Årlig rapport till regionstyrelsen enligt ledningssystemet för informationssäkerhet inklusive dataskydd 2021

REGION SKÅNE

Innehållsförteckning

1 Ledningssystem för informationssäkerhet och ledningens genomgång

Ledningssystemet för informationssäkerhet har sin grund i ISO/IEC 27000 och ska vara en integrerad del av organisationens processer och övergripande ledningsstruktur genom att informationssäkerhet beaktas i utformningen av processer, informationssystem och säkerhetsåtgärder. Denna årliga rapportering utgör ett underlag för Regionstyrelsen om status och effektiviteten i ledningssystemet för informationssäkerhet.[1]

Rapporten är framtagen av Region Skånes regionala funktioner för informationssäkerhet och dataskydd.

2 Status för åtgärder som beslutats vid tidigare genomgångar och måluppfyllnad

Långsiktiga mål för informationssäkerhet beslutades av Regionstyrelsen 2017-06-29. De kortsiktiga målen för informationssäkerhet beslutades av Regionstyrelsen 2021-04-29. Flera aktiviteter kopplade till målen är påbörjade och pågående, andra i uppstartsfas. Den regionala informationssäkerhetsfunktionen arbetar kontinuerligt med de lång- och kortsiktiga målen tillsammans med berörda verksamheter. Målen styr även det förvaltningsspecifika målarbetet. Eftersom Region Skånes förvaltningar är av skild karaktär gällande storlek, uppdrag och organisering skiljer det exakta tillvägagångssättet för detta sig åt mellan förvaltningarna.

Dataskyddsorganisationens mål för 2021 var att krav och risker kopplade till tredjelandsöverföring ska vara målgruppsanpassade och kommunicerade. Ett viktigt steg för att möjliggöra detta var att ta fram en mall för konsekvensbedömning avseende dataskydd och att implementera denna process i verksamheten. En kartläggning av Region Skånes tredjelandsöverföringar är genomförd och resultatet presenterades för Regionstyrelsen 2021-12-09. Arbete med en handlingsplan för

[1] Riktlinjer för informationssäkerhet, dnr 1604263

organisationens hantering av tredjelandsöverföring pågår. Handlingsplanen innefattar krav och risker kopplade till tredjelandsöverföring.

3 Förändringar i externa och interna frågor som är relevanta för ledningssystemet för informationssäkerhet

3.1 Externa förändringar

3.1.1 Tredjelandsöverföringar av personuppgifter

Om en organisation planerar överföring av personuppgifter till tredjeland så måste skyddet för personuppgifter vara likvärdigt det skydd som garanteras inom EU/EES. Den 18 juni 2021 antog Europeiska dataskyddsstyrelsen (EDPB) rekommendationer till kompletterande skyddsåtgärder för att tillgodose ett likvärdigt skydd. Av rekommendationen kan man dra slutsatsen att det är väldigt utmanande och ibland omöjligt att lagligt välja leverantörer som lyder under lagstiftning i tredjeland där adekvat skyddsnivå saknas. Det finns till exempel inga tillräckliga skyddsåtgärder för molntjänster där tjänsten kräver att personuppgifter hanteras i klartext i ett sådant tredjeland. I de fall säkerhetsåtgärder som kryptering och pseudonymisering används krävs hög kompetens hos organisationen för att kontinuerligt säkerställa att senaste tekniken tillämpas. Organisationen ska också klara av att hantera nyckelhanteringen så att leverantören inte får åtkomst till uppgifterna.

3.1.2 Integritetsskyddsmyndigheten (IMY)

Under 2021 fattade IMY beslut om en ny tillsynspolicy och tillsynsplan. Utöver sin årligen planerade tillsyn använder de sig nu också av en riskbaserad tillsyn. Den riskbaserade tillsynen kan initieras bland genom inkomna klagomål från enskilda, anmälda personuppgiftsincidenter samt tips och uppgifter i media. IMY inledde 2021 dubbelt så många granskningar som året innan och beslutade om administrativa sanktionsavgifter om sammanlagt 32,5 miljoner kronor i åtta ärenden, varav majoriteten rörde aktörer i offentlig sektor.

Under 2021 kom även IMY:s första rättsliga ställningstagande, ett format som myndigheten framöver kommer använda för att tydliggöra sin uppfattning i frågor där det fortfarande saknas praxis.

