Stockholms stad

Ledningens genomgång 2023

Bromma stadsdelsförvaltning

Beslutad 2023-11- 29
Reviderad 2023-11-12

Ledningens genomgång

Dnr: BRO 2023/526

Kontaktperson: Mattias Pettersson

1 Sammanfattning

Dokumentet Ledningens genomgång innehåller analyser och förslag på aktiviteter för att förbättra dataskyddsarbetet.

Bromma stadsdelsförvaltning och staden arbetar utifrån standard ISO 27001. Här finns det beskrivningar på hur arbetet ska genomföras utöver de angivna riktlinjerna.

Informationssäkerhet fastställs genom klassning och är en del av dataskydd utifrån fokus på it-tjänstens utformning och skyddsvärde.

Skyddsnivåerna kopplas till den information som förvaras eller behandlas där rutiner för användare, systemens innehåll och utformning, samt var systemen finns placerade fysiskt.

Förbättringsförslagen i detta dokument rör dokumentation, budget och organisering för år 2024, 2025, 2026.

Förklaringar av förkortningar eller processer förklaras i särskild bilaga med länkar.

Innehållsförteckning

2 Ledningssystem för informationssäkerhet - LIS

Ledningssystem för informationssäkerhet (LIS) är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter vilket består av Stockholms stads övergripande tillämpningsanvisningar för informationssäkerhet samt de rutiner, guider och anvisningar som finns antagna. Bromma stadsdelsförvaltning har den 25 april 2023 antagit lokala tillämpningsanvisningar. I de lokala tillämpningsanvisningarna finns till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning.

En stor del av arbetet med att driva ett ledningssystem, handlar om att informera medarbetare om de regler som ingår i ledningssystemet.

Ledningens genomgång är en del i ett systematiskt informationssäkerhetsarbete. Ledningen ska hålla sig informerad om informationssäkerheten i sin verksamhet. Stadsdelsnämnden är informations- och personuppgiftsansvarig medan förvaltningschefen är operativt ansvarig och ska se till att resurser finns, samt att medarbetare har den utbildning och information som krävs för uppdraget.

Övergripande informationssäkerhetsansvarig finns på stadsledningskontoret. Lokalt i nämnden finns en informationssäkerhetssamordnare (ISAM). Informationssäkerhetens ansvar ska följa linjeorganisationens. Nämnden arbetar utifrån stadens riktlinjer och tillämpningsanvisningar och ska anta den lokala anvisningen.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, *Ledningens genomgång,* från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för

utbildning av medarbetare eller om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltningschefen ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen, och i det interna arbetet uppnå tillräcklig intern kontroll.[1]

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024*[2] uppmanas samtliga nämnder och bolagsstyrelser att ta fram en treårig plan för informationssäkerhetsarbetet där dokumentet Ledningens genomgång ska biläggas verksamhetsplanen. Den treåriga planen ska följa dokumentet *Riktlinje för informationssäkerhet* i Stockholms stad och redovisas både i Ledningens genomgång och i nämndens verksamhetsplan under mål 3.5.

Inventering och informationsklassning är grunden i informationssäkerhetsarbetet. För 2024 är därför registerförteckning och informationsklassning särskilt prioriterat i *Ledningens genomgång*.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten, alternativt se över och uppdatera genomförda klassningar.

3 Omvärldsbevakning – hot, trender och ny lagstiftning

3.1 AI- utvecklingen

Informationen under rubriken AI-utveckling kommer från Myndigheten för digital förvaltning (Digg).

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet
[2] anvisningar-for-namndernas-arbete-med-verksamhetsplan-2024.pdf (stockholm.se)

Regeringen vill stärka Sveriges välfärd och konkurrenskraft genom att se till att myndigheter, kommuner och regioner blir bättre på att använda artificiell intelligens (AI). Det ska ske genom att samla kunskap och erfarenheten från de som kommit längst i AI-utvecklingen.

Om myndigheter, kommuner och regioner skulle införa den AI-teknik som finns idag skulle det kunna innebära att samhället sparade 140 miljarder kronor varje år. Det visar beräkningar som Digg har gjort. De största utmaningarna är bland annat kompetensbrist, tillgång till användbara data, kunskap om tillgänglig teknik samt juridiska och etiska frågor.

