Version: 260608

Uppdrag till Statistiska centralbyrån att utreda förutsättningar för att tillhandahålla säkra behandlingsmiljöer enligt EHDS, S2025/00975 (delvis)
Bilaga 2. Förmågor Säkra behandlingsmiljöer enligt EHDS

Producent:
SCB, Statistiska centralbyrån
Dataavdelningen
701 89 Örebro
010-479 40 00

Förfrågningar:
Jonas Dahlqvist
010-479 42 28
jonas.dahlqvist@scb.se

Assignment to Statistics Sweden to investigate conditions for organising and developing a system of secure processing environments according to EHDS

Producer:
Statistics Sweden, Department of Data Management
SE-701 89 Örebro, Sweden
+46 10-479 40 00

Enquiries:
Jonas Dahlqvist
+46 10-479 42 28
jonas.dahlqvist@scb.se

Denna publikation finns enbart i elektronisk form på www.scb.se
This publication is only available in electronic form on www.scb.se

Innehåll

Bakgrund 4

Inledande kommentar 4

Säkra behandlingsmiljöer (SPE) 6

Verksamhetsarkitektur för säkra behandlingsmiljöer 6

Hur man läser/tolkar modellen 6

Krav på en svensk säker behandlingsmiljö i linje med lagar, regelverk, riktlinjer och ramverk 7

Vad SPE har för yttre beroenden som HDAB inte styr över, men som måste fungera 8

Statlig e-legitimation – identitetsregistrering och certifikathantering på högsta tillitsnivå 8

Nationellt adressregister för säker krypterad kommunikation 9

Nationell kontaktpunkt som kopplar nationella system med EU:s infrastruktur 9

Resurser (förmågor, roller, IT-stöd) som behövs för utveckling, förvaltning och drift av säkra behandlingsmiljöer 9

Huvudförmåga 1. Tillhandahålla behandlingsmiljö för analys 10

Huvudförmåga 2. Hantera personalsäkerhet 13

Huvudförmåga 3. Hantera organisationens identiteter, autentisering och auktorisation 16

Huvudförmåga 4. Hantera krypterad digital kommunikation samt externa identiteter och signaturer 21

Huvudförmåga 5. Hantera IT-säkerhet och cybersäkerhet 25

Huvudförmåga 6. Hantera IT-förvaltning och driftsäkerhet 35

Huvudförmåga 7. Hantera leverantörer och tredjepartsrisker 42

Huvudförmåga 8. Hantera egendomsskydd, fysisk säkerhet 45

Huvudförmåga 9. Hantera säker utveckling och design 48

Huvudförmåga 10. Hantera omvärldsbevakning och risker 51

Huvudförmåga 11. Hantera efterlevnad och revision..... 55

Huvudförmåga 12. Ledning och styrning av säker miljö..... 57

Riskanalys 61

1. Risker och konsekvenser om förmågorna inte hanteras korrekt, baserat på kraven från EHDS, GDPR, NIS2 och SPE-specifikationerna. 62

1.1 Prioriterad risklista för bristande hantering av SPE-förmågeområden..... 64

2. Risker kopplade till Nationell Digital Infrastruktur..... 67

Bakgrund

Uppdraget handlar om att utreda hur ett system med säkra behandlingsmiljöer ska organiseras och utvecklas i Sverige inom ramen för EU:s förordning om European Health Data Space (EHDS). EHDS reglerar utbyte av hälsodata mellan organisationer och länder och omfattar bestämmelser för både primär- och sekundäranvändning av data. För sekundäranvändning ska varje medlemsstat utse ett eller flera organ, så kallade Health Data Access Bodies (HDAB), som ansvarar för att möjliggöra tillgång till hälsodata. Statistiska centralbyrån (SCB) har fått i uppdrag att utreda förutsättningarna för att tillhandahålla säkra behandlingsmiljöer enligt artikel 73 i förordningen.

Säkra behandlingsmiljöer ska begränsa tillgången till behöriga personer enligt datatillstånd, minimera risken för obehörig åtkomst eller ändring, och föra identifierbara loggar över aktiviteter. Dessutom ska de säkerställa efterlevnad och övervaka säkerhetsåtgärder.

För att realisera detta krävs en analys av yttre beroenden, resurser och förmågor kopplade till skydd av sekundära hälsodata samt drift av säkra system. Uppdraget omfattar att identifiera regelverk, aktörer och kompetenser, samt att ta fram en övergripande verksamhetsarkitektur med rekommendationer för utveckling, förvaltning och drift.

En central slutsats är att säkra system bygger på både tekniska och organisatoriska åtgärder. Tekniska lösningar är viktiga, men utan styrning, ansvar, policys, säkra processer och operativa kompetenser kan tekniken inte ensam garantera efterlevnad eller motståndskraft.

Inledande kommentar

Vi har arbetat utifrån tesen att förmågorna, som baseras **MSB:s Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter**, **CSL, NIS2 och ISO 27000 i stort är identiska med kraven från EHDS TEHDAS2. M7.4** Draft technical, functional and security specifications of Secure Processing Environments och EHDS Artikel 73 Krav på säker bearbetningsmiljö.

Men det är **ytterligare krav som tillkommer i en SPE** om man redan är en certifierad ISO 27000 organisation. Det finns gap mellan ISO 27001 certifiering och TEHDAS2 M7.4 SPE-efterlevnad.

ISO-certifieringen ger ett stabilt säkerhetsfundament, men TEHDAS2-efterlevnad kräver att organisationen också bygger en fullständig, tekniskt specificerad och federerad Secure Processing Environment enligt EHDS-kraven.

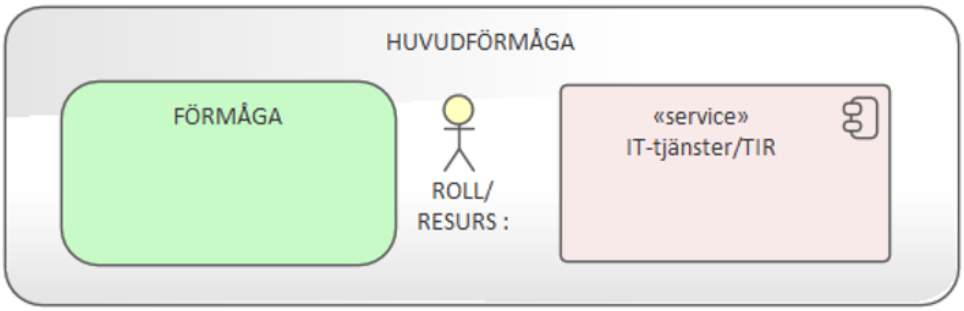
Åtgärder för ISO-certifierade organisationer för att nå SPE:

1. Att lägga till **TEHDAS2 specifika funktioner** (största gapet)
    - Bygg SPE-komponenterna enligt M7.4-specifikationen.
    - Säkerställ federation.
2. **Utöka loggning, monitorering och audit**
    - Implementera TEHDAS2-kompatibelt federerat audit-lager.
    - Harmonisering av loggformat (säkerställa att loggar från olika system går att korrelera) & retention (lagringstid).
3. **Implementera EHDS-dataflöden**
    - Datatillstånd (permits).
    - Datarequest pipelines (den tekniska processen för godkända aktörer genom en säker bearbetningsmiljö).
4. **Uppdatera ISMS för att inkludera EHDS-specifika processer**
    - Nya risker.
    - Nya roller.
    - Nya regulatoriska krav.

Säkra behandlingsmiljöer (SPE)

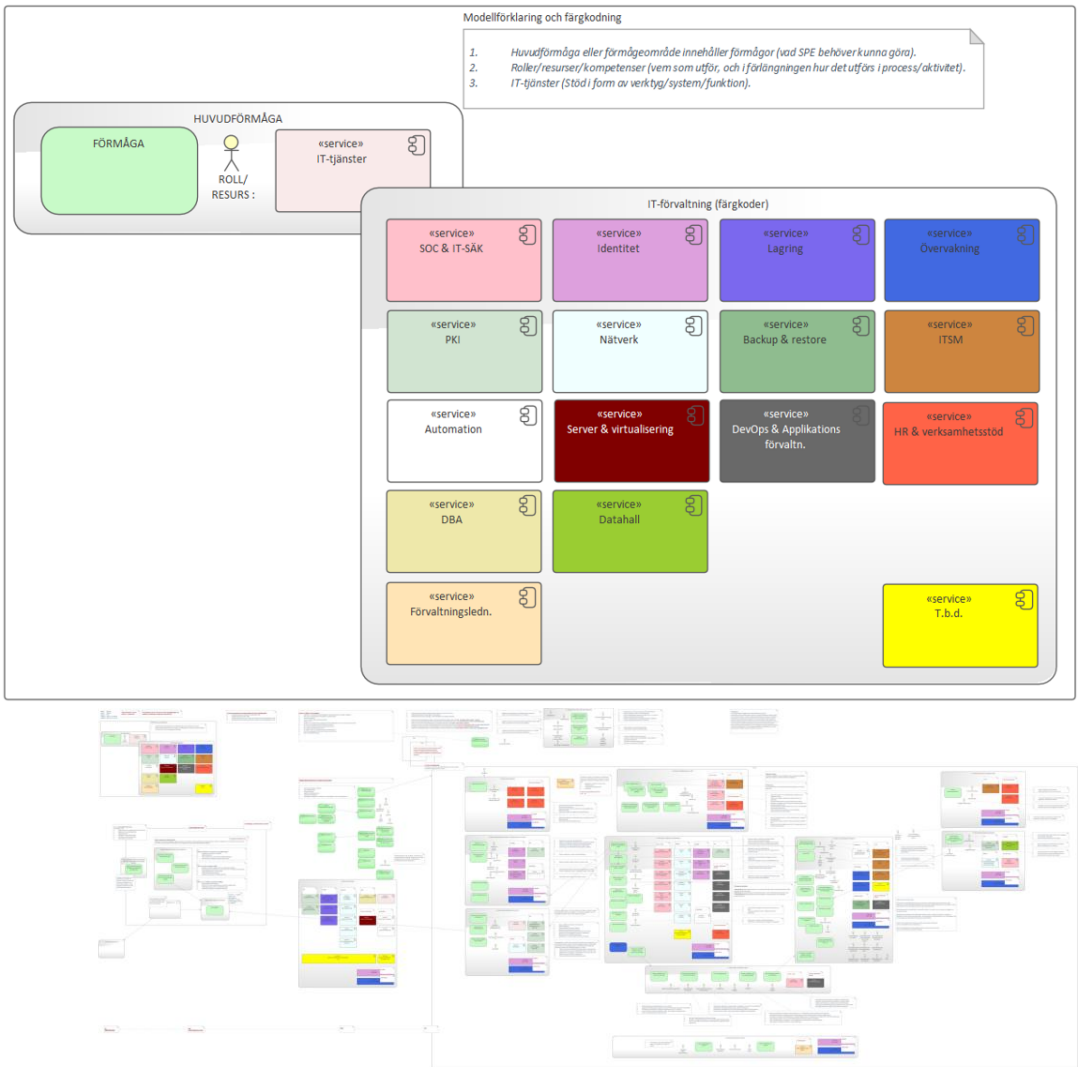
Verksamhetsarkitektur för säkra behandlingsmiljöer

Hur man läser/tolkar modellen



- Huvudförmåga eller förmågeområde innehåller förmågor (vad SPE behöver kunna göra).
- Roller/resurser/kompetenser (vem som utför, och i förlängningen hur det utförs i process/aktivitet).

- IT-tjänster (Stöd i form av verktyg/system/funktion).



Krav på en svensk säker behandlingsmiljö i linje med lagar, regelverk, riktlinjer och ramverk

Regelverk, riktlinjer, kravställning och ramverk att beakta:

- TEHDAS2. M7.4 Draft technical, functional and security specifications of Secure Processing Environments
- EHDS Artikel 73 – Krav på säker bearbetningsmiljö (Secure Processing Environment)

EU-regelverk

- GDPR Dataskyddsförordningen

- NIS2-direktivet (Directive (EU) 2022/2555)

Svenska regelverk

- Säkerhetsskyddslagen
- CSL Cybersäkerhetslagen
- MSBFS 2020:7 Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
- PMFS 2022–1 Säkerhetspolisens föreskrifter om säkerhetsskydd
- KSF MUST Krav på godkända säkerhetsfunktioner version 3–1

Internationella standarder

- ISO/IEC 27001 och ISO/IEC 27002 Säkerhetskontroller
- ISO 31000 och NIST CSF Riskhantering och omvärldsbevakning

Ramverk

- NIST SP 800–53 Kontroller för fysisk och miljömässig säkerhet.
- FitSM (Free, Lightweight ITSM Standard.) https://www.fitsm.eu/ nämns i ”TEHDAS2. M7.4 Draft technical, functional and security specifications of Secure Processing Environments” som ett rekommenderat ramverk för att hantera standardiserade förvaltningsprocesser inom säkra behandlingsmiljöer (SPE).

Vad SPE har för yttre beroenden som HDAB inte styr över, men som måste fungera

Beroenden i form av en nationell digital infrastruktur. En funktion som saknas i den digitala förvaltningens infrastruktur är en heltäckande och säker lösning för hantering av nationell identitetsregistrering och certifikatsutfärdning kopplad till statlig e-legitimation med högsta tillitsnivå, i enlighet med EU:s reviderade eIDAS-förordning. En annan är ett nationellt adressregister för säker krypterad kommunikation som fungerar central kontaktpunkt för att möjliggöra säker och krypterad kommunikation mellan myndigheter, organisationer och andra behöriga aktörer. En tredje är den nationella kontaktpunkten (NPC) som kopplar nationella system med EU:s infrastruktur.

Statlig e-legitimation – identitetsregistrering och certifikathantering på högsta tillitsnivå

En funktion som saknas i den digitala förvaltningens infrastruktur är en heltäckande och säker lösning för hantering av nationell identitetsregistrering och certifikatsutfärdning kopplad till statlig e-legitimation med högsta tillitsnivå, i enlighet med EU:s reviderade eIDAS-förordning. Denna funktion innefattar att Polismyndigheten verifierar användares identitet innan certifikat kan utfärdas, hanterar ansökningar, initierar certifikatsutfärdning genom kommunikation med

certifikatutfärdaren samt dokumenterar och loggar hela registreringsprocessen. Certifikatutfärdaren (CA) ansvarar för att generera och hantera nyckelpar, utfärda och signera digitala certifikat, lagra privata nycklar säkert via exempelvis smarta kort eller HSM, hantera certifikatprofiler enligt X.509-standard, samt utföra certifikatsförnyelse och återkallelse. CA tillhandahåller även information om ogiltiga certifikat genom CRL, stödjer realtidskontroll via OCSP, säkerställer tillgänglighet via säkra och redundanta kanaler, och möjliggör automatisk uppdatering och distribution till klienter. All certifikatsutfärdning loggas för att säkerställa spårbarhet och tillit i hela kedjan.

Funktionen är avgörande för att möjliggöra gränsöverskridande digital identifiering och för att uppfylla EU:s krav på nationella digitala identiteter. Polismyndigheten har fått uppdraget att ta fram denna lösning, men en tydlig och integrerad funktion för registrering och certifikathantering saknas ännu i den breda digitala förvaltningen.

Nationellt adressregister för säker krypterad kommunikation

Ett nationellt adressregister fungerar som en central kontaktpunkt för att möjliggöra säker och krypterad kommunikation mellan myndigheter, organisationer och andra behöriga aktörer. Registret innehåller verifierade adresser och certifikat som används för att identifiera mottagare och säkerställa att information överförs på ett sätt som uppfyller höga krav på integritet och tillit. Genom att använda detta adressregister kan aktörer enkelt hitta rätt kontaktpunkt och garantera att kommunikationen sker via godkända och säkra kanaler.

Nationell kontaktpunkt som kopplar nationella system med EU:s infrastruktur

En nationell kontaktpunkt (NCP) ska fungera som en central nod för att integrera svenska system med EU:s gemensamma digitala infrastruktur. Syftet är att säkerställa interoperabilitet, säker dataöverföring och enhetliga standarder mellan medlemsstater. Kontaktpunkten hanterar autentisering, certifikat och adressinformation, vilket gör det möjligt för myndigheter, organisationer och aktörer att kommunicera och utbyta information på ett säkert sätt inom ramen för europeiska regelverk.

Resurser (förmågor, roller, IT-stöd) som behövs för utveckling, förvaltning och drift av säkra behandlingsmiljöer

För att utveckla, förvalta och driva säkra behandlingsmiljöer krävs en kombination av resurser i form av organisatoriska förmågor, roller med specifika kompetenser samt IT-stöd. Regelverken ställer krav på att en säker behandlingsmiljö (SPE)

besitter ett antal förmågor som beskriver vad organisationen behöver kunna göra. Dessa förmågor realiseras genom roller som har rätt kompetenser och ansvar för att utföra arbetet, vilket i sin tur sker genom etablerade processer. För att kompetenserna ska kunna agera effektivt behövs stöd i form av verktyg, oftast IT-tjänster, som möjliggör säkra och effektiva arbetsflöden.

Huvudförmåga 1. Tillhandahålla behandlingsmiljö för analys

Behandlingsmiljö för analys handlar om att styra tillgången till data utifrån datatillstånd, skapa användarkonton och behörigheter i enlighet med dessa samt möjliggöra att HDAB och betrodda dataleverantörer tillgängliggör data korrekt. Miljön ska ge dataanvändare möjlighet att analysera data med rätt programvara och prestanda och göra kontrollerade uttag av anonymiserade resultat. SPE ska erbjuda teknisk support, logga aktiviteter, rapportera missbruk till HDAB och upprätta ett SLA med tydliga drift- och servicevillkor samt ansvarsfördelning. Det pågår fortfarande ett utredningsarbete inom Sverige och EU avseende förordningens implementering och kraven för Huvudförmåga 1 kommer under det arbetet detaljeras och utvecklas.

