tillämpa proportionerliga tekniska kontroller hos leverantörer, exempelvis kryptering, åtkomstbegränsningar och lagringsregler.

- Inför en enkel klassificeringsmodell (t.ex. Publik, Intern, Konfidentiell, Kritisk) och tilldela klassificering till informationskategorier som delas med leverantörer.
- Definiera minimikrav för skydd per klassificeringsnivå och inkludera dessa i leverantörsavtal.
- Uppdatera inventeringen av informationssystem med klassificeringsinformation för att underlätta kontrollurval.

Kontinuerlig förbättring 0%

Observationer

• Organisationen har **ingen genomförd oberoende granskning** av informationssäkerhetsarbetet eller styrningssystemets lämplighet.

• Det saknas helt processer och rutiner för att genomföra **praktiska tester** av befintliga cybersäkerhetsåtgärder, inklusive saknad av planering för testtyp, omfattning och frekvens.

• Det finns ingen dokumenterad mekanism för att **rapportera resultat** från tester eller granskningar till ledning eller för att säkerställa åtgärdsspärr och uppföljning av avvikelser.

• Den aktuella bristen utgör både en **regelverksrisk** med avseende på NIS2:s artikel 21 och en operativ risk då bristande testning och granskning ökar sannolikheten för oupptäckta sårbarheter.

Rekommendationer:

HÖG PRIORITET

Inför ett program för oberoende granskningar

Starta ett formellt program för **oberoende granskningar** av informationssäkerhetsarbetet och ledningssystemets lämplighet. Ett sådant program ska definiera ansvar, urvalskriterier för granskare, granskningsomfång samt rapporteringsvägar till ledningsorganet.

Genom att etablera regelbundna, oberoende granskningar förbättras styrning, transparens och möjligheten att tidigt identifiera systematiska brister i säkerhetsstyrningen.

- Definiera omfattning och mål för de oberoende granskningarna och koppla dem till organisationens riskregister.
- Anlita eller utse granskare med dokumenterad revisions- eller IT-säkerhetskompetens (**intern eller extern** beroende på kompetensbehov).
- Upprätta en årlig granskningsplan med minimiintervall och prioriterade områden (policy, riskhantering, tekniska kontroller).
- Säkerställ formell rapportering av granskningsfynd till ledningsorganet och definiera tid för åtgärdsplaner och uppföljning.

HÖG PRIORITET

Etablera policy och rutiner för säkerhetstester

Inför en dokumenterad **policy och procedur för säkerhetstester** som anger testtyper (sårbarhetsskanning, penetrationstest, konfigurationsgranskning, återställningstest med mera), ansvar, metodik och godkända verktyg.

Riktlinjerna ska baseras på riskbedömningar och tydligt ange hur testresultat hanteras, dokumenteras och åtgärdas för att uppfylla NIS2:s krav på utvärdering av åtgärdernas effektivitet.

- Utforma en policy för säkerhetstester som anger syfte, omfattning och ansvar.
- Fastställ testkatalog och frekvens baserat på riskklassificering av system och tjänster.
- Skapa standardiserade testplaner som inkluderar godkännande, genomförande, rapportering och återkoppling.
- Dokumentera och klassificera testfynd och koppla dem till remediationförlopp med **tidsfrister**.

MELLAN PRIORITET

Genomför snabba kontrolltester (snabbvinster)

På kort sikt, genomför enkla men effektiva tester av grundläggande kontroller för att snabbt skapa förbättrad säkerhetsställning och få tidiga insikter om brister.

Dessa snabbvinster ger konkret underlag för prioritering av åtgärder och ökar direkt motståndskraften mot vanliga hot.

- Utför verifiering av lösenordspolicy, multifaktorautentisering och åtkomsträttigheter.
- Genomför uppdaterings- och patchkontroller för kritiska system.
- Testa antivirus/endpointskydd och grundläggande nätverkstrafikfiltrering.
- Genomför återställningstest av säkerhetskopior för kritiska system.

MELLAN PRIORITET

Inför mätning, rapportering och åtgärdsspårning

Bygg en strukturerad process för **mätning och rapportering** av granskningar och säkerhetstester där resultaten regelbundet presenteras för ledningen och kopplas till uppföljningsåtgärder.

En tydlig rapporteringskedja och KPI:er säkerställer att brister åtgärdas i tid och att ledningsorganet kan fatta informerade beslut om resurser och prioriteringar.