Med anledning av detta gav regeringen Arbetsförmedlingen, Bolagsverket, Digg och Skatteverket i uppdrag att göra det enklare för offentlig förvaltning att använda sig av artificiell intelligens (AI) med syftet att stärka Sveriges välfärd och konkurrenskraft. Digg ledde uppdraget.

3.1.1 Påverkan Bromma stadsdelsförvaltning

AI-tekniken är ny och det finns en generell kompetensbrist i samhället. Utvecklingen av tekniken sker i snabb takt och eventuella hot är i dagsläget okända.

3.2 NIS2 – skärpta lagstiftningar

NIS står för ”The Directive on security of network and information systems”, och på svenska heter direktivet ”åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen”. Kortfattat ställer NIS-direktivet krav på säkerhet i nätverk och informationssystem för samhällsviktiga tjänster. Syftet med NIS2 är att säkerställa en hög nivå av informationssäkerhet i hela EU genom att stärka skyddet av samhällsviktiga tjänster som en följd av den ökade digitaliseringen och hotbilden av cyberhot.

Direktivet omfattar nedan områden och för stadsdelsnämnden är det specifikt direktiv gällande hälso- och sjukvård som är aktuell.

- Bankverksamhet
- Digital infrastruktur
- Energi
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Leverans och distribution av dricksvatten

- Transport

I februari 2024 är regeringens utredning klar om hur lagen ska omhändertas i Sverige.

3.2.1 Påverkan på Bromma stadsdelsförvaltning

Bromma stadsdelsnämnd kommer att påverkas av det uppdaterade NIS-direktivet då fler leverantörer kan bli berörda av direktivet än de är idag. Detta innebär att kravkompletteringar behöver ställas vid upphandlingar så att direktiven tas med. Befintliga rutiner vid Bromma stadsdelsnämnd behöver uppdateras och implementeras under 2024 och gälla från och med 2025.

3.3 Datorer och mobiler och IOT (Internet Of Things)

Fler enheter kommer att bli uppkopplade och fler enheter än tidigare kommer att ha fast eller trådlös uppkoppling. Detta är i de allra flesta fallen önskvärt, men ställer allt större krav på att vi vet hur enheterna fungerar, och att vi förstår hur information flödar mellan olika system och tjänster. Ett exempel inom verksamheterna i Bromma är att vissa robotdammsugare har kameror för bättre rumsorientering.

3.3.1 Påverkan på Bromma stadsdelsförvaltning

Med AI och uppkopplingar mot nätet kan bilder skickas från exempelvis verksamheter. Med bildigenkänning kan robotdammsugaren enkelt se allt du har i hemmet och identifiera vem du är med ansiktsigenkänning. Antingen som en del av tjänsten, eller om den hackas, kan enheten förmodligen skicka bilder och skanna synliga texter. Allt med risk för spridning.
Det kommer ställas stora krav på organisationen och enskilda medarbetare att hantera och veta vilken utrustning som får användas var. En utmaning är det ökade arbetet som sker från andra platser än kontoret, och uppkopplad utrustning som finns i till exempel hemmet.

3.4 Hotaktörer - cybersäkerhet

Det går att läsa följande i MSB:s rapport från 2020 ”De cyberhot som riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av aktörer. I huvudsak kan de delas upp i statliga aktörer och kriminella grupperingar. I viss omfattning förekommer även ideologiskt motiverade aktörer, såsom hacktivister eller

grupperingar med terrorkopplingar. Statliga aktörer som genomför cyberangrepp mot Sverige har oftast som syfte att inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen, eller att stärka det egna landets ekonomi och industriella utveckling genom industrispionage.

Kriminella grupperingar som genomför cyberangrepp vill i de flesta fall tjäna pengar genom till exempel ransomware-attacker där utsatta företag krävs på lösensummor, medan ideologiskt motiverade aktörer tenderar att agera enligt sina egna formulerade agendor.”

3.4.1 Påverkan på Bromma stadsdelsförvaltning

Fenomenet med hacktivister som vill meddela att säkerheten är dålig inom staden och till stadens leverantörer förekommer några gånger per år. Det behövs kunskap hos medarbetarna för att kunna möta upp de hot som finns från kriminella grupperingar. Rutiner för personalsäkerhet behöver också sammanlänkas med informationssäkerhetsarbetet.