Förmågor:

Hantera SPE krav (Forskning)

Krav i TEHDAS2. M7.4:

- *SPER-1. SPE MUST enable scientific research on sensitive data.*
- *SPER-5. SPE design SHOULD promote collaboration among authorised users.*
- *OPR-16. SPE Operator MUST track and log actions of each authorised project member, including instances of data access, processing, viewing and output.*
- *OPR-26. SPE Operator SHOULD define SLAs that include: uptime guarantees, response/resolution times for incidents include security SLAs, such as data encryption guarantees, incident response times, and audit logging.*
- *OPR-31. SPE Operator MUST provide dedicated technical support with clearly defined SLAs and escalation paths for addressing incidents and technical issues.*

Hantera Datatillstånd

Krav i TEHDAS2. M7.4:

- *SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.*
- *EHDSR-1. HDAB MUST grant access to EHD using a data permit.*

- *EHDSR-2. EHD MUST be accessed using an SPE. EHDSR-3. Natural persons listed in the data permit MAY access the identified*
- *EHD in SPE. EHDSR-4. TOMs MUST minimise the risk of unauthorised EHD access in SPEs.*
- *EHDSR-5. Authorised health data users MUST be strongly identified.*
- *EHDSR-10. EHD MUST be identified in the data permit.*
- *EHDSR-11. Health data holder MUST upload the permitted EHD to be available in an SPE for the health data user.*
- *EHDSR-12. Health data user MAY download only non-personal EHD from SPE. Anonymised personal data is non-personal.*
- *EHDSR-13. HDAB MUST ensure by reviewing that no personal data is taken out of the SPE by the health data user.*
- *OPR-1. The SPE operator MUST have procedures in place to enforce user authentication and access restrictions based on the data permit associated with the processing of health data.*
- *OPR-5. SPE Operator MUST implement mechanisms to terminate the secure processing environment upon expiration of the data permit. All electronic health data within the environment MUST be deleted or rendered unrecoverable within six months of permit expiry, including any backups or redundant copies. Procedures MUST be formally documented, monitored, and aligned with risk assessments and confidentiality requirements.*
- *OPR-12. SPE operators MUST conduct regular Data Protection Impact Assessments (DPIAs).*
- *OPR-23. Health data users, HDAB staff and SPE Operator staff who interact with the SPE MUST receive detailed, role-specific information or training covering health data processing, EHDS compliance requirements andsecurity best practices coming from GDPR.*
- *OPR-31. SPE Operator MUST provide dedicated technical support with clearly defined SLAs and escalation paths for addressing incidents and technical issues.*

Hantera krav på federation (Federated (FSPE) requirements)

Krav i TEHDAS2. M7.4: FSPER-1. Legal or contractual agreement MUST cover the SPE federation across organisations.

Krav i TEHDAS2. M7.4: FSPER-1. Legal or contractual agreement MUST cover the SPE federation across organisations.

Hantera felaktig användning och incidentrapporter till HDAB

Krav i TEHDAS2. M7.4:

- *OPR-18. A reporting process MUST be in place to notify HDABs and relevant authorities of security incidents or non-compliance findings including data breaches or misuse.*
- *OPR-19. SPE Operator SHOULD adopt and enforce defined timelines for communicating and reporting incidents to the HDAB: Early warning notification: within 24 hours of incident detection. Detailed incident notification: within 72 hours of incident detection. Final incident report: no later than one month after the incident.*
- *OPR-20. SPE Operator MUST be able to promptly halt access and processing activities within the SPE when misuse or data breaches are identified.*

Ladda data och hantera uttag

Krav i TEHDAS2. M7.4:

- *EHDSR-12. Health data user MAY download only non-personal EHD from SPE. Anonymised personal data is non-personal.*
- *EHDSR-13. HDAB MUST ensure by reviewing that no personal data is taken out of the SPE by the health data user.*

Skapa/uppdatera projekt, konton och behörigheter utifrån datatillstånd

Ta emot data till projekt enligt datatillstånd (från datahållare, HDAB och SPE)

Möjliggöra sekundär användning/ analys/ behandling/ bearbetning

Logga användning och anmäla missbruk

Möjliggöra export

Möjliggöra export av:

- Anonymiserade resultat
- Förädlade data till HDAB
- Betydande kliniska upptäckter

Hantera arbetsyta för externa användare (Bearbetningsyta för externa användare)

Krav i TEHDAS2. M7.4

- *SPER-6. Project-based user environments of SPE MUST be isolated from each other and open Internet.*
- *SPER-7. Authorised users MUST protect sensitive data they display.*
- *SPER-8. Authorised users MUST interact with their SPE project space only through secure protocols.*

Roller:

- ***SPE ansvarig.***
- ***SPE administratör.***
- ***Operatör.***
- ***Teknisk support.***
- ***Kontrollant.***
- ***Bearbetningsroller för stödsystem, anges när behov av och utformning av bearbetningsmiljö är klarlagd.***

IT-stöd: (*T.b.d.*)

- ***MFA. RBAC. Loggar. Övervakning.***
- ***Funktions komponenter för bearbetning. T.b.d.***
- ***Säkra bas Infra tjänster Tex DNSSEC, etc.***
- ***Meddelandesystem.***
- ***Krypterad överföring.***
- ***Orchestrator för tjänster.***
- ***Ostrukturerad lagring Tiering, replikering & kryptering.***
- ***Ransomware skydd.***
- ***Databas med kryptering.***
- ***Server & virtualisering.***
- ***Brandväggar i tieringdesign.***
- ***Microsegmentering.***
- ***SAN lagring, tiering, replikering & kryptering.***
- ***DC Lan Fysisk & virtuell.***
- ***ADC: Application delivery controller.***
- ***API gateway.***
- ***Tjänste-provisionering.***

MFA. RBAC. Loggar. Övervakning.

MFA (Multi-Factor Authentication) stärker säkerheten genom att kräva flera sätt att bekräfta en användares identitet, till exempel både lösenord och en engångskod via mobil. RBAC (Role-Based Access Control) innebär att åtkomsträttigheter styrs utifrån användarens roll i organisationen, vilket minimerar risken för obehörig åtkomst. Loggar används för att registrera händelser i systemet, vilket möjliggör spårbarhet, felsökning och säkerhetsanalys. Övervakning handlar om att kontinuerligt följa systemens hälsa och aktivitet för att snabbt upptäcka avvikelser, prestandaproblem eller säkerhetshot.

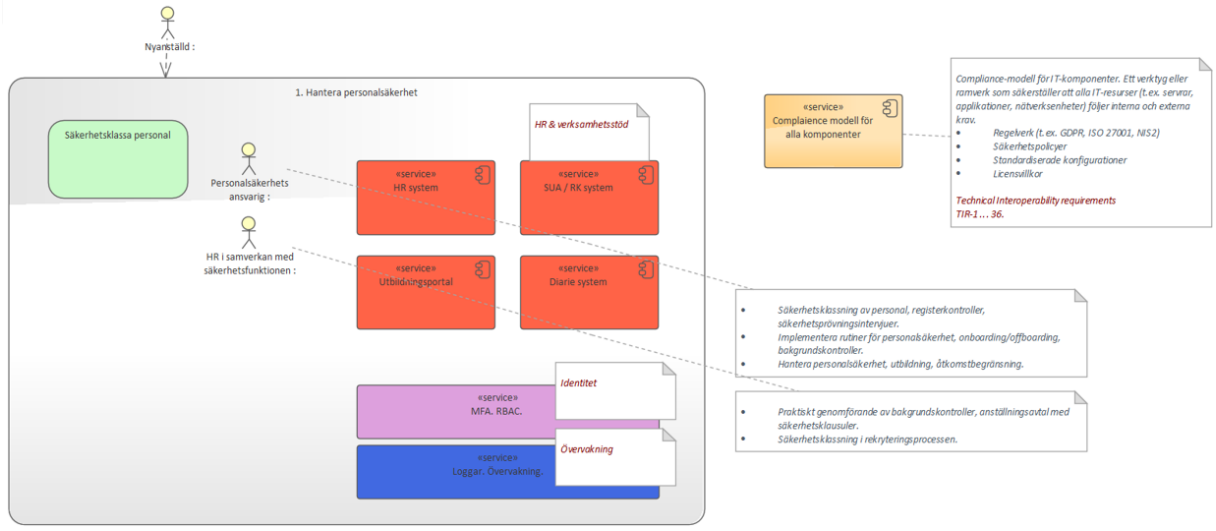
Huvudförmåga 2. Hantera personalsäkerhet

För att upprätthålla hög säkerhet hanteras personalens livscykel systematiskt. Innan anställning genomförs bakgrundskontroller och screening för att verifiera lämplighet och tillförlitlighet. Under anställningen erbjuds kontinuerlig

säkerhetsutbildning och medvetenhetsprogram för att stärka kunskap och minska risker. Vid avslut eller byte av anställning säkerställs en strukturerad hantering av avslut och rollförändringar, inklusive återlämning av utrustning och borttagning av åtkomsträttigheter.

Krav i TEHDAS2. M7.4:

- *SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.*
- *OPR-23. Health data users, HDAB staff and SPE Operator staff who interact with the SPE MUST receive detailed, role-specific information or training covering health data processing, EHDS compliance requirements and security best practices coming from GDPR.*



Förmågor:

Säkerhetsklassning av personal.

Säkerhetsklassning handlar om att bedöma och fastställa vilken nivå av säkerhetstillit en individ behöver för att kunna utföra sina arbetsuppgifter, särskilt i miljöer där känslig information eller kritiska system hanteras. Syftet är att säkerställa att varje medarbetare har en säkerhetsnivå som är anpassad till både arbetsuppgifterna och den åtkomst till information som rollen kräver.

Roller:

Personalsäkerhetsansvarig.

Rollen ansvarar för att säkerställa en hög nivå av personalsäkerhet inom organisationen. Detta omfattar genomförande av säkerhetsklassning av personal, registerkontroller och säkerhetsprövningsintervjuer. Vidare ingår att implementera rutiner för personalsäkerhet, inklusive onboarding och offboarding-processer samt bakgrundskontroller. Rollen hanterar även kontinuerlig personalsäkerhet genom utbildning, medvetenhetsinsatser och åtkomstbegränsning för att minimera risker och skydda känslig information.

HR i samverkan med säkerhetsfunktionen.

HR arbetar nära säkerhetsfunktionen för att säkerställa personalsäkerhet genom hela anställningsprocessen. Detta omfattar det praktiska genomförandet av bakgrundskontroller samt utformning av anställningsavtal med relevanta säkerhetsklausuler. Dessutom integreras säkerhetsklassning som en del av rekryteringsprocessen för att säkerställa att rätt nivå av säkerhetstillit tillämpas för varje roll.

IT-stöd:

HR system

HR-system (Human Resources System) är ett digitalt verktyg som används för att hantera personalrelaterade processer inom en organisation. Det fungerar som ett centralt system för att stödja HR-avdelningen i allt från rekrytering till lönehantering och kompetensutveckling.

SUA/RK system

SUA står för Säkerhetsskyddad Upphandling med säkerhetsskyddsavtal, och RK står för Registerkontroll. Dessa används inom upphandlingar och samarbeten där säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerade uppgifter hanteras.

Utbildningsportal

En utbildningsportal är en digital plattform som används för att planera, genomföra och följa upp utbildningar inom en organisation eller för externa användare. Den fungerar som ett centralt nav för lärande och kompetensutveckling.

Diariesystem

Ett diariesystem är ett digitalt system som används för att registrera, organisera och spåra ärenden och dokument inom en organisation, särskilt inom offentlig sektor. Det är ett centralt verktyg för att säkerställa transparens, spårbarhet och rättssäker hantering av information.

MFA. RBAC. Loggar. Övervakning.

MFA (Multi-Factor Authentication) stärker säkerheten genom att kräva flera sätt att bekräfta en användares identitet, till exempel både lösenord och en engångskod via mobil. RBAC (Role-Based Access Control) innebär att åtkomsträttigheter styrs utifrån användarens roll i organisationen, vilket minimerar risken för obehörig åtkomst. Loggar används för att registrera händelser i systemet, vilket möjliggör spårbarhet, felsökning och säkerhetsanalys. Övervakning handlar om att kontinuerligt följa systemens hälsa och aktivitet för att snabbt upptäcka avvikelser, prestandaproblem eller säkerhetshot.

Huvudförmåga 3. Hantera organisationens identiteter, autentisering och auktorisation

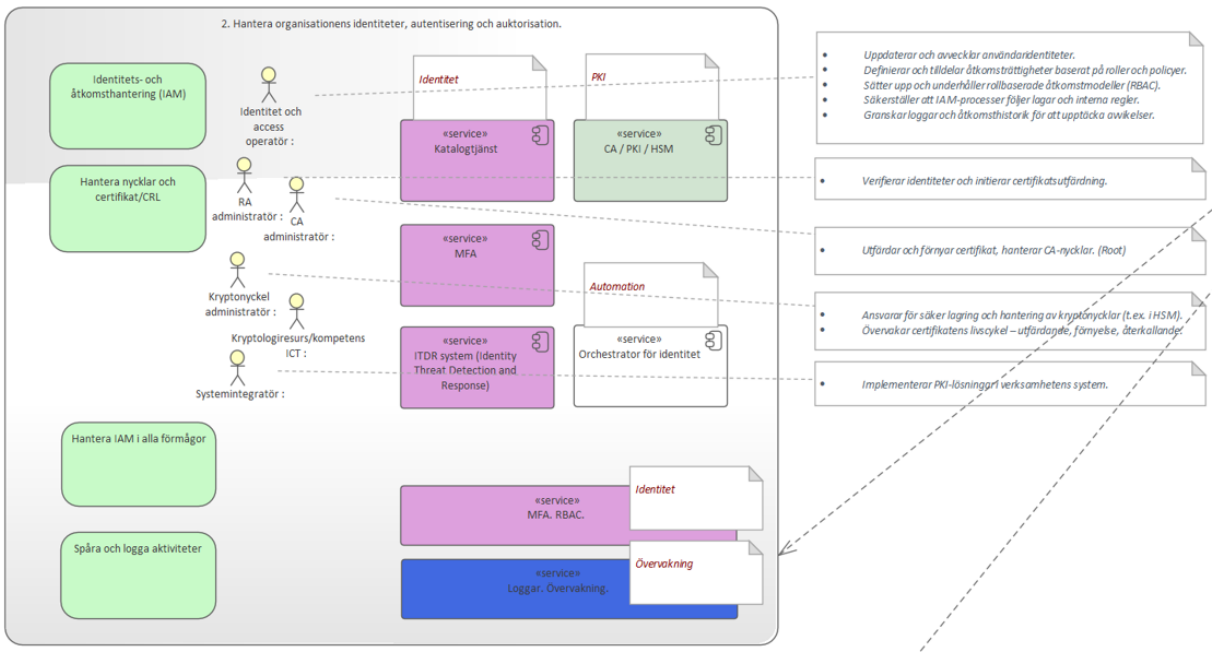
Behörigheter, digitala identiteter och autentisering.

SPE ska säkerställa att endast behöriga användare och informationssystem har åtkomst till IT-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.

Behörighetshanteringen bör säkerställa att digitala identiteter i produktionsmiljön är unika, digitala identiteter och behörigheter är godkända innan de kopplas till en användare eller ett informationssystem, tilldelade behörigheter är tidsbegränsade och kontrolleras en gång per år, behovet av att använda olika kataloger för digitala identiteter och behörigheter är identifierat och hanterat, och att olika digitala identiteter används vid åtkomst till utvecklings- och testmiljö respektive produktionsmiljö.

En digital identitet bör endast användas av en individ. Digitala identiteter och behörigheter som ger tillgång till externt åtkomliga informationssystem samt utvecklings-, test- och utbildningsmiljö bör hanteras i olika kataloger skilda från kataloger för produktionsmiljön.

Krav i TEHDAS2. M7.4: SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.



Förmågor:

Identitets- och åtkomsthantering (IAM)

Organisationen ska upprätta en tydlig åtkomstkontrollpolicy som definierar principer och riktlinjer för hantering av åtkomsträttigheter. Användaråtkomsthantering omfattar att tilldela, ändra och avlägsna åtkomsträttigheter och privilegier i enlighet med fastställda behov och säkerhetskrav. Det är också viktigt att säkerställa att alla användare förstår sitt ansvar när det gäller åtkomstkontroll, inklusive att skydda sina autentiseringsuppgifter och följa gällande rutiner.

Krav i TEHDAS2. M7.4:

- *SDR-2. Service administrators SHOULD NOT have access to sensitive data.*
- *OPR-2. SPE Operator MUST limit the number of authorised staff and any subcontractors who have high-privileged access enabling them to access or process health data and MUST implement effective procedures for managing and monitoring such access within the SPE infrastructure.*
- *OPR-23. Health data users, HDAB staff and SPE Operator staff who interact with the SPE MUST receive detailed, role-specific information or*

training covering health data processing, EHDS compliance requirements and security best practices coming from GDPR.

Hantera nycklar och certifikat/CRL

Organisationen ska definiera tydliga regler och riktlinjer för nyckel- och certifikathantering. Nycklar ska skapas med starka algoritmer som uppfyller godkända säkerhetsstandarder och lagras i säkra miljöer, exempelvis HSM eller krypterade lagringslösningar. Distribution av nycklar ska ske via säkra kanaler, och rutiner för regelbunden nyckelrotation, backup, återställning samt säker radering av nycklar som inte längre används ska finnas på plats.

Certifikathantering omfattar att skapa eller erhålla certifikat från betrodda certifikatutfärdare (CA) och placera dem på rätt system och tjänster. Det är viktigt att kontinuerligt validera certifikatens giltighet och CA:s betroddhet, samt att uppdatera certifikat innan de löper ut. Komprometterade eller inaktuella certifikat ska spärras omedelbart. För att minska risken för manuella fel och driftstopp bör automatiserade verktyg användas för hantering av nycklar, certifikat och spärrlistor (CRL).

Alla aktiviteter som rör nyckel- och certifikathantering ska spåras och loggas på ett säkert sätt. Detta inkluderar skapande, distribution, rotation, återställning och radering av nycklar samt utfärdande, förnyelse och spärrning av certifikat. Loggarna ska skyddas mot manipulation och granskas regelbundet för att upptäcka avvikelser eller misstänkt aktivitet. Spårbarhet är avgörande för att uppfylla krav på revision, incidenthantering och efterlevnad av säkerhetsstandarder.

Spåra och logga aktiviteter

För att säkerställa transparens, ansvar och efterlevnad av säkerhetskrav ska organisationen ha etablerade rutiner för spårning och loggning av aktiviteter. Alla kritiska system och processer ska generera loggar som dokumenterar åtkomst, ändringar och andra relevanta händelser. Loggarna ska skyddas mot manipulation, lagras på ett säkert sätt och granskas regelbundet för att upptäcka avvikelser, misstänkt beteende eller potentiella säkerhetsincidenter. Spårbarhet är en grundläggande komponent för revision, incidenthantering och kontinuerlig förbättring av säkerhetsarbetet.

Krav i TEHDAS2. M7.4:

- *OPR-15. SPEs SHOULD track and log actions of each authorised team member, including instances of data access, processing, viewing and output.*
- *SPER-9. All APIs connecting SPE components MUST be logged and monitored*

- *EHDSR-6. All access and operation logs of SPE MUST be available for verification and auditing. EHDSR-7. All SPE logs MUST identify the actor. EHDSR-8. All SPE logs MUST be kept at least for one year.*
- *OPR-7. SPE Operator MUST retain logs and access records to ensure traceability of all operations and enable audits or investigations when needed.*

Hantera IAM i alla förmågor

IAM är en central säkerhetsfunktion som styr vem som får åtkomst till vad, när och hur. För att fungera effektivt måste IAM integreras i alla organisationens förmågor och IT-tjänster, från interna system till molntjänster och externa integrationer.

