Granskning av informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet

Rapport

Region Skåne

KPMG AB

2024-12-17

Antal sidor 30

Region Skåne
Granskning av informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet

2024-12-17

Innehållsförteckning

1 Sammanfattning

KPMG har av Region Skånes revisorer fått i uppdrag att granska informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet (NORV). Syftet med granskningen har varit att bedöma om nämnden arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system.

Vår samlade bedömning utifrån granskningens syfte är att nämnden för operativ regiongemensam verksamhet delvis arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.

Revisionsfråga	Bedömning
Har nämnden beslutat om strategiska styrdokument som är relevanta för drift av verksamheten inom it?	Nej
Finns en ändamålsenlig organisation med roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan Region Skånes olika verksamheter och Digitalisering IT och MT?	Nej
Finns erforderlig kompetens för ett ändamålsenligt arbete med informations- och it-säkerhet och får medarbetare kontinuerlig utbildning inom området?	I allt väsentligt
Säkerställer NORV ett tillräckligt skydd för Region Skånes databaser och system inklusive molntjänster och att tekniska säkerhetsåtgärder vidtas utifrån de identifierade skyddsvärden från informationsklassning och riskbedömning?	I allt väsentligt
Genomförs systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder?	Ja
Har NORV säkerställt en ändamålsenlig incidenthantering?	Delvis
Har NORV säkerställt en ändamålsenlig kontinuitetshantering?	I allt väsentligt
Finns etablerade uppföljnings- och rapporteringsrutiner i enlighet med gällande krav i ledningssystem för informationssäkerhet?	Delvis
Får nämnden för operativ regiongemensam verksamhet tillräckligt med information för att kunna fullgöra sitt uppdrag och ta beslut om åtgärder vid behov?	Nej

Utifrån resultatet av vår granskning rekommenderar vi nämnden för operativ regiongemensam verksamhet att:

- Bedöma om nuvarande styrning av förvaltningarnas arbete inom informationssäkerhet och tekniska säkerhetsåtgärder är tillräckliga utifrån nämndens ansvar, samt vid behov besluta om eller bereda förslag till kompletterande instruktioner och anvisningar.
- Säkerställa att informationssäkerhetssamordnare inom Digitalisering IT och MT har förutsättningar att utföra uppdraget i enlighet med det mandat som tillskrivs rollen.
- Tillse att förvaltningsledningen från informationssäkerhetssamordnaren erhåller en årlig samlad rapportering av informationssäkerhetsarbetet inom den egna förvaltningen i syfte att säkerställa en ändamålsenlig rapportering till nämnden.
- Säkerställa att den årliga uppföljningen inkluderar regelefterlevnad av lagkrav och styrande dokument inom informationssäkerhet och att brister rapporteras till nämnden samt till informationssäkerhetschef på koncernkontoret.
- Tillse att nuvarande uppföljning och rapportering till nämnden kompletteras med väsentliga händelser inom informationssäkerhet, exempelvis inträffade incidenter eller andra faktorer som riskerar att påverka nämndens ansvar inom drift av it.
- Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom nämndens ansvarsområden.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Bereda förslag till nytt reglemente för regionstyrelsen och NORV i syfte att tydligare reglera ansvaret för Region Skånes informationssäkerhetsarbete. Vid revideringen bör beaktas att det inom informationssäkerhetsområdet finns behov av att fatta beslut som påverkar andra nämnder i Region Skåne.
- Revidera riktlinjer och tillhörande instruktioner så att dessa är aktualiserade i enlighet med Region Skånes nuvarande organisation och ansvar samt kompletteras med reglering av ansvar för informationssäkerhetsarbetets olika delområden.
- Följa upp att de prioriterade åtgärder för utveckling av informationssäkerhetsarbetet som föreslogs i informationssäkerhetsberättelsen har en framdrift och stärker Region Skånes arbete.
- Överväga om vissa aktiviteter och uppgifter inom informationssäkerhetsarbetet kan integreras i den nya styr- och ansvarsmodellen.
- Stärka uppföljning och kontroll av efterlevnad av fastställda styrdokument inom informationssäkerhet.

— Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom styrelsens ansvarsområden.

2 Bakgrund

KPMG har av Region Skånes revisorer fått i uppdrag att granska informations- och it-säkerhet inom nämnden för operativ regiongemensam verksamhet (NORV). Uppdragsledare från KPMG har varit Jenny Thörn. Simon Homander och Ida Larsson, KPMG, har ingått i granskningen som projektmedarbetare. Veronica Hedlund Lundgren, certifierad kommunal yrkesrevisor, har varit ansvarig för kvalitetssäkring för KPMG:s räkning. Kontaktperson från revisorskollegiet har varit förtroendevald revisor Eskil Engström.

Nämnden för operativ regiongemensam verksamhet är driftsledningsnämnd för förvaltningarna Digitalisering IT och MT och Medicinsk service. Digitalisering IT och MT har fått uppdraget att införa en modern och sammanhållen digital vårdmiljö parallellt med drift och effektiv konsolidering av dagens befintliga it-miljö. I detta uppdrag ingår förvaltning och support av befintliga och kommande system för alla Region Skånes verksamheter samt att ansvara för att, genom hela produktlivscykeln, upprätthålla driftsäkerheten av Region Skånes medicintekniska produkter och bistå Region Skånes olika verksamheter och samarbetspartners med teknisk kompetens och support.

I Region Skånes *Instruktion för informationsklassning* regleras att informationstillgångar i form av programvara, system, datorer och utrustning som krävs för hantering av information ska klassificeras och riskbedömas. Det pågår ett omfattande arbete enligt projektdirektiv U537 där samtliga Region Skånes ca 600–700 system ska riskbedömas och därefter ska beslut fattas av informationsägare avseende fortsatt drift.

Revisorerna avser att granska om nämnden för operativ regiongemensam verksamhets arbete vad gäller informations- och it-säkerhet av Region Skånes it-system är ändamålsenligt.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om nämnden för operativ regiongemensam verksamhet arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system.

Granskningen har omfattat följande revisionsfrågor:

- Har nämnden (NORV) beslutat om strategiska styrdokument som är relevanta för drift av verksamheten inom it?
- Finns en ändamålsenlig organisation med roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan Region Skånes olika verksamheter och Digitalisering IT och MT?
- Säkerställer NORV ett tillräcklig skydd för Region Skånes databaser och system inklusive molntjänster och att tekniska säkerhetsåtgärder vidtas utifrån de identifierade skyddsvärden från informationsklassning och riskbedömning?
- Genomförs systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder och har NORV säkerställt en ändamålsenlig incident-och kontinuitetshantering?

- Finns etablerade uppföljnings-och rapporteringsrutiner i enlighet med gällande krav i ledningssystem för informationssäkerhet?
- Finns erforderlig kompetens för ett ändamålsenligt arbete med informations-och it-säkerhet och får medarbetare kontinuerlig utbildning inom området?
- Får nämnden för operativ regiongemensam verksamhet tillräckligt med information för att kunna fullgöra sitt uppdrag och ta beslut om åtgärder vid behov?

Denna granskning är avgränsad till nämnden för operativ regiongemensam verksamhet (NORV) för it-säkerhet och informationssäkerhet genom det ansvar som nämnden får som driftsansvarig av Digitalisering IT och MT. Enligt projektplan för granskningen framgår även att regionstyrelsen utifrån det övergripande ansvaret för informationssäkerhet kan beröras samt nämnder som har driftansvar för de förvaltningar som blir utvalda för stickprovskontroller.

I revisionsfråga sju ingår också att svara på hur nämnden arbetar med att förbereda sig för de nya EU-direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet).

2.2 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

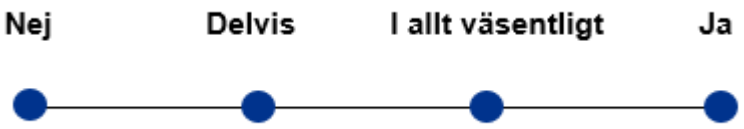
- Kommunallagen (2017:725) 6 kap. 6 §
- Dataskyddsförordningen (The General Data Protection Regulation)
- MSB FS 2021:9 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (NIS-direktivet)
- HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Säkerhetsskyddslag (2018:585)
- Offentlighets- och sekretesslag (2009:400)
- Patientdatalag (2008:355)
- Säkerhetspolicy (RF 2017-06-20)
- Säkerhetsstrategi (regionstyrelsen 2017-12-07)
- Riktlinjer för informationssäkerhet (regionstyrelsen 2017-12-07)
- Instruktioner och anvisningar för informationssäkerhet

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av reglemente för regionstyrelsen och NORV, ledningssystem för informationssäkerhet (informationssäkerhetspolicy, riktlinjer och instruktioner samt övrigt stödmaterial), styr- och samverkansmodell för IT med tillhörande ansvars- och metodbeskrivningar, statusrapportering för projekt U537, resultat av informationsklassningar och riskanalyser för respektive system utifrån avgränsning, åtgärdsplan för tekniska skyddsåtgärder tillhörande klassningar
- Intervjuer har genomförts med stabschef Digitalisering IT och MT, verksamhetschef infrastruktur och säkerhetschef Digitalisering IT och MT, enhetschef it-säkerhetsenheten Digitalisering IT och MT, informationssäkerhets- och dataskyddssamordnare Digitalisering IT och MT förvaltningsstabschef medicinsk service, områdeschef laboratorieteknik medicinsk service, strateger i förvaltningsstaben tillika informationssäkerhetssamordnare medicinsk service, informationssäkerhetschef Region Skåne samt systemansvariga eller andra nyckelfunktioner kopplade till granskade system.
- Systemgranskning enligt avgränsning omfattande totalt 15 system som ingår i ett regionövergripande arbete utifrån direktiv från regiondirektören, Projektdirektiv U537.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.