4 Vad händer inom staden – lokala förändringar eller satsningar

Nya e-utbildningar ska lanseras centralt av staden och kommer att innefatta åtta olika områden. Samtliga områden är under uppbyggnad och ett nytt område kommer att presenteras varje månad under 2024. Dessa utbildningar kompletterar det befintliga e-utbildningarna. Förvaltningsledningen genomgår dessutom en utbildning som erbjuds via stadsledningskontoret i informationssäkerhet under 2023.

Antalet it- tjänster ökar i Stockholms stad och så även i Bromma stadsdelsnämnd. It-tjänsterna blir ofta mer integrerade och flöden i och mellan system kräver informationsskydd under hela livscykeln. Det är viktigt att så långt som möjligt minimerar möjligheter till manuella fel, det vill säga. den mänskliga faktorn. Det är också viktigt att ställa höga krav på upphandlingar och upphandlingskrav både gällande it-design och it-arkitektkrav, fysisk teknik och även medarbetares kunskap och fortbildning.

Utmaningar och förseningar med olika leveranser till verksamheter gör att alternativa rutiner eller arbetssätt används, men även i dessa fall måste regelverken och rutiner uppfyllas. Ett exempel på detta är

när verksamheterna inte får tillgång till arbetsverktyg eller it-tjänster, och därför skapar egna manuella rutiner, vilka kan brista i säkerhet.

En tydligare skiljelinje mellan lokala system och molnbaserade system ökar. Lagar som GDPR och NIS2 påverkar olika leverantörer som erbjuder alternativ till molntjänster. Dessa har inte alltid de bästa verksamhets- och säkerhetslösningarna.

Med PM3-modellens införande i staden under kommande år, blir också kopplingen mellan verksamhetens behov och skyddskrav av information och central it-utveckling tydligare.

5 Uppföljning av tidigare beslut

Beslut om informationssäkerhetsarbete har tagits av förvaltningen genom att de lokala tillämpningsanvisningarna fastställdes av direktör 2023-04-25. I den beskrivs förvaltningsspecifik organisation, årshjul och rutiner för verksamheten som rör informationssäkerhetsarbetet.

5.1 Uppföljning av roller i de lokala tillämpningsanvisningarna

Tabellförklaring

Grönt	Gult	Rött
Inga anmärkningar eller brister behöver åtgärdas omgående	Brister och anmärkningar behöver åtgärdas med handlingsplan.	Omgående åtgärder behöver tas fram och implementeras.

Funktion i organisation	Roll enligt anvisning	Status
Ledning	Utse nödvändiga roller inom organisationen samt anta de lokala tillämpningsanvisningar. Tillse att resurser finns och medarbetare har den utbildning och information som krävs för uppdraget.	• Lokala tillämpningsanvisningar är antagna. • De flesta system som är identifierade har objektägare, men en del saknas. Bedömningen är att det saknas svar på cirka 30% av systemen. • Under 2024 bör fokus vara att sprida informationen från förvaltningsledningen till samtliga verksamheter.
Chefer	Utreda incidenter, säkerställa registervård, göra	• Stora kunskapsluckor finns om

	inköp i enlighet med gällande lagar och styrdokument, klassa viktiga tillgångar, ta fram lokala rutiner för den egna verksamheten utifrån behov.	informationssäkerhet och de arbetsuppgifter som finns angivna. • Brister förekommer i registervård och uppföljning. • Lokal förankring och dokumentation behöver förbättras.
Processägare	Äger processer inom verksamhetsområde inom klassificeringsstrukturen. Fattar beslut när osäkerhet uppstår vid hantering av information.	• Olika verksamheter har olika benämningar och alla har inte uttalade processägare. • Hanteringsanvisningens processer är inte implementerat vilket gör att det blir svårt att se vem som äger informationsflöden.
Objektägare	Ansvarar för informationstillgången (objekt) och utser objektledare.	• Delvis utsedd roll inom förvaltningens olika system. Behöver kompletteras under 2024.
Objektledare	Ansvarar för informationssäkerhet i objekt genom att se till att dokumentation finns på plats och att rutiner finns och följs.	• Objektledare är inte utsedda för samtliga objekt. • Objektledare arbetar inte självständigt och det finns osäkerhet i arbetsuppgiften för att till exempel ta fram rutiner. • Utbildning och information till rollinnehavaren behöver förbättras.
ISAM	Att vara kontaktpunkt, rådgöra, samverka och stödja,	• Bedömt av Stadsdels-direktören