Roller:

Identitet och access-operatör.

Rollen ansvarar för att hantera användaridentiteter och åtkomsträttigheter inom organisationen. Detta innefattar att uppdatera och avveckla identiteter samt definiera och tilldela åtkomsträttigheter baserat på roller och fastställda policyer. Operatören sätter upp och underhåller rollbaserade åtkomstmodeller (RBAC) för att säkerställa en strukturerad och säker hantering av behörigheter. Vidare ansvarar rollen för att IAM-processer följer gällande lagar, regelverk och interna riktlinjer. En viktig del av arbetet är att regelbundet granska loggar och åtkomsthistorik för att upptäcka avvikelser och minimera säkerhetsrisker.

RA administratör.

Verifierar identiteter och initierar certifikatsutfärdning.

CA administratör.

Utfärdar och förnyar certifikat, hanterar CA-nycklar.

Kryptonyckel administratör.

Rollen ansvarar för säker lagring och hantering av kryptonycklar, exempelvis i hårdvarubaserade säkerhetsmoduler (HSM), för att skydda mot obehörig åtkomst och manipulation. En central uppgift är att övervaka certifikatens livscykel, vilket inkluderar utfärdande, förnyelse och återkallande av certifikat i enlighet med organisationens säkerhetspolicy och gällande standarder.

Kryptologiresurs/kompetens ICT.

Specialistfunktion med fokus på att säkerställa att organisationens informations- och kommunikationssystem använder robusta kryptografiska lösningar.

Tillhandahåller expertkunskap inom kryptografi och säker kommunikation för att skydda data, autentisera användare och upprätthålla integritet i ICT-miljöer.

- Utforma och granska kryptografiska lösningar i system och applikationer.
- Säkerställa korrekt nyckel- och certifikathantering (PKI, HSM, CRL, OCSP).
- Rådgivning vid val av algoritmer och protokoll (TLS, IPsec, AES, RSA, ECC).
- Bedöma risker och sårbarheter i kryptosystem.
- Stöd incidenthantering vid kryptorelaterade problem.

Systemintegratör.

Implementerar PKI-lösningar i verksamhetens system.

IT-stöd:

Katalogtjänst.

En katalogtjänst är ett IT-system som används för att lagra, organisera och tillhandahålla information om användare, datorer, resurser och behörigheter i ett nätverk. Den fungerar som en central adressbok och identitetshanterare inom en organisation.

ITDR system (Identity Threat Detection and Response).

ITDR är en säkerhetslösning som fokuserar på att identifiera, övervaka och hantera hot mot identiteter och åtkomstsystem i en IT-miljö. Det kompletterar traditionella säkerhetslösningar genom att fokusera på identitetsbaserade attacker, som ofta utnyttjar stulna inloggningsuppgifter eller felaktiga behörigheter.

MFA.

Ett MFA-system är en säkerhetslösning som kräver att användare verifierar sin identitet med minst två olika typer av autentisering innan de får åtkomst till ett system eller en tjänst. Det kombinerar något användaren vet (t.ex. lösenord), något användaren har (t.ex. mobiltelefon eller säkerhetsnyckel), och/eller något användaren är (t.ex. fingeravtryck eller ansiktsigenkänning).

Orchestrator för identitet.

Ett ramverk för att orkestrera identitetsprocesser mellan olika system.

En Orchestrator för identitetssystem är en central komponent som samordnar och automatiserar hanteringen av digitala identiteter och åtkomsträttigheter i en organisation. Det fungerar som en "dirigent" som kopplar samman olika identitets- och åtkomstsystem (t.ex. AD, HR-system, molntjänster) för att säkerställa att rätt personer har rätt behörigheter vid rätt tidpunkt.

Orchestratorn är en säkerhetshöjande produkt som tillsammans med provisioneringssystem i de olika områdena minskar behovet av daglig administrativ åtkomst och höjer säkerheteten där åtgärder sker repetitivt utan påverkan från mänsklig faktor.

CA / PKI / HSM.

CA (Certificate Authority) är en betrodd part som utfärdar digitala certifikat för att bekräfta identiteter i ett nätverk. Dessa certifikat används inom PKI (Public Key Infrastructure), som är ett ramverk för att hantera krypteringsnycklar och möjliggöra säker kommunikation, autentisering och digitala signaturer. För att skydda de privata nycklarna som används i PKI används ofta en HSM (Hardware Security Module), vilket är en fysisk enhet som säkert genererar, lagrar och hanterar kryptografiska nycklar. Tillsammans utgör CA, PKI och HSM grunden för säker digital identitetshantering och dataskydd.

RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 4. Hantera krypterad digital kommunikation samt externa identiteter och signaturer

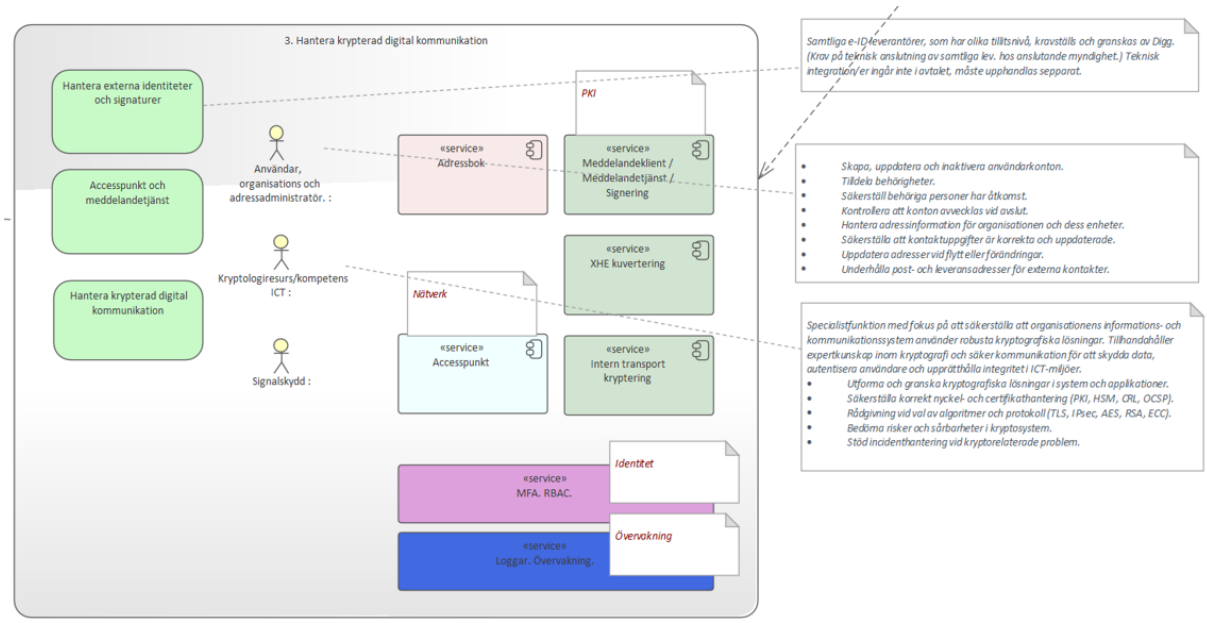
Organisationen ska säkerställa att all informationsöverföring, både inom och utanför organisationen, sker på ett säkert sätt. Detta innebär att använda krypterade kommunikationskanaler, autentisering av parter och skydd mot obehörig åtkomst eller manipulation av data under överföring. Säkerhetsåtgärder ska omfatta både elektroniska kommunikationsmedel, såsom e-post och nätverkstrafik, samt fysiska överföringsmetoder. Rutiner för spårning och loggning av överföringar ska finnas för att möjliggöra revision och upptäcka avvikelser.

När externa parter ges åtkomst till organisationens system eller information, ska deras identitet verifieras genom stark autentisering. Behörigheter ska tilldelas enligt principen om minsta privilegium och vara strikt begränsade till det som krävs för uppdragets genomförande. Åtkomst ska vara tidsbegränsad och regelbundet granskas. Rutiner för hantering av externa identiteter ska säkerställa att åtkomsträttigheter avvecklas omedelbart när behovet upphör.

Krav i TEHDAS2. M7.3: T.b.d.

Krav i TEHDAS2. M7.4:

- *SDR-3. Sensitive data MUST be in a protected format at rest and in transit.*
- *SDR-4. Sensitive data protection MUST be done with widely accepted, secure algorithms combined with effective isolation measures.*
- *SPER-3. It MUST be possible to transfer sensitive data between, in and out of SPEs.*
- *SPER-8. Authorised users MUST interact with their SPE project space only through secure protocols.*
- *OPR-26. SPE Operator SHOULD define SLAs that include: uptime guarantees, response/resolution times for incidents include security SLAs, such as data encryption guarantees, incident response times, and audit logging.*



Förmågor:

Hantera externa identiteter och signaturer.

Hantera externa användares (behöriga till bearbetningsytan) identiteter.

Krav i TEHDAS2. M7.4:

- *SDR-1. Unauthorised users MUST NOT be able to access sensitive . data.*
- *SPER-9. All APIs connecting SPE components MUST be logged and monitored.*
- *EHDSR-5. Authorised health data users MUST be strongly identified.*

- *OPR-1. The SPE operator MUST have procedures in place to enforce user authentication and access restrictions based on the data permit associated with the processing of health data.*

Hantera accesspunkt och meddelandetjänst.

Säker kommunikation bygger på att data krypteras, autentiseras och integriteten bevaras vid överföring mellan parter. Externt innebär detta att organisationen använder protokoll för att skydda trafik mot tredje part, samt att certifikat från betrodda CA används för att verifiera identitet. Intern kommunikation kräver samma skyddsnivå, särskilt vid vidarebefordran av meddelanden eller data mellan interna system, för att undvika läckage eller manipulation.

Vid vidarebefordran är det viktigt att säkerställa att meddelandet inte förlorar sin ursprungliga säkerhetsnivå. Detta kan göras genom end-to-end-kryptering, där innehållet förblir krypterat även om det passerar flera noder, samt genom att använda digitala signaturer för att bekräfta avsändarens identitet och integritet. Organisationen implementerar policyer som styr hur och när vidarebefordran får ske, samt logga alla händelser för spårbarhet.

För att uppnå detta krävs en kombination av tekniska lösningar (PKI, certifikat, krypteringsprotokoll), processer (nyckel- och certifikathantering, revokering) och utbildning av personal. Automatisering av certifikatförnyelse och status kontroller via OCSP eller CRL är avgörande i säker kommunikation.

Krav i TEHDAS2. M7.4:

- *SDR-3. Sensitive data MUST be in a protected format at rest and in transit.*
- *SDR-4. Sensitive data protection MUST be done with widely accepted, secure algorithms combined with effective isolation measures.*
- *SPER-3. It MUST be possible to transfer sensitive data between, in and out of SPEs.*
- *SPER-8. Authorised users MUST interact with their SPE project space only through secure protocols.*

Hantera funktioner i bearbetningsytans förmåga gällande säker kommunikation och identifikation samt behörigheter.

Roller:

Användar, organisations och adressadministratör.

Rollen ansvarar för att hantera användaridentiteter och adressinformation. Detta innefattar att skapa, uppdatera och inaktivera användarkonton samt tilldela behörigheter i enlighet med fastställda roller och policyer. Administratören ska säkerställa att endast behöriga personer har åtkomst till system och information, samt att konton avvecklas omedelbart vid avslut eller förändring av anställning.

Utöver identitetshantering ansvarar rollen för att underhålla korrekt adressinformation för organisationen och dess enheter. Detta inkluderar att säkerställa att kontaktuppgifter är aktuella och uppdaterade, hantera adressändringar vid flytt eller organisatoriska förändringar samt underhålla post- och leveransadresser för externa kontakter.

Kryptologiresurs/kompetens ICT.

Specialistfunktion med fokus på att säkerställa att organisationens informations- och kommunikationssystem använder robusta kryptografiska lösningar. Tillhandahåller expertkunskap inom kryptografi och säker kommunikation för att skydda data, autentisera användare och upprätthålla integritet i ICT-miljöer.

- Utforma och granska kryptografiska lösningar i system och applikationer.
- Säkerställa korrekt nyckel- och certifikathantering (PKI, HSM, CRL, OCSP).
- Rådgivning vid val av algoritmer och protokoll (TLS, IP sec, AES, RSA, ECC).
- Bedöma risker och sårbarheter i kryptosystem.
- Stöd incidenthantering vid kryptorelaterade problem.

Signalskyddsadministratör.

Hantering av kryptonycklar, kryptohandlingar och signalskyddsutrustning relaterat signalskydd.

IT-stöd:

Meddelandeklient / Meddelandetjänst / Signering.

En meddelandeklient är ett program eller en tjänst som används för att skicka, ta emot och hantera meddelanden, via e-post eller interna kommunikationssystem. En meddelandetjänst är den bakomliggande infrastrukturen som möjliggör själva överföringen av meddelanden mellan användare och/eller system. Signering innebär att ett meddelande eller dokument digitalt signeras med en privat nyckel för att säkerställa avsändarens identitet och att innehållet inte har manipulerats. Tillsammans bidrar dessa komponenter till säker och spårbar kommunikation inom och mellan organisationer.

Detta behöver anpassas så snart vi vet behov och krav på bearbetningsmiljön. Troligen är inte meddelandetjänsterna tillräckliga utan detta område behöver vävas ihop med en API gateway lösning.

Accesspunkt.

En accesspunkt i detta sammanhang är en teknisk komponent som fungerar som en säker inkörsport till ett system eller en tjänst, ofta inom ramen för meddelandetjänster och digital kommunikation. Den tar emot, validerar och

vidarebefordrar meddelanden – ofta i standardiserade format mellan olika organisationer och system. I kombination med meddelandeklienter, meddelandetjänster och digital signering säkerställer accesspunkten att kommunikationen är säker, spårbar och interoperabel, särskilt i miljöer där olika aktörer behöver utbyta känslig information, som inom offentlig sektor eller e-förvaltning.

Adressbok.

En adressbok i detta sammanhang är en digital katalog över organisationer, system eller mottagare som används av meddelandeklienter och accesspunkter för att kunna routa meddelanden korrekt. Den innehåller information som identifierare, tekniska adresser och certifikat, och används för att säkerställa att meddelanden skickas till rätt mottagare på ett säkert sätt. I kombination med meddelandetjänster, signering och accesspunkter möjliggör adressboken tillförlitlig och automatiserad kommunikation mellan olika parter i ett integrerat system.

XHE kuvertering.

XHE-kuvertering är en teknik som används för att paketera och strukturera meddelanden i ett standardiserat format innan de skickas via en meddelandetjänst. Det säkerställer att innehållet är korrekt formaterat, signerat och klart för överföring via en accesspunkt till rätt mottagare, enligt information i adressboken. Kuverteringen inkluderar ofta metadata, säkerhetsinformation och själva nyttolasten, vilket gör det möjligt att hantera meddelanden på ett säkert och spårbart sätt i system för elektronisk kommunikation mellan organisationer.

Intern transportkryptering.

Intern transportkryptering används för att skydda data som skickas inom ett system eller mellan interna komponenter, till exempel mellan applikationer, databaser och tjänster i ett datacenter eller molnmiljö. Till skillnad från extern kommunikation – där XHE-kuvertering, accesspunkter och adressböcker används för säker överföring mellan organisationer – fokuserar intern transportkryptering på att förhindra att data avlyssnas eller manipuleras inom det egna nätverket. Den bygger ofta på protokoll som TLS och används som en del av en "zero trust"-strategi för att säkerställa att även intern trafik är krypterad och verifierad.

MFA. RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

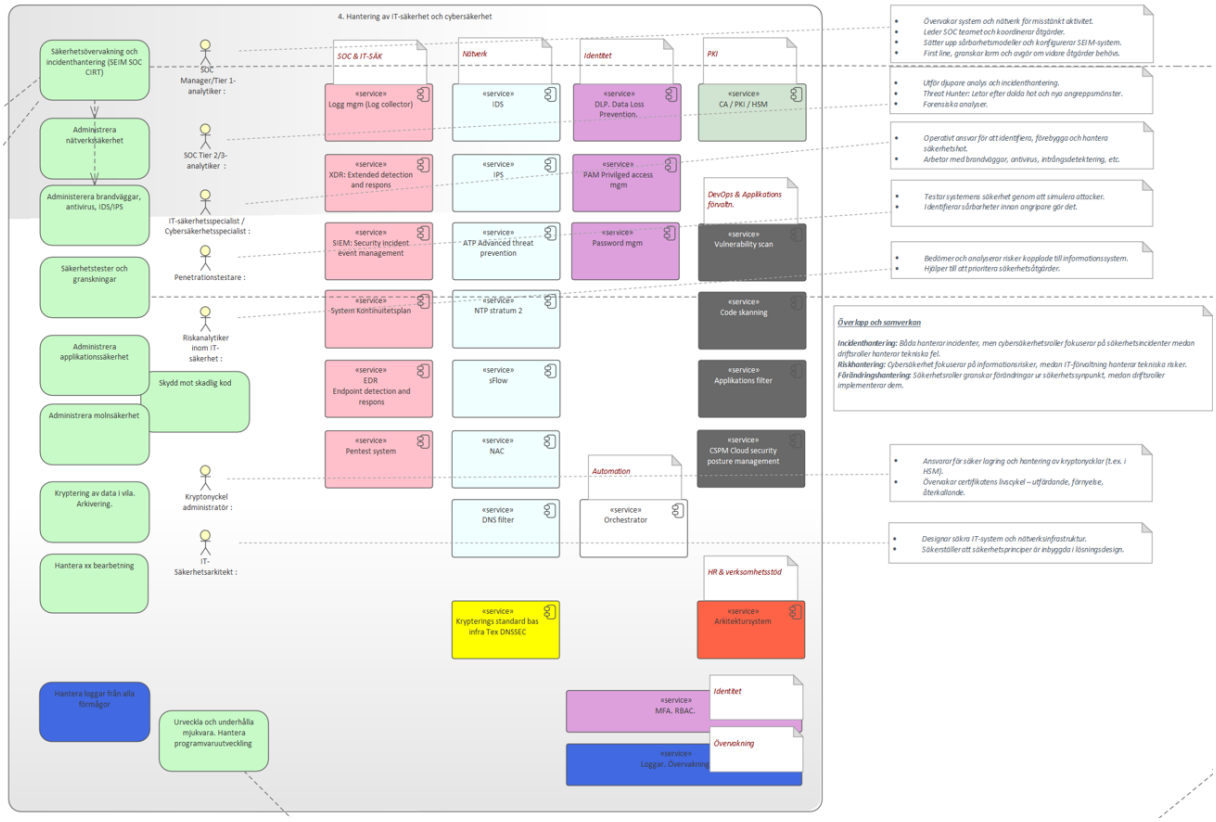
Huvudförmåga 5. Hantera IT-säkerhet och cybersäkerhet

Organisationen ska etablera ett systematiskt arbete för att identifiera, förebygga, upptäcka och hantera IT- och cybersäkerhetsrisker. Detta omfattar

implementering av tekniska skyddsåtgärder såsom brandväggar, intrångsdetektering, antiviruslösningar och segmentering av nätverk. Rutiner för incidenthantering ska finnas och inkludera snabb respons, analys och återställning vid säkerhetsincidenter. Organisationen ska även genomföra regelbundna sårbarhetsanalyser, penetrationstester och uppdateringar av säkerhetslösningar för att möta nya hot. Säkerhetsövervakning ska ske kontinuerligt och loggar ska granskas för att upptäcka avvikelser i realtid.

