Stockholms läns sjukvårdsområde
Närsjukvårdsdirektören

ANMÄLAN
2025-03-03

SLSO 2025-0840

Årsrapport informationssäkerhet för verksamhetsåret 2024

Årsrapport informationssäkerhet för verksamhetsåret 2024 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Årsrapport för informationssäkerhet 2024

Innehåll

Årsrapport för informationssäkerhet 2024 1
Inledning 3
Ett systematiskt och riskbaserat informationssäkerhetsarbete 4
Förslag till åtgärd 10
Informationssäkerhetssamordnarens roll 10
Förslag till åtgärd 11
Dataskyddsorganisation 12
Förslag till åtgärd 12
Egenkontroll och anskaffning av IT-stöd 12
Förslag till åtgärd 15
Utbildning 15
Förslag till åtgärd 17

Bild 1 6
Bild 2 7
Bild 3 7
Bild 4 8
Bild 5 8
Bild 6 8
Bild 7 9
Bild 8 9
Bild 9 13
Bild 10 15
Bild 11 16
Bild 12 16

Inledning

Information utgör en av SLSO:s mest betydande tillgångar och är en grundläggande förutsättning för en säker och effektiv verksamhet samt för framsteg inom digitaliseringen. Informationssäkerhet innebär att skydda informationen på ett säkert sätt, oavsett om den är lagrad på papper, digitalt eller muntligt.

Inom ramen för Region Stockholms övergripande ledningssystem för informationssäkerhet är det SLSO:s ansvar att styra och leda sitt informationssäkerhetsarbete genom ett ledningssystem inom sitt verksamhetsområde. Det lokala ledningssystemet ska säkra ett systematiskt informationssäkerhetsarbete och upprätthålla en riskavvägd skyddsnivå i verksamheten. Detta system är en integrerad del av nämndens eller bolagets ordinarie ledningsarbete. Region Stockholms riktlinje för informationssäkerhet, baserad på den internationella standarden för informationssäkerhet, ISO 27000-serien, konkretiserar Region Stockholms policy för verksamhetsskydd.

Inom det systematiska informationssäkerhetsarbetet är det av högsta vikt att identifiera hot, sårbarheter och risker. Därefter bör adekvata säkerhetsåtgärder införas för att minska dessa till en nivå som är acceptabel för SLSO, med hänsyn till konfidentialitet, riktighet och tillgänglighet. Det är avgörande att medborgare och medarbetare kan lita på att den information SLSO hanterar skyddas på ett tillfredsställande sätt. Ett systematiskt informationssäkerhetsarbete involverar strukturerad planering, resursallokering och medvetna beslut för att skydda rätt information på rätt sätt. Det systematiska informationssäkerhetsarbetet ska stärka förmågan att undvika negativa händelser som kan påverka SLSO:s verksamheter. Vid inträffandet av en negativ händelse bör den kunna hanteras på en acceptabel nivå, samtidigt som förtroendet från Region Stockholms intressenter bibehålls.

Om informationssäkerhetsarbetet inte följer de lagkrav som ställs kan det medföra konsekvenser, inklusive att arbetet inte upprätthålls med den kvalitet som förväntas. Detta kan i sin tur leda till att SLSO:s informationstillgångar inte hanteras på ett korrekt sätt.

Ledningens genomgång utgör en central del enligt standarden för informationssäkerhet (SS-ISO/IEC 270001:2017) och är även ett krav enligt Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40). Informationssäkerhetssamordnarens och ledningens roll är i

detta sammanhang att granska och revidera det systematiska informationssäkerhetsarbetet vilket syftar till att säkerställa informationssäkerhetsarbetets fortsatta lämplighet, tillräcklighet och effektivitet. Årsrapporten för informationssäkerhet utgör en viktig del av denna genomgång och redovisar informationssäkerhetssamordnarens iakttagelser och arbete under verksamhetsåret 2024.