IMY fick även i uppdrag av regeringen att genomföra metod- och kunskapsutvecklande insatser inom innovations- utvecklings- och införandeprocesser hos innovationsaktörer i såväl privat som offentlig sektor.

3.1.3 Civilt försvar – överenskommelse med SKR

Sveriges kommuner och regioner (SKR) och staten har ingått en överenskommelse om hälso- och sjukvårdens arbete med civilt försvar 2022[2]. Insatser som regionerna ska genomföra för att öka sin motståndskraft omfattar bland annat att bedriva ett systematiskt informationssäkerhetsarbete för att stärka förmågan att motstå cyberangrepp i de digitala system som är kritiska för att bedriva hälso- och sjukvård, vilket stärker behovet av ett uppdaterat ledningssystem i Region Skåne. Det finns starka beroenden till andra säkerhetsområden.

3.1.4 Strategier för informationssäkerhet och digitalisering

3.1.4.1 Struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

Myndigheten för samhällsskydd och beredskap (MSB) fick den 19 september 2019 i uppdrag av regeringen att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i offentlig förvaltning. 1 mars 2021 presenterade MSB en uppföljningsstruktur,[3] med målsättningen att statliga myndigheter, kommuner och regioner ska erbjudas stöd i sitt uppföljnings- och förbättringsarbete och att regeringen ska få en samlad nivåbedömning av det systematiska informationssäkerhetsarbetet i offentlig förvaltning. Slutsatser från rapporten är att uppföljningsstrukturen bedöms kunna bidra till ett förbättrat och mer enhetligt arbete med informationssäkerhet inom offentlig förvaltning. Detta förutsätter dock ett brett deltagande från offentlig förvaltning, främjande av en positiv och bejakande uppföljningskultur, samt resurssättning av identifierade förbättringsområden.

[2] Hälso-och sjukvårdens arbete med civilt försvar 2022
[3] En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

3.1.4.2 Vägen till det digitala årtiondet och digitala mål för 2030

EU-kommissionen lade i oktober 2021 fram ett förslag på ett policyprogram för Europas digitala omvandling fram till 2030.[4] Målen för de fyra nyckelområdena digital kompetens, digital infrastruktur, näringslivets digitala omvandling och digitalisering av offentliga tjänster liksom uppföljnings- och styrningsmekanismen motsvarar det som presenterades i meddelandet om en digital kompass 2030.[5] Regeringen anser bland annat att det är viktigt att den offentliga sektorn ligger i framkant vad gäller att använda digitaliseringens möjligheter och att åtgärder för den digitala omvandlingen av EU bör stöttas av nödvändiga informations- och cybersäkerhetsåtgärder.

3.1.4.3 God och nära vård 2022 – överenskommelse med SKR

Digitala vårdtjänster kan bidra till en nära, tillgänglig och jämlik hälso- och sjukvård, men det är viktigt att informationssäkerheten och skyddet för den personliga integriteten säkerställs. Därför ska informations- och cybersäkerheten vara en integrerad del av den digitala utvecklingen. I enlighet med överenskommelsen mellan SKR och regeringen om God och nära vård[6] ska det genomföras en uppföljning av regionernas arbete med informationssäkerhet. SKR har ansvarat för att etablera en gemensam struktur där varje region självständigt genomfört sin egen uppföljning. Regional informationssäkerhet svarade, tillsammans med IT, på uppföljningen för Region Skånes räkning i januari 2022. SKR kommer senare under året ha en dialog med regionernas it-/digitaliseringsdirektörer och informationssäkerhetsansvariga samt ta fram en övergripande sammanställning av resultaten som sedan presenteras för Regeringskansliet.

3.2 Interna förändringar

3.2.1 Årshjul för informationssäkerhet och dataskydd

Ett årshjul för informationssäkerhet har tagits fram och implementerats under hösten. Det kompletterar det befintliga årshjulet för dataskydd. Årshjulen stödjer förvaltningarna i det systematiska arbetet med informationssäkerhet och dataskydd och underlättar mätningen av det arbete som genomförts i organisationen. Det skapar också möjlighet att, på ett

[4] Beslut om programmet Vägen till det digitala årtiondet Fakta-PM om EU-förslag 2021/22:FPM4 COM (2021) 574 - Riksdagen
[5] Meddelande om digital kompass 2030 Fakta-PM om EU-förslag 2020/21:FPM94 COM(2021) 118 - Riksdagen
[6] God och nära vård 2022

strukturerat sätt, föra fram behov av åtgärder till ledningen. Årshjulen med tillhörande rapporter fungerar som ett verktyg för förbättring och är en viktig komponent i det systematiska informationssäkerhets- och dataskyddsarbetet.