Krav i TEHDAS2. M7.4.

- *SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.*
- *OPR-25. The SPE Operator MUST implement cybersecurity procedures to regularly evaluate the effectiveness of risk-management measures and promote fundamental cybersecurity practices and provide necessary training.*



Förmågor:

Säkerhetsövervakning och incidenthantering (SEIM SOC CIRT).

Krav i TEHDAS2. M7.4:

- *OPR-6. SPEs MUST retain logs and access records to ensure traceability of all operations and enable audits or investigations when needed.*
- *SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.*
- *SPER-9. All APIs connecting SPE components MUST be logged and monitored.*
- *EHDSR-6. All access and operation logs of SPE MUST be available for verification and auditing.*
- *EHDSR-7. All SPE logs MUST identify the actor.*
- *EHDSR-8. All SPE logs MUST be kept at least for one year.*
- *EHDSR-9. TOMs of SPEs MUST be monitored for security.*
- *OPR-7. SPE Operator MUST retain logs and access records to ensure traceability of all operations and enable audits or investigations when needed.*
- *OPR-16. SPE Operator MUST track and log actions of each authorised project member, including instances of data access, processing, viewing and output.*
- *OPR-17. SPE Operator MUST implement a secure storage process to retain logs of user access to the SPE for a minimum period of one year.*
- *OPR-18. A reporting process MUST be in place to notify HDABs and relevant authorities of security incidents or non-compliance findings including data breaches or misuse.*

Hantera loggar från alla förmågor.

Administrera nätverkssäkerhet.

Krav i TEHDAS2. M7.4:

- *SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.*
- *OPR-22. SPE operator MUST adopt robust security measures to protect data, including the use of firewalls, encryption, and intrusion detection systems, in order to prevent unauthorised access, modification, or removal of sensitive information.*

Administrera brandväggar, antivirus, IDS/IPS.

Krav i TEHDAS2. M7.4: OPR-22. SPE operator MUST adopt robust security measures to protect data, including the use of firewalls, encryption, and intrusion detection systems, in order to prevent unauthorised access, modification, or removal of sensitive information.

Säkerhetstester och granskningar.

Administrera applikationssäkerhet.

Krav i TEHDAS2. M7.4:

- *OPR-28. The SPE operator MUST implement a formal patch management policy to identify, evaluate, and apply security patches in a timely manner based on severity.*
- *OPR-29. SPE Operator MUST establish a system update process to ensure timely and secure updates of software, OS, and firmware, tested prior to deployment.*

Skydd mot skadlig kod.

Administrera molnsäkerhet.

Krav i TEHDAS2. M7.4: SPER-4. SPE MUST provide adequate protection against exposing sensitive data to unauthorised users.

Kryptering av data i vila. Arkivering.

Krav i TEHDAS2. M7.4:

- *SDR-3. Sensitive data MUST be in a protected format at rest and in transit.*
- *SDR-4. Sensitive data protection MUST be done with widely accepted, secure algorithms combined with effective isolation measures.*
- *OPR-24. The SPE Operator MUST implement strategies for backup management, disaster recovery, and crisis management.*

Utveckla och underhålla mjukvara. Hantera programvaruutveckling.

Det är systemutvecklarens ansvar att för aktuellt IT-system påvisa såväl ATT kravuppfyllnad föreligger som HUR kravuppfyllnad erhålls för de funktionella kraven.

Hantera funktioner i bearbetningsytan gällande IT-säkerhet och cybersäkerhet.

Roller:

SOC Manager/Tier 1-analytiker.

Rollen ansvarar för att övervaka organisationens system och nätverk för att upptäcka misstänkt aktivitet och potentiella säkerhetsincidenter. Som SOC Manager leder personen säkerhetsoperationscentret (SOC), koordinerar åtgärder vid incidenter och säkerställer att teamet arbetar effektivt. Rollen omfattar även att sätta upp sårbarhetsmodeller, konfigurera och underhålla SIEM-system för att möjliggöra effektiv övervakning och analys.

I funktionen som Tier 1-analytiker agerar personen som första linjens försvar, vilket innebär att granska inkommande larm, bedöma deras relevans och avgöra om vidare åtgärder krävs. Rollen samarbetar nära med logghantering och andra anslutande funktioner för att säkerställa korrekt incidentrespons och kontinuerlig förbättring av säkerhetsprocesser.

SOC Tier 2/3-analytiker.

Rollen ansvarar för avancerad analys och hantering av säkerhetsincidenter. Som Tier 2/3-analytiker utför personen djupgående utredningar av larm och incidenter, identifierar rotorsaker och föreslår åtgärder för att minimera risker. En viktig del av arbetet är att agera som *Threat Hunter* genom att proaktivt söka efter dolda hot, nya angreppsmönster och indikatorer på kompromettering i organisationens miljö. Rollen omfattar även forensiska analyser för att samla och tolka digitala bevis vid incidenter, vilket är avgörande för både intern utredning och eventuell rättslig process.

IT-säkerhetsspecialist / Cybersäkerhetsspecialist.

Rollen har ett operativt ansvar för att identifiera, förebygga och hantera säkerhetshot mot organisationens IT-miljö. Detta innefattar att implementera och underhålla skyddsåtgärder. Specialisten arbetar proaktivt med att analysera risker, övervaka nätverk och system samt vidta åtgärder för att minimera sårbarheter och säkerställa kontinuerlig drift. Rollen är central för att upprätthålla en robust cybersäkerhetsnivå och samarbetar ofta med andra funktioner inom IT och säkerhet för att hantera incidenter och förbättra organisationens säkerhetsarkitektur.

Penetrationstestare.

Rollen ansvarar för att testa organisationens system och applikationer genom att simulera verkliga attacker för att identifiera sårbarheter innan angripare gör det. Penetrationstestaren använder både manuella och automatiserade metoder för att utvärdera säkerhetsnivån, dokumentera upptäckta brister och ge rekommendationer för åtgärder. Arbetet är avgörande för att stärka organisationens motståndskraft mot cyberhot och säkerställa att säkerhetskontroller fungerar som avsett.

Riskanalytiker inom IT-säkerhet.

Rollen ansvarar för att bedöma och analysera risker kopplade till organisationens informationssystem och IT-infrastruktur. Riskanalytikern identifierar potentiella hot, sårbarheter och konsekvenser för verksamheten, samt hjälper till att prioritera säkerhetsåtgärder baserat på risknivå och affärskritikalitet. Arbetet innefattar att ta fram riskanalyser, stödja beslutsfattare med underlag för säkerhetsinvesteringar och bidra till att organisationen uppfyller relevanta regelverk och standarder.

Kryptonyckel administratör.

Rollen ansvarar för säker lagring och hantering av kryptonycklar, exempelvis i hårdvarubaserade säkerhetsmoduler (HSM), för att skydda mot obehörig åtkomst och manipulation. En central uppgift är att övervaka certifikatens livscykel, vilket omfattar utfärdande, förnyelse och återkallande av certifikat i enlighet med organisationens säkerhetspolicy och gällande standarder. Rollen bidrar till att upprätthålla en robust kryptografisk infrastruktur och säker kommunikation inom organisationen.

IT-Säkerhetsarkitekt.

Rollen ansvarar för att designa säkra IT-system och nätverksinfrastrukturer som uppfyller organisationens krav på informationssäkerhet och efterlevnad av regelverk. IT-Säkerhetsarkitekten säkerställer att säkerhetsprinciper och bästa praxis är inbyggda i lösningsdesignen från början, vilket inkluderar riskanalys, val av tekniska skyddsåtgärder och integration av säkerhetskontroller i arkitekturen. Rollen fungerar som en strategisk rådgivare vid utveckling av nya system och vid förändringar i befintliga miljöer, med fokus på att skapa robusta och framtidssäkra lösningar.

IT-stöd:

Logg management (Log collector).

Logghantering (Log Management) med logginsamlare (Log Collector) innebär att samla in, centralisera och hantera loggar från olika system, applikationer och enheter i en organisation. En logginsamlare är en komponent eller tjänst som automatiskt hämtar loggdata från källor som servrar, nätverksenheter och säkerhetssystem, och skickar dem vidare till en central plattform för forensisk analys, övervakning och arkivering. Detta möjliggör spårbarhet, incidentdetektion och efterlevnad, och är ofta en grund för SIEM-lösningar (Security Information and Event Management). Bidrar även till förhöjd driftstabilitet via proaktiv analys av driftloggar.

XDR: Extended Detection and Response.

XDR (Extended Detection and Response) är en säkerhetslösning som samlar in och korrelerar data från flera källor som klienter, servrar, nätverk och molntjänster, för att upptäcka, analysera och svara på hot i hela IT-miljön. Till skillnad från traditionella verktyg som fokuserar på enskilda delar (t.ex. EDR för enheter), ger XDR en samlad vy över säkerhetshändelser, vilket förbättrar hotdetektion, förenklar incidenthantering och möjliggör snabbare respons. XDR används ofta tillsammans med logghantering, övervakning och identitetsskydd för att skapa ett mer proaktivt och integrerat cyberskydd.

SIEM: Security Incident Event Management.

SIEM: Security Incident Event Management (logg och regel baserad detektering, automatisk hantering via SOAR) en säkerhetslösning som samlar in, analyserar och korrelerar loggar och händelsedata från olika IT-system i realtid. Syftet är att upptäcka säkerhetshot, analysera incidenter och stödja efterlevnad av regelverk. SIEM kombinerar funktioner för logghantering och övervakning med avancerad analys för att identifiera avvikelser och generera larm. Det är en central komponent i moderna säkerhetsövervakningsmiljöer och används ofta tillsammans med XDR, ITDR och logginsamlare för att skapa ett heltäckande skydd mot cyberhot.

NTP stratum 2.

NTP Stratum 2 är en nivå i hierarkin för Network Time Protocol (NTP), som används för att synkronisera klockor i datornätverk. En Stratum 2-server får sin tid från en Stratum 1-server, som i sin tur är direkt kopplad till en exakt tidskälla, till exempel en GPS-klocka eller atomur. Stratum 2-servrar fungerar som tidsförmedlare till andra system i nätverket och erbjuder en hög noggrannhet, ofta med bara millisekunders avvikelse från den ursprungliga källan. De används vanligtvis i organisationer för att säkerställa att alla system har korrekt och enhetlig tid, vilket är viktigt för loggning, säkerhet och systemkoordinering.

Password management.

Password management (lösenordshantering) handlar om att säkert skapa, lagra och hantera lösenord för användare och system. Ett password management-system hjälper till att generera starka lösenord, lagra dem krypterat och automatiskt fylla i dem vid inloggning. Det minskar risken för svaga eller återanvända lösenord och förenklar hanteringen för både användare och administratörer. Används ofta tillsammans med andra säkerhetslösningar som MFA och identitetshantering för att stärka den övergripande åtkomstsäkerheten.

Krypterings standard bas infra (DNSSEC).

DNSSEC är en säkerhetsstandard som skyddar DNS-systemet genom att använda digitala signaturer för att verifiera att DNS-information inte har manipulerats. Den är en del av basinfrastrukturen för internet och kompletteras av andra krypteringsstandarder som TLS för säkra webbanslutningar, IP sec för krypterad nätverkstrafik, och SSH för säker fjärråtkomst. Tillsammans bidrar dessa tekniker till att upprätthålla integritet, autenticitet och sekretess i digital kommunikation.

IDS.

Intrusion Detection System (IDS). Ett säkerhetssystem som övervakar nätverk eller system för misstänkt aktivitet eller policyöverträdelser. När ett sådant beteende upptäcks, skickar systemet varningar till administratörer eller loggar händelsen för vidare analys.

IPS.

Intrusion Prevention System (IPS). Ett nätverkssäkerhetssystem som upptäcker och förhindrar skadlig aktivitet i realtid. Det fungerar som en aktiv skyddsmekanism som inte bara varnar om hot (som ett IDS gör), utan också vidtar åtgärder automatiskt för att stoppa dem.

ATP Advanced Threat Prevention.

ATP (Advanced Threat Prevention) är en säkerhetslösning som används för att identifiera, blockera och reagera på avancerade cyberhot som traditionella antivirusprogram ofta missar. Den kombinerar flera tekniker, såsom beteendeanalys, maskininlärning och sandboxing tillsammans med redan kända attackmönster, för att upptäcka skadlig kod, nätfiske, ”zero day” attacker och andra sofistikerade hot i realtid. ATP används ofta i molntjänster, e-postskydd, endpoint-säkerhet och i nätverk för att ge ett proaktivt skydd mot moderna attacker.

System för kontinuitetsplan.

Ett system för kontinuitetsplanering syftar till att säkerställa att en organisation kan fortsätta sin verksamhet vid störningar, kriser eller katastrofer. Det omfattar identifiering av kritiska funktioner, riskbedömning, beredskapsplaner, återställningsstrategier och kommunikationsrutiner. Målet är att minimera avbrott, skydda resurser och snabbt återgå till normal drift. Ex. BCM-verktyg (Business Continuity Management) system som hjälper till att dokumentera, testa och uppdatera kontinuitetsplaner.

PAM Privileged Access Management

PAM (Privileged Access Management) är en säkerhetslösning som kontrollerar, loggar, övervakar och styr åtkomst till känsliga system och data för användare med höga behörigheter. Syftet är att minska risken för missbruk, dataintrång och interna hot genom att införa strikta kontroller för åtkomst och endpoint, tillfälligt ge åtkomst, logga aktiviteter och spela in sessioner samt använda multifaktor autentisering med rotation av användaruppgifter. PAM är centralt för att skydda kritiska IT-resurser i både lokala och molnbaserade miljöer.

Vulnerability Scan.

Ett vulnerability scan system är ett IT-säkerhetsverktyg som automatiskt identifierar sårbarheter i nätverk, system och applikationer. Det analyserar konfigurationer, programvaruversioner och kända svagheter för att upptäcka potentiella säkerhetsrisker. Syftet är att ge underlag för åtgärder innan sårbarheter kan utnyttjas av angripare.

Arkitektursystem.

Ett arkitektursystem inom IT är ett strukturerat ramverk som används för att planera, designa och dokumentera en organisations IT-landskap. Det stödjer beslutsfattande kring teknik, integration, säkerhet och verksamhetsbehov. Systemet hjälper till att visualisera samband mellan applikationer, data, infrastruktur och affärsprocesser, vilket underlättar styrning, förändringsarbete och långsiktig utveckling.

DLP Data Loss Prevention.

Data Loss Prevention (DLP) är en strategi och teknik som används för att förhindra att känslig information lämnar organisationen på ett otillbörligt sätt, oavsiktligt eller avsiktligt. DLP-system identifierar, övervakar och skyddar data i rörelse (t.ex. e-post), data i vila (t.ex. databaser) och data i användning (t.ex. dokument som öppnas och redigeras).

sFlow.

sFlow är en nätverksövervakningsteknik som samlar in statistik genom att slumpmässigt provta paket och gränssnittsinformation i realtid. Till skillnad från NetFlow, som registrerar hela trafikflöden, ger sFlow en bred och skalbar överblick över nätverksprestanda och användning. Det används för att upptäcka flaskhalsar, analysera trafikmönster och förbättra nätverkssäkerheten.

Orchestrator.

En orchestrator inom IT-säkerhet och infrastruktur är ett system som automatiserar, samordnar olika säkerhetsverktyg och processer, exempelvis ATP, PAM, sårbarhetsskanning och nätverksövervakning. Orchestratorn genomför repetitiva förändringar i säkerhetssystemen för att minska behovet av inloggning med högre behörigheter samt minimera säkerhetsrisken som finns vid misstag av människor. Syftet är att effektivisera incidenthantering, förbättra responsförmåga och minska manuellt arbete genom att koppla ihop och styra flera system från en central punkt. Orchestratorn möjliggör snabbare åtgärder vid hot och bättre överblick över säkerhetsläget.

EDR Endpoint detection and response.

EDR (Endpoint Detection and Response) är en säkerhetslösning som övervakar och analyserar aktiviteter på klienter och servrar (endpoints) för att upptäcka, undersöka och svara på hot i realtid. EDR samlar in data, identifierar misstänkt beteende och möjliggör snabb incidentrespons, vilket gör den till ett viktigt verktyg för att hantera avancerade attacker och förbättra organisationens cybersäkerhet.

NAC.

NAC (Network Access Control) är en säkerhetslösning som styr vilka enheter som får ansluta till ett nätverk. Den kontrollerar identitet, säkerhetsstatus och

policyefterlevnad innan åtkomst ges. NAC kan blockera, begränsa eller ge full tillgång beroende på enhetens tillstånd, vilket minskar risken för obehörig åtkomst och spridning av hot inom nätverket.

Code skanning.

Code-skanningsverktyg används för att automatiskt analysera källkod och identifiera säkerhetsbrister, buggar och kodstandardavvikelser. De hjälper utvecklare att upptäcka sårbarheter tidigt i utvecklingsprocessen, såsom SQL-injektioner, XSS eller osäker hantering av data. Verktygen kan vara statiska (analyserar kod utan att köra den) eller dynamiska (testar kod under körning) och är viktiga för att stärka applikationers säkerhet och kvalitet.

CSPM Cloud security posture management.

CSPM (Cloud Security Posture Management). System för att upptäcka avvikelser mot ”compliance standards”. Skanning efter sårbarheter och felkonfigurationer.

Pentest-system.

Pentest-system (penetrationstestverktyg) används för att simulera attacker mot IT-miljöer i syfte att identifiera sårbarheter innan verkliga angripare gör det. Systemet testar nätverk, applikationer och konfigurationer genom automatiserade och manuella metoder. Resultatet ger underlag för att stärka säkerheten.

CA / PKI / HSM.