Ett systematiskt och riskbaserat informationssäkerhetsarbete

Enligt avsnitt 1.2.1 i Region Stockholms riktlinjer för informationssäkerhet framgår att varje nämnd och bolag bör, inom ramen för Region Stockholms övergripande ledningssystem för informationssäkerhet, styra och leda sitt informationssäkerhetsarbete genom ett ledningssystem inom sitt verksamhetsområde. Det lokala ledningssystemet bör säkerställa ett systematiskt informationssäkerhetsarbete och en riskavvägd skyddsnivå i verksamheten och vara en integrerad del av nämndens eller bolagets ordinarie ledningsarbete.

Utöver kravet på ett systematiskt informationssäkerhetsarbete enligt Region Stockholms styrdokument, klassificeras även SLSO som en leverantör av en samhällsviktig tjänst enligt Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster – vanligtvis känd som NIS-direktivet. Enligt detta direktiv åligger det SLSO att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster inom hälso- och sjukvården. NIS-direktivet har sedan dess tillkomst ersatts av NIS2 vilken kommer införlivas i svensk rätt genom ny lag (Cybersäkerhetslagen) och förordning tidigast sommaren 2025. Efter att lag och förordning trätt i kraft kan föreskrifter utfärdas av utsedda myndigheter. I korthet innebär förändringen följande:

- **Utökat tillämpningsområde** – Fler sektorer och verksamheter omfattas, inklusive offentliga förvaltningar, livsmedelssektorn och tillverkning av kritiska produkter.
- **Skärpta säkerhetskrav** – Organisationer måste implementera mer omfattande cybersäkerhetsåtgärder, inklusive riskhantering, incidentrapportering och leverantörssäkerhet.
- **Strängare tillsyn och sanktioner** – Nationella myndigheter får större befogenheter att övervaka efterlevnad, och sanktioner för bristande efterlevnad blir hårdare.

- **Tydligare incidentrapportering** – Krav på snabbare rapportering av cybersäkerhetsincidenter, med initial rapport inom 24 timmar och en slutrapport inom en månad.
- **Bättre samarbete mellan EU-länder** – Ett starkare samarbete mellan medlemsländer och enhetligare regler för att hantera cybersäkerhetshot på EU-nivå.

Flertalet aktiviteter sker gemensamt inom Region Stockholm utifrån den förändrade kravbilden och drivs primärt utifrån avdelningen för informationssäkerhet på RLK.

För att bedöma om SLSO och dess verksamheter bedriver ett systematiskt informationssäkerhetsarbete kan informationssäkerhetssamordnaren använda Compliance Portalen, Region Stockholms IT-stöd för egenkontroller. Frågorna i egenkontrollen hämtas från kraven i Region Stockholms riktlinjer för informationssäkerhet samt ISO 27000-standarden. Svaren ger därmed en indikation om SLSO:s strategiska och verksamhetsnära arbete med informationssäkerhet och informationssäkerhetssamordnaren anser att det är av yttersta vikt att inte bara det strategiska arbetet kontrolleras utan att detta görs löpande i SLSO:s verksamheter. Egenkontrollen tar cirka en timme i anspråk och ger verksamheten möjlighet att förbättra sin informationssäkerhetskultur samt ger en bild av i vilken omfattning verksamheten uppfyller Region Stockholms informationssäkerhetskrav. Egenkontrollen leds av informationssäkerhetssamordnaren och oftast deltar två personer från verksamheten, vanligtvis verksamhets-/enhetschef samt en sekreterare. Utifrån egenkontrollerna så är det informationssäkerhetssamordnarens bedömning att det finns förbättringspotential i det systematiska och riskbaserade arbetssättet med informationssäkerhet.

Informationssäkerhetssamordnare kan styrka sin bedömning genom ett axplock av svar från elva egenkontroller från olika verksamheter gällande påstående huruvida verksamheten arbetar systematiskt med behörighetskontroller. Antalet genomförda egenkontroller kan anses vara lågt. Det ska sägas att en egenkontroll kan inbegripa flera verksamheter, exempelvis så är egenkontrollen av ”Hjälpmedelsverksamheterna” bestående av fem verksamheter.

