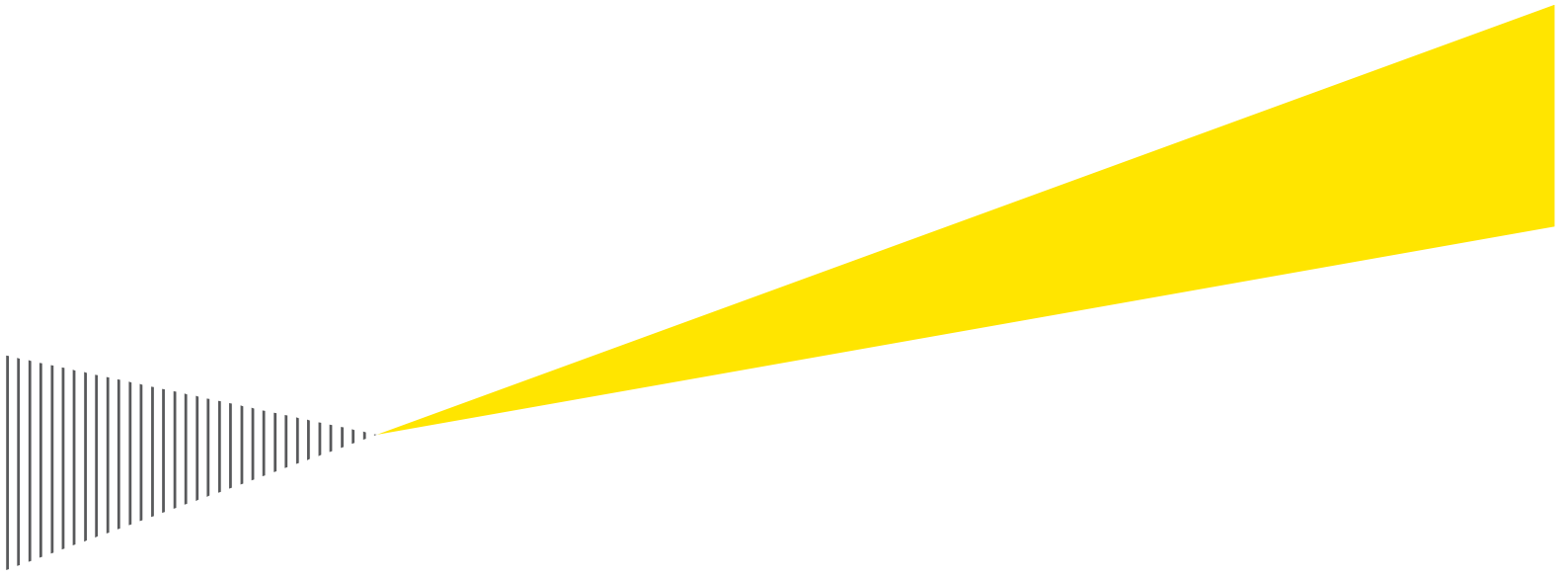
Granskningsrapport 2020
Genomförd på uppdrag av revisorerna
Juni - September 2020

Region Skåne

Granskning av IT- och informationssäkerhet



Building a better working world

Innehåll

Sammanfattning

EY har på uppdrag av Region Skånes revisorer granskat om Region Skånes arbete med informationssäkerhet och IT-säkerhet bedrivs på ett systematiskt och ändamålsenligt sätt inom regionstyrelsen och kollektivtrafiknämnden. Den övergripande bedömningen är att IT- och informationssäkerhetsarbetet inom granskade nämnder till stora delar bedrivs systematiskt och ändamålsenligt men i vissa delar är otillräckligt.

Granskningen påvisar en positiv utveckling inom området under de senaste åren, framför allt inom styrning och ledning med tydliggörande av ansvar och framtagande och fastställande av relevanta styrande riktlinjer och instruktioner från centralt håll. Region Skåne har även utformat en organisation för regionalt dataskyddsarbete som bedöms möjliggöra ett strukturerat och målinriktat arbete för anpassning gentemot GDPR.

Granskningen har påvisat brister i Region Skånes arbete med IT- och informationssäkerhet vilket har påverkat bedömningen negativt. Dessa brister rör primärt:

- Systematisk uppföljning, kontroll och utvärdering – Region Skåne saknar inom granskade nämnder i många hänseenden lämpliga rutiner, modeller och verktyg för att följa upp att beslutade krav och riktlinjer efterlevs, dels internt inom Region Skåne men även externt gentemot molntjänstleverantörer och andra tredjeparter.
- Utbildning – Utbildningsinsatser genomförs i varierande grad inom granskade nämnder. Dock påvisar granskningen att dessa inte genomförs i en omfattning som säkerställer att samtliga medarbetare genomgår grundläggande utbildning inom området, samt nödvändig kunskapsnivå hos medarbetare i ledande befattningar.
- Patientintegritet i journalsystem – Bedömningen utifrån granskningen är att patientintegriteten i journalsystem i dess nuvarande utformning och trots nuvarande rutiner för logguppföljning av journaler inte fullt kan säkerställas. EY har dock under granskningen informerats att det är en fråga som prioriteras inom ramen för införandet av Skånes Digitala Vårdsystem.

Utifrån granskningsresultatet rekommenderar vi regionstyrelsen och kollektivtrafiknämnden att:

- Genomföra en kartläggning av upprättade instruktioner inom området för informationssäkerhet i nämndens verksamheter och utvärdera om lämpliga instruktioner i enlighet med beslutade riktlinjer för informationssäkerhet har upprättats.
- Säkerställa att rutiner och ansvar för uppföljning av avtal med molntjänstleverantörer, personuppgiftsbiträden och andra tredjeparter med ansvar för IT-säkerhet, informationssäkerhet och dataskydd är tydligt definierade.
- Införa rutiner för regelbunden och systematisk uppföljning av informationssäkerhetsarbetet inom regionen för att utvärdera om beslutade riktlinjer efterlevs. I samband med detta utvärdera behov av resurser, systemstöd, metoder, eller instruktioner för att möjliggöra en effektiv uppföljning.
- Följa upp utbildningsinsatser inom nämnden för att dels kontrollera om samtliga medarbetare genomgår den grundläggande e-utbildningen i säker informationshantering och dels få insikt i hur många medarbetare som genomgått kompetenshöjande men ej obligatoriska utbildningar.

Regionstyrelsen rekommenderas även att:

- Årligen genomföra uppföljning av beslutade kortsiktiga mål för informationssäkerhetsarbetet i enlighet med riktlinjerna. I denna uppföljning tydligt utvärdera status per målsättning, om det anses vara uppfyllt, och om inte vilka åtgärder som behöver införas.
- Utvärdera behov och möjligheter för att tillsätta resurser med regionövergripande ansvar för ledning, kravställning, och uppföljning rörande IT-säkerhet.
- Utvärdera behov av- och möjligheter för att upprätta en dedikerad budget för IT-säkerhet, informationssäkerhet, och dataskydd med budgetansvar hos personer med regionövergripande ansvar för dessa områden.
- Tillse att regionövergripande process utarbetas för att tydliggöra dels hur krav på biträden som hanterar personuppgifter för Region Skånes räkning ska definieras och dels hur instruktioner för biträdenas behandling av personuppgifter ska utformas vid tecknande av avtal.
- Genomföra en översyn av nuvarande hantering av regionens registerförteckning av personuppgiftsbehandlingar i syfte att identifiera hur systemstöd kan utvecklas för att förbättra kvaliteten i registerförteckningen, samt underlätta uppföljning och kontroll av följsamheten gentemot GDPR.
- Följa upp projektet för införande av Skånes Digitala Vårdsystem avseende hur patientens integritet i det nya systemet kommer att säkerställas i enlighet med gällande lagstiftning genom exempelvis förbättrade behörighetsstrukturer eller automatiserad loggуppföljning.

1. Inledning

1.1. Bakgrund

Sveriges regioner behandlar vår allra känsligaste och viktigaste information. Om denna information hamnar i fel händer finns det risk för allvarliga konsekvenser, både för medborgarna och hela landet. Ett ändamålsenligt informationssäkerhetsarbete syftar till att minska denna risk, samtidigt som en god tillgänglighet upprätthålls där informationen behövs. I en stor organisation med en enorm mängd känslig information lägger ett systematiskt och ändamålsenligt informationssäkerhetsarbete grunden för effektivt nyttjande av information. Informationssäkerhetsarbetet är med andra ord en grundbult för att Region Skåne ska kunna uppfylla samhällets krav och förväntningar på verksamheten i en värld som är alltmer beroende av data.

Tidigare granskningar har visat att Region Skånes styrning och rutiner inte har varit ändamålsenliga. 2017 konstaterades att en fungerande styrmodell inte hade implementerats samt att det saknades resurser och dokumentation för de mest centrala aspekterna av informationssäkerhetsarbetet såsom incidenthantering. Sammantaget löpte Region Skåne hög risk för felaktig behandling av information och var inte förberett för kriser relaterade till detta.

Sedan dess har de regulatoriska kraven ökat med både GDPR och NIS-direktivet. I och med Covid-19 tillkommer ytterligare utmaningar då nya lösningar såsom hemarbete och distansmöten blir aktuella. Dessutom är risklandskapet under pandemin betydligt mer krävande. Sedan februari har antalet cyberattacker i Europa femdubblats, och Säpo har varnat myndigheter för intensifierade försök från främmande makter att komma över känslig information.