CA (Certificate Authority) är en betrodd part som utfärdar digitala certifikat för att bekräfta identiteter i ett nätverk. Dessa certifikat används inom PKI (Public Key Infrastructure), som är ett ramverk för att hantera krypteringsnycklar och möjliggöra säker kommunikation, autentisering och digitala signaturer. För att skydda de privata nycklarna som används i PKI används ofta en HSM (Hardware Security Module), vilket är en fysisk enhet som säkert genererar, lagrar och hanterar kryptografiska nycklar. Tillsammans utgör CA, PKI och HSM grunden för säker digital identitetshantering och dataskydd.

Applikationsfilter.

Applikationsfilter är säkerhetsverktyg som kontrollerar och begränsar vilka applikationer som får köras eller kommunicera över nätverket (även på enheter så att felaktig kod inte kan exekveras). De används för att öka kontrollen över trafikflöden, minska risken för skadlig kod och förbättra efterlevnad av policyer. I kombination med system som EDR, NAC och sårbarhetsskanning bidrar applikationsfilter till ett starkare skydd mot både interna och externa hot.

MFA. RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 6. Hantera IT-förvaltning och driftsäkerhet

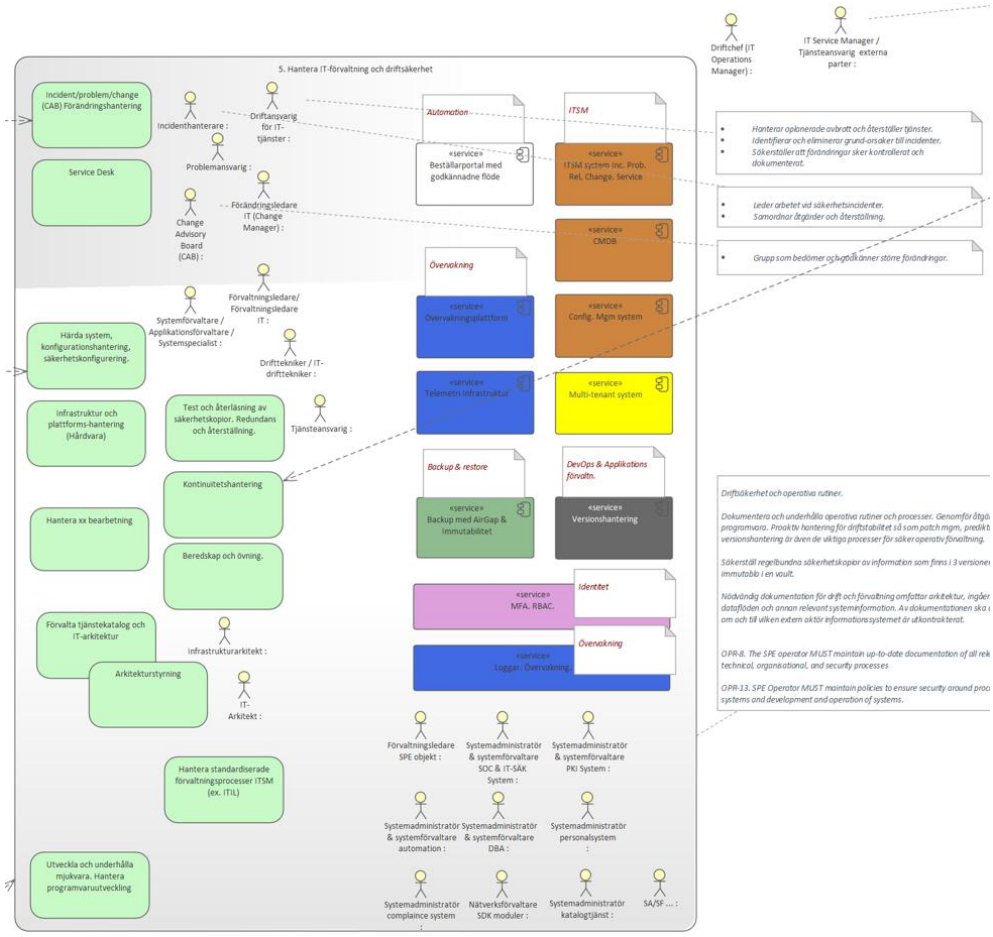
För att säkerställa driftsäkerhet och en robust IT-förvaltning ska organisationen etablera och underhålla dokumenterade operativa rutiner och processer. Dessa rutiner ska omfatta åtgärder för att skydda mot skadlig programvara, samt proaktiv hantering för driftstabilitet, såsom patchhantering, prediktiv driftanalys och kontinuerlig övervakning. Central versionshantering är en viktig komponent för att upprätthålla kontroll och spårbarhet i systemförvaltningen.

Regelbundna säkerhetskopior ska tas och finnas i tre versioner, varav en kopia är isolerad från nätverk (airgapad) och oföränderlig, lagrad i ett säkert lagringsutrymme. Detta minimerar risken för dataförlust vid incidenter.

Nödvändig dokumentation för drift och förvaltning ska inkludera systemarkitektur, ingående komponenter, konfigurationer, dataflöden och annan relevant information. Dokumentationen ska tydligt ange systemägare samt om och till vilken extern aktör informationssystemet är utkontrakterat. Detta är avgörande för ansvarsfördelning, spårbarhet och efterlevnad av regelverk.

Krav i TEHDAS2. M7.4:

- *OPR-8. The SPE operator MUST maintain up-to-date documentation of all relevant technical, organisational, and security processes.*
- *OPR-13. SPE Operator MUST maintain policies to ensure security around procurement systems and development and operation of systems.*



Förmågor:

Hantera standardiserade förvaltningsprocesser ITSM (ex. ITIL)

”TEHDAS2. M7.4 Draft technical, functional and security specifications of Secure Processing Environments” rekommenderar**:** FitSM (Free, Lightweight ITSM Standard.) https://www.fitsm.eu/

Incident/problem/change (CAB) Förändringshantering.

Krav på rapportering: Se till att incidenter rapporteras och hanteras effektivt (internt och externt).

Krav i TEHDAS2. M7.4:

- *OPR-17. A reporting process MUST be in place to notify HDABs and relevant authorities of security incidents or non-compliance findings including data breaches or misuse.*
- *OPR-14. SPEs SHALL adopt a release and deployment management process.*

- *OPR-11. SPE Operator SHOULD establish a Service Management System.*
- *OPR-14. SPEs SHOULD adopt change management process with impact and risk assessment.*
- *OPR-15. SPE Operator SHOULD adopt a release and deployment management process. OPR-30. A change management process SHOULD be used for assessing the impact of patches and updates before applying them to the production environment.*
- *OPR-31. SPE Operator MUST provide dedicated technical support with clearly defined SLAs and escalation paths for addressing incidents and technical issues.*

Service Desk.

Krav i TEHDAS2. M7.4:

- *OPR-31. SPE Operator MUST provide dedicated technical support with clearly defined SLAs and escalation paths for addressing incidents and technical issues.*
- *OPR-32. SPE Operator support staff SHOULD be trained in information security and privacy procedures, with roles and responsibilities clearly defined.*
- *OPR-33. A knowledge base and support documentation SHOULD be maintained to assist in common issue resolution and improve incident response times.*

Härda system, konfigurationshantering, säkerhetskonfigurering.

Krav i TEHDAS2. M7.4:

- *OPR-4. SPEs SHOULD maintain a configuration management database (CMDB).*
- *OPR-11. SPE Operator SHOULD establish a Service Management System.*

Test och återläsning av säkerhetskopior. Redundans och återställning.

Krav i TEHDAS2. M7.4:

- *OPR-20. SPEs MUST have procedures in place to fully recover the SPE user environment, including all critical data, configurations, and processing outputs, from clean backups and restore normal operations following an incident.*
- *OPR-23. The SPE provider SHOULD implement strategies for backup management, disaster recovery, and crisis management.*
- *OPR-5. SPE Operator MUST implement mechanisms to terminate the secure processing environment upon expiration of the data permit. All electronic health data within the environment MUST be deleted or rendered unrecoverable within six months of permit expiry, including any*

backups or redundant copies. Procedures MUST be formally documented, monitored, and aligned with risk assessments and confidentiality requirements.

- *OPR-27. The SPE Operator SHOULD regularly restore backups to the platform as part of standard feature development and operational activities, ensuring preparedness for incident response.*

Infrastruktur och plattforms-hantering (Hårdvara).

Krav i TEHDAS2. M7.4:

- *OPR-28. The SPE operator MUST implement a formal patch management policy to identify, evaluate, and apply security patches in a timely manner based on severity.*
- *OPR-29. SPE Operator MUST establish a system update process to ensure timely and secure updates of software, OS, and firmware, tested prior to deployment.*

Kontinuitetshantering.

Hanterar redundans och återställning inom Service Continuity Management (ITIL). (Samarbete med fysisk säkerhet.)

Krav i TEHDAS2. M7.4:

- *SPEs MUST have procedures in place to fully recover the SPE user environment, including all critical data, configurations, and processing outputs, from clean backups and restore normal operations following an incident. The SPE provider SHOULD implement strategies for backup management, disaster recovery, and crisis management.*
- *OPR-21. SPE Operator MUST have disaster recovery procedures in place to restore the availability and integrity of the SPE services, including critical system components, configurations, and platform-level functionality, from clean backups, and to resume normal service operations following an incident.*
- *OPR-24. The SPE Operator MUST implement strategies for backup management, disaster recovery, and crisis management.*

Beredskap och övning.

Krav i TEHDAS2. M7.4: OPR-23. The SPE provider SHOULD implement strategies for backup management, disaster recovery, and crisis management.

Förvalta tjänstekatalog och IT-arkitektur.

Krav i TEHDAS2. M7.4: OPR-3. SPE Operator SHOULD maintain a Service Portfolio including all services.

Arkitekturstyrning.

Utveckla och underhålla mjukvara. Hantera programvaruutveckling.

Det är systemutvecklarens ansvar att för aktuellt IT-system påvisa såväl ATT kravuppfyllnad föreligger som HUR kravuppfyllnad erhålls för de funktionella kraven.

Hantera förvaltning av bearbetningsyta.

Roller:

Driftchef (IT Operations Manager).

Rollen ansvarar för att leda driftteamet och säkerställa att IT-tjänster levereras i enlighet med avtalade servicenivåer (SLA). Driftchefen har fokus på tillgänglighet, prestanda och kontinuitet i IT-miljön, vilket innebär att övervaka driften, hantera incidenter och koordinera resurser för att minimera driftstörningar. Rollen är central för att upprätthålla stabilitet och effektivitet i organisationens IT-infrastruktur och arbetar nära andra funktioner för att säkerställa en robust drift.

IT Service Manager / Tjänsteansvarig externa parter.

Rollen ansvarar för att hantera och följa upp IT-tjänster som levereras av externa leverantörer. Detta innefattar att säkerställa att tjänsterna uppfyller avtalade krav på säkerhet, tillförlitlighet och prestanda. IT Service Manager fungerar som kontaktpunkt mellan organisationen och leverantörerna, övervakar SLA-efterlevnad och ser till att risker och incidenter hanteras effektivt. Rollen bidrar till att upprätthålla en stabil IT-miljö genom kontinuerlig kvalitetssäkring och förbättring av tjänsteleveranser.

Driftansvarig för IT-tjänster.

Rollen ansvarar för att säkerställa stabil och säker drift av organisationens IT-tjänster. Detta innefattar att hantera oplanerade avbrott och snabbt återställa tjänster för att minimera påverkan på verksamheten. Driftansvarig arbetar med att identifiera och eliminera grundorsaker till incidenter för att förebygga återkommande problem. En viktig del av rollen är att säkerställa att alla förändringar i IT-miljön sker kontrollerat, dokumenterat och i enlighet med fastställda processer och policyer.

Incidenthanterare.

Ansvarar för att leda arbetet vid säkerhetsincidenter och agera som central koordinator för alla åtgärder som krävs för att begränsa, åtgärda och återställa drabbade system och tjänster. Incidenthanteraren samordnar insatser mellan olika team och funktioner, säkerställer att kommunikation sker effektivt och att

återställning genomförs enligt fastställda rutiner. Rollen är avgörande för att minimera påverkan på verksamheten och för att dokumentera lärdomar som kan förbättra organisationens framtida incidentberedskap.

Problemansvarig.

Ansvarar för att identifiera och analysera grundorsaker till återkommande incidenter i IT-miljön. Problemansvarig arbetar proaktivt med att eliminera underliggande fel och sårbarheter för att förhindra framtida driftstörningar. Detta innefattar att samla in och analysera data från incidenter, föreslå långsiktiga lösningar och säkerställa att korrigerande åtgärder implementeras.

Förändringsledare IT (Change Manager).

Ansvarar för att alla förändringar i IT-miljön sker på ett kontrollerat sätt för att minimera risker och undvika driftstörningar. Förändringsledaren planerar, koordinerar och övervakar förändringsprocessen i enlighet med fastställda policyer och principer. Detta inkluderar att bedöma risker, säkerställa dokumentation och kommunikation samt att förändringar implementeras med godkända metoder och efterlevnad av säkerhetskrav.

Change Advisory Board (CAB).

Change Advisory Board (CAB) är en central del av Change Management-processen. En grupp som bedömer och godkänner större förändringar innan de implementeras. Syftet är att säkerställa att förändringar är väl genomtänkta, riskbedömda och inte påverkar verksamheten negativt. Representanter från olika delar av organisationen (IT, verksamhet, säkerhet, ibland leverantörer). Granskar förändringsförslag, bedömer risker, kostnader och påverkan. Godkänner eller avvisar förändringar.

Support.

Förvaltningsledare/ Förvaltningsledare IT.

Förvaltningsledare SPE objekt.

Systemförvaltare / Applikationsförvaltare / Systemspecialist.

Systemadministratör & systemförvaltare för samtliga system.

Nätverksförvaltare SDK moduler.

Drifttekniker / IT-drifttekniker.

Ansvarar för den dagliga driften av IT-infrastruktur, servrar, nätverk, etc.

IT-arkitekt.

Infrastrukturarkitekt.

IT-stöd:

***Beställarportal med godkännandeflöde*.**

En beställarportal med godkännandeflöde är ett digitalt system där användare kan begära tjänster, produkter eller förändringar, och där varje begäran följer ett definierat godkännandeflöde innan den verkställs. Portalen stödjer roller, behörigheter och automatiserade steg för granskning, godkännande och dokumentation. Detta skapar struktur, transparens och kontroll i beställningsprocessen, särskilt inom IT, inköp eller förändringshantering.

ITSM system.

Ett ITSM-system (IT Service Management) är ett verktyg som stödjer hantering av IT-tjänster enligt strukturerade processer. Det omfattar funktioner för incidenthantering (snabb lösning av störningar), problemhantering (analys av bakomliggande orsaker), ändringshantering (kontrollerad införsel av förändringar), releasehantering (planerad utrullning av nya versioner) och serviceförfrågningar (beställning av tjänster).

Backup med Air Gap och Immutabilitet.

Backup med Air Gap och Immutabilitet är en säkerhetsstrategi som skyddar data mot ransomware och andra attacker. Air Gap innebär att backupen är fysisk eller logiskt isolerad från nätverket, vilket förhindrar att angripare når den. Immutabilitet innebär att backupdata inte kan ändras eller raderas under en viss tid, vilket säkerställer att originalkopior förblir intakta. Tillsammans ger dessa tekniker ett robust skydd för kritisk information och möjliggör säker återställning vid incidenter.

Telemetrilnfrastruktur.

Telemetriinfrastruktur är den tekniska grund som samlar in, överför och analyserar data från olika IT-system och komponenter i realtid. Den används för att övervaka prestanda, säkerhet och användarbeteende, och är ofta integrerad med verktyg som EDR, NetFlow/sFlow, orchestratorer och ITSM-system. Genom att samla telemetridata från endpoints, nätverk, applikationer och molntjänster möjliggör infrastrukturen snabb incidentrespons, proaktiv felsökning och kontinuerlig förbättring av IT-miljön.

Övervakningsplattform.

En övervakningsplattform är ett centralt system som samlar in, analyserar och visualiserar data från IT-miljön för att upptäcka avvikelser, prestandaproblem och säkerhetshot. Den integreras ofta med telemetriinfrastruktur, EDR, NetFlow/sFlow, orchestratorer och ITSM-system för att ge en helhetsbild av systemstatus och säkerhetsläge. Plattformen möjliggör proaktiv övervakning,

snabb incidentrespons och effektiv felsökning, vilket stärker både drift och cybersäkerhet.

CMDB.

CMDB (Configuration Management Database) är ett centralt register i ett ITSM-system som innehåller information om IT-resurser (s.k. konfigurationsobjekt) och deras relationer. Det stödjer processer som incident, problem, change och releasehantering genom att ge insyn i hur system är uppbyggda och påverkar varandra. CMDB bidrar till bättre beslutsunderlag, snabbare felsökning och säkrare förändringshantering i komplexa IT-miljöer.

CMS.

Ett CMS (Configuration Management System) är ett verktyg som hanterar och dokumenterar konfigurationsdata för IT-resurser, ofta i nära samverkan med en CMDB. Systemet säkerställer att rätt versioner och inställningar används i olika miljöer (utveckling, test, produktion) och stödjer spårbarhet vid förändringar. I samband med ITSM, orchestratorer och övervakningsplattformar bidrar det till stabil drift, snabb felsökning och kontrollerad förändringshantering.

Versionshantering.

Ett versionshanteringssystem är ett verktyg som spårar ändringar i kod, konfigurationer och dokumentation över tid. Det möjliggör samarbete, historik, återställning och kontroll av olika versioner i utvecklings och testmiljöer. I samband med system som Git, konfigurationshantering och ITSM, bidrar versionshantering till strukturerad utveckling, säker förändringshantering och spårbarhet i hela livscykeln för IT-tjänster.

Multi-Tenant System.

Separation av kunder.

Compliance-modell för alla komponenter

Compliance-modell för IT-komponenter. Ett verktyg eller ramverk som säkerställer att alla IT-resurser (t.ex. servrar, applikationer, nätverksenheter) följer interna och externa krav.