Bild 1 åskådliggör att utav elva verksamheter så arbetar endast fem verksamheter systematiskt med att kontrollera medarbetares behörigheter till IT-system som används. Bristande behörighetskontroll är en allvarlig risk som utsätter SLSO för en rad sårbarheter och konsekvenser så som obehörig åtkomst, dataskyddsbrott och bristande efterlevnad av lagar och

styrdokument. Myndigheten för samhällsskydd och beredskap (MSB) nämner även i sin rapport ”Cyberangrepp mot samhällsviktiga informationssystem[1]” att behörighetshantering är en utav fem identifierade problemområden där statliga myndigheter och leverantörer av samhällsviktiga tjänster behöver stärka sitt skydd mot cyberangreppsförsök.

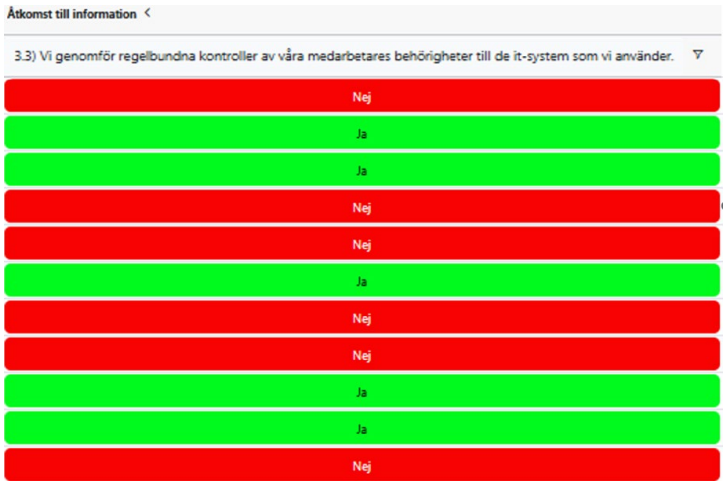


Bild 1

Av samma elva verksamheter är det endast fyra som arbetar systematiskt med att informera sina medarbetare om tystnadspliktens bestämmelser under och efter deras anställning eller uppdrag, se bild 2. Bristande insatser för att systematiskt informera om tystnadsplikten kan leda till att medarbetare oavsiktligt bryter mot patientsekretessen, vilket kan få allvarliga konsekvenser för patientrelationerna. Dessutom ökar risken för överträdelser av reglerna i Dataskyddsförordningen (GDPR), vilket i sin tur kan leda till exempelvis administrativa sanktionsavgifter.

[1] Myndigheten för samhällsskydd och beredskap (MSB), **Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp,** MSB2287



Bild 2

I egenkontrollerna framkommer även svar som antyder att verksamheten innehar kunskap och följer etablerade arbetssätt för åtminstone vissa moment. Till exempel har nio av elva verksamheter svarat att deras medarbetare är medvetna om hur incidenter, som har potential att skada verksamhetens informationssäkerhet, ska rapporteras, se bild 3. En snabb och effektiv hantering av incidenter är att anse som en högst betydelsefull aspekt inom informationssäkerheten.

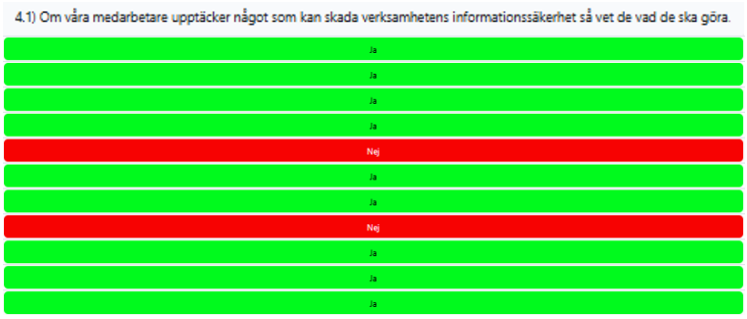


Bild 3

Informationssäkerhetssamordnaren vill även framhålla att verksamheten besitter god kunskap angående vilken information som är nödvändig för att bedriva sina verksamhetsprocesser samt vilken information som omfattas av sekretess och vart informationen lagras, se bild 4, 5 och 6.