Mot bakgrund av ovan har de förtroendevalda revisorerna beslutat att genomföra en granskning av arbetet med IT- och informationssäkerhet.

1.2. Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om arbetet med IT- och informationssäkerhet inom Region Skåne bedrivs på ett systematiskt och ändamålsenligt sätt.

Syftet besvaras med hjälp av följande revisionsfrågor:

- Bedriver Region Skåne ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för informationstillgångarna utifrån dagens krav?
- Säkerställs medborgarens integritet (GDPR) och är patientinformation i till exempel journalsystem skyddade mot obehöriga?
- Har Region Skåne ett tillräcklig skydd för sina databaser och system inklusive molntjänster mot utomstående intressen som antingen vill komma åt information eller skada verksamheten och hur påverkas detta skydd av att allt fler arbetar hemifrån och på distans?
- Hanteras avvikelser i form av driftavbrott och säkerhetsintrång på system och data och finns ändamålsenlig beredskap med resurser för åtgärder och rapportering av allvarliga incidenter enligt NIS-direktivet?
- Är utbildningen av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter ändamålsenlig?

Granskningen har även innefattat en kartläggning för att utreda hur riskanalyser genomförs inom området informationssäkerhet och vem som ansvarar för att de genomförs, dokumenteras och efterföljs, inklusive tjänster och system som är upphandlade och drivs av extern part.

1.3. Avgränsningar

Granskad nämnd har varit regionstyrelsen som har det övergripande ansvaret för arbetet med IT- och informationssäkerhet i Region Skåne, samt kollektivtrafiknämnden som utöver regionstyrelsen är den nämnd som har rapporteringsansvar enligt NIS-direktivet.

1.4. Genomförande

Granskningen grundas på intervjuer samt granskning av relevant styrande dokumentation för området. Intervjuer har genomförts med utvalda nyckelpersoner för arbetet med IT- och informationssäkerhet i Region Skåne. Se bilaga 1 för förteckning av intervjuade personer samt granskade dokument.

Granskningen är genomförd juni 2020 - september 2020. Projektledare från Region Skåne har varit certifierad kommunal revisor Fredrik Ljunggren och kontaktperson från revisorskollegiet var Eskil Engström.

1.5. Revisionskriterier

Kommunallagen (2017:725)

Enligt 6 kap. 6 § ska nämnderna var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten.

De ska även se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Detsamma gäller när skötseln av en kommunal angelägenhet med stöd av 10 kap. 1 § har lämnats över till någon annan.

Dataskyddsförordningen (The General Data Protection Regulation)
Den nya dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018. Europaparlamentets och rådets dataskyddsförordning (EU) 2016/679 gäller i hela EU och ersatte i Sverige den äldre personuppgiftslagen (PUL) från 1998. Det främsta syftet med dataskyddsförordningen är skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Andra syften med dataskyddsförordningen är att modernisera dataskyddsdirektivets regler från 1995 och att anpassa dessa till det nya digitala samhället.

I jämförelse med PUL ställer Dataskyddsförordningen högre krav på organisationers interna kontroll kopplat till hanteringen av personuppgifter. Vid överträdelse av förordningens artiklar föreligger också skärpta sanktioner:

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
I juli 2016 antog Europaparlamentet det så kallade NIS-direktivet med åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Enligt

NIS-direktivet ska företag som levererar samhällsviktiga och digitala tjänster inom EU följa samma krav på informationssäkerhet och incidentrapportering.

I juni 2018 beslutade riksdagen om den nya Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Lagen innebär i korthet krav på systematiskt informationssäkerhetsarbete och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster.

Säkerhetsskyddslagen (2018:585)

Säkerhetsskyddslagen (2018:585) innehåller krav på åtgärder som syftar till att skydda uppgifter som är av betydelse för Sveriges säkerhet eller som ska skyddas enligt ett internationellt åtagande om säkerhetsskydd. Även skyddet av annan säkerhetskänslig verksamhet, till exempel samhällsviktiga informationssystem, förstärktes i och med införandet av lagen.

Offentlighets- och sekretesslagen (2009:400)

Offentlighets- och sekretesslagen trädde i kraft den 30 juni 2009 och är en omarbetning av den tidigare sekretesslagen. Lagen består av sju avdelningar, vilka innehåller bestämmelser om myndigheters handläggning vid registrering, utlämnande och övrig hantering av allmänna handlingar. Lagen innehåller också bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Förbud att röja uppgift gäller om det sker muntligen eller genom utlämnande av allmän handling eller på något annat sätt.

Patientdatalagen (2008:355)

Behandling av personuppgifter inom hälso- och sjukvården regleras i patientdatalagen. Patientdatalagen ska tillämpas av alla vårdgivare, både i offentlig och privat regi. Patientdatalagen reglerar bland annat:

- Inre sekretess – en reglering som innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter. Detta förtydligas genom att det i lagen ställs krav på behörighetstilldelning och åtkomstkontroll.
- Sammanhållen journalföring, vilket innebär att flera vårdgivare kan ge och få direktåtkomst till varandras journalhandlingar om de uppfyller patientdatalagens krav.
- Patienten har rätt att spärra uppgifter både i vårdgivarens journalsystem och för andra vårdgivare vid sammanhållen journalföring.

Beslutade policies och styrande dokument inom Region Skåne

Region Skåne har flera beslutade policies och riktlinjer som rör IT- och informationssäkerhetsarbetet vilka utgör revisionskriterier för granskningen. Bl.a Säkerhetspolicy (RF 2017-06-20), Säkerhetsstrategi (RS 2017-12-07), Riktlinjer för informationssäkerhet (RS 2017-12-07), Instruktioner och anvisningar för informationssäkerhet. Dessa beskrivs närmare i avsnitt 2.1.1 i denna rapport.

2. Granskningsresultat

2.1. Styrande dokument

2.1.1. Iakttagelser

Ett omfattande arbete genomfördes under 2017 för att ta fram övergripande styrdokument som beskriver Region Skånes viljeriktning inom området för informationssäkerhet samt de övergripande riktlinjer som ska gälla för regionens verksamheter. Ambitionen hos regionen är att bedriva ett systematiskt informationssäkerhetsarbete enligt standarden för informationssäkerhet ISO/IEC 27001. De styrande dokumenten har utformats för detta syfte. Den övergripande strukturen för detta ramverk med styrande dokument innefattar:

- Säkerhetspolicy, fastställd av regionfullmäktige. Denna beskriver Region Skånes övergripande syn på säkerhetsarbetet och de principer som gäller för hela regionen.
- Riktlinjer för informationssäkerhet, fastställd av regionstyrelsen. Dessa syftar till att konkretisera säkerhetspolicyn och beskriva grundläggande informationssäkerhetskrav inom Regionen.
- Instruktion för tillämpning av riktlinjer för informationssäkerhet, beslutad av regiondirektör. Instruktionerna syftar till att tydliggöra och verka som stöd för hur arbetet ska bedrivas i regionens verksamheter utifrån de av regionstyrelsen beslutade riktlinjerna.

Utifrån instruktionerna är det förvaltningschefers ansvar att tillse att arbetet i verksamheten bedrivs i enlighet med riktlinjerna och att lokala instruktioner och rutiner tas fram för att understödja detta. Den som beslutar om instruktioner i regionens verksamheter har även mandat att besluta om eventuella avsteg från de övergripande riktlinjerna. Vid granskningen har relaterade instruktioner inom regionstyrelsens och kollektivtrafiknämndens förvaltningar granskats, så som processer för ändringshantering och incidenthantering.

Regionstyrelsen beslutade i december 2016 att ge regiondirektören i uppdrag att ta fram mål på kort och lång sikt rörande regionens informationssäkerhetsarbete. Dessa togs fram och beslutades under 2017 av regionfullmäktige (långsiktiga mål) och regionstyrelsen (kortsiktiga mål). I målen anges att de långsiktiga målen ska revideras vart fjärde år. De kortsiktiga målen ska följas upp och revideras vid behov årligen vid den rapportering av status på informationssäkerhetsarbetet som informationssäkerhetschefen delger regionstyrelsen vid ledningens genomgång. Den skriftliga rapportering som informationssäkerhetschefen delgett regionstyrelsen 2018 och 2019 innefattar beskrivning av flertalet områden som målen berör. Dock har inte de definierade målen följts upp var för sig med utvärdering om dessa bedöms vara uppfyllda, och om inte vilka åtgärder som i så fall behöver tas för att säkerställa måluppfyllelse. De kortsiktiga målen har heller inte reviderats eller uppdaterats efter att de beslutades 2017.

Regionstyrelsen eller regionfullmäktige har inte antagit regionövergripande riktlinjer för IT-säkerhetsområdet likt hur man har gjort för informationssäkerhetsområdet. Riktlinjerna för informationssäkerhet har heller inte dokumenterat ansvar och rollbeskrivning för regionövergripande IT-säkerhetsarbete. Riktlinjerna för informationssäkerhet beskriver dock till viss del delar som berör IT-säkerhet så som driftsäkerhet och kommunikationssäkerhet. Inom förvaltningen Digitalisering IT/MT har en strategisk handlingsplan och styrande dokument inom IT-arkitektur och IT-säkerhet tagits fram och beslutats av IT-chef.