MFA. RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

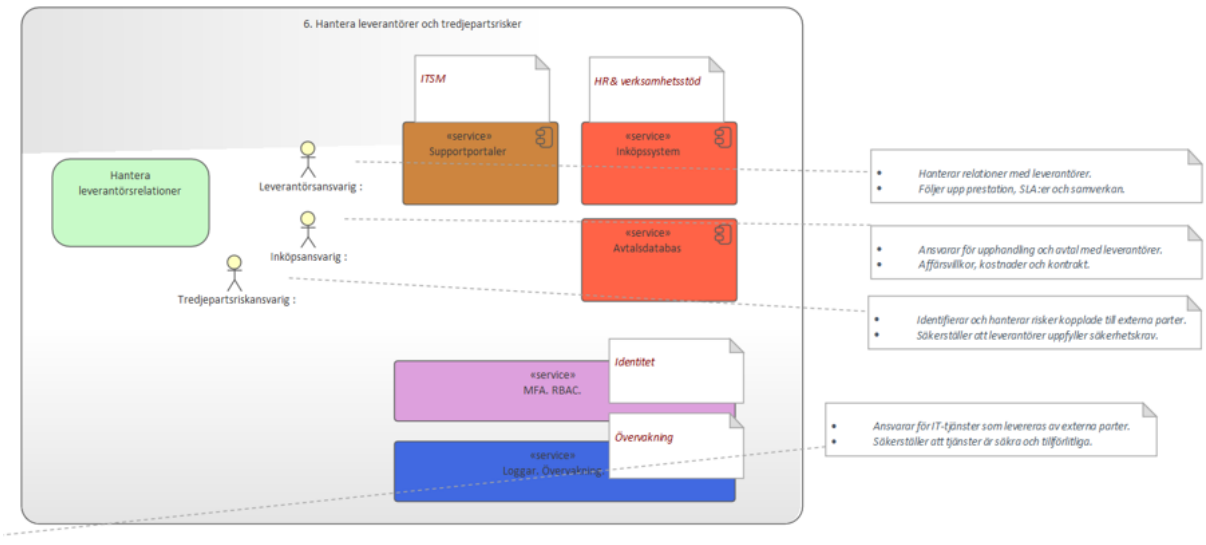
Huvudförmåga 7. Hantera leverantörer och tredjepartsrisker

Hantera leverantörsrelationer innebär att upprätthålla och utveckla ett strukturerat samarbete med externa leverantörer för att säkerställa att tjänster

och produkter levereras enligt överenskomna krav. Att aktivt arbeta med leverantörsrelationer genom regelbunden kommunikation och samordning, samt att hantera leverantörsavtal där särskild vikt läggs vid att säkerhetskrav är tydligt definierade och efterlevs. Utöver detta omfattar arbetet kontinuerlig övervakning av leverantörernas prestanda för att säkerställa kvalitet, tillgänglighet och att eventuella avvikelser hanteras snabbt och effektivt.

Krav i TEHDAS2. M7.4:

- *OPR-25. HDAB and SPEs SHOULD define SLAs that include: Uptime guarantees Response/resolution times for incidents Include security SLAs, such as data encryption guarantees, incident response times, and audit logging.*
- *OPR-13. SPE Operator MUST maintain policies to ensure security around procurement systems and development and operation of systems.*
- *OPR-26. SPE Operator SHOULD define SLAs that include: uptime guarantees, response/resolution times for incidents include security SLAs, such as data encryption guarantees, incident response times, and audit logging.*
- *OPR-31. SPE Operator MUST provide dedicated technical support with clearly defined SLAs and escalation paths for addressing incidents and technical issues.*



Förmågor:

Hantera leverantörsrelationer.

Hantera leverantörsrelationer innebär att upprätthålla och utveckla ett strukturerat samarbete med externa leverantörer för att säkerställa att tjänster och produkter levereras enligt överenskomna krav. Att aktivt arbeta med

leverantörsrelationer genom regelbunden kommunikation och samordning, samt att hantera leverantörsavtal där särskild vikt läggs vid att säkerhetskrav är tydligt definierade och efterlevs. Utöver detta omfattar arbetet kontinuerlig övervakning av leverantörernas prestanda för att säkerställa kvalitet, tillgänglighet och att eventuella avvikelser hanteras snabbt och effektivt.

Krav i TEHDAS2. M7.4:

- *OPR-2. SPE Operator MUST limit the number of authorised staff and any subcontractors who have high-privileged access enabling them to access or process health data and MUST implement effective procedures for managing and monitoring such access within the SPE infrastructure.*
- *OPR-25. HDAB and SPEs SHOULD define SLAs that include: Uptime guarantees Response/resolution times for incidents Include security SLAs, such as data encryption guarantees, incident response times, and audit logging.*

Roller:

Leverantörsansvarig.

Leverantörsansvarig säkerställer att samarbetet med externa leverantörer fungerar effektivt och i enlighet med verksamhetens krav. Rollen innebär att aktivt hantera relationer med leverantörer genom kontinuerlig kommunikation, samordning och problemlösning. En viktig del av ansvaret är att följa upp leverantörernas prestationer, inklusive att övervaka att avtalade servicenivåer (SLA: er) uppfylls och att samverkan sker på ett sätt som stödjer verksamhetens mål. Leverantörsansvarig fungerar som en länk mellan organisationen och leverantörerna för att säkerställa kvalitet och tillförlitlighet.

Inköpsansvarig.

Inköpsansvarig ansvarar för hela processen kring upphandling och avtal med leverantörer. Rollen omfattar att säkerställa att affärsvillkor, kostnader och kontrakt är tydligt definierade och förhandlade på ett sätt som gynnar verksamheten.

Tredjepartsriskansvarig.

Tredjepartsriskansvarig ansvarar för att identifiera, bedöma och hantera risker som är kopplade till externa parter och leverantörer. Rollen innebär att säkerställa att alla leverantörer uppfyller definierade säkerhetskrav och att risker relaterade till informationssäkerhet, regelefterlevnad och kontinuitet hanteras proaktivt. Detta inkluderar att genomföra riskanalyser, följa upp avtalade säkerhetsåtgärder och samverka med interna och externa intressenter för att minimera potentiella hot mot verksamheten. Målet är att skapa en trygg och compliant leverantörskedja.

IT-stöd:

Avtalsdatabas.

En avtalsdatabas är ett centralt verktyg för att hantera leverantörer och tredjepartsrisker. Den samlar och strukturerar avtal, vilket ger bättre kontroll över villkor, giltighetstider och efterlevnad. Genom att koppla avtal till riskklassificering och automatiska påminnelser bidrar databasen till att minska affärsrisker och säkerställa att organisationen agerar proaktivt vid förändringar eller incidenter.

Supportportaler.

En supportportal är ett viktigt komplement till avtalsdatabasen vid hantering av leverantörer och tredjepartsrisker. Den fungerar som en strukturerad kanal för kommunikation, ärendehantering och uppföljning av leverantörsrelaterade frågor. Genom att samla supportärenden, dokumentation och kontaktinformation på ett ställe skapas bättre transparens och spårbarhet. Portalen bidrar till att säkerställa att avtalade servicenivåer följs, att incidenter hanteras effektivt och att risker kan identifieras och åtgärdas i tid.

Inköpssystem.

Ett inköpssystem är ett viktigt stöd vid hantering av leverantörer och tredjepartsrisker. Det möjliggör strukturerad upphandling, spårbarhet i inköpsprocessen och säkerställer att avtalade villkor följs. Genom att koppla inköpssystemet till avtalsdatabasen och supportportalen skapas en helhet där avtal, ärenden och inköp kan följas upp samlat, vilket minskar risken för avvikelser och förbättrar kontrollen över externa relationer.

MFA. RBAC. Loggar. Övervakning.

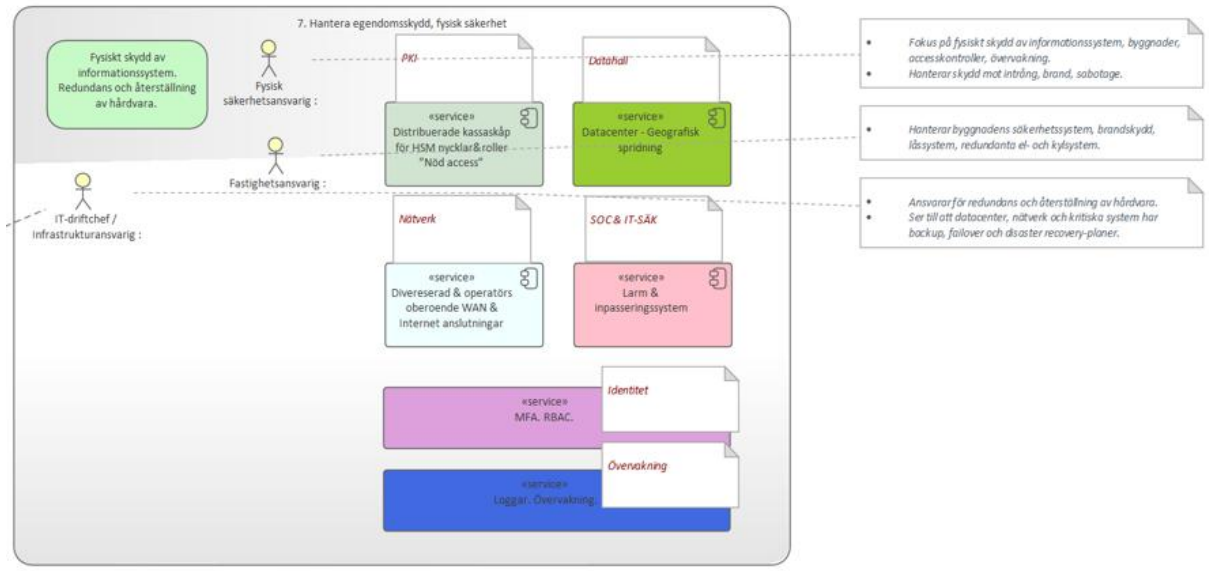
Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 8. Hantera egendomsskydd, fysisk säkerhet

Säkerställ att utrustning och anläggningar är skyddade mot skador, obehörig åtkomst och miljömässiga risker. Detta omfattar både fysisk och miljömässig säkerhet, inklusive att skapa säkra områden där informationstillgångar finns. Centrala servrar och nätverksutrustning ska placeras i särskilda IT-utrymmen med restriktiv behörighetstilldelning. Behovet av övervakning och larm i dessa utrymmen ska identifieras och hanteras, och tillträde ska registreras på individnivå med dokumentation som sparas enligt fastställd bevarandetid. Interna regler ska finnas för hur mobil utrustning skyddas. Dessutom ingår redundans och återställning av hårdvara för att säkerställa driftsäkerhet och kontinuitet vid incidenter. Målet är att minimera risker och garantera att informationssystemets fysiska komponenter är robusta och skyddade.

Krav i TEHDAS2. M7.4:

- *SPEs MUST have procedures in place to fully recover the SPE user environment, including all critical data, configurations, and processing outputs, from clean backups and restore normal operations following an incident. The SPE provider SHOULD implement strategies for backup management, disaster recovery, and crisis management.*
- *OPR-21. SPE Operator MUST have disaster recovery procedures in place to restore the availability and integrity of the SPE services, including critical system components, configurations, and platform-level functionality, from clean backups, and to resume normal service operations following an incident.*
- *OPR-24. The SPE Operator MUST implement strategies for backup management, disaster recovery, and crisis management.*



Förmågor:

Hantera fysiskt skydd av informationssystem. Redundans och återställning av hårdvara.

Säkerställ att utrustning och anläggningar är skyddade mot skador, obehörig åtkomst och miljömässiga risker. Detta omfattar både fysisk och miljömässig säkerhet, inklusive att skapa säkra områden där informationstillgångar finns. Centrala servrar och nätverksutrustning ska placeras i särskilda IT-utrymmen med restriktiv behörighetstilldelning. Behovet av övervakning och larm i dessa utrymmen ska identifieras och hanteras, och tillträde ska registreras på individnivå med dokumentation som sparas enligt fastställd bevarandetid. Interna

regler ska finnas för hur mobil utrustning skyddas. Dessutom ingår redundans och återställning av hårdvara för att säkerställa driftsäkerhet och kontinuitet vid incidenter.

Roller:

Fysisk säkerhetsansvarig.

Har ansvar för att skydda organisationens informationssystem och byggnader mot fysiska hot och intrång. Rollen omfattar att implementera och övervaka accesskontroller, säkerställa att övervakningssystem fungerar effektivt samt hantera skydd mot brand, sabotage och andra miljömässiga risker. Fysisk säkerhetsansvarig arbetar med att skapa säkra områden för kritisk IT-utrustning, upprätthålla rutiner för tillträdesregistrering och larm, samt samordna åtgärder för att minimera risken för obehörig åtkomst och skador. Målet är att garantera en robust fysisk säkerhetsmiljö som stödjer verksamhetens kontinuitet och säkerhet.

Fastighetsansvarig.

Ansvarar för byggnadens säkerhet och driftmiljö för att stödja verksamhetens kontinuitet och skydda kritiska system. Rollen omfattar hantering av säkerhetssystem, brandskydd och låssystem för att förebygga intrång och skador. Dessutom ingår ansvar för redundanta el- och kylsystem som säkerställer stabil drift av IT-utrustning och andra tekniska installationer.

IT-driftchef / Infrastrukturansvarig.

Ansvarar för redundans och återställning av hårdvara. Ser till att datacenter, nätverk och kritiska system har backup, failover och disaster recovery-planer.

IT-stöd:

Distribuerade kassaskåp för HSM nycklar.

Distribuerade kassaskåp för HSM-nycklar och roller med stöd för ”nödaccess” är en viktig komponent inom egendomsskydd och fysisk säkerhet. De möjliggör säker lagring och åtkomst av kryptografiska nycklar och behörigheter, samtidigt som de minimerar risken för obehörig användning. Funktionen för nödaccess säkerställer att organisationen kan agera snabbt vid incidenter eller systemfel, utan att kompromissa med säkerheten. Genom att använda distribuerade lösningar ökar redundansen och tillgängligheten, vilket stärker det övergripande skyddet av kritisk infrastruktur.

Diversifierade och operatörsoberoende WAN och Internetanslutningar.

Diversifierade och operatörsoberoende WAN och internetanslutningar är en viktig del av egendomsskydd och fysisk säkerhet. Genom att använda flera oberoende nätverksleverantörer och tekniker minskar risken för avbrott och ökar tillgängligheten till kritiska system, inklusive HSM-nyckelhantering och nödaccesslösningar. Detta stärker organisationens motståndskraft mot både tekniska fel och riktade attacker, och säkerställer att säkerhetsfunktioner förblir åtkomliga även vid störningar i enskilda nätverk.

Datacenter - Geografisk spridning.

Datacenter med geografisk spridning är en viktig del av robust fysisk informationssäkerhet. När dessa uppförs enligt MSB:s Vägledning för fysisk informationssäkerhet i it-utrymmen säkerställs att de uppfyller krav på skydd mot brand, inbrott, vattenläckage och andra fysiska hot. Geografisk spridning minskar risken för total driftstörning vid lokala incidenter och möjliggör redundans, kontinuitet och säker åtkomst till kritiska system och nyckelhantering, även vid kris eller nödaccess.

Larm och inpasseringssystem.

Larm- och inpasseringssystem är centrala komponenter i fysisk säkerhet och egendomsskydd. De kontrollerar och loggar åtkomst till känsliga utrymmen, inklusive datacenter och HSM-kassaskåp, vilket minskar risken för obehörig åtkomst. Genom att integrera dessa system med övriga säkerhetslösningar, som nödaccess och geografiskt spridda datacenter, stärks den övergripande säkerhetsnivån och möjliggör snabb respons vid incidenter.

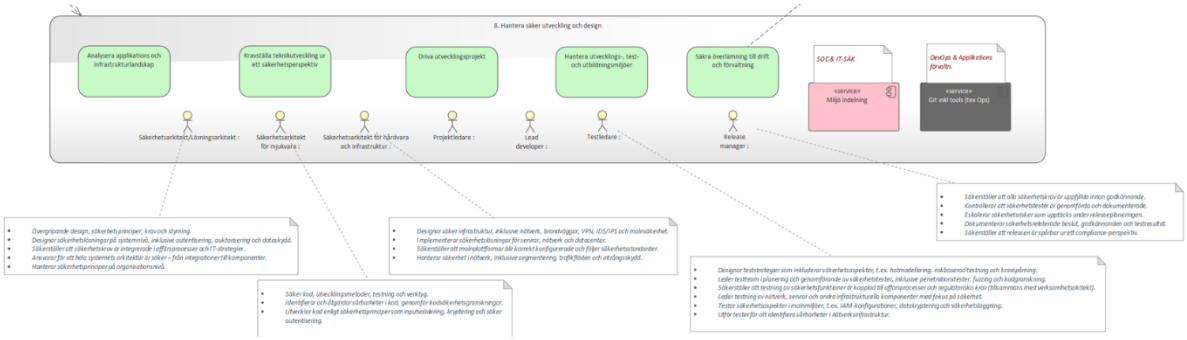
MFA. RBAC. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 9. Hantera säker utveckling och design

Hantera säker utveckling och design innebär att säkerställa att IT-säkerhet integreras i hela livscykeln för systemutveckling och underhåll. Säkerheten ska byggas in från början och inte läggas till som en avslutande åtgärd. Detta omfattar att definiera tydliga säkerhetskrav för nya system i enlighet med gällande regelverk och att ställa krav under utvecklingsprocessen för att garantera att systemet uppfyller både funktionella och säkerhetsmässiga behov. Vidare ingår att säkerställa användning av säkra utvecklingsmetoder, inklusive kodgranskning, testning och hantering av sårbarheter. Målet är att skapa robusta och förtroendevärda system som motstår hot och uppfyller organisationens säkerhetskrav.

Krav i TEHDAS2. M7.4: OPR-13. SPE Operator MUST maintain policies to ensure security around procurement systems and development and operation of systems.



Förmågor:

Analysera applikations och infrastrukturlandskap.

Analysera applikations- och infrastrukturlandskapet innebär att skapa en helhetsbild av organisationens systemmiljö för att säkerställa att den är effektiv, säker och skalbar. Som arkitekt eller utvecklare handlar det om att kartlägga befintliga applikationer, integrationer och tekniska plattformar, samt identifiera beroenden och risker. Analysen omfattar att bedöma säkerhetsnivåer och hur väl lösningarna stödjer verksamhetens mål. Syftet är att skapa en robust och framtidssäker arkitektur som möjliggör säkerhet, innovation och minimerar komplexitet.

Kravställa teknikutveckling ur ett säkerhetsperspektiv.

Krav i TEHDAS2. M7.4: Technical Interoperability (TIR) requirements.

Driva utvecklingsprojekt.

Hantera utvecklings-, test- och utbildningsmiljöer.

Säkra överlämning till drift och förvaltning.

Krav i TEHDAS2. M7.4: OPR-15. SPE Operator SHOULD adopt a release and deployment management process.

Roller:

Säkerhetsarkitekt/Lösningsarkitekt.

Ansvarar för den övergripande designen av system och lösningar med fokus på säkerhetsprinciper, krav och styrning. Rollen innebär att utforma säkerhetslösningar på systemnivå, inklusive mekanismer för autentisering, auktorisering och dataskydd. Säkerhetsarkitekten säkerställer att säkerhetskrav

integreras i både affärsprocesser och IT-strategier, och att hela systemets arkitektur är säker – från integrationer till enskilda komponenter. Dessutom hanteras säkerhetsprinciper på organisationsnivå för att skapa en enhetlig och robust säkerhetsram som stödjer efterlevnad av regelverk.