Rapporten har skickats på faktakontroll till samtliga intervjupersoner.

3 Resultat av granskningen

3.1 Systematiskt informationssäkerhetsarbete

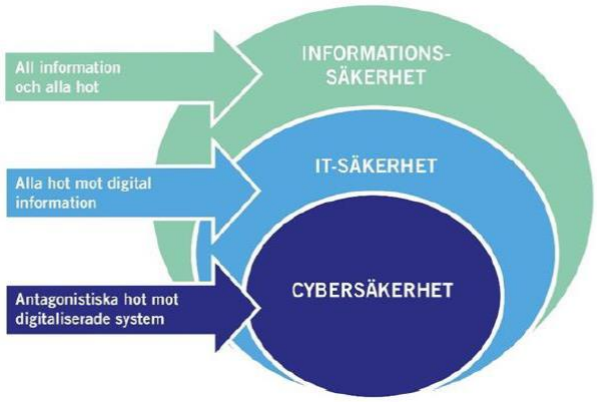
I ett systematiskt informationssäkerhetsarbete ingår fyra områden av säkerhetsåtgärder. Dessa är:

1. Organisatorisk säkerhet (ibland benämnd administrativ säkerhet)
2. Teknisk säkerhet (it-säkerhet och cybersäkerhet)
3. Personalrelaterad säkerhet
4. Fysisk säkerhet

I granskningen har vi fått till oss att det råder en begreppsförvirring inom informationssäkerhetsområdet i Region Skåne. Detta uppges försvåra genomförandet av de processer som krävs för att arbetet ska vara systematiskt och utveckla Region Skånes mognadsgrad inom området.

Denna granskning avgränsas till informationssäkerhet på en övergripande nivå samt arbetet med de tekniska säkerhetsåtgärderna (it-säkerhet och cybersäkerhet). Bilden nedan illustrerar hur dessa förhåller sig till varandra.

Figur 2.1 Av figuren framgår hur begreppen cybersäkerhet, it-säkerhet och informationssäkerhet förhåller sig till varandra



[1]

Enligt de styrande dokumenten i Region Skåne ska informationssäkerhetsarbetet utgå från den etablerade standarden SS-ISO/IEC 27001 (ramverk för hur ett ledningssystem för informationssäkerhet ska utformas) samt SS-ISO/IEC 27002 (de säkerhetsåtgärder som arbetet ska inkludera). Dessa standarder innehåller ett stort antal krav för att informationssäkerhetsarbetet ska vara systematiskt och motsvarar även den nivå som kravställs i nu gällande lagkrav och föreskrifter inom området. Region Skåne omfattas

[1] Figuren är hämtad från Cybersäkerhetsutredningen: Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem SOU (2021:63).

av dessa lagkrav[2] inom sektorn hälso- och sjukvård[3]. Nu gällande riktlinjer för informationssäkerhet följer strukturen för ovan nämnda standarder och tillhörande instruktion konkretiserar kraven. Dessa beskrivs i delar i kommande avsnitt.

3.1.1 Styrning och politisk ansvarsfördelning

3.1.1.1 Reglementen

Av regionstyrelsens reglemente[4] framgår att regionstyrelsens arbetsutskotts beredningsansvar omfattar utveckling av digitaliseringsfrågorna.

Av reglementet för nämnden för operativ regiongemensam verksamhet (NORV) framgår att nämnden är driftsledningsnämnd för förvaltningarna Digitalisering IT och MT samt Medicinsk service. NORV ska inom ramen för sitt uppdrag fastställa verksamhetsplan och internbudget med tillhörande uppföljning enligt ordinarie rutiner samt fastställa internkontrollplan och följa upp denna samt rapportera till regionstyrelsen om resultatet.

I reglementen går det inte att utläsa hur ansvaret för informationssäkerhetsområdet är fördelat mellan regionstyrelsen och NORV.

3.1.1.2 Styrande dokument

De styrande dokument som reglerar säkerhetsarbetet på regionövergripande nivå, säkerhetspolicy och säkerhetsstrategi, inkluderar både informationssäkerhet och it-säkerhet som begrepp. Det ansvar som regleras är regionstyrelsens ansvar som är att besluta och följa upp strategin. I övrigt beskrivs att ansvaret följer linjeansvaret. Av strategin framgår även att regionövergripande säkerhetsfunktioner är samordnande, utvecklande och stödjande.

Underliggande och kompletterande styrdokument inom informationssäkerhetsområdet är inte uppdaterade efter att NORV bildades som nämnd eller sedan förvaltning Digitalisering IT och MT placerades under NORV. Det saknas således beskrivningar om fördelning av uppdrag och ansvar mellan regionstyrelsen och NORV och dess tillhörande förvaltningar.

Av 2023 års rapport till regionstyrelsen enligt ledningssystemet för informationssäkerhet[5] (härefter benämnd årsrapporten) framgår att uppdatering av styrdokument är en prioriterad åtgärd under 2024. I samband med den här granskningens genomförande så är uppdatering av styrdokument inte slutfört.

Vi kan därtill konstatera att NORV inte har beslutat om några kompletterande instruktioner eller anvisningar som gäller för de förvaltningar som lyder under nämnden. Den har inte heller berett några förslag till kompletterande styrdokument för beslut i regionstyrelsen i de fall besluten skulle omfatta övriga nämnders verksamheter

[2] Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet)
[3] Nytt lagförslag som ska gälla från 1 januari 2025 genom Cybersäkerhetslagen (svensk tillämpning av EU-direktivet NIS2) föreslår dock att hela den offentliga förvaltningen som sektor ska omfattas av lagkraven och inte som tidigare endast vissa delar av verksamheten.
[4] Reglemente för styrelse och nämnder, beslutad av regionfullmäktige 2022-12-13 §11
[5] Framtagen av informationssäkerhetschef, avser period 2023-04-19 – 2024-04-19

och förvaltningar i Region Skåne. Underlag i form av rutiner eller instruktioner för Digitalisering IT och MT på en operativ och taktisk nivå har dock vid behov fattats i förvaltningen för att styra arbetet inom den egna förvaltningen.

I intervjuer lyfts återkommande uppfattningen att den regionövergripande ledningen och regionstyrelsen i nuläget inte är tillräckligt involverade i informations-säkerhetsfrågor, vilket anses försämra förutsättningarna för informerade och förankrade beslut. Iakttagelser som bekräftar detta uppfattar vi är bland annat bristen på uppdaterade styrdokument, bristen på en anpassad organisation som möter ledningssystemets och verksamheternas behov inom informationssäkerhetsarbetet samt att uppföljning av efterlevnad av styrande dokument inte gjorts i enlighet med fastställda rutiner.

3.1.2 Organisation, ansvar och roller

Enligt intervjuer finns tre styrdokument som har högst status inom informationssäkerhetsområdet i Region Skåne, *Riktlinjer för informationssäkerhet* [6], *Instruktion för tillämpning av riktlinjer för informationssäkerhet* [7] och *beslut om informationsägare* [8].

I de styrande dokumenten beskrivs organisationen och ett antal roller. *Regiondirektörens* roll är att besluta om regionövergripande instruktioner och anvisningar samt besluta om informationsägare för regiongemensamma informationstillgångar.

Vi har tagit del av beslutet om *informationsägare* vilket tilldelar detta ansvar till ett antal direktörer samt en av förvaltningscheferna. Beslutet inkluderar även förteckning av de uppgifter och ansvar som tillhör rollen. Av beslutet framgår även att *Digitaliserings- och it-direktör*, tillika förvaltningschef Digitalisering IT och MT, är informationsägare för informationstillgångar avseende it-system och utgör *systemägare* för regiongemensamma system.

Förvaltningschef har, inom sin förvaltning, ansvaret för att utforma och kommunicera innehållet i styrande dokument för informationssäkerhet, verkställa och följa upp beslut samt för att all informationshantering sker i enlighet med fastställda styrande dokument. Förvaltningschef ska inom sin förvaltning utse *informationssäkerhets-samordnare* som ska ha ett tydligt mandat och uppdrag att leda, utveckla, samordna och följa upp informationssäkerhetsarbetet i förvaltningen utifrån regionövergripande styrande dokument.