3.2.2 Förbättringsåtgärder kopplade till patientsäkerhet

Under året har det införts förbättrande åtgärder avseende patienter med skyddade personuppgifter. Den tidigare rutinen för hantering av patienter med skyddade personuppgifter medförde patientsäkerhetsrisker och försvårade kommunikation med andra myndigheter och vårdgivare. För att öka kunskapen och förebygga incidenter inom ämnet har en e-utbildning tagits fram. Även ramverket för åtgärder vid misstanke om dataintrång avseende patientuppgifter har förbättrats med förtydliganden kring arbetsrättslig utredning och vad som gäller för anställdas åtkomst till patientuppgifter ur ett legalt perspektiv. Ett målgruppsanpassat informationsblad riktat till personal har tagits fram i syfte att förebygga incidenter.

3.2.3 Informationsstrategi

Region Skåne har tagit fram en informationsstrategi och arbete pågår med att implementera denna. Informationsstrategin är Region Skånes gemensamma strategi för hur data och information ska hanteras, struktureras och tillgängliggöras för verksamhetsutveckling, forskning och skapande av digitala datadrivna lösningar. Enligt DIGG som arbetar för att främja tillgängliggörande och vidareutnyttjande av data från offentlig förvaltning så är ett riskbaserat och systematiskt informationssäkerhetsarbete en förutsättning inför och under tillgängliggörandet av information för vidareutnyttjande.[7]

3.2.4 Resurser och kompetens

Ökad kunskap i verksamheten om informationssäkerhetens betydelse och en vilja att hantera informationen korrekt bidrar till ett ökat tryck på befintliga personalresurser, inte minst vid införarande av nya rutiner och processer.

För att stärka Region Skånes förmåga inom informationssäkerhet och dataskydd har regionala funktioner tillsammans med förvaltningarnas samordnare genomfört en omfattande informationssäkerhetsutbildning

[7] Öppna och delade data från offentliga aktörer | DIGG

kopplad till ISO 27001 – Ledningssystem för informationssäkerhet, och ISO 27701, Krav och vägledning för hantering av personuppgifter.

Antalet resurser för informationssäkerhet och dataskydd har ökat i fyra av tolv förvaltningar. Även på regional nivå har det tillkommit resurser. Koncernstab HR har inrättat en dedikerad resurs för informationssäkerhet och dataskydd som stöd till informationsägaren.

4 Ledningssystemets, informationssäkerhetens och dataskyddets prestanda

4.1 Avvikelser, incidenter och korrigerande åtgärder

Personuppgiftsincidenter hanteras systematiskt och strukturerat i Region Skåne. Hanteringen av informationssäkerhetsincidenter som inte rör personuppgifter är i behov av utveckling, varför redovisningen nedan endast inbegriper personuppgiftsincidenter.

Under perioden 2020-10-01–2021-10-01 registrerades 730 personuppgiftsincidenter i ärendehanteringssystemet för incidenter. Majoriteten av incidenterna avsåg konfidentialitetsbrott, exempelvis genom att en medarbetare begått dataintrång eller att information inte skyddats på rätt sätt vid överföring eller lagring. 67 av incidenterna bedömdes utgöra en risk för enskilda, varför de anmäldes till IMY.

I Region Skåne saknas dock tillförlitlig statistik över antalet dataintrångsärenden. Exempelvis är statistiken bristfällig vad gäller hur många dataintrångsärenden som leder till en polisanmälan, vilka ärenden som leder till arbetsrättsliga åtgärder samt hur många av dataintrången som rapporteras till IMY i egenskap av att också vara personuppgiftsincidenter. Pågående förbättringsåtgärder omfattar regional ärendehantering och gemensamma mallar för att underlätta mätningar.