Säkerhetsarkitekt för mjukvara.

Säkerhetsarkitekten för mjukvara ansvarar för att säkerställa att applikationer utvecklas enligt etablerade säkerhetsprinciper och metoder. Rollen omfattar att definiera och implementera säkra utvecklingsmetoder, använda verktyg för kodanalys och genomföra omfattande testning för att identifiera och åtgärda sårbarheter. Säkerhetsarkitekten genomför kodsäkerhetsgranskningar och ser till att utvecklingen följer principer som inputvalidering, kryptering och säker autentisering.

Säkerhetsarkitekt för hårdvara och infrastruktur.

Ansvarar för att designa och implementera en säker IT-infrastruktur som skyddar organisationens system och data. Rollen omfattar att utforma lösningar för nätverkssäkerhet, inklusive brandväggar, VPN, IDS/IPS och molnsäkerhet, samt att säkerställa korrekt konfiguration av molnplattformar enligt etablerade säkerhetsstandarder. Säkerhetsarkitekten implementerar skydd för servrar, nätverk och datacenter, och hanterar säkerhetsåtgärder som nätverkssegmentering, kontroll av trafikflöden och intrångsskydd.

Testledare.

Testledaren ansvarar för att utforma och leda teststrategier som säkerställer att säkerhetsaspekter integreras i hela testprocessen. Rollen omfattar att designa strategier som inkluderar hotmodellering, riskbaserad testning och kravspårning, samt att leda testteam i planering och genomförande av säkerhetstester såsom penetrationstester, fuzzing och kodgranskning. Testledaren säkerställer att testning av säkerhetsfunktioner är kopplad till affärsprocesser och regulatoriska krav i samarbete med verksamhetsarkitekten. Dessutom ingår ansvar för testning av nätverk, servrar och infrastrukturella komponenter med fokus på säkerhet, samt att utföra tester i molnmiljöer, exempelvis IAM-konfigurationer, datakryptering och säkerhetsloggning. Rollen omfattar även att identifiera sårbarheter i nätverksinfrastruktur och säkerställa att dessa åtgärdas.

Release manager.

Ansvarar för att säkerställa att alla säkerhetskrav är uppfyllda innan en release godkänns. Rollen omfattar att kontrollera att säkerhetstester är genomförda och dokumenterade, samt att eskalera eventuella säkerhetsrisker som upptäcks under releaseplaneringen. Release Manager dokumenterar alla säkerhetsrelaterade beslut, godkännanden och testresultat för att skapa spårbarhet och uppfylla compliance-krav. Dessutom säkerställs att releasen är

fullt spårbar ur ett regulatoriskt perspektiv, vilket bidrar till en säker och kontrollerad leveransprocess.

IT-stöd:

Git inkl. tools (t.ex. Ops).

Git är ett versionshanteringssystem som används för att spåra ändringar i kod och möjliggöra samarbete mellan utvecklare. Det fungerar som en central källa för kodhistorik och möjliggör parallell utveckling via grenar. Git används ofta tillsammans med plattformar som GitHub, GitLab eller Bitbucket, där kod kan lagras, granskas och distribueras. I moderna DevOps och GitOps-miljöer används Git även för att styra infrastruktur och applikationsdrift, där ändringar i kod automatiskt kan trigga bygg, test och utrullning via CI/CD-pipelines. Genom att integrera verktyg för kodskanning och säkerhet blir Git en viktig del i att upprätthålla både kvalitet och säkerhet i utvecklingsprocessen.

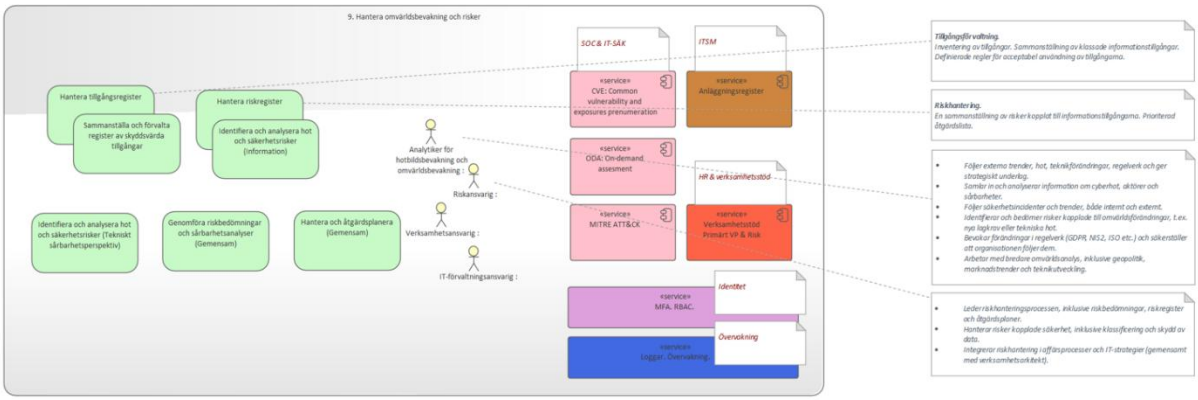
Miljöindelning.

Vid utveckling och test delas IT-miljön ofta in i olika faser för att säkerställa kvalitet och kontroll. Vanliga miljöer inkluderar utvecklingsmiljö, där kod skrivs och testas av utvecklare; testmiljö, där funktioner verifieras och kvalitetssäkras; staging miljö, som speglar produktion och används för slutgiltiga tester; samt produktionsmiljö, där systemet är i drift för användare. Denna indelning möjliggör strukturerad hantering av kod, säkerhet, prestanda och förändringar innan de når slutanvändare.

Huvudförmåga 10. Hantera omvärldsbevakning och risker

Organisationen ska kontinuerligt bevaka omvärlden för att identifiera nya hot, sårbarheter och regulatoriska förändringar som kan påverka säkerheten. Detta innefattar att följa nationella och internationella säkerhetsvarningar, delta i relevanta nätverk och analysera trender inom cybersäkerhet. Riskhantering ska integreras i verksamheten genom att regelbundet uppdatera riskanalyser, prioritera åtgärder och dokumentera risker i ett riskregister. Syftet är att proaktivt minska sannolikheten för incidenter och säkerställa att organisationen är förberedd på förändringar i hotbilden.

Krav i TEHDAS2. M7.4: EHDSR-15. SPE TOMs MUST undergo risk assessments.



Förmågor:

Hantera tillgångsregister.

Hantera tillgångsregister innebär att upprätthålla en strukturerad och aktuell översikt över organisationens informationstillgångar. Detta omfattar tillgångsförvaltning och inventering av alla relevanta tillgångar, inklusive system, applikationer, data och hårdvara. Arbetet innefattar att sammanställa klassade informationstillgångar enligt fastställda säkerhetsnivåer och att definiera regler för acceptabel användning av dessa tillgångar. En central del är att skapa och förvalta ett register över skyddsvärda tillgångar, vilket ger en grund för riskhantering, säkerhetskontroller och regelefterlevnad. Målet är att säkerställa spårbarhet, kontroll och skydd av organisationens mest kritiska resurser.

Hantera riskregister.

Hantera riskregister innebär att systematiskt identifiera, dokumentera och följa upp risker som är kopplade till organisationens informationstillgångar. Arbetet omfattar att sammanställa ett strukturerat register över dessa risker, inklusive bedömning av sannolikhet, konsekvens och prioritet. Utifrån analysen skapas en prioriterad åtgärdslista som ligger till grund för riskreducerande aktiviteter och beslut. Syftet är att ge en tydlig översikt över risklandskapet, möjliggöra spårbarhet och säkerställa att riskhanteringen är integrerad i organisationens styrning och säkerhetsarbete.

Identifiera och analysera hot och säkerhetsrisker (Information).

Identifiera och analysera hot och säkerhetsrisker (Tekniskt sårbarhetsperspektiv).

Genomföra riskbedömningar och sårbarhetsanalyser (Gemensam)

Krav i TEHDAS2. M7.4: OPR-14. SPEs SHOULD adopt change management process with impact and risk Assessment.

Hantera och åtgärdsplanera (Gemensam).

Krav i TEHDAS2. M7.4: EHDSR-16. HDABs MUST ensure that SPE TOMs audits are carried out and that risk assessments lead to risk mitigations.

Roller:

Analytiker för hotbildsbevakning och omvärldsbevakning.

Ansvarar för att följa och analysera externa trender, hot, tekniska förändringar och regelverk för att ge strategiskt underlag till organisationens säkerhetsarbete. Rollen omfattar insamling och analys av information om cyberhot, aktörer och sårbarheter, samt bevakning av säkerhetsincidenter och trender både internt och externt. Analytikern identifierar och bedömer risker kopplade till omvärldsförändringar, exempelvis nya lagkrav eller tekniska hot, och säkerställer att organisationen följer aktuella regelverk som GDPR, NIS2 och ISO-standarder. Arbetet inkluderar även bredare omvärldsanalys, såsom geopolitik, marknadstrender och teknikutveckling, för att ge en helhetsbild av risklandskapet.

Riskansvarig.

Leder organisationens riskhanteringsprocess och ansvarar för att risker identifieras, bedöms och hanteras på ett strukturerat sätt. Rollen omfattar att genomföra riskbedömningar, upprätthålla ett riskregister och ta fram prioriterade åtgärdsplaner. Riskansvarig hanterar särskilt risker kopplade till informationssäkerhet, inklusive klassificering och skydd av data, och ser till att dessa integreras i affärsprocesser och IT-strategier i nära samarbete med verksamhetsarkitekten. Målet är att skapa en proaktiv riskkultur som minimerar hot mot verksamheten och säkerställer efterlevnad av regelverk.

Verksamhetsansvarig.

Identifierar och hanterar risker inom sitt område.

IT-förvaltningsansvarig.

Identifierar och hanterar risker inom sitt område.

IT-stöd:

CVE: Common Vulnerability and Exposures prenumeration.

En CVE-prenumeration innebär att man automatiskt får information om nya kända sårbarheter i mjukvara och system. CVE är en global standard för att identifiera och namnge säkerhetsbrister. Genom att prenumerera på CVE-uppdateringar via e-post, RSS eller API kan organisationer snabbt bli medvetna om nya hot och vidta åtgärder, som att uppdatera system eller blockera sårbara komponenter. Det är en viktig del i ett proaktivt säkerhetsarbete och används ofta tillsammans med sårbarhetsscanning och patchhantering.

ODA: On Demand Assessment.

ODA (On Demand Assessment) är en metod eller tjänst för att snabbt och vid behov utvärdera säkerhetsläget i ett system, en applikation eller en infrastruktur. Det kan inkludera sårbarhetsskanning, konfigurationsgranskning eller identitetsanalys ofta kopplat till prenumerationer på t.ex. CVE eller andra hotkällor. I kombination med tidigare nämnda komponenter som loggar, övervakning och identitetssystem, ger ODA en flexibel och situationsanpassad säkerhetskontroll som kan användas vid förändringar, incidenter eller regelbundna kontroller.

MITRE ATT&CK.

MITRE ATT&CK är en öppen kunskapsbas som beskriver taktiker, tekniker och metoder som angripare använder vid cyberattacker. Den används av säkerhetsteam för att förstå, upptäcka och försvara sig mot hotaktörer genom att kartlägga attacker mot en strukturerad modell. ATT&CK hjälper organisationer att identifiera svagheter, förbättra detektering och planera motåtgärder, ofta i kombination med loggning, övervakning och hotanalys.

Anläggningsregister.

Ett register med detaljer om installationer, underhållsplaner och livscykeldata.

Verksamhetsstöd Primärt VP och Risk.

Verksamhetsstöd för VP (Verksamhetsplanering) och Risk omfattar digitala verktyg och processer som hjälper organisationer att planera, följa upp och hantera mål, aktiviteter och risker. Inom VP används stödet för att strukturera strategier, bryta ner mål till konkreta åtgärder och följa upp resultat. Inom riskhantering används det för att identifiera, bedöma, åtgärda och övervaka risker som kan påverka verksamheten. Tillsammans ger verksamhetsstödet en samlad överblick och styrning som stärker beslutsfattande, efterlevnad och kontinuerlig förbättring.

MFA. RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 11. Hantera efterlevnad och revision

Säkerställ efterlevnad av relevanta lagar och förordningar. Genomför regelbundna säkerhetsgranskningar och revisioner.

Krav i TEHDAS2. M7.4:

- *EHDSR-15. SPE TOMs MUST undergo risk assessments.*
- *OPR-5. SPEs MUST undergo regular internal and external security audits.*
- *EHDSR-14. Regular internal and external security audits MUST be done on SPE.*

Förmågor:

Intern granskning och revision.

Krav i TEHDAS2. M7.4:

- *EHDSR-14. Regular internal and external security audits MUST be done on SPE TOMs.*
- *OPR-6. SPE Operator MUST undergo regular internal and external security audits to assess compliance with security, data protection, and operational requirements.*

Extern granskning och revision.

Krav i TEHDAS2. M7:

- *EHDSR-14. Regular internal and external security audits MUST be done on SPE TOMs.*
- *EHDSR-16. HDABs MUST ensure that SPE TOMs audits are carried out and that risk assessments lead to risk mitigations.*
- *OPR-6. SPE Operator MUST undergo regular internal and external security audits to assess compliance with security, data protection, and operational requirements.*

Roller:

Compliance Officer / Säkerhetsrevisor.

Säkerställer att organisationen följer lagar, regler och standarder (t.ex. GDPR, ISO 27001).

Krav i TEHDAS2. M7.4: OPR-9. The SPE operator SHOULD assign a Compliance Officer or designate responsibilities to ensure adherence to legal, ethical, and technical obligations.

Revisionsledare / Koordinator.

Verksamhetsansvarig.

Extern revisor.

IT-stöd:

CMS: Compliance management system.

CMS (Compliance Management System) är ett system som hjälper organisationer att följa lagar, regler och interna policyer. Det övervakar efterlevnad, dokumenterar åtgärder och identifierar risker kopplade till exempelvis dataskydd, informationssäkerhet och verksamhetskrav. CMS kan integreras med andra säkerhetssystem som CSPM, PAM och sårbarhetsskanning för att ge en helhetsbild av organisationens säkerhets- och regelefterlevnad.

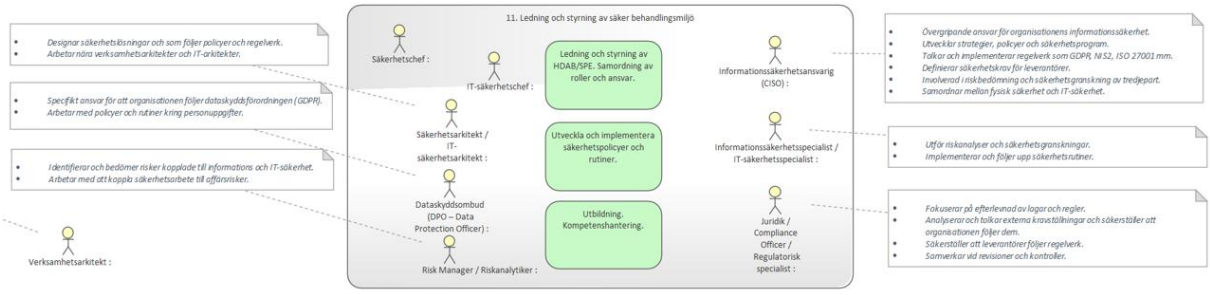
MFA. RBAC. Loggar. Övervakning.

Se MFA. RBAC. Loggar. Övervakning. Förmågeområde 1.

Huvudförmåga 12. Ledning och styrning av säker miljö

Integrera informationssäkerhet i organisationens arbete med affärskontinuitet och krishantering. Detta innebär att säkerhetsaspekter ska vara en naturlig del av Business Continuity Management (BCM) och att kontinuitetsplaner utformas för att skydda kritiska tillgångar, inklusive information, system och infrastruktur. Arbetet omfattar att definiera roller och ansvar, säkerställa att säkerhetskrav är inbyggda i processerna och att planer regelbundet testas genom övningar och scenarier för att verifiera effektiviteten. Planerna ska uppdateras vid förändringar i verksamheten, tekniken eller hotbilden. Upprätta och förvalta en compliance-modell för samtliga IT-komponenter. Syftet är att skapa en robust och säker miljö som kan upprätthålla funktionalitet även vid incidenter, störningar eller kriser.

Krav i TEHDAS2. M7.4: EHDSR-17. When SPEs mentioned in the EU Data Act are used for EHD, EHDS rules and requirements MUST be followed.



Förmågor:

Ledning och styrning av HDAB/SPE. Samordning av roller och ansvar.

Organisation av informationssäkerhet, roller och ansvar. Definiera och fördela säkerhetsansvar. Säkerställa samordning mellan olika delar av organisationen. Upprätta och förvalta en compliance-modell för samtliga IT-komponenter.

Krav i TEHDAS2. M7.4:

- *The SPE operator SHOULD assign a Compliance Officer or designate responsibilities to ensure adherence to legal, ethical, and technical*

obligations.The organisation of the SPE MUST have an operating information security management system (ISMS).

- *OPR-8. The SPE operator MUST maintain up-to-date documentation of all relevant technical, organisational, and security processes.*
- *OPR-10. SPE Operator MUST have an operating information security management system (ISMS).*
- *OPR-12. SPE operators MUST conduct regular Data Protection Impact Assessments (DPIAs).*

Utveckla och implementera säkerhetspolicyer och rutiner.

Policyutveckling: Upprätta och underhålla policyer för informationssäkerhet. Policygranskning: Granska och uppdatera regelbundet policyer för att säkerställa att de förblir relevanta.

Krav i TEHDAS2. M7.4: OPR-13. SPE Operator MUST maintain policies to ensure security around procurement systems and development and operation of systems.

Utbildning. Kompetenshantering.

Krav i TEHDAS2. M7.4:

- *OPR-23. Health data users, HDAB staff and SPE Operator staff who interact with the SPE MUST receive detailed, role-specific information or training covering health data processing, EHDS compliance requirements and security best practices coming from GDPR.*
- *OPR-32. SPE Operator support staff SHOULD be trained in information security and privacy procedures, with roles and responsibilities clearly defined.*

Roller:

Säkerhetschef.

Säkerhetschefen har det övergripande ansvaret för organisationens säkerhetsarbete, vilket omfattar fysisk säkerhet, egendomsskydd, säkerhetsskydd samt informations- och cybersäkerhet. Rollen innebär att säkerställa att policys, riktlinjer och rutiner finns på plats och efterlevs, inklusive skydd av anläggningar och utrustning. Säkerhetschefen har även det övergripande ansvaret för säkerhetsskydd, vilket innefattar personalsäkerhet och genomförande av säkerhetsprövningar. Syftet är att skapa en heltäckande säkerhetsstruktur som skyddar organisationens tillgångar, människor och information mot hot och risker.