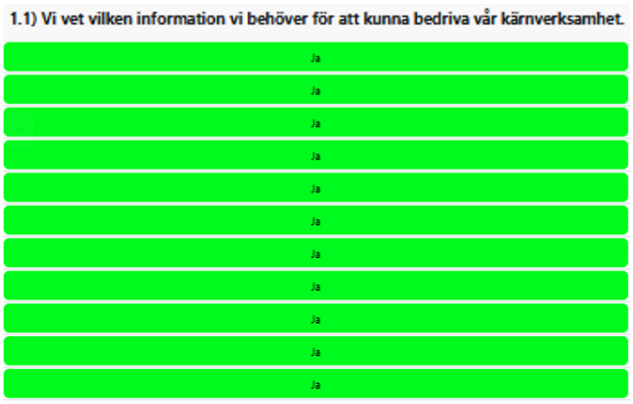


Bild 4

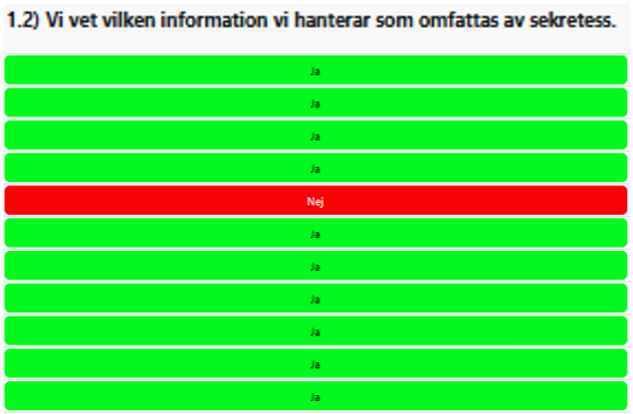


Bild 5

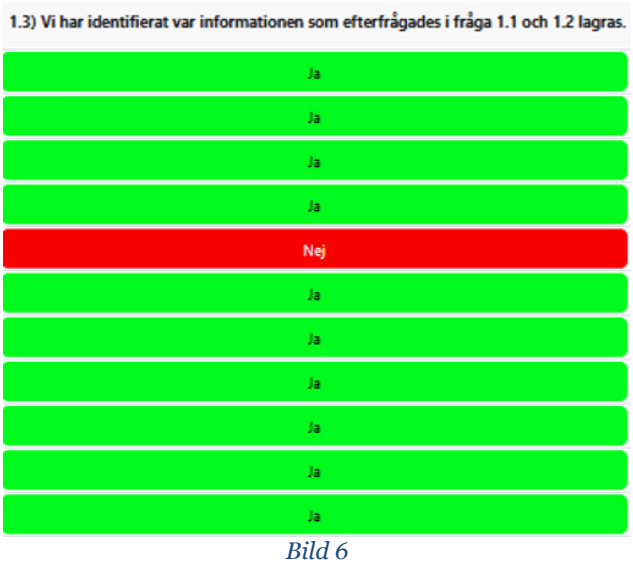


Bild 6

Under 2024 genomfördes elva egenkontroller i verksamheten vilket informationssäkerhetssamordnaren anser vara något för få kontroller. Noterbart är som nämnts ovan att en egenkontroll kan representera flera enheter. I syfte att öka genomförandegraden så använder informationssäkerhetssamordnaren sitt moment under utbildningspasset på BAS-utbildningen till att införskaffa mer kunskap beträffande hur verksamheten arbetar med informationssäkerhet och vad deras uppfattning om informationssäkerhet är. En informell undersökning men svaren från enhets- och verksamhetschefer ger likväl en antydan att det finns utrymme för förbättring när det gäller hur arbetet med informationssäkerhet bedrivs på verksamhetsnivå. Bild 7 och 8 är ett axplock av svar, se nedan.