	omvärldsbevaka och följa upp.	
DSO	Vägleda, informera, självständigt bevaka de registrerades intressen.	• Bedömt av Stadsdels-direktören
ILS-samordnare	Stödjande inom sina respektive områden.	• Utveckla samarbetet med informationssäkerhet för att förankra exempelvis utbildningskrav i verksamheten och integrera som en del av arbetssättet att få fler brister åtgärdade.
Arkivansvarig och arkivarie	Stödjande inom sina respektive områden.	• Bedöms ge det stöd som behövs i verksamheterna.
Stadsdelsarkivarie	Stödjande inom sina respektive områden.	• Bedöms ge det stöd som behövs i verksamheterna.

5.1.1 Uppföljning årshjul

Aktivitet	Resultat
Tertial 1 Ambassadörsnätverk Årsrapport Ledningens genomgång Klassning av förvaltningens mest skyddsvärda information Årlig klassning, som en del av det systematiska informationssäkerhetsarbetet, av förvaltningens mest skyddsvärda information	Under tertial 1 2023 har nätverket med så kallade ambassadörer ersatts av objektägare och objektledare enligt PM3-modellen Årsrapport inlämnad till Bromma stadsdelsnämnd 2022 Arbetet påbörjat enligt PM3-modellen

Uppdatering av årshjul gällande informationssäkerhet	Startar 2024
Dataskyddsombudet anordnar utbildningstillfälle för stadsdelsnämnden	Årshjulet uppdaterat
Dataskyddsombudets årsrapport lämnas till nämnden	Genomfört vid dragning av Dataskyddsombudets årsrapport
Objektledarna ska genomföra kontroller av behörigheter	
Uppdatera rutin för NIS-incidenter	Genomfört januari 2023 för år 2022
T1 rapport	Arbetet påbörjat 2023 och pågår under 2024
	Genomfört genom Medicinskt ansvarig sjuksköterska (MAS) Behöver ses över efter NIS2 utredningen är klar i februari 2024
	Genomfört
Tertial 2 Uppdatera registerförteckning personuppgiftsbehandlingar	Uppdatering genomförd
Ta fram/ uppdatera verksamhetens rutiner för informationssäkerhet/GDPR	Rutin framtagen för utlämnande av allmänna handlingar, gallring av arkivhandlingar, behörighetsrutiner, rutin för e-post och posthantering, och rutin för rent skrivbord, ren skärm, förvaring av dokument samt rutin för
Kontrollera och uppdatera informationstillgångarna i ISAMs förteckning	

Granska PUB-avtal/leverantör (DSO och Arkivarie) T2 rapport	utskrifter, rutin för diarieföring och hantering av allmänna handlingar Pågår löpande Redovisas i Dataskyddsombudets årsrapport Genomfört
Tertial 3 Granska och uppdatera styrande dokument gällande: • incidenthantering • hantering av personuppgifter • lokala tillämpningsanvisningen • information på Intranätet • upphandling Kontrollera och uppdatera informationsklassningarna Följa upp informationssäkerhetsincidenter som skett under året Se över dataskydds- och informationssäkerhetsorganisationen Uppföljning genomförda utbildningar för medarbetare och chefer. (ISAM tar ut rapport) Verksamhetsberättelse ISAM Rapport Ledningens genomgång	Genomfört Genomförs löpande Görs kontinuerligt under året Genomförs av förvaltningsledningen Genomfört Genomfört

GDPR Årsrapport framtagning (DSO)	Pågår

5.1.2 Uppföljning av mål i verksamhetsplanen (VP) 2023

VP mål	Resultat
Förvaltningens enheter har genomfört åtgärder som innebär att informationssäkerhetsarbetet inom förvaltningens verksamheter har stärkts	Har delvis genomförts under 2023. Brister finns då annat har prioriterats av verksamheterna.
Föreläsning/workshop för chefer om vad det innebär att arbeta systematiskt med informationssäkerhet på avdelnings- och enhetsnivå (T1).	Genomförts T1
Alla enheter ska under tertial 1 identifiera behov av åtgärder som säkerställer att stadens riktlinjer för informationssäkerhet tillämpas inom förvaltningens alla verksamheter	Har delvis genomförts under 2023. Brister finns då annat har prioriterats av verksamheterna.