- Definiera KPI:er för testtäckning, öppna och stängda fynd samt tid till remediation.
- Skapa en rapportmall för gransknings- och testresultat riktad till ledningsorganet.
- Implementera ett verktyg eller register för att spåra åtgärder, ägare och status.
- Planera återkommande avstämningar mellan säkerhetsfunktion och ledning för genomgång av status.

LÅG PRIORITET

Bygg intern kompetens eller säkra extern expertis

För att upprätthålla långsiktig förmåga att genomföra oberoende granskningar och avancerade tester behöver organisationen antingen utveckla intern kompetens eller etablera avtal med kvalificerade externa leverantörer.

Rätt kompetens minskar beroendet av punktinsatser och gör det möjligt att genomföra kontinuerliga förbättringar.

- Kartlägg nuvarande kompetenser inom revision och säkerhetstestning och identifiera luckor.
- Ta fram en kompetensutvecklingsplan för intern personal inklusive formella utbildningar och certifieringar.
- Upprätta ramavtal med externa leverantörer för penetrationstester och oberoende revisioner vid behov.

Fysiskt skydd och åtkomst 75%

Observationer

• Organisationen har till största delen implementerat fysisk skyddskartläggning och åtgärder för informationssystem, vilket återspeglas i ett sammanlagt betyg om 75/100.

• Åtkomst till IT-utrymmen är i hög grad åtkomstkontrollerad och spårbar, men det finns utrymme för förbättrad loggintegration och regelbundna granskningar för att stärka spårbarheten.

• Tekniska skydd mot strömbortfall, kabelavbrott och andra fysiska störningar är huvudsakligen på plats och redundans används där det bedömts nödvändigt, men proaktiv övervakning och komponenters livscykelhantering behöver förbättras.

• Det finns en grundläggande överensstämmelse med NIS2:s krav på fysiska säkerhetsperimeterar och åtkomstbegränsning, men dokumentation och automatiserad incidentindikation kan ytterligare minska risk för driftstörningar och obehörig åtkomst.

Rekommendationer:

MELLAN PRIORITET

Rutininspektioner och sensoralarm för fysiskt skydd

Genom att införa regelbundna rutininspektioner och automatiserade sensoralarm stärks det förebyggande skyddet mot brand, översvämning, inbrott och sabotage. Detta minskar risken för oidentifierade svagheter i skyddet och möjliggör snabbare åtgärd vid avvikelse.

Förväntad nytta är minskad sannolikhet för fysisk påverkan på kritiska informationssystem och förbättrad uppföljning av öppna åtgärder via ett centralt register med ansvariga och mål för åtgärd.

- Inför en schema för kvartalsvisa rutininspektioner av serverrum och kritiska infrastrukturytor.
- Implementera sensorer för rök, vatten, temperatur och otillåten åtkomst kopplade till ett incidenthanteringssystem.
- Skapa ett register över inspektionsfynd med angivna ansvariga och mål för åtgärdsdatum.
- Utför årlig översyn av sensornätverkets täckning och funktionalitet.

MELLAN PRIORITET

Integrera åtkomstloggar med SIEM och genomför regelbundna åtkomstgranskningar

För att säkerställa spårbarhet och upptäckt av obehöriga inpasseringar bör fysiska åtkomstloggar (kortläsare, biometriska händelser, dörrlarm) integreras med organisationens SIEM eller motsvarande logghanteringsplattform.

Detta möjliggör korrelation mellan fysiska och logiska händelser, snabbare detektion av anomalier och effektivare efterforskning vid incidenter. Kvartalsvisa åtkomstgranskningar minskar risken för ackumulerade åtkomsträttigheter som inte längre är motiverade.

- Kartlägg alla fysiska åtkomstkällor och konfigurera central loggning till befintlig SIEM.
- Upprätta process för kvartalsvisa åtkomstgranskningar med dokumenterade beslutsmöten och åtgärder.
- Automatisera larm för ovanliga mönster såsom inpassering utanför arbetstid eller dörrhållning.
- Dokumentera åtkomstpolicyer och koppla dem till roller och behov till kännedom (need-to-know).