2.1.2. Bedömning

Strukturen över regionala styrande dokument är tydlig och vi bedömer att de har beslutats i lämpliga instanser avseende dokumentens syfte och inriktning. Vår bedömning efter granskning av regionövergripande riktlinjer och instruktioner för tillämpning av riktlinjer är att de är väl utformade och stipulerar tydliga och lämpliga krav inom informationssäkerhetsområdet. Även ansvarsfördelningen för Region Skånes informationssäkerhetsarbete är väl beskriven i styrande dokument. För granskade lokala instruktioner finns dock i vissa fall en otydlighet i deras koppling gentemot de regionövergripande riktlinjerna. Det har heller inte identifierats rutiner för att dokumentera eventuella avsteg från de regionövergripande riktlinjerna.

Ansvar och krav kopplat till teknisk IT-säkerhet är inte lika väl beskrivna även om riktlinjerna i viss omfattning beskriver IT-säkerhetskrav. Detta kan antas bero på att ansvaret för IT-säkerhet i praktiken ligger inom respektive förvaltning som handhar drift av IT (Inom ramen för denna granskning regionstyrelsens förvaltning Digitalisering IT/MT och kollektivtrafiknämndens förvaltning Skånetrafiken). Digitalisering IT/MT har i viss mån ett regionövergripande ansvar då de hanterar driften av majoriteten av regionens IT, men de har inte ett övergripande ansvar för kravställning kring IT-säkerhet gentemot övriga förvaltningar.

Det är positivt att långsiktiga och kortsiktiga mål för informationssäkerhetsarbetet tagits fram och beslutats av regionfullmäktige respektive regionstyrelsen. Beslutade mål anger riktning och tydlighet samt ett ramverk för att kontinuerligt utvärdera framsteg. Dock har ingen tydlig uppföljning gentemot beslutade mål identifierats. Målen anger fokusområden för de regionala funktionerna för informationssäkerhet och dataskydd, och beskrivning av arbetet inom dessa områden ges av informationssäkerhetschefen i den skriftliga årliga berättelsen som delges regionstyrelsen. Det görs däremot ingen uppföljning per målsättning för att bedöma om man anser sig ha uppfyllt målet, och om inte vilka ytterligare åtgärder eller beslut som behöver tas. Löpande uppföljning av beslutade mål är en förutsättning för att kontinuerligt förbättra informationssäkerhets- och dataskyddsarbetet.

2.2. Organisation och ansvar

2.2.1. Iakttagelser

Vid tillfället för granskningen omfattade den centrala organisationen för informationssäkerhet inom Region Skåne tre personer placerade i enheten för krisberedskap, säkerhet, och miljöledning inom koncernkontoret. Även den centrala organisationen för dataskydd innefattade tre personer inom koncernkontoret. För arbetet i regionens verksamheter finns minst en informationssäkerhetssamordnare och en dataskyddsamordnare i varje förvaltning. I vissa fall är det samma person som är samordnare för bägge delar, medan det i vissa fall har separerats. Vid tillfället för granskningen fanns 13 informationssäkerhetssamordnare och 14 dataskyddssamordnare fördelat på 15 förvaltningar. Deras uppgift är att leda, utveckla, samordna och följa upp informationssäkerhets- och dataskyddsarbetet utifrån regionövergripande styrande dokument. Samordnarna arbetar deltid i dessa roller och lägger varierande stor del av sin tid på detta i tillägg till andra ansvarsområden deras tjänst kräver.

Regiondirektören beslutade 2018 om att samtliga informationstillgångar ska ha en utsedd informationsägare. Dessa utses av förvaltningschef om informationstillgången enbart hanteras inom en förvaltning, eller av regiondirektör om den hanteras inom flera. Informationsägarna har ett stort ansvar avseende det faktiska informationssäkerhets- och dataskyddsarbetet. Ytterst är det informationsägaren som ansvarar för att se till att

information hanteras och skyddas utifrån riktlinjer och lagkrav, till exempel genom riskanalys och informationsklassning.

Det finns definierade forum för samverkan mellan de regionala funktionerna för informationssäkerhet och dataskydd och de samordnare som finns i förvaltningarna för att löpande diskutera frågor, initiativ, och status på arbetet. Det har dock framkommit vid intervju med representanter från de regionala funktionerna att man inte alltid, i tillägg till att verka som kravställare och samordnare, hinner stödja samordnarna i det praktiska genomförandet av aktiviteter i den mån som hade varit önskvärt från dem. Det har också framkommit att det långsiktiga strategiska arbetet för de regionala funktionerna blir lidande på grund av detta. Detta är en uppfattning som delas av intervjuade samordnare som uttrycker ett behov av mer stöttning i det praktiska genomförandet från centralt håll.

Som beskrivet i bedömning 2.1.2 ovan finns ingen central regionövergripande funktion för IT-säkerhet. Inom regionstyrelsens förvaltning som hanterar IT-drift, Digitalisering IT/MT, finns en IT-säkerhetsansvarig och en IT-säkerhetsarkitekt som i viss mån har ett regionövergripande ansvar då förvaltningen hanterar majoriteten av den IT som används inom Region Skåne. Däremot har de inte ett regionövergripande ansvar för utformning av riktlinjer, kravställning, och uppföljning av IT-säkerhet i hela regionen, inklusive IT som hanteras inom andra förvaltningar, så som Skånetrafiken.

Det finns ingen dedikerad budget för dataskydd, informationssäkerhet eller IT-säkerhet, varken inom de regionala funktionerna för informationssäkerhet och dataskydd, eller hos ansvariga för IT-säkerhet i de granskade driftsorganisationerna Digitalisering IT/MT och Skånetrafiken. Kostnader för att investera i IT-säkerhetslösningar eller andra insatser så som oberoende tester, granskningar m.m. är implicit inkluderade i budget för övriga verksamhetsområden. Vid behov eller önskemål om investeringar inom området är man därför beroende av beslut av budgetansvarig i andra delar av verksamheten.

2.2.2. Bedömning

Ansvaret för arbetet med IT- och informationssäkerhet samt dataskydd bedöms vara väl definierat och avgränsat utifrån de roller och ansvarsbeskrivningar som har identifierats i granskningen. Det framgår tydligt vilka funktioner och roller som ansvarar för olika delar av arbetet. Dock verkar det i det praktiska genomförandet finnas ett gap där de regionövergripande funktionerna inte har tid eller resurser att stötta samordnare i förvaltningarna i den omfattning som de upplever hade varit nödvändigt. Detta gap kan till viss del överbryggas genom fortsatt kontinuerlig utbildning och information för samordnare i de nätverk som finns. Klart är även att utökade resurser inom de regionövergripande funktionerna hade förbättrat möjligheterna att bistå med expertstöd för förvaltningarna i större omfattning i det praktiska genomförandet.

Ansvar för regionövergripande arbete med IT-säkerhet kan tydliggöras. Resurser med ansvar för IT-säkerhet finns utsedda inom de två förvaltningar som hanterar IT-drift inom de två granskade nämnderna, regionstyrelsen och kollektivtrafiknämnden. Deras ansvar är främst att operativt hantera IT-säkerhetsfrågor och hantera relation och dialog med driftsleverantörer ansvarar för kontroller och rutiner kopplat till IT-säkerhet. För att oberoende styra, kravställa och följa upp IT-säkerhetsarbetet inom hela regionen skulle en centralt placerad resurs eller funktion underlätta.

Att det inte finns någon dedikerad budget för dataskydd, informationssäkerhet eller IT-säkerhet innebär inte att investeringar inte görs inom dessa områden. Vid tillfället för

granskningen var exempelvis ett nytt systemstöd för riskhantering under införande. Däremot innebär avsaknaden av dedikerad budget inom områdena att principer för planering och beslut om investeringar blir komplexa. För effektivt arbete med IT- och informationssäkerhet är det fördelaktigt om investeringsbeslut fattas oberoende av beslut om investeringar i andra områden som i dagsläget ligger hos de budgetansvariga.

2.3. Arbete med riskanalys och informationsklassning

2.3.1. Iakttagelser

Enligt riktlinjerna för informationssäkerhet och tillhörande instruktioner ska riskanalys och informationsklassificering genomföras för att säkerställa att information ges rätt skyddsnivå och att risker identifieras, bedöms och hanteras. Riskanalyser och informationsklassning ska enligt riktlinjerna genomföras regelbundet, både vid införande av nya system och informationsbehandlingar eller vid förändringar som påverkar nuvarande rutiner för hantering av information.

För att konkretisera riktlinjerna har instruktioner både för informationsklassificering samt riskhantering avseende informationstillgångar tagits fram av informationssäkerhetschef och beslutats av regiondirektören. Vidare har även handledningar inom dessa två områden utarbetats av informationssäkerhetschefen för att ge verksamheten ytterligare vägledning kring hur instruktionerna för informationsklassificering och riskhantering ska tillämpas. I instruktionerna och handledningarna ges beskrivning av hur dessa ska genomföras enligt regionens modell, de lagar som ligger till grund för krav på att de ska genomföras, samt vem som ansvarar för att de genomförs i verksamheten.

