Granskning av IT-säkerhet

Rapport

Region Jämtland Härjedalen

KPMG AB

2021-03-25

Antal sidor 31

Bilaga 1

Innehållsförteckning

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Region Jämtland Härjedalen fått i uppdrag att genomföra en granskning av regionens arbete med IT-säkerhet. Granskningen har syftat till att svara på om regionens organisation och interna kontroll är ändamålsenlig gällande IT-säkerhet. Uppdraget ingår i revisionsplanen för 2020.

Vår sammanfattande bedömning är att regionen delvis har en ändamålsenlig organisation för arbetet med IT-säkerhet men att den interna kontrollen avseende efterlevnaden av lagar, förordningar och interna regelverk för IT-säkerhet är bristfällig.

Vi baserar vår bedömning på följande iakttagelser:

- Det finns en övergripande styrning genom ett implementerat ledningssystem för informationssäkerhet. I ledningssystemet finns en dokumenterad ansvarsfördelning och organisation för arbetet som tillsammans med styrande dokument har tydliggjort hur arbetet ska bedrivas. En informationssäkerhetsberättelse tas fram som underlag för beslut om åtgärder och prioriteringar för att förbättra informations- och IT-säkerhetsarbetet.
- Det finns risk att nuvarande organisation är sårbar då det vilar ett stort ansvar för både det strategiska och operativa arbetet på de nyckelpersoner som leder arbetet med informationssäkerhet och IT-säkerhet. Vid eventuella personal- eller organisationsförändringar kan det leda till att kontinuitet och kunskap går förlorad.
- Vi noterar att det finns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som utpekas i dokumenterad ansvarsfördelning inte uppfylls av avdelnings- och områdeschefer. Vi konstaterar att det till stor del beror på att det upplevs saknas resurser som kan utgöra ett stöd till cheferna för det praktiska arbete som behöver ske i respektive förvaltning och enhet.
- Medarbetare har inte fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar generellt.
- Det saknas ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar. IT-säkerhetsåtgärder inrättas därmed till stor del utifrån den kunskap och förutsättningar som IT-enheten har. Detta riskerar att införda säkerhetsåtgärder inte står i relation till hur skyddsvärd informationen som den avser att hantera är. Vi ser det som en särskild risk då IT-driften är outsourcad till stor del.
- Det finns inte ändamålsenliga rutiner för behörigheter och lösenord. Det finns ett flertal styrande och stödjande dokument men vi noterar att dessa i praktiken inte får genomslag och att rutiner inte efterlevs i tillräckligt hög grad. Den bristande behörighetshanteringen bedömer vi påverkar regionens förmåga att säkerställa medborgarnas integritet avseende patientinformation i journalsystem.
- Hantering av behörigheter inom IT-enheten för externa leverantörer avseende IT-drift bedöms som ändamålsenliga. Det finns etablerade rutiner och processer

för hanteringen och en tillräcklig loggkontroll som synliggör hur tilldelade behörigheter används. Vår granskning har inte omfattat hantering av behörigheter för enskilda verksamhetssystem och vilka rutiner som tillämpas för externa leverantörer i dessa system.