4.2 Resultat från årsrapporter och granskningar

Årshjulen med tillhörande rapporter från förvaltningarna fungerar som ett verktyg för uppföljning och är en viktig komponent i det systematiska informationssäkerhets- och dataskyddsarbetet. Följande analyser bygger på förvaltningarnas respektive redovisningar samt en genomlysning av processen för informationsklassificering, riskbedömning och vägen till beslut.

4.2.1 Ledningens engagemang

Ledningens engagemang är avgörande för att ett framgångsrikt informationssäkerhets- och dataskyddsarbete ska kunna bedrivas. Det gäller den centrala ledningen så väl som förvaltningarnas ledningsgrupper. I de genomlysningar som gjorts har det lyfts att dialogen mellan samordnare och ledning i vissa förvaltningar anses vara **otillräcklig,** vilket påverkar möjligheten till ständig förbättring i förvaltningen. Det har också framkommit ett behov av ökat stöd till de informationsägare som inte är förvaltningschefer.

4.2.2 Utvecklingsbehov av arbetssätt och organisation

Det har under perioden varit ett stort fokus på att utveckla både arbetssätt och organisation för informationssäkerhet och dataskydd. Förståelsen för behovet varierar i förvaltningarna. Faktorer som anses påverka är förvaltningens uppdrag och storlek, antal medarbetare, geografisk spridning samt resurser. Flera förvaltningar rapporterar om att samordnarna har **otillräckliga** resurser i form av tid och personal för att utföra sina uppdrag.

Alla förvaltningar har eller planerar för förvaltningsövergripande nätverk av kontaktpersoner som implementerar ledningssystemet i verksamheterna. Kontaktpersonerna saknar ofta rätt mandat för att tillse att informationssäkerhet och dataskydd beaktas vid utformningen av processer, informationssystem och säkerhetsåtgärder, vilket försvårar uppdraget.

Majoriteten av förvaltningarna har en gemensam informationssäkerhets- och dataskyddsorganisation. I vissa förvaltningar bedrivs arbetet systematiskt tillsammans med närliggande säkerhetsprocesser, medan det i andra förvaltningar uppmärksammats ett ökat behov av samverkan med andra säkerhetsområden inom förvaltningen. Exempelvis patientsäkerhet, säkerhet och beredskap samt säkerhetsskydd.

Informationssäkerhetsarbetet ses fortfarande ofta som en egen process utan koppling till andra verksamhetsprocesser och inkluderas därför inte i annan process- eller verksamhetsutveckling. Exempelvis saknas insikt i hur processerna för informationsklassificering och riskanalys resulterar i kravställning av säkerhetsåtgärder för den informationshantering som sker i verksamheten. Detta resulterar i att flera förvaltningar saknar en organisation för att stödja verksamheterna i arbetet med informationsklassificering och riskanalys.

4.2.3 Systematisk riskhantering

Genomlysningar visar att tydliga processer och metodstöd är viktiga för förvaltningarnas arbete med informationssäkerhet och dataskydd. Processen för informationsklassificering, riskbedömning, och vägen till beslut bedöms generellt som **funktionell och värdeskapande**.

Bristen på uppdaterade och kvalitetssäkrade register över informationstillgångar och personuppgiftsbehandlingar komplicerar riskhanteringsarbetet. Förbättring av detta, tillsammans med mer stöd i form av analysunderlag, styrande/stödjande dokument och kompetenshöjande insatser bedöms kunna ge ett mer samstämmigt och kvalitativt resultat av informationsklassificering, riskbedömning och konsekvensbedömning (avseende dataskydd). Behov finns också av en utveckling av arbetet med kravanalys och hur informationen presenteras för beslutsfattaren.

Hantering av åtgärder bedöms vara **bristfällig**. Åtgärder identifieras vid personuppgiftsincidenter och annan riskhantering men saknar ofta tydligt uppföljningsdatum och kopplat ansvar. Även rutinerna för uppföljning av åtgärderna är **bristfälliga**.

Stöd har under året tagits fram för att säkerställa att Region Skåne tar hänsyn till integritetsskyddsreglerna och informationssäkerhetskrav redan när it-system och rutiner utformas, samtidigt som svåra utmaningar identifierats vad gäller ett lyckat omhändertagande i organisationen på grund av avsaknad av tydliga verksamhetsprocesser och processbeskrivningar.