5.1.3 Uppföljning av tidigare förslag från ISAM

Rekommendation	Resultat
• Fastställa och anta lokal anvisning gällande informationssäkerhet enligt tillämpningsanvisning från SLK	Genomförd 2023-04-25
• Fastställa och kommunicera budget och mandat	Nytillträdd förvaltningschef 2023 i T3. Mandat och budget för 2024 inväntas vid rapportens skrivning
• Fastställa ”Laglista” om den saknas eller inte är uppdaterad. De lagar vi stödjer oss främst	Författningsanalys behöver kompletteras av verksamheten 2024

på i våra personuppgiftsbehandlingar	
• Se över rutiner för LISsystem	Ej genomfört och ska kompletteras med införande av PM3-organisationen

5.2 Resultatet från revisioner

Avseende informationssäkerhet har en revision, ”Efterlevnad till NIS-direktivet” genomförts. Granskning har genomförts i syfte att bedöma om kommunstyrelsen och stadens nämnder bedriver ett informations-säkerhetsarbete i enlighet med de bestämmelser som framgår av NIS-direktivet och stadens riktlinjer.

Slutsatsen är att det inte bedrivs ett systematiskt arbete i enligt med de lagkrav som finns. Lagkravet är ett EU-direktiv som avser att uppnå en hög gemensam säkerhetsnivå i hela EU. I Sverige regleras NIS-direktivet genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. I korthet innebär lagstiftningen krav på systematiskt informationssäkerhetsarbete och incidentrapportering för verksamheter som ansvarar för tjänster som är av avgörande betydelse för att upprätt-hålla viktiga samhällsfunktioner.

Revision har gjorts i maj genom granskning av EK-katalogen och ett frågeformulär, utan anmärkning.
Behörighetskontroll i systemet Life-Care genomförts på uppdrag av systemägaren Region Stockholm, utan anmärkning.

5.2.1 Risker som identifierats i dataskyddsombudets årsrapport 2022

Redovisas i dataskyddsombudets årsrapport för 2023 i samband med verksamhetsberättelsen.

6 Förbättringar för verksamhetens LIS

Förslagen till förbättringar avser perioden 2024-2026 utifrån dagens omvärldsläge och styrkor/svagheter i nämndens arbete. Då ledningens genomgång sker årsvis som en del av det systematiska arbetet, kommer anpassningar och nya krav att hanteras och föreslås., Detta som en naturlig del av arbetet kommande år.

Denna rapport utvärderar innevarande och föregående års aktiviteter. Eventuella förbättringsförslag eller bristeranalyseras och förslag läggs fram vid nästa rapport som kommer 2024.

6.1 Förbättringsaktiviteter under 2024

- Uppdatera tillämpningsanvisning gällande rutiner för NIS2 och de senaste lagkraven inom till exempel AI och policys från staden.

- Alla it- tjänster ska ha objektägare och objektledare utnämnda, enligt PM3-modellen. De beskrivs i tillämpningsanvisningen.

    - För att kunna genomföra de klassningar, handlingsplaner och riskanalyser som krävs, måste det finnas personer utsedda att göra detta.

- Alla it- tjänster ska vara inventerade och klassningsnivå ska vara fastställd för respektive system. KRT, det vill säga Konfidentialitet, Riktighet och Tillgänglighet ska finnas och ligga till grund för prioriteringsordning.

    - Enheter ska inventera it- tjänster och dessa ska dokumenteras enligt PM3-modellen.

- Prioritera klassningar av system som omfattas av NIS2-lagstiftningen.

- NIS2 ställer mycket högre krav än den tidigare versionen, NIS. Denna omfattar samhällsviktiga system som kan påverka många eller samhället i stort. Riktade insatser så att nyckelpersoner utbildas i de lokala tillämpningsanvisningarna.