IT-säkerhetschef.

IT-säkerhetschefen har det övergripande ansvaret för organisationens IT-miljö ur ett säkerhetsperspektiv. Rollen omfattar att säkerställa att IT-infrastrukturen, system och applikationer är skyddade mot cyberhot och att säkerhetskrav integreras i alla IT-processer. IT-säkerhetschefen leder arbetet med att utveckla och implementera säkerhetspolicys, övervaka efterlevnad av regelverk och hantera incidenter.

Informationssäkerhetsansvarig (CISO).

Informationssäkerhetsansvarig (CISO) har det övergripande ansvaret för organisationens informationssäkerhet och fungerar som strategisk ledare för säkerhetsarbetet. Rollen omfattar att utveckla och implementera säkerhetsstrategier, policyer och program som skyddar organisationens informationstillgångar. CISO tolkar och omsätter regelverk som GDPR, NIS2 och ISO 27001 till praktiska åtgärder och säkerställer efterlevnad. En viktig del är att definiera säkerhetskrav för leverantörer och delta i riskbedömningar samt säkerhetsgranskningar av tredjepart. Rollen samordnar även arbetet med IT-säkerhet för att skapa en heltäckande säkerhetsstruktur.

Säkerhetsarkitekt / IT-säkerhetsarkitekt.

Ansvarar för att designa och implementera säkerhetslösningar som följer organisationens policyer, regelverk och best praxis. Rollen innebär att skapa en säkerhetsarkitektur som täcker hela IT-miljön, från nätverk och system till applikationer och integrationer. Säkerhetsarkitekten arbetar nära verksamhetsarkitekter och IT-arkitekter för att säkerställa att säkerhetskrav integreras i både affärsprocesser och tekniska lösningar.

Informationssäkerhetsspecialist / IT-säkerhetsspecialist.

Ansvarar för att genomföra riskanalyser och säkerhetsgranskningar för att identifiera sårbarheter och hot mot organisationens informationstillgångar. Rollen omfattar att implementera säkerhetsrutiner och följa upp att dessa efterlevs i praktiken. Specialisten arbetar nära andra IT- och säkerhetsfunktioner för att säkerställa att tekniska och organisatoriska skyddsåtgärder är effektiva och uppdaterade. Minska risker, stärka motståndskraft mot cyberhot och säkerställa att verksamheten följer gällande regelverk och interna policyer.

Dataskyddsombud (DPO – Data Protection Officer).

Specifikt ansvar för att organisationen följer dataskyddsförordningen (GDPR). Arbetar med policyer och rutiner kring personuppgifter.

Risk Manager / Riskanalytiker.

Risk Manager / Riskanalytiker ansvarar för att identifiera, analysera och bedöma risker kopplade till informations- och IT-säkerhet. Rollen innebär att kartlägga hot och sårbarheter, bedöma sannolikhet och konsekvens, samt föreslå åtgärder för

riskreducering. En central del är att koppla säkerhetsrisker till affärsrisker för att säkerställa att riskhanteringen stödjer organisationens strategiska mål. Riskanalytikern arbetar nära verksamhetsarkitekter och IT-säkerhetsfunktioner för att integrera riskhantering i processer, projekt och styrning.

Juridik / Compliance Officer / Regulatorisk specialist.

Fokuserar på efterlevnad av lagar och regler. Analyserar och tolkar externa kravställningar och säkerställer att organisationen följer dem. Säkerställer att leverantörer följer regelverk. Samverkar vid revisioner och kontroller.

Kommunikatör.

Ekonomiansvarig.

Verksamhetsarkitekt.

Säkerställer att verksamhetens mål och processer tillsammans med IT-stöd är i linje. En tvärfunktionell funktion med både affärs- och teknikfokus. Har helhetsperspektiv på styrning, förmågor, informationsflöden och strategisk utveckling.

- Säkerställ att säkerhetsstrategier integreras i verksamhetsarkitekturen (tillsammans med CISO). Strategisk säkerhet, policyer, styrning.
- Anpassa tekniska säkerhetslösningar till verksamhetens behov och arkitektur (tillsammans med säkerhetsarkitekt). Design av säkerhetslösningar.
- Tolka krav som påverkar verksamhetsprocesser och arkitektur (tillsammans med Juridik). Efterlevnad av regelverk.
- Implementera rutiner som stödjer verksamhetsarkitekturens säkerhetskrav (tillsammans med informationssäkerhetsspecialist). Operativt säkerhetsarbete.
- Identifiera risker kopplade till verksamhetsförändringar och arkitektur (tillsammans med risk manager). Riskbedömning och hantering.
- Säkerställa att dataskydd integreras i informationsflöden och processer (tillsammans med dataskyddsombud). GDPR och personuppgiftshantering.

IT-stöd:

Complaience modell för alla komponenter

Compliance-modell för IT-komponenter. Ett verktyg eller ramverk som säkerställer att alla IT-resurser (t.ex. servrar, applikationer, nätverksenheter) följer interna och externa krav.

- Regelverk (t.ex. GDPR, ISO 27001, NIS2)
- Säkerhetspolicyer

- Standardiserade konfigurationer
- Licensvillkor

Krav i TEHDAS2. M7.4: Technical Interoperability requirements. TIR-1 ... 36.

Riskanalys

Om SPE:s verksamhetsarkitektur inte hanterar de definierade förmågeområdena korrekt uppstår brister i lagstadgad efterlevnad, vilket kan leda till höga sanktioner och att förtroendet för HDAB äventyras.

Bland de grundläggande principerna i dataskyddsförordningen ingår att personuppgifterna ska skyddas, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs. Man ska också kunna visa att man lever upp till dataskyddsförordningen och hur man gör det. Integritetsskyddsmyndigheten (IMY) utövar tillsyn och det kan bli aktuellt med varning, reprimand, förbud eller sanktionsavgift när man bryter mot dataskyddsförordningen.

Flera myndigheter utövar tillsyn och får fatta beslut om att ta ut en sanktionsavgift till följd av en överträdelse av de skyldigheter som avses i cybersäkerhetslagen och cybersäkerhetsförordningen.

1. Risker och konsekvenser om förmågorna inte hanteras korrekt, baserat på kraven från EHDS, GDPR, NIS2 och SPE-specifikationerna.

Huvudförmåga 1. Hantera personalsäkerhet

RISK: Obefogad åtkomst och dataexponering (intern risk).

Känsliga data kan exponeras för obehöriga användare om personalens lämplighet inte har verifierats genom säkerhetsklassning och bakgrundskontroller, eller om åtkomsträttigheter inte dras in vid rollbyte/avslut.

Huvudförmåga 2. Hantera identiteter, autentisering och auktorisation

RISK: Förlust av spårbarhet och revisionsförmåga.

Organisationen misslyckas med att föra identifierbara loggar, vilket gör det omöjligt att verifiera eller granska aktiviteter. Detta leder till bristande ansvarsskyldighet vid incidenter.

Huvudförmåga 3. Hantera krypterad digital kommunikation

RISK: Avlyssning och dataläckage under överföring.

Känsliga data exponeras eller manipuleras om kryptering i vila och under överföring inte upprätthålls, eller om externa användare inte identifieras med stark autentisering.

Huvudförmåga 4. Hantering av IT-säkerhet och cybersäkerhet

RISK: Dataintrång och höga sanktionsavgifter.

Brist på robusta säkerhetsåtgärder (brandväggar, IDS/IPS) resulterar i obehörig åtkomst, modifiering eller borttagning av känslig information.

Bristande incidentrapportering leder till att HDAB och myndigheter inte notifieras i tid. Höga sanktionsavgifter kan utdömas om NIS2-kraven inte efterlevs.

Huvudförmåga 5. Hantera IT-förvaltning och driftsäkerhet

RISK: Driftstörningar och dataförlust/återställningsfel.

System kan inte snabbt återställas från rena backuper efter en incident, vilket äventyrar kontinuiteten. Systemfel kan uppstå på grund av bristande patchhantering eller okontrollerad förändringshantering. Juridisk non-compliance om EHD inte raderas eller görs oåterkallelig inom sex månader efter att datatillståndet löpt ut.

Huvudförmåga 6. Hantera leverantörer och tredjepartsrisker

RISK: Kompromettering via leverantörskedjan.

Om SPE Operatören inte begränsar och övervakar underleverantörer med höga behörigheter kan dessa externa parter obehörigt få tillgång till eller behandla hälsodata.

Huvudförmåga 7. Hantera egendomsskydd, fysisk säkerhet

RISK: Fysisk kompromettering och totalt avbrott.

Bristande fysisk säkerhet i datacenter kan leda till att kritisk hårdvara eller infrastruktur skadas av brand, inbrott eller sabotage, vilket leder till systemavbrott.

Huvudförmåga 8. Hantera säker utveckling och design

RISK: Inbyggda sårbarheter.

System och applikationer utvecklas och implementeras med säkerhetsbrister om säkerhet inte byggs in från början i designen.

Huvudförmåga 9. Hantera omvärldsbevakning och risker

RISK: Strategisk riskexponering.

Organisationen misslyckas med att identifiera nya hot, sårbarheter eller regelverksförändringar (t.ex. kring NIS2). Riskbedömningar genomförs, men leder inte till nödvändiga/aktuella åtgärder.

Huvudförmåga 10. Hantera efterlevnad och revision

RISK: Brist på bevisbar efterlevnad.

Inga regelbundna interna och externa revisioner genomförs, vilket gör det omöjligt att bedöma huruvida SPE uppfyller säkerhets, dataskydds och operativa krav.

Huvudförmåga 11. Ledning och styrning av säker miljö

RISK: Organisatoriskt misslyckande och brist på ansvarsskyldighet.

Organisationen saknar ett fungerande ledningssystem för informationssäkerhet (ISMS), vilket är grundläggande. Regelbundna konsekvensbedömningar avseende dataskydd genomförs inte, vilket bryter mot lagkravet.

Huvudförmåga 12. Bearbetningsyta för externa användare

RISK: Datamissbruk och dataläckage.

SPE misslyckas med att snabbt stoppa åtkomst och bearbetningsaktiviteter när missbruk eller dataintrång identifieras. Försenad rapportering till HDAB vid incidenter.

1.1 Prioriterad risklista för bristande hantering av SPE-förmågeområden

KRITISKA RISKER *(Grundläggande efterlevnad och förtroende). Risker i förmågor direkt kopplade till lagkraven om spårbarhet, radering och organisatorisk legitimitet. Ett misslyckande här undergräver hela SPE-konceptet.*

Huvudförmåga 2. Identiteter, Autentisering & Auktorisation

Förlust av spårbarhet och revisionsförmåga. Loggar som identifierar aktören kan inte garanteras eller sparas i minst ett år. Användare kan inte identifieras med stark autentisering.

EHDS (EHDSR-6, EHDSR-7, EHDSR-8, EHDSR-5). Utan loggning och stark autentisering är revision omöjlig och EHDS-kraven är brutna.

KRITISK RISK #1

Huvudförmåga 5. IT-förvaltning och driftsäkerhet

Juridisk non-compliance vid avveckling och dataförlust. Organisationen misslyckas med att radera eller göra all EHD oåterkallelig inom sex månader efter att datatillståndet löpt ut, inklusive backupkopior.

EHDS (OPR-5). Direkt brott mot krav på dataavveckling efter tillståndstidens slut. Samt risk för systemavbrott utan återställning från "rena backuper".

KRITISK RISK #2

Huvudförmåga 10. Efterlevnad och revision

Brist på bevisbar efterlevnad. Inga regelbundna interna eller externa revisioner genomförs för att bedöma efterlevnad av säkerhets, dataskydds och operativa krav.

EHDS (EHDSR-14, OPR-6). SPE-miljön förlorar sin tillit eftersom efterlevnad inte kan bevisas.

KRITISK RISK #3

Huvudförmåga 11. Ledning och styrning av säker miljö

Organisatoriskt misslyckande och brist på ansvarsskyldighet. Organisationen saknar ett fungerande Ledningssystem för informationssäkerhet (ISMS) och att konsekvensbedömning avseende dataskydd inte utförs regelbundet.

GDPR (OPR-12), ISO 27001 (OPR-10). Bristande styrning och ledningsansvar undergräver alla tekniska skydd.

KRITISK RISK #4

Huvudförmåga 12. Bearbetningsyta för externa användare

Datamissbruk och obehöriga datauttag. SPE misslyckas med att snabbt stoppa åtkomst och bearbetningsaktiviteter när missbruk eller dataintrång identifieras. Personliga data kan laddas ner.

EHDS (OPR-20, EHDSR-13). Misslyckande med att begränsa uttag av data är ett grundläggande brott mot hela sekundäranvändningsprincipen.

KRITISK RISK #5

HÖGA RISKER *(Cybermotståndskraft och datasekretess). Risker i förmågor centrala för att skydda data i operativ drift och skydd mot yttre hot (NIS2).*

Huvudförmåga 4. Hantering av IT-säkerhet och cybersäkerhet

Dataintrång och höga sanktionsavgifter. Brist på robusta säkerhetsåtgärder (brandväggar, kryptering, IDS/IPS) och otillräcklig incidentrapportering till HDAB och relevanta myndigheter.

NIS2 Direktivet, EHDS (OPR-18, OPR-22). Den nya cybersäkerhetslagen (NIS2) medför högre sanktionsavgifter vid bristande efterlevnad. Fel i incidenthanteringen riskerar böter och förtroendeförlust.

HÖG RISK #6

Huvudförmåga 3. Krypterad digital kommunikation

Avlyssning och dataläckage under överföring. Känsliga data exponeras eller manipuleras om de inte är i skyddat format i vila och under överföring.

EHDS (SDR-3, SDR-4). Direkt brott mot kravet på kryptering. Utan fungerande Statlig e-legitimation på högsta tillitsnivå (yttre beroende till SPE), kan stark identifiering (EHDSR-5) inte garanteras.

HÖG RISK #7

Huvudförmåga 9. Hantera omvärldsbevakning och risker

Strategisk riskexponering utan åtgärd. Riskbedömningar genomförs, men leder inte till nödvändiga åtgärder. Omvärldsbevakare och analytiker misslyckas med att notera förändringar i regelverk som NIS2 och GDPR m.m.

EHDS (EHDSR-15, EHDSR-16). Riskhanteringsprocessen blir verkningslös och organisationen utsätter sig för okända hot och regulatoriska brott.

HÖG RISK #8

MEDELRISKER *(Stödjande säkerhet och kontinuitet). Risker i förmågan att stärka organisationen inifrån och skydda mot fysiska händelser. Konsekvensen är hög men oftast sekundära till KRITISK/HÖG, kan i vissa fall mildras genom redundans.*

Huvudförmåga 1. Hantera personalsäkerhet

Obefogad åtkomst och dataexponering (intern risk). Personal som inte genomgått rollspecifik utbildning i GDPR/säkerhet eller säkerhetsklassning ges åtkomst till känsliga data.

Säkerhetsskyddslagen, GDPR (OPR-23). Risk för interna hot eller oavsiktlig exponering av data (SPER-4).

MEDEL #9

Huvudförmåga 7. Hantera egendomsskydd, fysisk säkerhet

Fysisk kompromettering och totalt avbrott. Brist på redundans och geografisk spridning av datacenter eller avlyssning/intrång i säkra IT-utrymmen.

CER-direktivet, MSB Vägledning. Äventyrar kontinuitet (OPR-24) men katastrofskydd finns ofta via backup.

MEDEL #10

Huvudförmåga 6. Hantera leverantörer och tredjepartsrisker

Kompromettering via leverantörskedjan. SPE Operatören misslyckas med att begränsa antalet underleverantörer med höga behörigheter.

EHDS (OPR-2). Risk för att en extern part obehörigt får tillgång till hälsodata via en opålitlig leverantör.

MEDEL #11

LÄGRE RISK *(Proaktiv kvalitetssäkring). Detta område är viktigt för långsiktig stabilitet och för att minska framtida risker, men dess misslyckande leder inte omedelbart till ett brott mot EHDS:s operativa krav (OPR) utan snarare till inbyggda sårbarheter.*

Huvudförmåga 8. Hantera säker utveckling och design

Inbyggda sårbarheter. System och applikationer utvecklas utan att säkerhetskrav byggs in från början, vilket leder till ökade sårbarheter.

OPR-13. Brist på säkerhetsarkitektur och kodgranskning, vilket riskerar systemens långsiktiga hållbarhet.

De kritiska förmågeområdena (2, 5, 10, 11 och 12) är i prioritet, eftersom de rör den obligatoriska juridiska strukturen (GDPR, EHDS) och SPE:s existensberättigande. Utan stark styrning och spårbarhet kan ingen mängd teknisk säkerhet rädda miljön från sanktioner eller förlust av auktorisation.

2. Risker kopplade till Nationell Digital Infrastruktur

RISK: Avsaknad av lösning för statlig e-legitimation med högsta tillitsnivå**.**

Utan en heltäckande lösning för identitetsregistrering och certifikathantering enligt EU:s reviderade eIDAS-förordning riskerar Sverige att:

- *Inte uppfylla EU:s krav på nationella digitala identiteter.*
- *Förlora interoperabilitet med andra medlemsstater, vilket försvårar gränsöverskridande digitala tjänster.*
- *Skapa säkerhetsluckor vid identitetsverifiering och certifikatsutfärdning.*
- *Bristande spårbarhet i registreringsprocessen underminerar tillit och rättssäkerhet.*

RISK: Avsaknad av nationellt adressregister för säker krypterad kommunikation.

Utan ett centralt adressregister med verifierade adresser och certifikat riskerar den digitala förvaltningen att:

- *Kommunikationen mellan myndigheter och organisationer sker via osäkra eller inofficiella kanaler.*
- *Ökad risk för dataintrång, informationsläckage och man-in-the-middle-attacker.*
- *Försvårad identifiering av behöriga aktörer.*
- *Ineffektivitet och höga kostnader för att upprätthålla säker kommunikation på egen hand.*

RISK: Avsaknad av nationell kontaktpunkt (NCP) mot EU:s digitala infrastruktur.

Utan en fungerande NCP som kopplar svenska system till EU:s gemensamma digitala infrastruktur riskerar Sverige att:

- *Inte kunna delta fullt ut i europeiska digitala tjänster och datautbyten.*
- *Skapa hinder för interoperabilitet och standardisering mellan medlemsstater.*
- *Öka risken för felaktig autentisering och certifikathantering vid gränsöverskridande kommunikation.*

Bilaga 1: Verksamhetsarkitektur för säkra behandlingsmiljöer (SPE).