Riskanalyser ska även ta i beaktande personuppgiftsbehandlingar för att säkerställa att risker för de registrerade identifieras och hanteras. Vid tidpunkten för granskningen framkom vid intervju med dataskyddsombud och den regionala dataskyddsorganisationen att det återstår arbete med att integrera detta i den övergripande riskanalysprocessen. Däremot har en initial mall för en så kallad konsekvensbedömning utarbetats som vid tidpunkten för granskningen inte var helt färdigställd men hade börjat appliceras av vissa av regionens verksamheter.

Ansvar för att tillse att informationsklassificering och riskanalys för informationstillgångar i verksamheten genomförs ligger ytterst på förvaltningschefen i den/de förvaltningar som informationen behandlas i. För det praktiska genomförandet ansvarar informationsägare, som är de av förvaltningschefen utsedda personer som ansvarar för beslut och behandling av informationstillgångar i verksamheten. Informationsägare ansvarar för att information klassificeras och att riskanalys för att analysera hot, risker och sårbarheter gentemot informationstillgången har genomförts. Det är sedan informationsägarens ansvar att tillse att information ges rätt skydd enligt de krav som kommer från klassificering och riskanalys genom dialog och kravställning gentemot systemägare för IT-system.

Som stöd för informationsägaren och verksamheten i att genomföra informationsklassificering och riskanalys enligt den modell som beskrivs i riktlinjer för informationssäkerhet finns ett av informationssäkerhetschefen utarbetat riskhanteringsverktyg i Excel. Detta innehåller vägledning och modeller för att genomföra klassning och riskanalys enligt förekommande lagkrav. Vid intervju med informationssäkerhetschef, informationssäkerhetssamordnare och dataskyddssamordnare framkom att verktyget i sin nuvarande form upplevs vara komplext och svårt att applicera. Vid tidpunkten för granskningen var ett nytt systemstöd för riskhantering under införande,

vilket av de intervjuade bedömdes möjliggöra förenklad hantering av dessa moment, samt förbättra möjligheter för uppföljning av genomförandegrad för regionens informationsbehandlingar.

2.3.2. Bedömning

Regionen bedöms ha goda riktlinjer, rutiner och modeller för informationsklassificering och riskanalys vilka tydligt beskriver hur dessa moment ska genomföras inom regionens verksamheter, samt vilka som ansvarar för att tillse att de genomförs. Det riskhanteringsverktyg som i dagsläget används upplevs på flera håll inom verksamheten vara något komplext, samtidigt är det väl utarbetat och tar hänsyn till de krav som ställs på informationsklassificering och riskanalys genom lagar, förordningar och regionens riktlinjer, varför det i granskningen bedöms vara lämpligt.

Enligt intervjuer med informationssäkerhetschef och informationssäkerhetssamordnare har framgått att genomförandegraden avseende informationsklassificering och riskanalys har gått framåt de senaste åren, i synnerhet vad gäller informationsbehandlingar av högre risknivå. Samtidigt har noterats att riskanalyser och informationsklassificering inte alltid sker vid införande av nya system eller förändringar i befintliga informationsbehandlingar, eller att dessa moment kommer in för sent till exempel i upphandlingsprocessen för att kunna bidra med det syfte och den kravställning som de ska. Det har även noterats att riskanalys för personuppgiftsbehandlingar och relaterade konsekvensbedömningar inte är fullt integrerade med den övergripande riskanalysprocessen. Därav är bedömningen att arbetet fortsatt behöver accelereras, samt löpande följas upp för att kartlägga och utvärdera genomförandegraden. Det senare är ett arbete där förutsättningar kommer att förbättras i och med införande av det nya riskhanteringsverktyget som skapar en central plats för informationsklassificering och riskanalys av regionens informationstillgångar.

2.4. Teknisk säkerhet för system, molntjänster och distansarbete

2.4.1. Iakttagelser

Ansvaret för teknisk säkerhet inom regionstyrelsen och dess förvaltning som hanterar IT-drift, Digitalisering IT/MT, ligger dels hos IT-säkerhetsansvarig och IT-arkitekter genom att arbeta med kravställning och stöttning inom området. Till stor del är dock ansvaret fördelat inom förvaltningens enheter med olika ansvar inom området. Handledningar har tagits fram av IT-säkerhetsansvarig och IT-arkitekt för att ge vägledning kring teknisk säkerhet för system och tjänster som hanteras inom förvaltningen, t.ex. *Regelverk för Serverbaserade applikationer inom Region Skåne* och *Strategisk handlingsplan IT-säkerhet*. Inom arkitektrådet har även en kravkatalog utformats som syftar till att innehålla Region Skånes samlade säkerhetskrav, inom relevanta områden som applikationssäkerhet, fysisk säkerhet, drift, kommunikationssäkerhet, åtkomst m.m. Denna kravkatalog är dock inte beslutad och är mer av vägledande karaktär för regionens systemansvariga och ansvariga för samverkan med tredjeparter.

Inom kollektivtrafiknämnden och dess förvaltning som hanterar IT-drift, Skånetrafiken, ligger ansvaret för teknisk säkerhet inom enheten för Information Kommunikation och Teknik. Denna grupp innefattar elva anställda med olika ansvar inom området, som till exempel brandvägg, patchning, databas, nätverk, etc. I granskningen har inga styrande instruktioner eller handledningar inom området identifierats utöver de delar inom de regionövergripande riktlinjerna för informationssäkerhet som man ska förhålla sig till.

Granskningen har identifierat att system som driftas av de två förvaltningar inom ramen för denna granskning, Digitalisering IT/MT och Skånetrafiken, har tekniska skydd inkluderande brandväggar, skydd mot skadlig kod, antivirusskydd, IPS, IDS, sårbarhetsscanning m.m. Digitalisering IT/MT:s två stora sourcingpartners för IT-driften Tieto/Evry och Telia/Cygate har dessutom dedikerade SOC:s (Security Operations Centers) som är dedikerade för att löpande bevaka säkerhetsrelaterade händelser, hot, och sårbarheter.

Omfattande arbete har genomförts de senaste åren för att segmentera Region Skånes nätverk (uppdelning av nätverket i mindre delar vilket ger ett bättre skydd). Inom Skånetrafiken genomförs penetrationstester en gång per år för att identifiera sårbarheter i nätverk och system. Inom Digitalisering IT/MT görs dock inte regelbundna externa penetrationstester då det saknas budget för detta.

Användandet av molntjänster inom Region Skåne har ökat de senaste åren. Enligt intervju med informationssäkerhetschef finns ingen uttalad strategi eller policy för vilka system och tjänster man får köpa in som molntjänster och inte, så länge leverantören kan leva upp till lagkrav och Region Skånes riktlinjer. Däremot kan det enligt intervjuer ofta uppstå frustration i verksamheten i samband med upphandling av molntjänster. Detta då utfallet från informationsklassificering och riskanalyser ofta mynnar ut i krav som få eller inga leverantörer av molntjänster kan uppfylla när det gäller hantering av personuppgifter och sekretessbelagd information. Samt i andra fall då dessa analyser görs för sent efter att molntjänsten redan har upphandlats och utfallet av klassificering och riskanalys blir att det upphandlade systemet inte kan användas som avsett.

Kravkatalogen med IT-säkerhetskrav som utformats av arkitektrådet inom Region Skåne ska även verka som stöd för projektorganisationen vid upphandling av molntjänst. Vid intervjuer har framkommit att denna kravkatalog inte alltid används vid upphandlingar. Det har även noterats att ansvar för kravställning vid upphandlingar ligger hos koncerninköp och det är sällan IT-arkitekt, IT-säkerhetsansvarig, informationssäkerhetschef eller andra expertroller är involverade vid tecknande av avtal. Region Skånes upphandlingspolicy och relaterade anvisningar fastställer inte heller ansvar för kravställning gällande IT-säkerhet eller informationssäkerhet. Det pågår dock ett initiativ som involverar koncerninköp, informationssäkerhet, och andra funktioner så som den regionala dataskyddsorganisationen för att tydliggöra hur relevanta krav ska införlivas till högre grad i upphandlingsprocessen.

Inloggning till Region Skånes IT-miljö för distansarbete hanteras via en VPN-lösning kallad RSVPN. VPN är en etablerad lösning för fjärråtkomst och innebär att en säker förbindelse upprättas mellan användarens dator och organisationens servrar. För att möjliggöra distansarbete via VPN behöver ansökan om tillgång göras enligt intern rutin där beställande chef ska godkänna. Först därefter installeras RSVPN-klienten på medarbetarens dator, vilket enbart görs på datorer som administreras av Region Skåne. Medarbetare kan alltså inte ansluta till Region Skånes system via privata datorer. För Region Skånes VPN-användning kan användaren antingen autentiseras genom sitt RSID-kort som behöver vara insatt i datorn vid anslutning eller genom ett certifikat som lagras på datorn och installeras i samband med att medarbetaren har godkänts RSVPN-åtkomst.

2.4.2. Bedömning

Det står klart att IT-säkerhet arbetas med aktivt och att system inom Region Skånes driftansvar (både inom Regionstyrelsen och Kollektivtrafiknämnden) innefattar omfattande skydd mot sårbarheter och hot. Den övergripande bedömningen är att Region Skåne har

lämpligt tekniskt skydd för databaser och system. Vi bedömer dock att tydligare ansvarsfördelning för kravställning och uppföljning kring IT-säkerhet, både vad gäller system som driftas av Region Skåne och vad gäller system som köps in som molntjänster, behöver definieras.