  - Utöver alla chefer och medarbetare som ska arbeta med informationssäkerhet, behöver vissa nyckelroller ytterligare kunskaper. Fokus bör ligga på att stärka kunskap och förståelse för informationssäkerhet och hur den ska efterlevas i verksamhetsplanen, ILS och budgetarbete hos förvaltningens samtliga metodutvecklare, processägare och verksamhetskontrollers.

- Förslag på fler uppföljningstillfällen som följer VP-arbetet i övriga förvaltningen.
  - Informationssäkerhetsarbetet stäms av i formella processer årligen. Arbetet med detta behöver delas upp och bättre hanteras löpande under ett verksamhetsår. Att göra bra analyser samtidigt som arbetet med verksamhetsberättelsen pågår i slutet av året, är en utmaning. Den bör följa stadens övriga tertialarbete.

6.2 Förbättringsaktiviteter under 2025

- NIS2 ska vara implementerad inom Bromma stadsdelsnämnd.

- Fokusera på kontinuitetsplaner och riskanalyser för de system som saknar sådana.
  - Alla staden processer bör riskbedömas för de processer som bedöms behöva det, hanteringsanvisning tas fram gällande dataskydd, förslagsvis tillsammans med säkerhetssamordnare.

- Stärka och förbättra rutinerna gällande informationssäkerhet vid upphandlingar och inköp.
  - Redan vid inköp och i referensgrupper för upphandlingar bör dataskydd beaktas. Kan i värsta fall ur ekonomisk synvinkel leda till att man inte kan använda nya it-tjänster. De blir betydligt dyrare efter extra skyddsåtgärder, eller så införs system utifrån riskfaktorer som inte är tillräckligt säkra.

- Förslag på hur man bör säkerställa kunskapsöverföring vid omorganisationer eller vid personalförändringar.
  - Att jobba på ett bra sätt med informationssäkerhet tar tid att lära sig. Man måste tillägna sig kunskaper som man oftast inte har fått via skolans utbildningar eller via den

kärnverksamhet där man är verksam. Man behöver öva dessa i praktiskt arbete och sätta sig in i rutiner och processer. Det är idag en utmaning när medarbetare slutar/börjar. Det tar lång tid att lära upp, men den största förlusten är verksamhetskännedomen, medarbetare som slutar har unik kunskap om sin verksamhet som riskerar att gå förlorad.

- Intern förankring av beslut och rekommendationer att säkerställa information i linjeorganisationen.
  - Det finns idag olika kunskap hos chefer, både inom och mellan våra förvaltningsområden. Vanligaste förklaringen till att man inte har hört om det kan vara att man inte förstått, men slutresultatet är ofta det samma. Det är brister i rutiner och processer.

- Förslag på kontroll och genomförandet av obligatoriska utbildningar. Kurser bör genomföras enskilt, kunskapstestet slår inte väl ut när det genomförs i grupp. Statistik och uppföljning, vilka som gått obligatoriska kurser är svart att följa upp.
  - En bättre uppföljning av vilka kurser, deras innehåll och hur de genomförs skulle förbättra förankringen hos den enskilda medarbetaren. Uppföljning försvåras om kurser som är tänka att vara individuell genomförs i grupp. De som saknar viss kunskap får inte den chans de behöver för att tillägna sig den.

6.3 Förbättringsaktiviteter under 2026

- Under 2026 utveckla rutiner där säkerhetssamordnare och ISAM kartlägger risker kopplat till dataskydd, där informationssäkerhet är en delmängd. En helhetssyn tas fram för informationssäkerhetsarbete med berörda samordnare som gör gemensam risk- och sårbarhetsanalyser.

- Tydligare mandat och en budgetstyrning kopplad mot dataskydd bör tas fram. Medel måste reserveras utöver det som rör inköp och upphandling. Det arbete som måste läggas ner på kontroller och skapande av formalia, är i många fall en stor del av kostnaden i tid räknat vid införande av nya it- tjänster.

7 Länkarkiv

Ledningssystem för informationssäkerhet (LIS) (msb.se)

Dataskydd för verksamheter | IMY

NIS 2 | SKR

IoT – så funkar det - IoT Sverige

Sverige ska bli ledande inom artificiell intelligens | Digg

Hotaktörer (msb.se)

KLASSA, informationsklassning | SKR