4.2.4 Kompetens

Trots att pandemin även detta år påverkat planerade utbildningsinsatser har målgruppsanpassade och verksamhetsnära utbildningar kunnat genomföras, om än inte i den omfattning som vore önskvärt. Formerna för utbildning skiljer sig åt mellan förvaltningarna, beroende på storlek och organisation.

Gemensamt för majoriteten av förvaltningarna är att Region Skånes grundläggande e-utbildning ”Säker informationshantering” anses vara central och att den får goda omdömen av deltagarna. Trots det är genomförandegraden låg.

Samordnarna signalerar att de behöver ytterligare kompetens avseende it-säkerhet och relevant lagstiftning för att kunna utföra sina uppdrag på ett tillfredsställande sätt.

4.3 Resultat från externa granskningar

Secure State Cyber tog fram en rapport rörande Region Skånes tredjelandsöverföringar på uppdrag av Informationsstyrningsrådet under hösten 2021.[8] Rapporten visar på ett stort förbättringsbehov. Kartläggningen av tredjelandsöverföringar speglar inte verkligheten då dokumentationen av personuppgiftsbehandlingar är **bristfällig**. Ytterligare ett problem är avsaknad av den kompetens som krävs för att avgöra om en tredjelandsöverföring förekommer.

Inspektionen för vård och omsorg granskade Skånes Digitala Vårdsystem (SDV) utifrån lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Myndigheten har granskat arbetet med riskanalys och åtgärder, inte tekniken bakom systemet. Arbetet har bedömts som **godtagbart**.

5 Förbättringsåtgärder för ledningssystemet

5.1 Vidareutveckling av ledningssystemet – från LIS till LISD

Region Skånes nuvarande ledningssystem för informationssäkerhet fungerar **inte tillfredsställande** utifrån rådande interna och externa behov. Region Skåne behöver vidta åtgärder för att säkerställa att organisationen har ett ändamålsenligt, verksamt och effektivt ledningssystem för både informationssäkerhet och dataskydd (LISD) för att kunna digitalisera i

[8] *Slutsatser av Region Skånes kartläggning av överföring av personuppgifter till tredjeland*, dnr 2021-O002446

önskad takt i enlighet med Sveriges och EU:s strategier för digitalisering och samtidigt säkra och stärka skyddet för individen, verksamheten och Sveriges säkerhet. Ett kvalitativt LISD är en förutsättning för att Region Skånes strategier för digitalisering samt tillgängliggörande och vidareutnyttjande av data ska kunna förverkligas. Region Skånes informationssäkerhetsarbete behöver bedrivas med ett helhetsperspektiv utifrån den lagstiftning som kräver att organisationen bedriver ett systematiskt informationssäkerhetsarbete:

- Säkerhetsskyddslag (2018:585)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Den allmänna dataskyddsförordningen, GDPR (”dataskyddsförordningen”) och lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (”dataskyddslagen”)
- Patientdatalag (2008:355) och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

Att vidareutveckla ledningssystemet är ett långsiktigt arbete som kommer att kräva omfattande analyser och åtgärder i samverkan med övriga säkerhetsfunktioner samt förvaltningen Digitalisering IT och MT. Målet är ett tydligt och heltäckande ramverk där informationssäkerhet och dataskydd ingår, samt processer som möjliggör proaktivitet såsom en sammanhängande incident- och riskhantering. Detta kommer att stärka Region Skånes motståndskraft. Ett vidareutvecklat ledningssystem kommer att stärka vår förmåga att uppnå organisationens mål för informationssäkerhet och dataskydd.

För att möjliggöra vidareutvecklingen är det av stor vikt att de funktioner vid Koncernkontoret som ansvarar för att leda och förvalta ledningssystemet kan rekrytera och behålla personalresurser med den strategiska kompetens och specialistkompetens som krävs för att arbetet ska kunna gå i takt med pågående initiativ i regionen med beroenden till ledningssystemet.

För att förbereda inför vidareutvecklingen av ledningssystemet har vissa initiativ påbörjats. Exempelvis kommer årshjulen för informationssäkerhet och dataskydd att slås samman. Vidare kommer MSB:s nya direktiv för mätning och uppföljning implementeras för att utöver de planerade analyserna undersöka vilken nivå informationssäkerhets- och dataskyddsarbetet befinner sig på i organisationen och hur det kan utvecklas.