Informationssäkerhetschefen ansvarar för att leda, utveckla, samordna och övergripande följa upp informationssäkerhetsarbetet inom Region Skåne. I ansvaret ingår att förvalta riktlinjen för informationssäkerhet, regionövergripande instruktioner och anvisningar samt den övergripande handlingsplanen och målen för informationssäkerhet.

[6] Beslutad av regionstyrelsen 2017-12-07
[7] Beslutad av regiondirektör 2020-05-22
[8] Beslutad av regiondirektör 2018-05-22

3.1.2.1 Organisatorisk säkerhet

Enligt årsrapporten så arbetar enheten för informationssäkerhet, dataskydd och informationsoffentlighet som finns på koncernkontoret med det organisatoriska delområdet och Digitalisering IT och MT arbetar med det tekniska delområdet.

Informationssäkerhetschef leder arbetet enligt tidigare beskrivning i styrdokumenten. Arbetet genomförs med stöd av informationssäkerhetssamordnare som finns i respektive förvaltning.

I årsrapporten konstateras att nuvarande organisation och resurser inte är tillräckliga. Flera förvaltningar har enligt rapporten utryckt behov av mer stöd från regionövergripande enheter för att utföra ett tillräckligt arbete inom informationssäkerhet och dataskydd.

Enligt årsrapporten är efterlevnaden av ledningssystemet och dess styrdokument relativt låg inom verksamheterna. I årsrapporten och vissa intervjuer lyfts bland annat följande aspekter.

- Risk för att de funktioner som ska utgöra nyckelroller i det operativa arbetet inte är tillräckligt dimensionerade efter de krav och behov som ställs på arbetet.
- Rollen informationsägare är inte tillräckligt etablerad så att det arbete som åligger rollen utförs i enlighet med beslutade styrdokument.

Digitalisering IT och MT har beslutat om organisation för informationssäkerhet och dataskydd[9] som beskriver förvaltningsintern organisation, roller och ansvar. Medicinsk service har ett pågående arbete att upprätta motsvarande underlag för sin förvaltning. Båda förvaltningarna har utsedda informationssäkerhetssamordnare som lyft behov av ett tydliggörande av informationssäkerhetsorganisationen som del i förvaltningarnas utvecklingsarbete inom informationssäkerhet.

Utöver ovan nämnda utvecklingsbehov lyfts i intervjuer en utmaning kring den organisatoriska tillhörigheten eller placeringen för centrala roller som uppfattas vara alltför långt från ledningen. Det kan påverka mandatet att leda och utveckla arbetet (i enlighet med styrande dokument.

Iakttagelsen görs på samtliga nivåer. Dels inom koncernkontoret i förhållande till regiondirektör vilket även påverkar regionstyrelsens involvering i de strategiska informationssäkerhetsfrågorna. Dels inom förvaltningarna vad gäller informationssäkerhetssamordnarrollen i förhållande till förvaltningschefer/stabschefer. Vi konstaterar att Medicinsk service utgör ett undantag där informationssäkerhetssamordnaren (titeln strateg för informationssäkerhet och dataskydd) ingår i förvaltningens stab.

3.1.2.2 Teknisk säkerhet (it-säkerhet och cybersäkerhet)

Som nämnts tidigare i rapporten saknas i nuläget i de styrande dokumenten en dokumenterad ansvarsfördelning av det strategiska ansvaret för det tekniska säkerhetsperspektivet motsvarande det som finns för det organisatoriska

[9] Beslutad av förvaltningschef 2024-03-19

säkerhetsperspektivet. Exempelvis saknas en uttalad ledande roll med ansvar för regionövergripande it-säkerhet, motsvarande den roll som informationssäkerhetschef har ur ett strategiskt perspektiv. De styrande dokumenten hänvisar till att ansvaret regleras genom Region Skånes *verksamhetsstyrda styr- och förvaltningsmodell för IT och MT-system*. Roller och ansvar i modellen beskrivs i kommande avsnitt.

I Verksamhetsplan 2024 som NORV beslutat om för Digitalisering IT och MT framgår följande uppdrag för förvaltningen, ”*att införa en modern och sammanhållen digital vårdmiljö parallellt med drift och effektiv konsolidering av dagens befintliga IT-miljö. I det uppdraget ingår förvaltning och support av befintliga och kommande system för alla regionens verksamheter samt att ansvara för att, genom hela produktlivscykeln, upprätthålla driftsäkerheten av Region Skånes medicintekniska produkter*”.

För Digitalisering IT och MT innebär detta att ett operativt arbete bedrivs med tekniska säkerhetsåtgärder för system som har regionövergripande räckvidd. I intervjuer beskrivs att arbetet tar sin utgångspunkt i de regionövergripande styrdokumenten inom informationssäkerhet. Intervjuer med företrädare för förvaltningen uppges att de inte sett några ytterligare behov av styrning från nämnden för att verkställa sitt uppdrag.

Trots reglementets formulering att NORV är en driftsledningsnämnd uppfattar vi genom viss dokumentation vi erhållit samt i våra intervjuer att Digitalisering IT och MT, i nuläget innehar det strategiska ansvaret och leder it-säkerhetsutvecklingen för gemensamma informationstillgångar i hela Region Skåne (utom Skånetrafiken). Regiondirektörens beslut om informationsägare har som vi nämnt tidigare därtill tilldelat Digitaliserings- och IT-direktör systemansvaret för gemensamma it-system.

Enligt intervjuade uppfattas en risk att Digitalisering IT och MT:s tekniska säkerhetsarbete inte sker tillräckligt integrerat i det systematiska informations-säkerhetsarbetet i Region Skåne i stort, varken ur ett organisatoriskt eller processorienterat perspektiv. Bland annat lyfts i faktakontrollen att beslut fattats inom förvaltningen som strider mot beslutade styrdokuments reglering. Exemplet avser åtkomsthantering där tekniska krav på lösenordshantering inte längre följer instruktion för tillämpning av riktlinjer för informationssäkerhet. Ett annat exempel som lyfts är att Region Skåne beslutat om följsamhet till standarden ISO27001 och 27002 men av intervjuade framgår att Digitalisering IT och MT arbetar utifrån en annan vedertagen modell, kallad NIST.

Även om viss dialog och samverkan har etablerats noterar vi från både intervjuer och dokumentstudier att kvarstående brister i den organisatoriska säkerheten och nuvarande resurser i arbetet påverkar Region Skånes förmåga att bedriva ett systematiskt och integrerat informationssäkerhetsarbete. Det påverkar även förutsättningarna i arbetet med teknisk säkerhet.

3.1.2.3 Personrelaterad och fysisk säkerhet

Utöver de organisatoriska och tekniska delområdena framgår även av årsrapporten ett behov av att förtydliga ansvaret för delområdena fysisk och personrelaterad säkerhet, Dessa delområden beskrivs utgöra en organisatorisk, strukturell och slutligen en säkerhetsrisk. Delområdena personrelaterad och fysisk säkerhet har inte ingått i granskningen.

3.1.3 Bedömning

Vi bedömer att NORV inte beslutat om strategiska styrdokument som är relevanta för drift av verksamheten inom it.

Vi kan konstatera att det saknas en tydlig reglering i reglementen avseende ansvarsfördelning mellan regionstyrelsen och NORV. Vi bedömer att detta utgör en risk för att det saknas en strategisk inriktning för och styrning av arbetet med de tekniska skyddsåtgärderna i Region Skåne.

Vår tolkning av reglementen och styrande dokument i Region Skåne är att den strategiska styrningen av informationssäkerhet inklusive de tekniska säkerhetsåtgärderna kravställs genom det regionövergripande ledningssystemet för informationssäkerhet. De regionövergripande styrdokumenten som i huvudsak utgör ledningssystemet beslutas av regionfullmäktige och regionstyrelsen.

Då den samlade kompetensen inom drift av it och tillhörande säkerhet finns inom NORVs verksamheter så är det väsentligt att nämnden vid behov bereder ärenden och underlag för beslut i regionstyrelsen, om behov av detta identifieras.

Vi bedömer att det inte finns en ändamålsenlig organisation med roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan Region Skånes olika verksamheter och Digitalisering IT och MT.

Enligt bedömningen ovan saknas tydlig rollbeskrivning både i reglementen och de regionövergripande styrdokumenten utifrån nuvarande organisation och hur arbetet genomförs i praktiken. Därutöver finns utmaningar i att anpassa organisationen efter kraven i ledningssystemet för informationssäkerhet och aktuell lagstiftning. Vi bedömer att dessa utmaningar medför bristande förutsättningar för att uppnå ett systematiskt informationssäkerhetsarbete.

Region Skånes informationssäkerhetsarbete når i nuläget inte upp till den systematik som styrande dokument och lagkrav ställer krav på. Vi bedömer att arbetet inte genomförs i en sammanhållen process där samtliga säkerhetsområden är integrerade och baseras på en tydlig roll- och ansvarsfördelning. Det är inte heller klarlagt hur samordning av delområdena ska ske för att Region Skåne ska ha en helhetsbild av arbetet.