För molntjänster hanteras tekniskt skydd av leverantören. Vi bedömer att det finns lämpliga rutiner i projekt- och förstudiefaser för att utvärdera lämpligheten hos leverantörer vid upphandling genom riskanalyser och informationsklassificering. Däremot bedömer vi att tydligare anvisningar och ansvar behövs för att säkerställa att lämpliga krav rörande IT- och informationssäkerhet samt dataskydd förs in i avtal med molntjänstleverantörer.

Vår bedömning är att Region Skåne använder etablerade och säkra lösningar för distansarbete som möjliggör en säker anslutning till Region Skånes IT-miljö. Riskerna ökar dock generellt vid distansarbete till följd av oaktsamhet av den enskilda personen. Hantering av denna risk bedöms i första hand kunna överbryggas med ökat fokus och frekvens för utbildning för medarbetare (se även bedömning 2.6.2).

2.5. Kontinuerlig uppföljning och förbättringsarbete

2.5.1. Iakttagelser

Det är beskrivet i regionens riktlinjer för informationssäkerhet att informationssäkerhetschefen är ansvarig för uppföljning av att beslutade riktlinjer efterlevs inom Region Skåne, samt dataskyddsombudets ansvar att bevaka att dataskyddsförordningen och andra tillämpliga lagar följs i regionens verksamheter.

Naturlig uppföljning sker löpande i den dialog de regionövergripande funktionerna för informationssäkerhet och dataskydd har med informationssäkerhets- och dataskyddssamordnare. Detta genom regelbundna nätverksmöten samt från delar av den dagliga verksamheten där man deltar för att stötta verksamheten. Informationssäkerhetschefen sammanställer årligen en skriftlig rapport till regionstyrelsen utifrån bedömd status på prioriterade områden inom informationssäkerhetsarbetet samt inträffade viktiga händelser under det senaste året.

Det sker ingen strukturerad uppföljning av att regionens verksamheter efterlever beslutade riktlinjer för informationssäkerhet. Inom dataskyddsarbetet har initiala steg tagits under 2020 för att arbeta enligt ett årshjul där verksamheterna själva ska göra en revision för att status och följsamhet gentemot GDPR-direktivet.

Även gällande uppföljning av att tredjeparter efterlever avtalat ansvar och har lämpliga rutiner och kontroller på plats för att hantera IT- och informationssäkerhetsrelaterade risker sker viss naturlig uppföljning i de samverkansforum som finns med de viktigaste tredjeparterna. Dessa är Tieto/Evry som levererar server- och applikationsdrift och Telia/Cygate som levererar nätverks- och telefonitjänster för regionstyrelsens förvaltning som ansvarar för IT-drift (Digitalisering IT/MT). Vid intervjuer har dock uttryckts att uppföljningen som görs i detta forum är ad hoc och att det i många fall kan vara en otydlighet i återkoppling kring hur problemområden som diskuteras sedan faktiskt hanteras av leverantören. Inom Digitalisering IT/MT har initiala steg tagits under hösten 2019 och våren 2020 för att återkommande granska dessa leverantörer i form av en årlig revision. Denna granskning har dock inte identifierat att dessa revisioner har gjorts med syfte att följa upp leverantörernas

följsamhet specifikt gentemot regionens beslutade riktlinjer och krav för IT- och informationssäkerhet.

2.5.2. Bedömning

Vår bedömning är att det finns brister i systematiken avseende uppföljning av informationssäkerhetsarbetet. Det ska klargöras att denna bedömning inte innebär att uppföljning av arbetet inte genomförs. De centrala informationssäkerhets- och dataskyddsorganisationerna följer upp och bevakar aktiviteter kopplat till detta arbete som en naturlig del av det dagliga arbetet och återrapportering sker till regionstyrelsen i form av en årlig skriftlig rapport som beskriver status på arbetet. Däremot är bedömningen att Region Skånes rutiner för intern uppföljning av IT- och informationssäkerhetsarbetet behöver stärkas för att skapa en bättre systematik i hur uppföljning bedrivs. Det sker inte enligt någon definierad granskningsplan eller utvärderingsmall vilket gör att utvärdering avseende status på informationssäkerhetsarbetet och verksamheternas efterlevnad i viss mån blir subjektiv och inte identifierar trender och utveckling över tid. Ett effektivt ledningssystem för informationssäkerhet är beroende av kontinuerlig uppföljning och granskning för att säkerställa att beslutade policies och riktlinjer efterlevs, och om de inte gör det tydligt identifiera problemområden och definiera aktiviteter för förbättring.

Även uppföljningen av outsourcade tjänster bör stärkas. Framförallt för de viktigaste tredjeparterna Tieto/Evry och Telia/Cygate. Det har under granskningen framkommit att löpande dialog för uppföljning förs och då de har haft en tjänsteleverans gentemot regionen under lång tid finns en stor tillit parterna emellan. Även om Region Skåne har outsourcat ansvar för drift och tillhörande IT-säkerhetsarbete är IT- och informationssäkerhetsrisker regionens ansvar. För att säkerställa att tredjeparter följer Region Skånes riktlinjer och instruktioner krävs ett mer strukturerat uppföljningsarbete än vad som bedrivs idag.

Den främsta orsaken till bristen på systematisk uppföljning av IT- och informationssäkerhetsarbetet utges från intervjuade personer vara tids- och resursbrist samt att arbetet fram tills nu har fokuserat på att etablera strukturer, ansvar och central kravställning. Majoriteten av den tillgängliga tiden går åt till att bistå och stödja verksamheten i olika delar av arbetet. En högre mognadsgrad i det systematiska uppföljningsarbetet utges därför av intervjuade vara beroende antingen av utökade resurser eller att verksamheternas mognadsgrad i IT- och informationssäkerhetsarbetet höjs genom ökad förståelse. Detta skulle göra dem mer självständiga i IT- och informationssäkerhetsarbetet och frigöra tid för de regionövergripande funktionerna som kan fokuseras på uppföljning i högre grad.

2.6. Utbildning

2.6.1. Iakttagelser

I instruktioner för tillämpning av riktlinjer för informationssäkerhet som har beslutats av regiondirektören beskrivs att samtliga medarbetare ska ges den utbildning i informationssäkerhet som krävs för att de ska kunna genomföra sina arbetsuppgifter på ett säkert sätt. Det finns en framtagen e-utbildning för säker informationshantering vars syfte är att kunna ge samtliga regionens medarbetare grundläggande kunskaper och förståelse för deras ansvar inom området. Denna utbildning innefattar informationssäkerhet, IT-säkerhet, dataskydd, samt arkiv- och informationshantering. I ovan nämnda riktlinjer beskrivs vidare att samtliga anställda minst ska ha genomgått denna grundläggande e-utbildning. Det har dock

noterats i granskningen att det inte har säkerställts att samtliga anställda har genomgått denna utbildning. Det är upp till varje förvaltning att besluta vilka utbildningskrav som ställs på nyanställda eller befintliga anställda. I förvaltningarna berörda av denna granskning, koncernkontoret, Skånetrafiken, och Digitalisering IT/MT är e-utbildningen obligatorisk. Det har dock inte i granskningen identifierats några uppföljningar i förvaltningarna av vilka medarbetare som har genomgått utbildningen.

Vidare genomförs löpande utbildning och informationsspridning i och med de nätverk med informationssäkerhetssamordnare och dataskyddssamordnare som samverkar med de regionala funktionerna. Samordnarna har i sina roller ansvar för att informera, utbilda och bistå med rådgivning inom deras respektive verksamheter. De regionala funktionerna för informationssäkerhet och dataskydd bistår i att ta fram utbildningsmaterial och information som sedan sprids vidare av samordnarna i olika forum. Dessa utbildningsinsatser är dock sporadiska i den mån att de inte genomförs strukturerat enligt planerad frekvens och för definierade målgrupper enligt en utbildningsplan eller liknande.

Informationssäkerhetschefen och dataskyddsombudet besökte under 2019 förvaltningarnas ledningsgrupper för att informera om regionens informationssäkerhets- och dataskyddsarbete samt informera om interna riktlinjer och gällande regelverk. Det har dock vid intervjuer i granskningen med de regionövergripande funktionerna för informationssäkerhet och dataskydd framgått att förståelse, primärt inom de lagar och förordningar som är gällande, på ett generellt plan fortsatt behöver höjas. Framförallt hos medarbetare i ledande befattningar för att driva på och prioritera arbetet i förvaltningarna och införliva IT- och informationssäkerhet samt dataskydd i relevanta verksamhetsprocesser.

2.6.2. Bedömning

För ett effektivt arbete med IT- och informationssäkerhet samt dataskydd är det av stor vikt att samtliga medarbetare har den kunskapsnivå som krävs för att införliva lämpliga rutiner och lämpligt handhavande i den dagliga verksamheten. Granskningen har identifierat att ramverk och rutiner för utbildningar finns, och att det bedrivs löpande arbete och insatser för att höja medvetandenivån inom regionens verksamheter. Dock är bedömningen att utbildningsinsatser fortsatt behöver accelereras då anpassning gentemot rådande riktlinjer och lagkrav till stor del är beroende av prioriteringar och beslut av medarbetare i ledande befattningar, och stora delar av de risker som föreligger vid informationshantering finns i de rutiner som den enskilde medarbetaren efterlever i det dagliga arbetet.