Bild 7

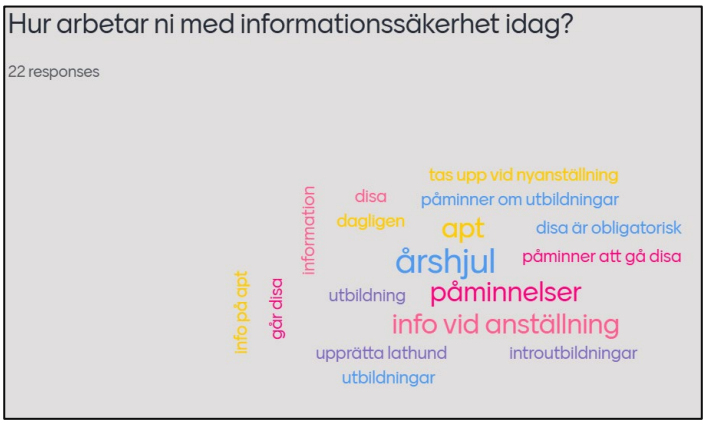


Bild 8

Informationssäkerhetssamordnarens ambition med frågorna är att hjälpa de nya cheferna att förstå att arbetet med informationssäkerhet inte behöver vara ”komplext” utan att det finns stöd och hjälp att använda för att skapa ordning och systematik. Detta stöd är egenkontrollerna avseende

informationssäkerhet. Givet att egenkontrollen tar en timme i anspråk och ger mycket värdefull kunskap för verksamheten så är det för informationssäkerhetssamordnaren svårt att förstå varför inte fler verksamheter drar nytta av detta arbetsmoment. Särskilt med tanke på att samma verksamheter anser att ämnet är något som inte är prioriterat och komplext samt ett område som ”många har dålig koll” på.

Informationssäkerhetssamordnarens huvudsakliga budskap under utbildningstillfället är att de ska kontakta densamma i syfte att genomföra en egenkontroll vilket, tyvärr, sker alldeles för sällan.

Förslag till åtgärd

Informationssäkerhetssamordnare har tillsammans med VS Kommunikation gjort en kommunikativ insats gällande reglerna kring tystnadsplikt.

I syfte att öka genomförandegraden av egenkontrollerna kommer informationssäkerhetssamordnaren göra en kommunikationsinsats via lämpliga kanaler. Bland annat kommer en film med uppmuntran till att göra egenkontroller att spelas in och spridas inom SLSO. Utöver detta så kommer informationssäkerhetssamordnare fortsätta att betona vikten av detta moment under BAS-utbildningen.

Utöver detta vore det lämpligt att SLSO:s ledning via exempelvis verksamhetsområdescheferna tillskrev SLSO:s verksamheter om lämpligheten att göra en egenkontroll.

Informationssäkerhetssamordnarens roll

För att utveckla och underhålla ett systematiskt och riskbaserat informationssäkerhetsarbete anser informationssäkerhetssamordnaren att tid och resurser behöver fördelas både i ett strategiskt och operativt arbete. Eftersom funktionen för informationssäkerhet för närvarande endast består av en person, som dessutom är dataskyddsombud, är det utmanande att arbeta både strategiskt och operativt. Utöver svårigheten att bedriva ett funktionellt operativt och strategiskt arbete uppstår osäkerhet kring arbetsuppgifter och ansvar för vilka delar i informationssäkerhetsarbetet som utförs av vem. Detta i sin tur ger upphov till en del frustration inom SLSO.

Informationssäkerhetssamordnaren bör, likt dataskyddsombudet, vara en roll av strategisk karaktär. Exempelvis ska dataskyddsombudet ge råd och

stöd, erbjuda utbildningar, men även genomföra tillsyn samt anmäla brister i verksamheterna till Integritetsskyddsmyndigheten, IMY. Informationssäkerhetssamordnarens arbete bör utgå från liknande premisser genom att exempelvis säkerställa att styrande och stödjande dokument finns på plats, genomföra utbildningar och informationsinsatser, ge råd och stöd samt utföra egenkontroller. De strategiska arbetsuppgifterna anser informationssäkerhetssamordnaren på ett övergripande plan går att läsa in i Region Stockholms riktlinje för informationssäkerhet under punkt 3.2.1: 'Varje nämnd och bolag ska utse en informationssäkerhetssamordnare som har i uppgift att samordna och följa upp arbetet med informationssäkerhet inom den egna organisationen.'

Att 'samordna och följa upp' kan i många fall uppfattas som att informationssäkerhetssamordnaren ska göra mycket operativt arbete, vilket i stället för dess ursprungliga intention – att följa upp och säkerställa att arbetet görs i verksamheten. I samband med denna något oklara fördelning av arbetsuppgifter för informationssäkerhetssamordnaren har avdelningen för informationssäkerhet på Regionledningskontoret tagit fram ett utkast till rollbeskrivning, rollbeskrivningen antogs tyvärr inte under 2024 av olika anledningar. Rollbeskrivning kommer förtydliga de strategiska arbetsuppgifter som informationssäkerhetssamordnaren ska arbeta med och exemplifiera typiska arbetsuppgifter som inte ska utföras av en informationssäkerhetssamordnare utan i stället av andra intressenter.