Vår bedömning är att informationssäkerhetsrollerna saknar förankring på ledningsnivå, på både regionövergripande och förvaltningsspecifik nivå. Sådan förankring bedömer vi är en förutsättning för att arbetet ska kunna bedrivas i enlighet med ledningssystemets ansvarsfördelning. Det är väsentligt att informationssäkerhetsroller får den tyngd och närhet till ledningen som krävs för att ge mandat att leda och utveckla arbetet. Vi ser att det är väsentligt för att förvaltningscheferna i sin tur ska kunna efterleva sitt tilldelade ansvar för *att utforma och kommunicera innehållet i styrande dokument för informationssäkerhet, verkställa och följa upp beslut samt ansvara för att all informationshantering sker i enlighet med fastställda styrande dokument.*

3.2 Kompetens och utbildning

Av årsrapporten framgår att utbildning är ett prioriterat område och att en översyn av utbildningar och behov av kompetenshöjning i syfte att höja mognaden samt förbättra och förstärka säkerhetskulturen i Region Skåne behöver genomföras. Från koncernkontoret finns en ambition att planera och implementera en ny regionövergripande utbildning i syfte att öka riskmedvetenheten inom samtliga fyra delområden som ingår i informationssäkerheten. Valet av plattform för utbildningen ska även inkludera möjlighet att kontinuerligt följa upp deltagarantalet. Uppföljning av deltagarantalet har varit utmanande för nuvarande utbildning då ansvaret för genomförande och uppföljning varit fördelat till respektive chef.

Enligt de uppgifter som lämnades vid tidigare granskning av informations- och it-säkerhet med fokus patientdata 2023 var genomförandegraden generellt låg. Utifrån lämnade intervjuuppgifter i den här granskningen har vi inte noterat att några särskilda insatser gjorts för att öka genomförandegraden. Under 2024 har en ny obligatorisk utbildning tagits fram som finns tillgänglig på intranätet. Digitalisering IT och MT har en genomförandegrad på 90 % för den utbildningen. Övriga förvaltningar uppges ha en varierande genomförandegrad.

Digitalisering IT och MT har tagit fram ett antal initiativ för att höja säkerhetsmedvetenheten och stärka kunskap inom området:

- Månadsvisa interna utbildningspass för medarbetarna inom Digitalisering IT och MT. Utbildningen har enligt intervju haft 200–300 deltagare per tillfälle.
- Kvartalsvisa kompetensutvecklingshalvdagar för medarbetarna inom IT-säkerhetsenheten, med både interna och externa föredragande.
- Digitalisering IT och MT har tagit fram ett APT-material (arbetsplatsträff) med fokus på IT- och cybersäkerhet, innefattande bland annat en film – ”Fem snabba tips om IT-säkerhet”
- Löpande omvärldsbevakning och dialog med externa leverantörer i syfte att ha aktuell kunskap och kännedom om hot, risker och säkerhetsåtgärder.

3.2.1 Bedömning

Vi bedömer att det i allt väsentligt finns erforderlig kompetens för ett ändamålsenligt arbete med informations- och it-säkerhet i förvaltningarna under NORV och att medarbetarna i förvaltningen får kontinuerlig utbildning inom området.

Vi bedömer dock att det ur ett regionövergripande perspektiv behöver säkerställas att det finns en erforderlig kompetens genom ett aktivt utbildningsarbete av medarbetare i övriga förvaltningar och verksamheter. Vi ser positivt på att det är en prioriterad åtgärd att etablera en ny utbildning som enklare ska kunna följas upp utifrån genomförandegrad. Vi bedömer att det är väsentligt att regionstyrelsen tillser att kompetensen stärks i övriga förvaltningar i Region Skåne för att kunna bedriva ett systematiskt informationssäkerhetsarbete på alla nivåer i Region Skåne.

3.3 Systematiskt arbete med tekniska säkerhetsåtgärder för system

3.3.1 Roller och ansvar enligt verksamhetsstyrd styr- och förvaltningsmodell

Styrande dokument för informationssäkerhet anger att arbetet med informationssystem ska genomföras i enlighet med Region Skånes fastställda förvaltningsmodell, Verksamhetsstyrd styr- och förvaltningsmodell för IT- och MT-system[10]. Modellen beskriver samarbetsformerna för styrning och förvaltning av it- och medicintekniska system där ansvarsfördelning och uppgifter för roller tydliggörs genom ett antal instruktioner och bilagor.

På den operativa nivån sker arbetet i enlighet med modellen med förvaltningsgrupper med utsedda representanter. Representanterna är dels verksamhetsansvariga (VA) från verksamheterna som nyttjar systemen, dels systemansvariga (SA) som tillhör förvaltningarna Digitalisering IT och MT alternativt Medicinsk service.

Enligt beslut om informationsägare har informationsägaren ansvar för informationstillgångar och beslutar om informationshantering inom ramen för befintlig lagstiftning och interna regelverk. Informationsägaren ansvarar för att klassificera information, genomföra riskbedömning och ställa krav på hantering av informationen.

Systemägaren har ett överordnat ansvar för administration, drift och säkerhet. Systemägaren ska utifrån informationsägarens krav utforma systemet så att informationen skyddas på adekvat sätt.

Utöver dessa roller finns även verksamhetsspecialister och systemspecialister inom ramen för styr- och förvaltningsmodellen. Verksamhetsspecialisterna stödjer den dagliga verksamheten i systemen och hanterar uppföljningen av de ingående tjänsterna. De genomför också utbildningar och samlar in behov av utbildning, ändringar eller nya tjänster. Systemspecialisterna stödjer systemansvariga och utför aktiviteter fastställda i aktivitetslistan. Beroende på systemets kategorisering kan detta även innefatta teknisk och funktionell support.

Vi har i intervjuer fått beskrivet att arbetet med samtliga 15 system i vårt urval i hög grad genomförs i enlighet med gällande styr- och förvaltningsmodell. För system som sträcker sig över flera olika verksamheter/förvaltningar finns vid behov flera parallella förvaltningsgrupper och en övergripande förvaltningsgrupp.

Vi har dock kunnat konstatera att informationssäkerhetsperspektivet saknas i styr- och förvaltningsmodellen. Exempelvis är informationssäkerhetssamordnarrollen i förvaltningarna inte representerade i arbetet, varken utifrån systemägaren eller informationsägarens förvaltning.

Ny Styr och ansvarsmodell

I verksamhetsberättelsen för 2023 som NORV beslutat om för Digitalisering IT och MT framgår att regiondirektören beslutat om den övergripande strukturen för en ny styr- och ansvarsmodell. Beslut om själva modellen förväntades fattas av regiondirektören

[10] Beslutad 2022-10-27 på tjänstemannanivå

under april 2024. Den nya modellen hade inte beslutats eller etablerats vid tid för intervjuerna.

Av beskrivningen av modellen som ges i verksamhetsberättelsen lyfts främst att den ska möjliggöra strategisk styrning av digitalisering och digital transformation. Vi uppfattar dock av intervjuade att modellen fortsatt ska omfatta de aktiviteter som i nuläget ingår i Verksamhetsstyrd styr- och förvaltningsmodell (vidmakthållande och förvaltning av system) men justeras från fokus på systemleverans till fokus på tjänsteleverans.

Enligt uppgift är inte informationssäkerhetschef involverad i utvecklingen av den nya modellen och vi har inte kunnat verifiera hur den nya modellen beaktar informationssäkerhet.

3.3.2 Systemgranskning

Som metod i granskningen har ingått att genomföra en systemgranskning för ett urval av system som är i drift eller ska tas i drift i närtid i Region Skåne. Syftet har varit att bedöma om säkerhetsåtgärder och uppföljning baseras på tillräckliga analyser och bedömningar av exempelvis skyddsbehov och risker för den information som hanteras i system.

Urval

Urval av system har gjorts i samråd med revisionskontoret utifrån en lista av system som omfattats i ett regionövergripande arbete utifrån direktiv från regiondirektören, *Projektdirektiv U537*. Enligt granskningens projektplan så efterfrågades utöver urvalet från projektdirektivet även att Skånes Digitala Vårdsystem (SDV) skulle ingå i systemgranskningen. SDV består av flera system som tillsammans utgör den nya digitala miljön som är tänkt att driftsättas i sin helhet med start under våren 2025. De nya implementeringarna innebär även att vissa befintliga system som är i drift i Region Skåne, enligt uppgift runt ett 30-tal äldre centrala informationssystem, kommer att fasas ut i en övergångsperiod

Krav för riskhantering av informationssystem

Region Skåne har en fastställd metod och mall för riskhantering av informationssystem. Enligt dokumentet består riskhanteringsprocessen av de tre aktiviteterna informations-klassificiering, riskbedömning och åtgärdsanalys. Beslut om driftgodkännande sker när åtgärder som tidigare beslutats av informationsägaren har genomförts och verifierats. Ett beslut om driftgodkännande är en verifiering av att riskerna, när beslutet fattas, är acceptabla och att systemet uppfyller lagkrav och verksamhetskrav.