2.7. Incident- och avvikelsehantering

2.7.1. Iakttagelser

Granskningen har identifierat att det finns en övergripande instruktion, som beslutades av regiondirektören 2017, för hantering av informationssäkerhetshändelser och incidenter. Instruktionen beskriver kriterier, principer och rutiner för prioritering och hantering av både informationssäkerhetsincidenter och personuppgiftsincidenter. Vidare innefattar denna instruktion beskrivning av hur processer ska vara utformade för att regionens verksamheter ska hantera och förebygga incidenter.

Utifrån instruktionen är informationsägare, chefer, verksamhetsansvariga, systemansvariga, informationssäkerhetssamordnare och IT-säkerhetsansvariga ansvariga för att upprätta rutiner och informera medarbetare för att ge förutsättningar att hantera incidenter enligt

kraven i instruktionen. I de två förvaltningarna med IT-driftsansvar inom ramen för denna granskning, regionstyrelsens förvaltning Digitalisering IT/MT och kollektivtrafiknämndens förvaltning Skånetrafiken finns dokumenterade instruktioner. Dessa beskriver hur man ska arbeta med incidenter i dessa verksamheter specifikt och vilket ansvar medarbetare har i att rapportera incidenter samt hur de ska gå tillväga för att göra detta. Inom Digitalisering IT/MT finns även ytterligare instruktioner för hantering av stora incidenter i IT och telefoni samt för problemhantering.

Vid tidpunkten för granskningen hade precis ett nytt systemstöd för rapportering och hantering av incidenter implementerats inom Digitalisering IT/MT. Detta är ett väletablerat system på marknaden som i sin utformning möjliggör ett strukturerat handhavande för prioritering, eskalering, hantering och kommunikation kring identifierade incidenter.

Efter införandet av NIS-direktivet har en regionövergripande beskrivning av processer för att säkerställa rapportering av incidenter enligt direktivet utformats av informationssäkerhetschef och beslutats av områdeschef för Krisberedskap, Säkerhet och Miljöledning. Vid granskning av instruktionen för hantering av stora incidenter inom Digitalisering IT/MT noterades att denna inkluderar beskrivning av hur incidenter ska hanteras enligt NIS-direktivet. Inom Skånetrafiken har en kartläggning gjorts för att identifiera vilka tjänster som omfattas av direktivet och en instruktion för incidenthantering som beskriver hur incidenter ska hanteras enligt NIS-direktivet har tagits fram.

Det har noterats att det saknas dokumenterade rutiner och modeller för att övergripande och över tid följa upp incidenthanteringsarbetet, dels avseende effektivitet i processer för att identifiera förbättringsområden i arbetet med att hantera incidenter och dels för att följa upp om införda åtgärder och information för verksamheten får tilltänkt effekt.

2.7.2. Bedömning

Bedömningen är att Region Skåne i allt väsentligt har en god struktur och beredskap för identifiering, hantering, och rapportering av incidenter. Den regionövergripande instruktionen för informationssäkerhetsrelaterade incidenter tillsammans med beskrivning av incidenthantering enligt NIS-direktivet tar relevanta lagkrav i beaktning och beskriver väl ansvar och rutiner för att säkerställa ändamålsenlig hantering av incidenter. Granskning av de verksamhetsspecifika instruktionerna inom regionstyrelsens förvaltning Digitalisering IT/MT och kollektivtrafiknämndens förvaltning Skånetrafiken visar att de är utformade i enlighet med den regionövergripande instruktionen och tar NIS-direktivet i beaktning.

Effektivt incidenthanteringsarbete är inte enbart beroende av beredskapen för att hantera och åtgärda identifierade incidenter. Det är även i hög utsträckning beroende av medvetenheten och benägenheten hos samtliga regionens medarbetare att identifiera incidenter då de inträffar och skyndsamt rapportera dessa enligt definierad rutin. Flera intervjuade i granskningen uttryckte att det troligtvis finns ett stort mörkertal i incidenter som sker men inte rapporteras på grund av okunskap hos medarbetare. Som noterats i avsnitt 2.5.2 är bedömningen att utbildningsnivån fortsatt behöver höjas inom regionen, vilket är en förutsättning även för ett höjt medvetande rörande deras ansvar och följsamhet gentemot incidentrapporteringsrutiner för regionens medarbetare.

För proaktivt arbete och kontinuerlig förbättring av incidenthantering krävs uppföljningsmekanismer. Viss kontinuerlig uppföljning av informationssäkerhetsrelaterade driftsincidenter har identifierats i samverkansforum mellan Region Skåne och Tieto/Evry samt av KPI:er kopplade till incidenthantering som följs upp av Tieto som en del av deras

ansvar i tjänsteleveransen. Rutiner, modeller och målsättningar i denna uppföljning behöver dock tydliggöras för att möjliggöra utvärdering av om genomförda åtgärder eller utbildningar får tilltänkt effekt i form av fler eller färre rapporterade incidenter.

2.8. GDPR och patientintegritet

2.8.1. Iakttagelser

Detta avsnitt är fokuserat på Region Skånes arbete med att säkerställa hantering av persondata enligt GDPR, samt patientintegritet i journalsystem där journalsystemet Melior har varit objekt för denna granskningen. Det ska noteras att gällande arbetet med GDPR hanteras även stora delar av detta inom övriga avsnitt i rapporten, 2.1 till och med 2.7.

2.8.1.1 Arbete för att säkerställa personuppgiftshantering i enlighet med GDPR

Regionstyrelsen har tillsett en organisation för arbete med dataskydd (GDPR) med syftet att säkerställa att förordningen efterlevs och att integriteten i personuppgifter säkerställs i enlighet med gällande lagstiftningar. Regionstyrelsen har givit regiondirektören i uppdrag att utse dataskyddsombud samt en regional dataskyddsorganisation vilket skedde under 2018. Dataskyddsombudet och den regionala dataskyddsfunktionen ansvarar för att leda, utveckla och följa upp regionens dataskyddsarbete och hantering av personuppgifter. Däremot har även dataskyddssamordnare i respektive verksamhet en viktig roll i att driva arbetet och se till att implementera nödvändiga rutiner och följa upp arbetet.

Avseende styrande dokument för regionens hantering av personuppgifter togs i samband med att GDPR trädde i kraft en instruktion för Region Skånes behandling av personuppgifter fram av dåvarande dataskyddsombud. Instruktionen beskriver ansvar och krav rörande denna hantering. Det finns även en instruktion kallad ”Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav” som definierar lagmässiga och interna krav på personuppgiftsbehandling. Det finns en framtagen hjälptext för tecknande av personuppgiftsbiträdesavtal som beskriver syftet med dessa samt vems ansvar det är att tillse att de tecknas, samt mallar för ansvariga att basera dessa på. Granskningen har däremot identifierat en avsaknad av mer praktiska instruktioner eller handledningar (så som handledning för genomförande av konsekvensbedömningar, gallring av personuppgifter, tecknande av personuppgiftsbiträdesavtal etc.) som på övergripande nivå styr och informerar kring hur aktiviteter ska genomföras enligt GDPR.

Från att GDPR trädde i kraft har ingen formaliserad löpande uppföljning gjorts för att kartlägga och utvärdera hur väl man efterlever kraven enligt GDPR i regionens verksamheter utan stort ansvar har legat på dataskyddssamordnare att ansvara för att löpande driva på arbetet i sin förvaltning och aktivt delta i forum med den regionala dataskyddsfunktionen. Initiala steg har dock tagits av den regionala dataskyddsfunktionen under 2020 för att arbeta enligt ett årshjul där verksamheterna själva ska revidera status och följsamhet gentemot förordningen.

Registerförteckning av Region Skånes personuppgiftsbehandlingar finns i Sharepoint och det är dataskyddssamordnares ansvar att upprätthålla denna förteckning och se till att personuppgiftsbehandlingar identifieras och dokumenteras i enlighet med förordningens krav i registerförteckningen. Dokumentation i förteckningen enligt nuvarande format sker manuellt och saknar funktionalitet för att till exempel flagga för om förteckningen fylls i i enlighet med de krav som finns.

2.8.1.2 Rutiner för att säkerställa patientintegritet - Melior

Instruktionen *Styrning av behörigheter för åtkomst till uppgifter om patienter* har utarbetats av informationssäkerhetschef och beslutats av Hälso- och sjukvårdsdirektör. Enligt denna ska en behovs- och riskanalys göras innan medarbetare tilldelas behörighet i vårdsystem. Verksamhetschef är ytterst ansvarig för att behörigheter hanteras enligt denna rutin. Som en del av rutinen ansvarar också verksamhetschefen, eller medarbetare med delegerat ansvar, för att genomföra årliga kontroller för att säkerställa att varje medarbetares behörighet överensstämmer med de arbetsuppgifter medarbetaren har. Vid intervju med systemansvarig för Melior kunde verifieras att rutinen för tilldelning följer instruktionen. Efterlevnaden av rutinen för årlig kontroll av medarbetares behörigheter har inte kunnat verifieras då ansvaret ligger inom verksamheten och det saknas central funktion för att koordinera och följa upp på om dessa genomgångar görs.