I revisionen av SLSO:s systematiska informationssäkerhetsarbete noterades en diskrepans mellan beskrivningen av informationssäkerhetssamordnarens roll i lagstiftning[2], i Region Stockholms riktlinje för informationssäkerhet[3], samt den beskrivning av rollen som uppgavs vid intervjuer under revisionen. I lagstiftning anges att samordnaren ska ”leda och samordna”, i riktlinjen anges att uppgifterna är att samordna och följa upp, samt att rollen ska uppfylla lagstiftningens krav, och i intervjuer uppges att funktionen är att ge stöd, samordna och följa upp.

Förslag till åtgärd

Informationssäkerhetssamordnaren anser att en tydlig rollbeskrivning bör fastställas så snart som möjligt vilket densamma hoppas kunna ge förutsättningar att minimera potentiella organisatoriska luckor som kan uppstå kring förväntningar och arbetsinsatser. En klar och väldefinierad

[2] HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
[3] Riktlinjer för informationssäkerhet, Dnr: RS 2020-0148

rollbeskrivning ger inte bara medarbetarna en tydlig vägledning om deras ansvar och förväntningar, utan det kan också öka effektiviteten och samarbetet inom SLSO som bidrar till att upprätthålla ett välfungerande arbete med informationssäkerhet.

Informationssäkerhetssamordnaren ansvarar för att en rollbeskrivning tas fram och beslutas om under 2025.

Dataskyddsorganisation

För att stödja och förbättra det systematiska arbetet med informationssäkerhet och dataskydd har dataskyddskoordinatorer utsetts på vårdområdesnivå och inom stödjande verksamhet. Tyvärr täcker inte denna struktur i nuläget hela SLSO och informationssäkerhetssamordnaren ser tydliga utmaningar i försöken att inkludera de stora vårdgrenarna på grund av dess geografiska spridning, organisatoriska storlek och det faktum att varje enhet/verksamhet drivs relativt oberoende av andra enheter/verksamheter. Tillsammans med informationssäkerhetssamordnaren och dataskyddsombudet (DSO) är avsikten att dessa koordinatorer ska hjälpa till att samordna arbetet med informationssäkerhet och dataskydd inom sina specifika vårdområden och den stödjande verksamheten.

Under verksamhetsåret 2024 har fokus huvudsakligen legat på att höja kunskapsnivån inom gruppen. Eftersom koordinatorerna inte officiellt har utsetts att arbeta med informationssäkerhet och dataskydd, har informationssäkerhetssamordnaren observerat att det är utmanande att påbörja operativa åtgärder bland deltagarna i gruppen.

Förslag till åtgärd

Arbetet kommer att fortsätta där informationssäkerhetssamordnare och DSO enligt organisationen ska bli tydligare i sin förväntansbild när det gäller operativa åtgärder. Det kan inkludera att säkerställa genomförandegraden för de obligatoriska utbildningarna i den specifika verksamhet eller enhet som de representerar.

Egenkontroll och anskaffning av IT-stöd

Egenkontroll av informationssäkerheten i ett IT-system eller en IT-komponent ger förvaltningen möjligheten att bedöma informationssäkerheten i det IT-system eller en IT-komponent som de förvaltar. Genom att besvara påståendena i egenkontrollen får förvaltningen en bild av i vilken omfattning IT-systemet eller IT-

komponenten uppfyller bland annat Region Stockholms informationssäkerhetskrav. Utifrån resultatet kan förbättringsområden identifieras och åtgärder vidtas för att skydda IT-systemets information vilket bidrar till förbättringsarbetet av Region Stockholms informationssäkerhet. Nio egenkontroller av IT-stöd gjordes under 2024.