Projektdirektiv U537 har syftat till att informationsklassning och riskanalyser ska göras på drygt 600 system i Region Skåne. Projektdirektivet löper ut vid årets slut och arbetet pågår vid tiden för granskningen. Prioritering av vilken ordning som system ska klassas har enligt intervjuer dels skett utifrån en övergripande riskbedömning av systemen, dels utifrån framtida integrationer för systemet i förhållande till SDV.

I intervjuer beskrivs att vissa omprioriteringar har behövt göras mot bakgrund av att verksamheterna inte genomfört informationsklassningar i enlighet med

informationsägaransvaret. Det har inneburit att systemägare inte kommit vidare i processen. I dessa fall har ett mer generellt arbete fått inledas parallellt med att man går vidare med andra system. Det uppges i intervjuer att Digitalisering IT och MT tryckt på betydelsen av att informationsägare tar sitt ansvar i arbetet.

Vid den här granskningens genomförande hade klassningar och åtgärder påbörjats/slutförts för drygt 25 informationssystem och närmare 30 tillhörande applikationer inom ramen för projektet. En övervägande del av systemen är Digitalisering IT och MT systemägare för, och resterande system är Medicinsk service systemägare för.

Ansvariga på Digitalisering IT och MT ser behov av att ansvaret för genomförande av det stora antal informationsklassningar och riskanalyser som krävs behöver skjutas tillbaka till informationsägarna i enlighet med Region Skånes beslutade ansvarsfördelning. Detta då arbetet är mycket resurskrävande och inte kan prioriteras av Digitalisering IT och MT för återstående system samtidigt som det behövs en snabbare framdrift i arbetet. Att behoven är så stora beror på att informationsklassning och riskanalyser inte har genomförts tidigare i enlighet med Region Skånes riktlinjer och instruktioner.

3.3.2.1 Resultat av systemgranskning 14 system som är i drift i Region Skåne

I granskningen har vi genomfört granskning av 15 system utifrån ett antal olika frågeställningar som besvarats av aktuella systemägare och de roller som är utsedda med ansvar för respektive system i enlighet med Region Skånes verksamhetsstyrda styr- och förvaltningsmodell. Vi redogör för resultatet av systemgranskningen för 14 av systemen nedan. Resultat av systemgranskning avseende SDV redovisas i avsnitt 3.3.3.2.

Vår stickprovsgranskning visar att informationsklassningar och riskanalyser genomförts för samtliga granskade system i urvalet. Enligt uppgift har representanter från verksamheterna varit med i arbetet tillsammans med systemansvariga och projektledare och utsedda funktioner som riskanalysledare med flera.

För ett antal system har fördjupade riskanalyser behövt genomföras där några är pågående vid tiden för granskningen. Det kan bland annat vara mer komplexa juridiska eller tekniska avväganden som krävs.

För majoriteten av systemen har behov av både tekniska och organisatoriska åtgärder identifierats vilka föranleder ett antal åtgärder. Vi har kunnat konstatera att systemansvariga säkerställer att behov av tekniska säkerhetsåtgärder genomförs och följs upp. Verksamhetsansvariga får i uppdrag att säkerställa att de organisatoriska åtgärderna hanteras.

En problematik som lyfts i samband med genomgång av systemen är att det finns tekniska begränsningar för äldre system där funktionaliteten inte medger att nödvändiga åtgärder vidtas.

För vissa av de system som ingått i urvalet har systemansvariga identifierat att den fortsatta processen efter klassning och riskanalys, där informationsägaren ska besluta om riskacceptans och driftsgodkännande inte är tillämplig. Detta beror på att vissa

system får så höga riskvärden att informationsägaren inte har rätt att besluta om riskacceptans och driftsgodkännande.

Då systemen redan är i drift sedan många år så skulle det inte vara möjligt utan alltför stor påverkan på verksamheten att stoppa driften och nyttjandet på grund av riskvärderingen. Då ingen ny rutin har fastställts finns idag inte en lösning för hur bedömningar och åtgärder ska prioriteras för flera av systemen. Det finns inte någon kommunicerad lösning till systemansvariga kring hur detta ska hanteras idag.

Gällande nya system finns inget problem med processen då det ställs krav på att informationsklassning och riskanalyser genomförs inför upphandling och införande. Detta innebär att identifierade risker och behov av åtgärder kan åtgärdas eller kravställas och processen och arbetet kan sedan ha sin fortsatta gång i enlighet med ordinarie process som leder till ett driftgodkännande.

3.3.2.2 Resultat av Systemgranskning Skånes Digitala Vårdsystem (SDV) som ska tas i drift

Som vi beskrivit tidigare har SDV varit ett av de 15 system som ingått i urvalet. Samtliga system som ingår under paraplyet SDV är inte i drift ännu och den mest omfattande implementeringen kvarstår att göra under våren 2025. I vår systemgranskning har ingått att jämföra hur SDV-programmet beaktat de krav som Region Skåne har inför implementering av informationssystem med tillhörande riskhanteringsprocess i ett informationssäkerhetsperspektiv. Granskningen har inte avsett funktionalitet eller teknisk kapacitet.

Arbetet med SDV leds av en programchef och det finns även en medicinsk programchef. SDV är ett omfattande program som drivits i flera år utifrån beslut i regionstyrelsen 2016 om en strategi för en sammanhållen digital vårdmiljö. Detta blev sedan starten på upphandlingsprocess av nytt digitalt vårdsystem.

En styrgrupp utsågs som inledningsvis var mottagare av rapportering från programmet. Sedan ett tag utgör dock koncernledningen styrgrupp för SDV. De formella besluten fattas av regionstyrelsen men även NORV uppges löpande ha fått information om SDV. Genom protokollsgranskning för regionstyrelsen under 2024 kan vi notera att ett ärende har hanterats som rör SDV, vilket vi redogör för nedan. Av protokollsgranskning för NORV under 2024 kan vi inte notera något specifikt ärende om SDV. Av dagordningen inför nämndens sammanträde 29 februari 2024 framgår dock att programchef för SDV skulle ha en föredragning utifrån temat *Vad Digitalisering IT och MT gör för att förbereda för SDV*. Enligt intervjuuppgifter genomfördes denna dragning men protokollfördes inte.

Inom programmet finns en projektledare med ansvar för regelefterlevnad och som stöd finns även ett regelefterlevnadsråd med bred representation från Region Skånes olika verksamheter. Bland andra ingår informationssäkerhetschef, chefsjurist, Region Skånes dataskyddsombud och representanter från Digitalisering IT och MT med specialistkunskap inom it-säkerhet.

I intervjuer bekräftas att införande av nya informationssystem i hög grad sker med grund i den fastställda process som Region Skåne har i styrande dokument. Detta har

även kunnat verifieras genom de underlag vi tagit del av i granskningen som specifikt rör SDV.

Intervjuade beskriver att det finns flera informationsägare för SDV, där ansvaret är uppdelat med grund i den information som hanteras i de olika delarna av systemet. Detta har identifierats vid informationsklassningar. Exempelvis är hälso- och sjukvårdsdirektören informationsägare för patientdata medan HR-direktören är informationsägare för den information i systemen som hanterar uppgifter om anställda i Region Skåne. Därutöver är IT-direktör, tillika förvaltningschef Digitalisering IT och MT informationsägare för den information som avser systemdokumentation och även avtalsägare i förhållande till den externa leverantören av systemet.

I intervjuer beskrivs att informationsklassningar och riskanalyser har gjorts i omgångar för olika delar av systemen, detta då systemets komponenter har olika skyddsnivåer och skyddsbehov. Det största systemet i SDV är det som efter implementeringen ska hantera patientdata och utgöra Region Skånes journalsystem. Information som berör patientdata får alltid den högsta klassningen och därigenom högt ställda krav om säkerhetsåtgärder i syfte att inte det ska finnas risk för att inte konfidentialitet, riktighet, tillgänglighet eller spårbarhet ska kunna säkerställas. Andra delar av systemet där inte patientuppgifter hanteras kan i klassning ha fått något lägre klassningsresultat i någon av aspekterna och säkerheten kan därigenom anpassas efter det faktiska behovet.

Informationsklassning och riskanalyser identifierade inledningsvis ett stort antal risker med höga riskvärden. Efter det har säkerhetsåtgärder och anpassningar vidtagits löpande för att nå fram till acceptabla risknivåer. Dessa har sedan informationsägaren, eller vid särskilda fall, regionstyrelsen, fattat beslut om. Föredragande för regionstyrelsen uppges ha varit medicinsk programchef, regiondirektör och chefsjurist. Dessa delbeslut är tänkta att leda fram till ett slutligt driftsgodkännande som innebär att systemen får implementeras och tas i drift.