Då behörighetsstrukturer i Region Skånes journalsystem är breda och inte i samtliga fall kan begränsas i den omfattning som är nödvändig för att säkerställa att personal enbart har åtkomst till de journaler de har behov av i sitt arbete, i enlighet med patientdatalagen, har beslut tagits om att införa en kompenserande kontroll med uppföljning av aktiviteter i loggar från journalsystem. Denna loggkontroll finns beskriven i en instruktion om loggkontroll för granskning av åtkomst till patientuppgifter som beskriver hur loggkontroller avseende åtkomst till patientuppgifter ska genomföras i Region Skåne. Enligt instruktionen är riktmärket för loggkontroll att 10% av personalen ska kontrolleras månadsvis under en 24-timmarsperiod, eller vid misstanke om obehörig åtkomst. Det är verksamhetschef som ansvarar för att se till att dessa kontroller utförs. För de stickprov som kontrolleras utvärderas om medarbetare är behöriga att arbeta med journaler som de har tittat på eller arbetat i. Avvikelser ska rapporteras av enligt en separat instruktion, *Dataintrång - åtgärder vid misstanke om olovlig åtkomst*. Det finns inga automatiserade rutiner för att stödja loggуppföljningen, utan all granskning sker manuellt. Detta kräver stora resurser och säkerställer kontroll endast för en mindre del av personalen och deras åtkomst till journaler. I granskningen har också noterats att riktlinjerna om 10% inte alltid efterlevs. Diskussion har förts inom Region Skåne att införa automatiserade verktyg för att underlätta uppföljningen men har inte prioriterats. Detta då införandet av Skånes Digitala Vårdsystem bedöms säkerställa en mer separerad behörighetsstruktur och förbättrade möjligheter till automatiserad uppföljning.

2.8.2. Bedömning

Vår bedömning är att de granskade nämnderna bedriver ett aktivt arbete med att säkerställa patientintegritet och god hantering av personuppgifter enligt GDPR och andra gällande lagstiftningar. Det bedrivs ett strukturerat arbete av dataskyddsombud och den regionala dataskyddsfunktionen. Dock innebär ansvarsfördelningen i arbetet att stort ansvar ligger hos dataskyddssamordnare i förvaltningarna att driva informera, utbilda och följa upp att hantering sker ändamålsenligt i verksamheten. Bedömningen är att arbete fortsatt behöver bedrivas för att säkerställa att dataskyddssamordnare och verksamheten har den kompetensnivå som krävs för att säkerställa att förordningen efterlevs (se även bedömning 2.6.2 angående utbildning). Strukturen på styrande dokument inom GDPR-området kan även tydliggöras från centralt håll för att mer enhetligt beskriva krav och rutiner på verksamheten.

Initiala steg har tagits för att arbeta mer strukturerat med självutvärdering och status på verksamheternas arbete med anpassning gentemot GDPR. Detta är ett bra initiativ och en förutsättning för att bedriva ett effektivt arbete på lång sikt. Den uppföljning som görs sker dock i dagsläget manuellt och kan därför riskera att till viss del bli subjektiv. Ett utökat

systemstöd till exempel för hantering av regionens registerförteckning skulle möjliggöra ett mer heltäckande och objektivt uppföljningsarbete.

Den breda behörighetsstrukturen i Melior medför att integriteten för patienter vars information behandlas i systemet inte helt kan säkerställas i enlighet med gällande lagstiftning. Detta är ett faktum som konstaterats vid flera tidigare granskningar och tillsyner av regionen. Loggуppföljningar som har införts för att kompensera denna brist är omfattande och innebär stor resursåtgång. Då denna loggуppföljning endast omfattar en liten del av den aktivitet som sker och då det finns fördröjning mellan det att aktiviteter sker och när uppföljningar görs, föreligger det en risk för patientintegriteten med nuvarande rutiner och behörighetsstruktur.

3. Sammanfattande bedömning

Region Skånes informationssäkerhetsarbete inom regionstyrelsen och kollektivtrafiknämnden bedöms till stora delar vara ändamålsenligt men i andra delar otillräckligt. Regionstyrelsen har inom sitt ledningssystem för informationssäkerhet utformat styrande riktlinjer och metoder för verksamheten för att tydliggöra ansvar och tillhandahålla stöd i det dagliga arbetet som involverar informationssäkerhet. Organisation och ansvar för informationssäkerhetsarbetet är tydligt definierat, däremot är bedömningen att antalet medarbetare som arbetar regionövergripande med informationssäkerhet är förhållandevis få för en organisation av Region Skånes storlek. Bedömningen är att det finns brister i Region Skånes arbete med att följa upp att beslutade riktlinjer efterlevs, dels internt men även gentemot drifts- och molntjänstleverantörer. Initiala steg har tagits för sådan uppföljning inom dataskyddsarbetet, men rutiner för denna typ av uppföljning saknas inom övriga delar av informationssäkerhetsarbetet. Regionstyrelsen har fastställt mål för informationssäkerhetsarbetet, dock sker uppföljning av dessa mål inte strukturerat för att löpande utvärdera och besluta om åtgärder för att kunna uppnå målen.

Bedömningen är att regionstyrelsen har tillsett ett strukturerat arbete avseende anpassning och efterlevnad gentemot GDPR som tar samtliga delar av förordningen i beaktning. Säkerställande av att förordningen efterlevs är dock beroende av fortsatt utbildning av samtliga medarbetare för att förbättra förståelse för kraven och införliva dem i högre utsträckning i verksamhetsprocesser. Patientintegriteten i journalsystemet (Melior) som ingått i denna granskning bedöms inte fullt säkerställas i och med nuvarande behörighetsstruktur, trots de rutiner för loggуppföljning av journaler som finns. Vi har dock under granskningen förstått att detta är ett område som prioriteras inom ramen för införandet av Skånes Digitala Vårdsystem.

Vi bedömer att Region Skåne inom regionstyrelsen och kollektivtrafiknämnden har ändamålsenliga skyddsmekanismer för system som hanteras av driftsorganisationerna inom ramen för denna granskning. Samtidigt kan ansvar för regionövergripande kravställning inom området tydliggöras. För närvarande är IT-säkerhetsansvariga placerade inom driftsorganisationerna vilket medför utmaningar i deras oberoende vad gäller kravställning och uppföljning.

Molntjänster används i allt högre utsträckning inom Region Skåne. Andelen molntjänster som hanterar kritisk information är dock begränsad då genomförandegraden av riskanalys och informationsklassificering vid införande av nya lösningar är hög. Dessa rutiner bedöms identifiera fall där leverantörer inte lever upp till gällande lagkrav. Ansvar för att säkerställa att Region Skånes krav på IT-säkerhet, informationssäkerhet och dataskydd i avtal med molntjänstleverantörer, samt att följa upp att dessa krav efterlevs bedöms däremot kunna tydliggöras.

Den övergripande bedömningen är att Region Skåne inom regionstyrelsen och kollektivtrafiknämnden har goda rutiner och beredskap för att identifiera, rapportera, och hantera incidenter och avbrott. Lämpliga riktlinjer finns beslutade centralt och instruktioner har utformats lokalt. Dessa har även anpassats gentemot NIS-direktivet efter dess införande.

Strukturerade utbildningsinsatser genomförs i olika former inom Region Skåne. Det är dock vår bedömning att omfattningen av dessa insatser inte kan anses tillräckliga. Utbildningsinsatser behöver utökas då anpassning gentemot rådande riktlinjer och lagkrav till stor del är beroende av medarbetares förståelse för dessa. Dels genom prioriteringar och

beslut av medarbetare i ledande befattningar, och dels genom den dagliga informationshanteringen av samtliga medarbetare i verksamheten.

Revisionsfrågor	Svar
Bedriver Region Skåne ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för informationstillgångarna utifrån dagens krav?	Ja, vi anser att Region Skåne inom regionstyrelsen och kollektivtrafiknämnden bedriver ett ändamålsenligt arbete avseende styrning och ledning av informationssäkerhetsarbetet inom regionen. Delvis. Organisationsstrukturen och ansvarsfördelningen är tydlig. Däremot anser vi att antalet resurser inom regionstyrelsen med regionövergripande ansvar för informationssäkerhetsarbetet är relativt få givet organisationens storlek, den information som behandlas, och komplexiteten av de lagkrav som berör Region Skåne. Nej, såtillvida att vi anser att lämpliga rutiner och modeller inte har implementerats för att följa upp att beslutade krav och riktlinjer efterlevs, dels internt inom Region Skåne men även externt gentemot tredjeparter.
Säkerställs medborgarens integritet (GDPR) och är patientinformation i till exempel journalsystem skyddade mot obehöriga?	Ja, vi anser att Region Skåne inom regionstyrelsen och kollektivtrafiknämnden bedriver ett ändamålsenligt arbete för anpassning av verksamheten gentemot dataskyddsförordningen. Fortsatta insatser, primärt för utbildning av medarbetare, behöver dock genomföras för att förbättra efterlevnad av krav i verksamhetens processer. Nej, då journalsystem med nuvarande behörighetsstruktur inte kan anses säkerställa att patientinformation är skyddad mot obehörig åtkomst. Kompenserande kontroller i form av loggуppföljning genomförs men då de endast omfattar en liten del av de aktiviteter som genomförs hanterar dessa inte hela risken.
Har Region Skåne ett tillräcklig skydd för sina databaser och system inklusive molntjänster mot utomstående intressen som antingen vill komma åt information eller skada verksamheten och hur påverkas detta skydd av att allt fler arbetar hemifrån och på distans?	Ja, vi bedömer att Region Skåne har ett ändamålsenligt skydd för databaser och system som hanteras av de två driftsorganisationerna inom ramen för denna granskning. Dels inom Regionstyrelsens förvaltning Digitalisering IT/MT (där driften är outsourcad till tredjepart) och dels inom Kollektivtrafiknämndens förvaltning Skånetrafiken. Ja, vi anser att Region Skåne har tillräckligt skydd för att möjliggöra arbete på distans och att detta skydd inte påverkas av att andelen medarbetare som arbetar hemifrån har ökat. Delvis, avseende skydd för system som köps som molntjänster är vår bedömning dock att ansvaret för att säkerställa att lämpliga IT- och informationssäkerhetskrav förs in i avtal med leverantören behöver tydliggöras. Detta gäller även ansvaret för att löpande granska att leverantörer efterlever avtalade krav.
Hanteras avvikelser i form av driftavbrott och säkerhetsintrång på system och data och finns ändamålsenlig beredskap med resurser för åtgärder och rapportering av allvarliga incidenter enligt NIS-direktivet?	Ja, vi bedömer att Region Skåne inom regionstyrelsen och kollektivtrafiknämnden har ändamålsenlig beredskap och resurser för att hantera avvikelser och avbrott. Granskningen har även visat att rutiner för att hantera incidenter har anpassats i enlighet med NIS-direktivet.