MELLAN PRIORITET

Övervakning och proaktiv ersättning av kritiska infrastrukturkomponenter

Aktiv övervakning av strömförsörjning, temperatur och nätverkslänkar samt tydliga processer för livscykelhantering föråldrade komponenter minskar risken för oplanerade avbrott. Månadsvisa genomgångar av övervakningsloggar och trendanalys identifierar åldrande utrustning innan den fallerar.

Genom att kombinera redundans med övervakning kan organisationen uppfylla återhämtningsmål och säkerställa kontinuitet för skyddade informationssystem.

- Aktivera och konfigurera övervakning för UPS, generatorer, datarumstemperatur och länkstatus mot ett centraliserat övervakningssystem.
- Inför månadsvisa genomgångar av infrastruktur- och övervakningsloggar med ansvarig infrastrukturägare.
- Upprätta en livscykelplan för kritiska komponenter med proaktivt byte baserat på driftstid och tillverkarrekommendationer.
- Testa redundanslösningar minst årligen enligt kontinuitetsplanens återhämtningsmål.

Slutsatser

För att stänga de mest akuta efterlevnadsgapen måste organisationen prioritera två parallella spår: **styrning och operativ beredskap**. Inledande fokus (0–6 månader) bör vara att etablera ett implementerbart ramverk (LIS), formalisera riskhanteringsmetodik, införa en fungerande incidenthanteringspolicy samt starta obligatorisk grundutbildning för personal och riktad utbildning för ledning/styrelse.

På medellång sikt (6–24 månader) krävs investering i teknisk mognad: fullt implementerat IAM, flerfaktorsautentisering för kritiska system, integration av tillgångsregister med driftprocesser, kontinuitets- och återställningsplaner samt ett program för oberoende granskningar och säkerhetstester. Parallellt måste leverantörshantering professionaliseras genom leverantörsregister, leverantörsriskbedömningar och avtalsmässiga säkerhetskrav.

Genom att kombinera snabba operationella åtgärder med strukturella förbättringar i styrning skapas förutsättningar för kontinuerlig förbättring och långsiktig NIS2 efterlevnad. Prioritera åtgärder som ger hög riskreduktion per investerad krona och säkerställ att ledningen får regelbunden, dokumenterad rapportering för beslut och resurstilldelning.

Rekommendationer på kort sikt:

• Starta omedelbar implementering av ett formellt **ledningssystem för informationssäkerhet (LIS)** med scope, ägare och resurser.

• Besluta och publicera en formell riskhanteringsmetodik och utse riskägare för kritiska domäner.

• Etablera en incidenthanteringspolicy och införa intern incidentrapportering med tydliga kontaktvägar.

• Inför en process för rapportering till CSIRT/tillsynsmyndighet och förbered mallar för initial rapportering.

• Genomför en grundläggande informationsklassificering för affärskritiska tillgångar och uppdatera tillgångsregistret.

• Rulla ut flerfaktorsautentisering (MFA) för administratörs- och fjärråtkomst till kritiska system.

• Starta obligatorisk grundutbildning i cybersäkerhet för alla anställda och ett kort ledningsprogram för styrelse/högre ledning.

• Skapa ett leverantörsregister och genomför en initial leverantörsriskbedömning för de mest kritiska leverantörerna.

• Utför snabba kontrolltester (sårbarhetsskanning, backup verifiering, åtkomstgranskning) för att få snabb lägesbild.

• Inför formell, återkommande rapportering till ledningen om informationssäkerhetens status och öppna åtgärder.

Rekommendationer på lång sikt:

• Fullborda och driftsätt ett komplett **LIS** integrerat med riskhantering, kontinuitetsarbete och leverantörsstyrning.

• Implementera ett IAM-program med livscykelhantering för konton, rollbaserad åtkomst och regelbundna åtkomstgranskningar.

• Integrera tillgångsregister med drift- och säkerhetsprocesser (patchning, incidenthantering, change management).

• Utveckla och testa kontinuitets- och återställningsplaner (RTO/RPO) och etablera en formell krisorganisation.

• Inför ett program för oberoende granskningar och regelbundna säkerhetstester (penetrationstest, återställningstest).

• Formaliserar leverantörsavtal med tydliga cybersäkerhetskrav, SLA krav och rutiner för löpande uppföljning och revision.