Systemen kommer levereras som en så kallad SaaS[11]-lösning, vilket innebär att Region Skåne nyttjar systemen som en tjänst från leverantören. Det innebär i sin tur att Region Skåne är kravställare av informationssäkerhetskrav till systemleverantören vilket regleras i avtal parterna emellan. Enligt intervjuade har samtliga kravställningar utgått från resultat i informationsklassning och krav enligt ISO27000-serien (vilket är den nivå som Region Skåne internt ställt som krav i LIS men som även motsvarar krav som nuvarande lagstiftning har för samhällsviktiga tjänster). Intervjuade anger att de säkerhetsåtgärder som de ställt krav på och anpassningar som har behövt åtgärdats har verkställts.

Som del i programmets åtgärder inför beslut om riskacceptans och driftsgodkännande har representanter från SDV gjort kontroller hos leverantören, exempelvis i det datacenter där Region Skånes information ska lagras. Anpassningar för att följa lagkrav om hantering av personuppgifter har även säkerställts. Därutöver har även loggar vad gäller drift- och säkerhetshändelser tillhandahållits från leverantören löpande där utsedda funktioner inom SDV-programmet har kunnat göra analyser och utvärderingar för att bedöma systemets säkerhet.

[11] Software as a Service

Regionstyrelsen fattade beslut om driftsgodkännande vid sammanträde i september 2024[12]. Detta då omfattande åtgärder vidtagits inom samtliga delområden (organisatoriska, tekniska, fysiska och personrelaterade) för att nå en acceptabel nivå och få godkännande om att gå i drift.

Intervjuade beskriver att det omfattande arbetet som gjorts inom SDV identifierat brister i nuvarande ledningssystem för informationssäkerhet. Detta då programledningen för SDV sett andra behov, med högre kravställning, av säkerhetsåtgärder än nuvarande styrdokument ställer. Detta gäller både ledningssystemet i sig och även den kravkatalog som Region Skåne utgår från i nuläget. När avsteg har behövt göras har dialog med informationssäkerhetschef och informationsägare genomförts. Uppfattningen från representanter från SDV är att programmet identifierat väsentliga förbättringsbehov i Region Skånes LIS, vilka kan tas tillvara i det kommande utvecklingsarbetet med uppdaterade styrdokument som utgör grunden i LIS.

En annan utmaning som lyfts i intervjuer är beslut och implementering av den nya Styr- och ansvarsmodellen vilket sammanfaller med när SDV behöver gå från nuvarande organisering i program till att placeras in i någon av de styr- och ansvarsområden (SOA) som finns i Region Skåne. Som vi beskrivit tidigare i rapporten så förväntades beslut om modellen i april 2024 men hade vid tid för intervjuer inte fattats.

3.3.3 It-säkerhetsåtgärder för informationstillgångar inom Digitalisering IT och MT

Utifrån ovan beskrivningar av process för att identifiera skyddsbehov och säkerhetsåtgärder så är Digitalisering IT och MT både informations- och systemägare för regiongemensamma informationstillgångar, exempelvis nätverk, servrar, plattform osv. I ansvaret som driftsorganisation innehar Digitalisering IT och MT ansvar för motsvarande processer för de informationstillgångarna i syfte att anpassade säkerhetsåtgärder ska vidtas.

Vi har genom intervjuer fått beskrivet att Digitalisering IT och MT har ett aktivt arbete med tekniska säkerhetsåtgärder för de informationstillgångar som förvaltningen är systemägare för. Arbetet utgår från en fastställd ”säkerhetsroadmap” som vi har tagit del av i granskningen. Enligt uppgift fungerar den som en handlingsplan för prioritering av åtgärder och sträcker sig fyra år i taget med löpande revidering.

Inom ramen för handlingsplanen görs exempelvis hotaktörsanalys och hotaktörsförmågeanalyser. Utifrån analyserna tittar man på den interna sårbarheten och vilka kritiska system som påverkas av sårbarheten utifrån olika perspektiv, exempelvis tjänster, produkter och rutiner.

Arbetet drivs av it-säkerhetsenheten men genomförs i samverkan mellan olika enheter under Digitalisering IT och MT. Löpande kommunikation finns gentemot systemansvariga för berörda system. Exempelvis som ett resultat av de informationsklassningar och riskanalyser som genomförts.

Parallellt sker ett arbete med externa aktörer som gör veckovisa sårbarhetsskanningar som kommuniceras till it-säkerhetsspecialisterna på enheten. Behov av åtgärder för

[12] Regionstyrelsen 2024-09-05 §148

exempelvis servrar kan då hanteras med stöd av it-säkerhetsspecialisterna direkt utifrån resultatet. Under 2024 har it-säkerhetsenheten också börjat genomföra egna penetrationstester på nya system innan driftsättning.

3.3.4 Bedömning

Vi bedömer att NORV i allt väsentligt säkerställer ett tillräcklig skydd för Region Skånes databaser och system inklusive molntjänster och att tekniska säkerhetsåtgärder vidtas utifrån de identifierade skyddsvärden från informationsklassning och riskbedömning.

I vår bedömning vill vi dock poängtera att nämnden i låg grad är involverad i säkerställandet av skydd. Detta då varken information eller beslut om risker, åtgärder eller uppföljning i nuläget hanteras av NORV, vilket även konstaterats i tidigare bedömningar.

Vi baserar vår bedömning på att Digitalisering IT och MT vidtar åtgärder som baseras på identifierade skyddsvärden i de fall sådana underlag finns tillgängliga och att arbetet fungerar enligt beslutade strukturer och processer för nya införanden av IT och MT-system. Vi har särskilt noterat att kommande implementering av SDV på ett tydligt sätt har följt den internt fastställda processen och krav på riskhantering inför driftsgodkännande. Vi ser därtill att den representation av tvärfunktionella kompetenser som varit involverade samt den dialog som etablerats med informationsägarna på ett systematiskt och riskbaserat sätt beaktat informationssäkerhet utifrån samtliga aspekter.

Vi bedömer dock att ett betydande hinder för att få framdrift i arbetet, så att Digitalisering IT och MT ska ha underlag att basera skyddsåtgärder på, är att informationsägarskapet brister. Det återstår ett stort antal system som ännu inte har en aktuell informationsklassning och genomförd riskanalys till följd av att informationsägare inte tagit sitt ansvar enligt rollbeskrivning i styrande dokument. Det innebär att det saknas underlag för att anpassa tekniska eller andra säkerhetsåtgärder utifrån risker och skyddsvärden.

Vi ser också en brist i att informationssäkerhetsperspektivet inte tydligare ingår i nuvarande processer inom ramen för Region Skånes Verksamhetsstyrda styr- och förvaltningsmodell för IT och MT-system. Detta då vi ser att det skulle kunna integreras på ett mer effektivt sätt och resurserna i systemförvaltningsgrupperna nyttjas i högre grad även i informationssäkerhetsarbetet.

Vi bedömer att det genomförs systematiska uppföljningar och kontroller av vidtagna säkerhetsåtgärder.

Vi baserar vår bedömning på att det inom Digitalisering IT och MT löpande sker en uppföljning och anpassning av relevanta säkerhetsåtgärder, både ur ett förebyggande och utifrån identifierade sårbarheter uppföljande perspektiv. Vi kan dock konstatera att NORV inte i nuläget är involverade mer än i den uppföljning som görs genom verksamhetsberättelsen och intern kontroll, (se avsnitt 3.5.2)

3.4 Incident- och kontinuitetshantering

3.4.1 Incidenthantering

3.4.1.1 Informationssäkerhetsincidenter

På en regionövergripande nivå finns en instruktion för informations-säkerhetsincidenter[13] och som samtliga förvaltningar i Region Skåne har att förhålla sig till.

Det identifieras i årsrapporten enligt ledningssystemet att nuvarande rutiner för incidenthantering behöver kompletteras med tydlig beskrivning av ansvar, processer och eskaleringsvägar i händelse av olika incidenttyper. Vidare framgår att rutinerna behöver etableras i organisationen samt att inträffade incidenter behöver analyseras och utgöra underlag för att identifiera förbättringsbehov på regionsövergripande nivå. Informationssäkerhetschef med stöd av informationssäkerhetsorganisationen kommer under 2024 att göra en översyn av processen för hanteringen av informationssäkerhetsincidenter samt berörda styrdokument, bland annat instruktionen för informationssäkerhetsincidenter.

I beslut om organisation och ansvar för informationssäkerhetsarbetet som fattats av förvaltningschef Digitalisering IT och MT framgår ansvar och uppgifter för flera av rollerna avseende incidenter. Bland annat ska informationssäkerhetssamordnaren vara första kontaktpunkt i händelse av incidenter. Det saknas beskrivning av vilka typer av incidenter som avses och hur dessa ska eskaleras från övriga funktioner inom förvaltningen, exempelvis de som är incidentansvariga internt och externt.