Är utbildningen av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter ändamålsenlig?	Ja, såtillvida att relevant utbildning för samtliga medarbetare rörande IT- och informationssäkerhet samt dataskydd har tagits fram i form av en e-utbildning. Denna har genomgåtts av en stor del av medarbetare inom regionstyrelsen och kollektivtrafiknämnden. Även riktade utbildningsinsatser bedrivs av de regionala funktionerna och av informationssäkerhets- och dataskyddssamordnare. Nej, såtillvida att det inte säkerställts och följts upp att samtliga medarbetare inom regionstyrelsen och kollektivtrafiknämnden har genomgått den framtagna e-utbildningen. Det är även vår bedömning att riktade utbildningsinsatser, framför allt för medarbetare i ledande befattningar behöver utökas för ett förbättrat informationssäkerhets- och dataskyddsarbete i hela regionen.

Utifrån granskningsresultatet rekommenderar vi regionstyrelsen och kollektivtrafiknämnden att:

- Genomföra en kartläggning av upprättade instruktioner inom området för informationssäkerhet i nämndens verksamheter och utvärdera om lämpliga instruktioner i enlighet med beslutade riktlinjer för informationssäkerhet har upprättats.
- Säkerställa att rutiner och ansvar för uppföljning av avtal med molntjänstleverantörer, personuppgiftsbiträden och andra tredjeparter med ansvar för IT-säkerhet, informationssäkerhet och dataskydd är tydligt definierade.
- Införa rutiner för regelbunden och systematisk uppföljning av informationssäkerhetsarbetet inom regionen för att utvärdera om beslutade riktlinjer efterlevs. I samband med detta utvärdera behov av resurser, systemstöd, metoder, eller instruktioner för att möjliggöra en effektiv uppföljning.
- Följa upp utbildningsinsatser inom nämnden för att dels kontrollera om samtliga medarbetare genomgår den grundläggande e-utbildningen i säker informationshantering och dels få insikt i hur många medarbetare som genomgått kompetenshöjande men ej obligatoriska utbildningar.

Regionstyrelsen rekommenderas att:

- Årligen genomföra uppföljning av beslutade kortsiktiga mål för informationssäkerhetsarbetet i enlighet med riktlinjerna. I denna uppföljning tydligt utvärdera status per målsättning, om det anses vara uppfyllt, och om inte vilka åtgärder som behöver införas.
- Utvärdera behov och möjligheter för att tillsätta resurser med regionövergripande ansvar för ledning, kravställning, och uppföljning rörande IT-säkerhet.
- Utvärdera behov av- och möjligheter för att upprätta en dedikerad budget för IT-säkerhet, informationssäkerhet, och dataskydd med budgetansvar hos personer med regionövergripande ansvar för dessa områden.
- Tillse att regionövergripande process utarbetas för att tydliggöra dels hur krav på biträden som hanterar personuppgifter för Region Skånes räkning ska definieras och dels hur instruktioner för biträdenas behandling av personuppgifter ska utformas vid tecknande av avtal.
- Genomföra en översyn av nuvarande hantering av regionens registerförteckning av personuppgiftsbehandlingar i syfte att identifiera hur systemstöd kan utvecklas för att förbättra kvaliteten i registerförteckningen, samt underlätta uppföljning och kontroll av följsamheten gentemot GDPR.

- Följa upp projektet för införande av Skånes Digitala Vårdsystem avseende hur patientens integritet i det nya systemet kommer att säkerställas i enlighet med gällande lagstiftning genom exempelvis förbättrade behörighetsstrukturer eller automatiserad logguppföljning.

Malmö den 2 november 2020

Aleksandar Jovanovic Oscar Rydén
EY

Bilaga 1: **Källförteckning**

Intervjuade funktioner:

- Informationssäkerhetschef - Koncernstab kansli, KSM
- Dataskyddsombud - Koncernstab kansli
- Handläggare (regionalt dataskydd) - Koncernstab kansli, Informationsstyrning
- Handläggare (regionalt dataskydd) - Koncernstab kansli, Informationsstyrning
- Informationssäkerhetssamordnare och dataskyddssamordnare - Digitalisering IT/MT
- IT-säkerhetsansvarig - Stab säkerhet, verksamhetsutveckling och -stöd, Digitalisering IT/MT
- Enhetschef - Stab säkerhet, verksamhetsutveckling och -stöd, Digitalisering IT/MT
- Kvalitetssäkrare - Stab säkerhet, verksamhetsutveckling och -stöd, Digitalisering IT/MT
- Processledare IT (Incidenthantering) - Stab säkerhet, verksamhetsutveckling och -stöd, Digitalisering IT/MT
- Change Manager - Stab säkerhet, verksamhetsutveckling och -stöd, Digitalisering IT/MT
- Systemansvarig - Melior
- Verksamhetschef – Verksamhetsområde IT, Digitalisering IT/MT
- Enhetschef – Infrastruktur, Verksamhetsområde IT, Digitalisering IT/MT
- Enhetschef – Stödsystem, Verksamhetsområde IT, Digitalisering IT/MT
- IT-arkitekt – Avdelning för Infrastruktur, Verksamhetsområde IT, Digitalisering IT/MT
- Risk och Säkerhetsansvarig (Informationssäkerhetssamordnare) – Skånetrafiken, Enheten Kvalitet
- Dataskyddssamordnare – Skånetrafiken, Enheten Kvalitet
- Enhetschef – Skånetrafiken, Enheten för Information Kommunikation och Teknik
- IT-säkerhetskoordinator – Skånetrafiken, Enheten för Information Kommunikation och Teknik
- Objektledare IT-drift – Skånetrafiken, Enheten för Information Kommunikation och Teknik

Dokument:

- Säkerhetspolicy v. 1,0
- Säkerhetsstrategi
- rs__161_09_riktlinjer_for_informationssakerhet
- Instruktion-for-tillampning-av-riktlinje-for-informationssakerhet
- beslut-om-dataskyddsorganisation-i-region-skane
- Rapport Informationssäkerhetsarbetet 2018
- Rapport till Regionstyrelsen om informationssäkerhetsarbetet 190131.docx
- instruktion-om-forvaltningarnas-organisation-for-dataskydd-2018-11-19
- personuppgiftsbehandling-i-region-skane---sammanstallning-av-regler-och-krav
- Beslut om informationsägare
- Mål med informationssäkerhetsarbetet lång sikt
- Mål med informationssäkerhetsarbetet kort sikt
- Instruktion Informationssäkerhetsincidenter
- Instruktion incidenthantering NIS-direktivet (Skånetrafiken)
- Incidentrapportering enligt NIS-direktivet
- Instruktion incidenthantering (Digitalisering IT/MT)
- Instruktion för hantering av stor incident IT och telefoni (Digitalisering IT/MT)
- Instruktion problemhantering (Digitalisering IT/MT)
- Utkast till Instruktion för förändingsprocess (Digitalisering IT/MT)

- INSTRUKTION Dataintrång - åtgärder vid misstanke om olovlig åtkomst.pdf
- Instruktioner om loggkontroll för granskning av åtkomst till patientuppgifter.docx
- UPPHANDLINGSPOLICY för Region Skåne
- Tillämpningsanvisningar till Upphandlingspolicy
- Riskhanteringsverktyg för informationssystem
- Instruktion för informationsklassificering
- Klassificera informationstillgångar HANDLEDNING
- Instruktion för riskhantering avseende informationstillgångar
- Riskhantering informationstillgångar HANDLEDNING
- Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter
- Hantera incidenter i nätverk
- Instruktion för personuppgiftsbehandling i Region Skåne
- Region Skånes hjälptext för personuppgiftsbiträdesavtal
- Mall för personuppgiftsbiträdesavtal
- Mall för instruktion för personuppgiftsbiträdesavtal
- Årshjul för dataskyddssamordare
- Dataskyddssamordnares internrevision 2020
- Instruktion informationssäkerhetsincident (Skånetrafiken)
- Mall utreda informationssäkerhetsincident (Skånetrafiken)
- Instruktion för informationssäkerhetsincident (Skånetrafiken)