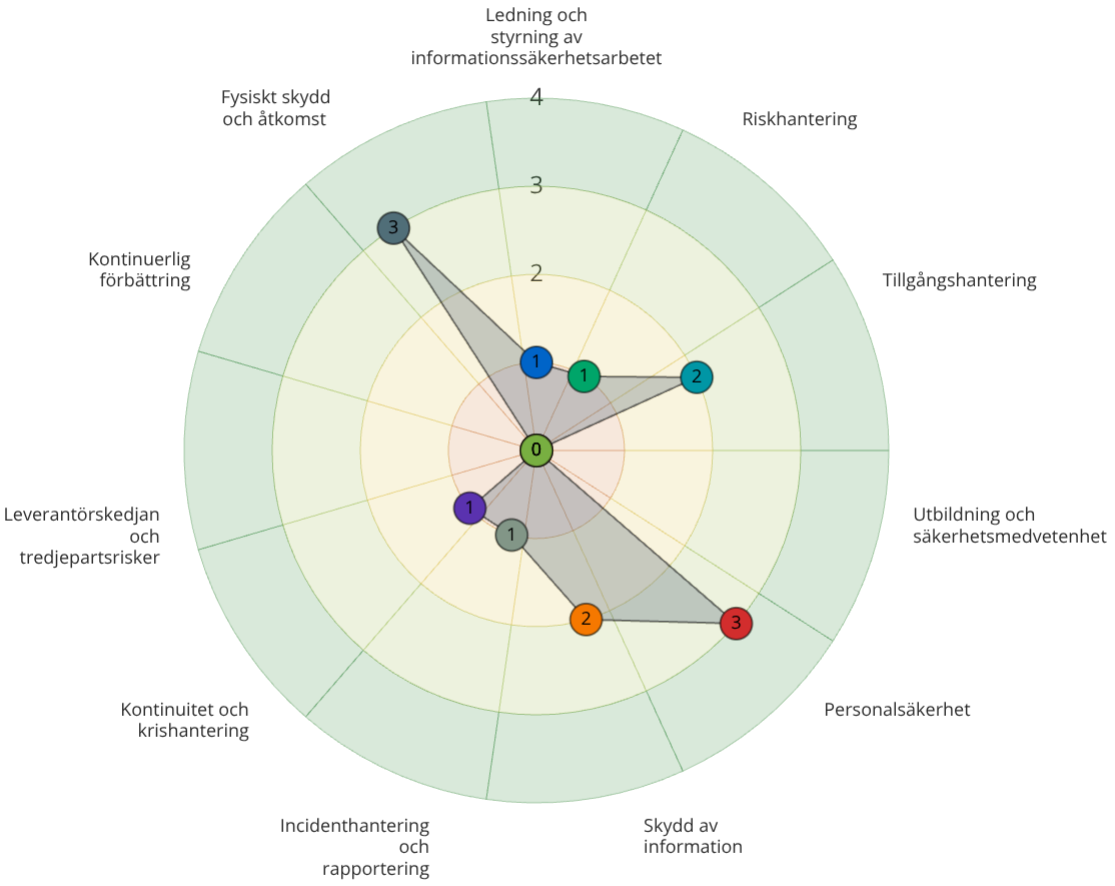
• Etablera ett kontinuerligt hotbilds- och underrättelseflöde som matas in i riskbedömningar och patchprioritering.

• Integrera fysisk åtkomstloggning med SIEM och utveckla korrelation för detektion av kombinerade fysiska och logiska incidenter.

• Inför en dokumenterad policy för säker systemutveckling och kravställning i upphandlingar samt leverantörstestning.

• Formalisera rapportering av test- och granskningsresultat till ledningsorganet och följ upp åtgärdseffektivitet över tid.

Tabeller



Ej implementerat	Planerat eller påbörjat	Pågående	Till största delen implementerat	Optimerat
Arbetet är reaktivt eller ad hoc; ingen formell metod eller dokumentation finns.	Avsikt finns och inledande steg är tagna, men praktiken är inte etablerad; dokumentation saknas i stort.	Processer finns, är dokumenterade och förstås men tillämpas endast delvis; effekt och täckning är begränsad.	Processer och rutiner är införda och helt dokumenterade, personalen är utbildad och aktiviteter styrs, men systematisk mätning och kontinuerlig förbättring är begränsad.	Proesser och rutiner är fullt införda, dokumenterade, fortlöpande mätta och proaktivt förbättrade; personalens kompetens verifieras och resultat granskas regelbundet.