Vi har i intervjuer fått bekräftat att det finns problem kopplat till hanteringen av informationssäkerhetsincidenter. Information om informationssäkerhetsincidenter når många gånger inte rätt funktioner, exempelvis informationssäkerhetssamordnare i förvaltningarna eller informationssäkerhetschef på regionövergripande nivå då verksamheter inte vet hur incidenter ska kategoriseras för att nå rätt funktioner. Detta försämrar också möjligheterna att sammanställa och aggregera olika typer av incidenter för att kunna arbeta med att identifiera och vidta åtgärder för att minska antalet incidenter förvaltningsövergripande och regionövergripande som del i förbättringsarbetet.

3.4.1.2 It- och cybersäkerhetsincidenter

Digitalisering IT och MT har tre olika incidenthanteringsrutiner. En rutin finns för generella incidenter[14] där en utsedd incident manager finns inom Digitalisering IT och MT. Inom ramen för den rutinen regleras den mer generella rutinen för att anmäla, hantera och avsluta incidenter.

Därtill finns även en rutin för it-säkerhetsincidenter[15] som träder i kraft vid incidenter med risk för dataförlust, större otillgänglighet på grund av antagonistisk påverkan,

[13] Beslutad av regiondirektör 2021-01-04
[14] Senast reviderad 2023-08-28
[15] Senast reviderad 2023-08-28

förvanskning av data samt risk för obehörig part att tillskansa sig tillgång/ behörighet till Region Skånes digitala miljö.

Vidare finns en rutin för stora incidenter[16]. Vid incidenter som omfattar flera parter koordineras incidentärendet av en Incident Manager med koordineringsansvar och övriga parter bidrar med kunskap inom sitt område för att lösa incidenten. Region Skåne har två externa SOC-tjänster (Security Operations Center) hos leverantörer, som har i uppdrag att övervaka och agera på it-säkerhetshändelser dygnet runt. I avtalen om tjänsterna ingår rollen Incident Manager för stora incidenter. Digitalisering IT och MT har it-chef i beredskap vilken är den funktion som ingår i den eskaleringskedja som beslutats i händelse av allvarlig störning eller it-säkerhetsincident.

I intervjuer beskrivs att arbetet enligt rutinerna i allt väsentligt fungerar väl och att rutinerna är kända i organisationen.

3.4.2 Kontinuitetshantering

Kontinuitetsplanering kan ske utifrån två olika perspektiv för ett system, it-perspektivet respektive verksamhetens perspektiv. I ett it-perspektiv har vi fått beskrivet att driften av system i stor utsträckning är outsourcat till externa leverantörer vilket innebär att kontinuitetsplaneringen i hög grad åligger de externa leverantörerna. Det som görs från Region Skånes sida är att ställa krav på exempelvis återställning och support genom SLA (service level agreement) som ingår i avtalsprocessen och reglerar de krav på tjänstenivåer som efterfrågas. Det blir enligt intervjuade upp till leverantören att säkerställa att det finns en tillräcklig planering för att kunna efterleva de krav som ställs i SLA. Uppföljning av att avtalade servicenivåer erhålls sker genom löpande avstämningar och forum som etablerats med de externa leverantörerna.

Att det finns kontinuitetsplaner inom respektive verksamhet är en del av krisberedskapsarbetet och ingår i verksamhetsansvaret. Vi har utifrån syftet och avgränsningen i den här granskningen inte granskat sådana planer men har genom förvaltningarnas verksamhetsberättelser kunnat notera att Medicinsk service bedriver ett aktivt arbete med kontinuitetsplanering där planer har formulerats under året. Dessa innefattar åtgärder och reservrutiner för kort- och långsiktiga avbrott, störningar och kriser. Förvaltningen har även säkerställt att införa automatiserade larm vid driftsstopp för en del av systemen.

Av verksamhetsberättelse 2023 för Digitalisering IT och MT framgår att förvaltningen under året har stärkt förmågan att kommunicera med kritisk it-leverantör i händelse av störning eller avbrott. Därtill har en kartläggning genomförts för att identifiera kritiska leveranser med tillhörande stödprocesser samt förmåga, sårbarheter och behov av åtgärder kartlagts som del i förvaltningens krisberedskapsarbete. Resultatet av arbetet har enligt berättelsen kommunicerats till Koncernkontoret.

Vi har även fått information om att det finns väl utarbetade rutiner för detta inom övriga förvaltningar och verksamheter som del i att kunna utföra patientnära arbete även utan tillgång till digitala system. Detta testas löpande då både planerade och oplanerade

[16] Senast reviderad 2023-08-28

driftsstopp inträffar mer eller mindre regelbundet. Därtill beskriver systemansvariga i intervjuer, att de utifrån de behov som identifieras, lämnar förslag om kompletterande manuella rutiner för verksamhetsansvariga att ta fram för specifika system.

3.4.3 Bedömning

Vi bedömer att NORV delvis säkerställt en ändamålsenlig incidenthantering och i allt väsentligt säkerställt en ändamålsenlig kontinuitetshantering.

Vår bedömning baseras på att det finns rutiner utifrån it-säkerhetsincidenter. Däremot bedömer vi att det är en brist att det saknas en fungerande incidenthantering för informationssäkerhetsincidenter, vilket är ett regionövergripande problem som även påverkar ändamålsenligheten i NORV:s förvaltningars incidenthantering.

Informationssäkerhetssamordnarrollens förankring i incidenthanteringsrutinerna bör övervägas på förvaltningsnivå för att NORV ska kunna säkerställa en ändamålsenlig incidenthantering och för att erfarenheter ska kunna tillvaratas i förbättringsarbetet och motverka att incidenter sker på nytt. Utifrån nämndens ansvar för robust drift ser vi det även som väsentligt att NORV på en aggregerad nivå erhåller information om incidenter som sker tillsammans med analyser som kan påvisa vilka förstärkningar eller åtgärder som det kan finnas behov av.

3.5 Uppföljning

3.5.1 Uppföljnings- och rapporteringsrutiner enligt ledningssystem för informationssäkerhet

Enligt instruktionen för tillämpning av riktlinjen för informationssäkerhet på regionövergripande nivå ska uppföljning ske enligt följande:

1) Förvaltningar ska löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.
2) Förvaltningar ska regelbundet granska sin informationssäkerhet. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas.
3) Varje år ska förvaltningarnas informationssäkerhetssamordnare rapportera arbetet med informationssäkerheten till förvaltningschef.

Intervjuade uppger att den uppföljning och rapportering som kravställs enligt ovan inte genomförts för 2023 inom varken Digitalisering IT och MT eller Medicinsk service. Informationssäkerhetssamordnarna har dock gjort en sammanställning av förvaltningens arbete som underlag till informationssäkerhetschef rapport till regionstyrelsen. Vi noterar att det i nuläget inte finns någon kravställning om uppföljning och rapportering till nämnderna av informationssäkerhetsarbetet.

Tidigare år uppges koncernkontoret ha kommunicerat olika kontroller och uppgifter till förvaltningarnas informationssäkerhetssamordnare som de sedan har haft som grund i en planering för året. Detta hade inte gjorts vid september månads utgång 2024.

3.5.2 Uppföljning i verksamhetsberättelser och genom intern kontroll

Vi kan konstatera att de verksamhetsberättelser som NORV beslutat om för båda förvaltningarna för år 2023 innehåller avsnitt om informationssäkerhet. För Medicinsk service lyfts i berättelsen att förvaltningen har arbetat med informationsklassning och riskanalyser samt införande av nya system. För Digitalisering IT och MT framgår liknande information under avsnittet informationssäkerhet där arbetet utifrån projektdirektiv U537 översiktligt återges med kommentaren att Digitalisering IT och MT får ta ett större ansvar inom området på grund av resursbrist hos andra förvaltningar.

Verksamhetsberättelsen för Digitalisering IT och MT innehåller, mot bakgrund av den verksamhet som förvaltningen ansvarar för, en stor del information som har beröring på granskningen då ett stort fokus inom förvaltningen de senaste åren varit att höja säkerheten och tillse en robust it-miljö som är förberedd för högre digitaliseringstakt.

Flertalet av de mål som Digitalisering IT och MT har beslutat om som följs upp i verksamhetsberättelsen inkluderar aktiviteter inom informationssäkerhet, främst med fokus på tekniska säkerhetsåtgärder. I verksamhetsberättelsen beskrivs väsentliga aktiviteter som genomförts för att nå målen vilket till viss del kan ses som en uppföljning av förvaltningens informationssäkerhetsarbete.

Inom ramen för NORV:s ansvar enligt reglementet genomförs uppföljning utifrån riskanalys- och riskhanteringsplan inom ramen för internkontroll.

I granskningen kan vi konstatera att nämnden följer vissa risker kopplat till informations- och it-säkerhet, framför allt kopplat till riskanalys och riskhanteringsplanen 2024–2026 för Digitalisering IT och MT [17]. Motsvarande riskanalys- och riskhanteringsplan 2024–2026 för Medicinsk service saknar risker med tydlig koppling till granskningsområdet.