Ett huvudfynd som informationssäkerhetssamordnaren gjorde i samband egenkontrollerna under 2023 var den relativt höga frekvensen av både obefintlig IT-förvaltning samt sådan förvaltning där informationssäkerhetssamordnaren upplever att det finns utmaningar i både riskarbetet och i det tekniska perspektivet i en IT-förvaltning. Denna utmaning kvarstår vilket belyses av bild 9. Där framgår att endast fem av nio IT-stöd har en etablerad förvaltning.



Bild 9

Problematiken med bristande IT-förvaltning bekräftas och förstärks av IT-säkerhetsprojekt som pågått under 2024, slutrapporten presenterades till styrgruppen och SLG i februari 2025. I slutrapporten kunde projektet konstatera att ”*Under 20 % av IT-tjänsterna har etablerad förvaltning, ca 35 % en informell förvaltning och resterande saknar förvaltning*”[4] Av SLSO:s totalt 181[5] registrerade IT-tjänster saknar nästan hälften en etablerad förvaltning i enlighet med de tre nivåer som föreslagits i IT-säkerhetsprojektet. I syfte att nyansera frågan om IT-förvaltning finns etablerad till respektive IT-stöd så har projektet tagit fram tre olika nivåer

[4] Slutrapport IT-säkerhetsprojekt.
[5] Fler IT-tjänster kan förekomma då det saknas processer för att identifiera befintliga IT-tjänster och beslut att Digitala tjänster ska informeras samt att systemlistan i analysen avser omfatta samtliga system.

av IT-förvaltning (stor, mellan, liten) utifrån antalet användare och vilken typ av informations som hanteras i IT-stödet.
En bristande IT-förvaltning kan ge upphov till sårbarheter i system och nätverk, vilket i sin tur ökar risken för dataintrång och cyberattacker. Detta kan innebära att känslig information hamnar i orätta händer. Vidare kan brister i IT-förvaltningen medföra att SLSO inte uppfyller lagar och föreskrifter, vilket potentiellt leder till juridiska påföljder och negativa konsekvenser för förtroendet. I de fall där ingen förvaltning existerar, saknas även en mottagare av egenkontrollen och de eventuella åtgärder som kan behöva vidtas. Utan möjligheten att genomföra adekvata åtgärder efter en egenkontroll blir arbetsmomentet nästintill meningslöst, då SLSO endast har identifierat möjliga brister utan förmåga att vidta några åtgärder.

Utöver det nämnda har informationssäkerhetssamordnaren under de senaste åren konstaterat att SLSO saknar en övergripande process för anskaffning av alla former av IT-stöd. Bristen på en väldefinierad process, som sträcker sig från behovsanalys till driftsättning, ger upphov till flera sårbarheter inom SLSO. Dessa inkluderar inte bara otillräcklig förvaltning och bristande kontroll över hanteringen av personuppgifter, känsliga patientdata samt en inaktuell IT-arkitektur, utan även andra betydande risker så som otillräcklig kravställning avseende informationssäkerhet. Förmågan att bedriva ett systematiskt informationssäkerhetsarbete försvåras även signifikant. Bristen eller avsaknaden av en strukturerad anskaffningsprocess kan potentiellt leda till förseningar och frustration i implementeringen av nya IT-system, vilket i sin tur kan påverka SLSO:s förmåga att anpassa sig till de snabba förändringar i teknologin som sker. Slutligen ökar även risken för säkerhetsincidenter, då en otydlig process kan underlätta obehörig åtkomst till känslig information och öppna upp för potentiella cyberhot eftersom inte adekvata säkerhetskrav ställs i samband med inköp och/eller upphandling.

Anmärkning av en bristande anskaffningsprocess har resulterat i att området är under genomlysning och förbättring inom ramen för IT-säkerhetsprojektet. Slutrapporten för projektet visade i enlighet med informationssäkerhetssamordnarens bedömning av det fanns gap och förbättringspotential där gap primärt har identifierats vid kravställning, förvaltning och avveckling. Se bild 10.