5.2 Implementering av ledningssystemet

Ledningssystemet för informationssäkerhet och dataskydd har ett starkt beroende till andra säkerhetsområden inom Region Skåne, såsom säkerhet och beredskap, säkerhetsskydd och it-säkerhet. En samlad styrning av berörda säkerhetsområden, oberoende av linjeorganisationen, behövs för att säkerställa samstämmiga metoder och rapportering samt för att de övergripande informationssäkerhetsprocesserna ska kunna implementeras i förvaltningarnas verksamhetsprocesser på ett bättre sätt. En god samordning av säkerhetsområdena på central nivå stöttar förvaltningarna i deras tillämpning av ledningssystemet och ger förutsättningar för en säkerhetsorganisation med motståndskraft.

Informationssäkerhets- och dataskyddsprocesserna behöver också integreras på ett bättre sätt i regionövergripande processer. Ett exempel är upphandlingsprocessen där det finns mycket att vinna på en tydligare integrering av informationssäkerhets- och dataskyddsprocesserna för att möjliggöra säkra upphandlingar. Med hjälp av en dokumenterad informationsklassificering och riskbedömning kan man fastställa vilka skyddsåtgärder systemet eller tjänsten som ska upphandlas omfattas av. Skyddsåtgärderna ska sedan finnas med i den kravspecifikation som används vid upphandlingen. Om detta inte görs riskerar Region Skåne att upphandla system som inte är säkra nog att hantera den information de är tänkta att hantera.

En bedömning av nödvändiga resurser för att implementera ledningssystemet behöver göras utifrån respektive förvaltnings storlek, struktur och verksamhet. Detta synsätt bör också genomsyra nyrekrytering. Uppskattning av arbetsbelastning måste stå i proportion till de av förvaltningsledningen fastställda prioriteringarna, exempelvis accelererad digitalisering av sin verksamhet. Om det inom förvaltningen hanteras stora mängder känsliga uppgifter i komplexa informationshanteringsprocesser innebär det fler informationssäkerhetsrisker och fler risker för den registrerades rättigheter och friheter. Då måste även antalet personalresurser som upprätthåller informationssäkerhets- och dataskyddsarbetet i förvaltningen matcha behovet. Förvaltningarna behöver skapa utrymme för både operativt och strategiskt arbete för att uppnå rätt nivå av skydd samt ständiga förbättringar enligt LISD.

5.3 Kompetens och medvetenhet

För att informationssäkerhetsarbetet ska kunna bedrivas systematiskt och bli en del av det dagliga arbetet krävs att kunskapsnivån i organisationen höjs ytterligare. Ledande befattningar på olika nivåer i organisationen behöver visa att informationssäkerhetsfrågor är prioriterade och öka sin kompetens inom området för att säkerställa ledningssystemets verkan i hela organisationen. Att arbeta efter etablerade ISO-standarder säkerställer att Region Skånes informations- och dataskyddsarbete håller en hög kvalitet och att organisationen etablerar ett relevant, långsiktigt och systematiskt arbetssätt för dessa frågor.

För att kunna implementera ett LISD i förvaltningarna behöver dataskyddssamordnarna ha den nivå av sakkunskap om lagstiftning och praxis avseende dataskydd som krävs utifrån de personuppgiftsbehandlingar som utförs i förvaltningen samt den nivå av skydd som personuppgifterna kräver. Om behandlingen av personuppgifter är särskilt komplex eller omfattar en stor mängd känsliga uppgifter kan dataskyddssamordnaren till exempel behöva stöd från sin förvaltningsledning och närmaste chef i form av ekonomiska resurser och tid för deltagande i fortbildningskurser om dataskydd och andra yrkesutvecklingskurser.

Vidareutveckling av den grundläggande utbildningen i säker informationshantering för alla medarbetare och utbildningsinsatser i förvaltningarna sker löpande, men det krävs ytterligare insatser för att öka medarbetarnas medvetenhet utifrån roll, ansvar och kunskaper. Det är av stor vikt att varje medarbetare kan upprätthålla informationssäkerheten inom sittarbetsområde och i den miljö där de är verksamma, vilket kräver att de har kunskap om kända hot i sin verksamhet, vad de kan göra för att minska riskerna och vem som ska kontaktas vid problem och incidenter.