Utifrån vår protokollgranskning och genom det som har förmedlats i intervjuer har vi inte kunnat se att nämnden hanterat några ärenden med beröring på granskningsområdet utöver ovan obligatoriska uppföljning genom verksamhetsberättelser och intern kontroll. Nämnden har även under 2024 lämnat yttrande över tidigare revisionsgranskningar inom informationssäkerhetsområdet.

3.5.3 NIS2-direktivet

Medlemsländer i EU, däribland Sverige, har sedan 2018 haft EU-direktivet NIS[18] att följa. Den svenska tillämpningen av direktivet regleras i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Direktivet syftade till att öka säkerheten i nätverk och informationssystem inom samhällsviktiga verksamheter, där konsekvenser vid it-bortfall skulle kunna leda till allvarliga konsekvenser med samhällsstörningar som följd. I den lagstiftning som gällt sedan 2019 fanns endast sju sektorer som omfattades av kraven. Region Skåne har stått under kraven avseende verksamheten inom sektor hälso- och sjukvård.

2022 beslutade EU-parlamentet om ett nytt direktiv, benämnt NIS2, med förstärkta krav och en utökning av verksamheter och sektorer som ska omfattas av lagen för att ytterligare stärka säkerheten och även samordningen inom området. I Sverige har en utredning på uppdrag av regeringen genomförts som nu presenterats i ett lagförslag i form av Cybersäkerhetslagen. Lagen förväntas träda i kraft 1 januari 2025.

Av utredning och lagförslag framgår ett antal förändringar mot det första NIS-direktivet, exempelvis de nedan som Sveriges kommuner och regioner, SKR, lyfter som väsentliga för kommuner och regioner:

- NIS2 ställer tydligare krav på riskanalyser och säkerhetskrav, men också på ledningens deltagande i cybersäkerhetsarbetet.
- NIS2 innebär också att hela verksamheten kommer att omfattas av lagstiftningen.
- NIS2 omfattar betydligt fler aktörer än nuvarande lagstiftning (NIS), antalet sektorer ökar från sju till 18.
- En av de nya sektorerna är offentlig förvaltning, vilket innebär att kommuner och regioner kommer att omfattas i högre utsträckning av lagstiftningen.
- NIS2 innebär också att en administrativ sanktionsavgift införs, för offentlig förvaltning föreslås den ligga på minst 5. 000 kr och som mest 10. 000 000 kr.

[17] Beslutad av nämnden för operativ regiongemensam verksamhet, 2024-02-29 §5
[18] NIS står för ”The Directive on Security of Network and Information Systems”

Utöver ovan punkter som SKR redovisar så tolkas lagförslaget som att styrelser och nämnder i högre grad måste vara involverade och ta ansvar i informations- och cybersäkerhetsarbetet.

Mot bakgrund av att ny lagstiftning förväntas inom granskningsområdet, har vi i granskningen i uppdrag att bedöma om NORV initierat ärende eller efterfrågat information om Digitalisering IT och MT:s nuläge i förhållande till krav i ny lagstiftning för att identifiera vilka anpassningar som behöver göras för att nå en efterlevnad av direktivet och den svenska tillämpningen. Vi har i de underlag vi tagit del av inte kunnat notera något uppdrag eller ärende från NORV till Digitalisering IT och MT.

Vi har genom intervjuer fått uppgift att ställningstagande i frågan har efterfrågats av Digitalisering IT och MT från koncernkontoret mot bakgrund av deras övergripande ansvar för styrningen av informationssäkerhet. Det har dock inte presenterats något ställningstagande eller initierat ett arbete i förhållande till ny lagstiftning.

Enligt intervjuade har det inför implementeringen av SDV skett en dialog i programmets regelefterlevnadsråd om de säkerhetsåtgärder som kravställts är tillräckliga även för efterlevnad av NIS2. Programledningen har efter dialogen gjort bedömningen att det inte finns ytterligare behov av åtgärder i förhållande till nya lagkrav.

En enskild medarbetare inom Digitalisering IT och MT har på eget initiativ påbörjat en GAP-analys av nuläget i Region Skåne i förhållande till kraven i NIS2 utifrån det tekniska perspektivet. Detta i syfte att ha en beredskap om det inte kommer något från regionalt håll. Arbetet är dock i en inledande fas och har inte varit uppe för information eller beslut om åtgärder i förvaltningsledning eller nämnd.

3.5.4 Bedömning

Vi bedömer att det delvis finns uppföljnings- och rapporteringsrutiner i enlighet med gällande krav i ledningssystem för informationssäkerhet.

Vår bedömning grundas i att det görs viss uppföljning av informationssäkerhets-samordnare som rapporteras till koncernkontoret för gemensam sammanställning och rapportering i enlighet med ledningssystemets krav.

Däremot sker inte någon rapportering till förvaltningsledningarna i enlighet med ledningssystemets krav som möjliggör att förvaltningsledning har tillräcklig kunskap för att kunna vidta relevanta åtgärder eller lyfta åtgärder till nämnd.

I nuläget saknas dock krav på att nämnden ska följa upp informationssäkerhetsarbetet och vi kan konstatera att det inte heller gjorts någon sådan. Den uppföljning och rapportering till nämnden som genomförts har varit utifrån ordinarie fastställda uppföljningskrav för NORV där informationssäkerhet i begränsad omfattning ingår. Vi kan dock inte se att efterlevnad av interna styrdokument är en del i nuvarande uppföljning som snarare består av uppföljning av mål och aktiviteter.

Vi bedömer att NORV inte får tillräckligt med information för att kunna fullgöra sitt uppdrag och ta beslut om åtgärder vid behov.

Det är positivt att nämnden får information inom ramen för intern kontroll och verksamhetsberättelse vad avser Digitalisering IT och MT, men vi kan inte se att motsvarande moment finns med utifrån Medicinsk services uppdrag. Vi kan inte härleda att informationen idag fyller en funktion utifrån ett tydligt uppdrag för nämnden att vara en beslutande eller beredande funktion då inga beslut om åtgärder har fattats av NORV. Vi bedömer mot bakgrund av NIS2-direktivets förstärkta krav att dylika frågeställningar sannolikt kommer behöva beslutas eller beredas av nämnden i närtid för att säkerställa följsamhet mot direktivet.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om nämnden för operativ regiongemensam verksamhet arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system.

Vår samlade bedömning utifrån granskningens syfte är att nämnden för operativ regiongemensam verksamhet delvis arbetar ändamålsenligt och effektivt med informations- och it-säkerhet avseende Region Skånes it-system.

Utifrån resultatet av vår granskning rekommenderar vi nämnden för operativ regiongemensam verksamhet att:

- Bedöma om nuvarande styrning av förvaltningarnas arbete inom informationssäkerhet och tekniska säkerhetsåtgärder är tillräckliga utifrån nämndens ansvar, samt vid behov besluta om eller bereda förslag till kompletterande instruktioner och anvisningar.
- Säkerställa att informationssäkerhetssamordnare inom Digitalisering IT och MT har förutsättningar att utföra uppdraget i enlighet med det mandat som tillskrivs rollen.
- Tillse att förvaltningsledningen från informationssäkerhetssamordnaren erhåller en årlig samlad rapportering av informationssäkerhetsarbetet inom den egna förvaltningen i syfte att säkerställa en ändamålsenlig rapportering till nämnden.
- Säkerställa att den årliga uppföljningen inkluderar regelefterlevnad av lagkrav och styrande dokument inom informationssäkerhet och att brister rapporteras till nämnden samt till informationssäkerhetschef på koncernkontoret.
- Tillse att nuvarande uppföljning och rapportering till nämnden kompletteras med väsentliga händelser inom informationssäkerhet, exempelvis inträffade incidenter eller andra faktorer som riskerar att påverka nämndens ansvar inom drift av it.
- Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom nämndens ansvarsområden.

Utifrån resultatet av vår granskning rekommenderar vi regionstyrelsen att:

- Bereda förslag till nytt reglemente för regionstyrelsen och NORV i syfte att tydligare reglera ansvaret för Region Skånes informationssäkerhetsarbete. Vid revideringen bör beaktas att det inom informationssäkerhetsområdet finns behov av att fatta beslut som påverkar andra nämnder i Region Skåne.
- Revidera riktlinjer och tillhörande instruktioner så att dessa är aktualiserade i enlighet med Region Skånes nuvarande organisation och ansvar samt kompletteras med reglering av ansvar för informationssäkerhetsarbetets olika delområden.

- Följa upp att de prioriterade åtgärder för utveckling av informationssäkerhets-arbetet som föreslogs i informationssäkerhetsberättelsen har en framdrift och stärker Region Skånes arbete.
- Överväga om vissa aktiviteter och uppgifter inom informationssäkerhetsarbetet kan integreras i den nya styr- och ansvarsmodellen.
- Stärka uppföljning och kontroll av efterlevnad av fastställda styrdokument inom informationssäkerhet.
- Säkerställa att en analys genomförs utifrån eventuellt nya krav med anledning av NIS2-direktivet samt att åtgärder vidtas i syfte att efterleva direktivet inom styrelsens ansvarsområden.