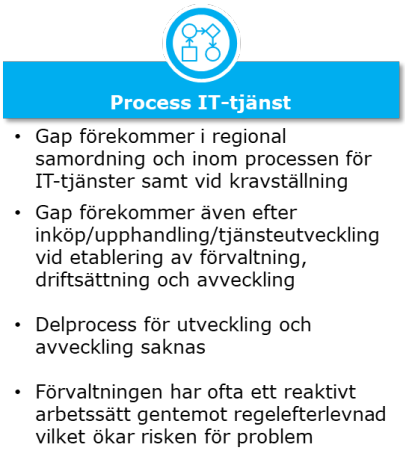


Bild 10

Projektet har i samband med nulägesbedömning även gjort en aktivitetsplan i vilken livscykelprocessen ingår.

Förslag till åtgärd

Informationssäkerhetssamordnare är delaktig i både styr- och projektgrupp för IT-säkerhetsprojektet och följer där utvecklingen inom området.

Utbildning

För SLSO kvarstår det brister i utbildningsgenomförandet av den obligatoriska utbildningen DISA: datorstödd informationssäkerhetsutbildning för användare. Trots flera års insatser för att öka genomförandegraden har dessa, beklagligt nog, haft begränsad effekt. Baserat på genomförandegraden kan informationssäkerhetssamordnare anta att varken enhets- eller verksamhetschefer fullt ut följer sitt ansvar att säkerställa att deras medarbetare genomför de obligatoriska utbildningarna. Egenkontrollerna visar att 73 % av SLSO:s enheter/verksamheter säkerställer att deras medarbetare gjort DISA-utbildningen. Med ”säkerställer” menas att verksamheten informerar om DISA vid anställning och regelbundet följer upp vilka medarbetare som gjort utbildningen. Bild 11 presenterar svar på frågan om verksamheten säkerställer genomförande av DISA.



Bild 11

Region Stockholms systemstöd för digitala utbildningar, Lärtorget, ger varken SLSO eller informationssäkerhetssamordnaren de förutsättningar som behövs för att kunna arbeta med en effektiv uppföljning av utbildningar. Uppföljningen av genomförandegraden på vårdgivarnivå kommer inte att fortsätta givet utmaningar att få fram en tillförlitlig siffra givet den information som tillhandahålls av Lärtorget. Bedömningen för 2024 är att 71 % (8 518/12 000) av de anställda genomfört utbildningen vilket ligger i linje med egenkontrollerna med svaren för egenkontrollen.

I januari 2026 lanseras det nya IT-stödet Kompetenstorget som ersätter dagens Lärtorget och Heroma kompetens. Syftet med Kompetenstorget är att varje verksamhet inom Region Stockholm ska ha tillgång till ett verksamhetsanpassat, flexibelt och modernt IT-stöd för området kompetensplanering och kompetensutveckling. Ett sammanhållet systemstöd för kompetensplanering och kompetensutveckling innebär att det kommer finnas en koppling mellan kompetenser och utbildningar, vilket det inte gör i dagens IT-stöd. Medarbetaren får en överblick över vilka utbildningar hen behöver genomföra utifrån sin roll, samt kan få förslag på andra utbildningar som kan vara relevanta.

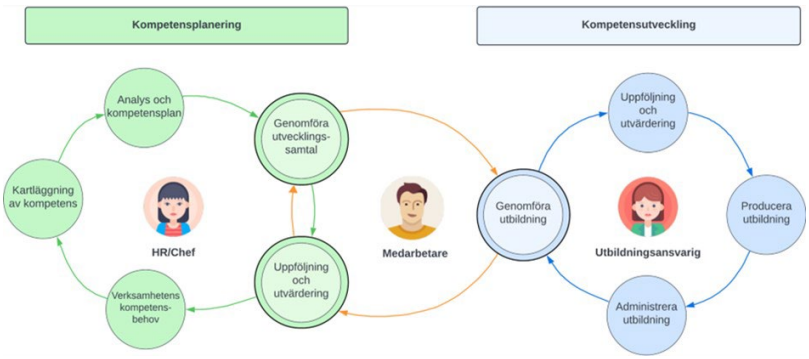


Bild 12

Förslag till åtgärd

Uppföljning av utbildningen DISA sker inom ramen för egenkontroller kommande år. Informationsinsatser för att öka medvetenheten kommer även göras likt tidigare år. Därutöver sätts en tilltro till att förmågan till effektiv uppföljning blir bättre kommande år när det nya IT-stödet är implementerat.