- Riskanalyser inom IT-säkerhet sker på ett delvis tillfredsställande sätt. Det har upprättats analyser över sårbarheter för enskilda delar av IT-miljön för att identifiera brister. Vi anser dock att arbetet med riskanalyser kan utvecklas och utgöra ett underlag för prioritering av IT-säkerhetslösningar där dessa tar utgångspunkt från de mest väsentliga riskerna.
- Det finns till viss del rutiner för att säkerställa att nya risker och hot identifieras genom regelbunden omvärldsbevakning samt genom de riskanalyser som genomförts med externa konsulter. Sårbarhetsscanning genomförs systematiskt med en genomgång av samtliga servrar och klienter och ger automatiskt en riskprioritering per sårbarhet.
- Det saknas en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter. Det sker i nuläget ingen övergripande sammanställning över inträffade incidenter så att dessa kan utvärderas och ligga till grund för regionens förbättringsarbete genom att de då kan vidta åtgärder så att dessa inte sker igen.
- Regionen har ett aktivt arbete med IT-säkerhet genom vilket de har tillsett att det ska finnas säkerhetsåtgärder för att skydda regionens information inklusive lagrade patientdata. Det har vidtagits ett flertal åtgärder, exempelvis segmenterade nätverk, funktioner för övervakning, säkra inloggningsfunktioner samt en regelbunden sårbarhetsscanning för att upptäcka sårbarheter. Det har därtill genomförts en analys utifrån NIS-direktivets krav om säkerhet vilken ligger till grund för förbättringsarbete för IT-säkerheten.
- Kontinuitetsplan avseende IT-drift finns men den är inte uppdaterad. I nuvarande form finns det risk att det saknas tillräckliga underlag för att upprätthålla kontinuiteten i verksamheten vid större händelser i form av avbrott eller störning.
- Det genomförs en regelbunden och systematisk uppföljning av informationssäkerhetsarbetet som en del i internrevisioner för det övergripande ledningssystemet. Genom interna revisioner kan avvikelser påpekas men ansvaret för åtgärder följer verksamhetsansvaret. Det finns inga kontrollområden avseende information- eller IT-säkerhet i internkontrollplaner för 2020. Vi anser att det är en brist då den kan utgöra en viktig uppföljning över hur de verksamhetsansvariga har säkerställt att de lagar och regler samt interna styrdokument efterlevs i respektive avdelning/område.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen att:

- Säkerställa att avdelningar och områden tillsätter resurser och tar sitt ansvar för det systematiska informationssäkerhetsarbetet i enlighet med ledningssystem för informationssäkerhet.
- Säkerställa att informationsklassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.
- Säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.
- Riskanalyser upprättas regelbundet för IT-infrastruktur och drift.
- Upprätta en riskanalys över att privata enheter kan ansluta via fjärraccess till regionens IT-miljö och utifrån dessa risker fatta beslut om relevanta åtgärder för att möta dessa.
- Uppdatera kontinuitetsplan för IT-driften.
- Besluta om regionövergripande rutin för incidenthantering och rapportering för informationssäkerhetsincidenter samt kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av samtliga inträffade incidenter så att dessa kan beaktas i förbättringsarbetet.
- Säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.

2 Bakgrund

KPMG har av de förtroendevalda revisorerna i Region Jämtland Härjedalen fått i uppdrag att genomföra en granskning av regionens arbete med sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2020.

Det övergripande syftet med informationssäkerhet är att säkerställa att information hanteras med utgångspunkt i sekretess, integritet och tillgänglighet till information för medarbetare och intressenter till regionen. Hög IT-säkerhet är grundläggande för till exempel all hantering av patientdata. Där det är möjligt kan detta ske genom ändamålsenliga tekniska kontroller men även andra former av kontroller kan användas.

Organisationer i offentlig sektor blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker. Kommunikationen med omvärlden ökar i omfattning och systemen blir mer integrerade, såväl inom regionen som med andra intressenter. Utvecklingen av nya e-tjänster inom vården ställer ytterligare krav på säkra IT-system. Digitala e-tjänster innebär att verksamheter öppnar upp och exponerar sin interna IT-miljö mot externa IT-miljöer. Detta ställer krav på genomtänkta riskanalyser och ett väl fungerande säkerhetsarbete.

Den globala hotbilden med risker för intrång förändras kontinuerligt. Informationen måste skyddas mot obehörig åtkomst, såväl externt som internt samtidigt som den skall finnas tillgänglig och dessutom vara tillförlitlig -rätt information i rätt tid och för rätt personer.

Regionens revisorer genomförde en förstudie av IT-säkerhet/informationssäkerheten 2016 där det konstaterades att det pågick ett aktivt arbete mot målet att säkerställa informationssäkerheten. Det fanns dock en mängd kända brister av varierande allvarlighetsgrad.

Regionens revisorer har mot bakgrund av sin risk-och väsentlighetsanalys bedömt det angeläget att genomföra en granskning av IT-säkerheten.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen har varit att svara på om regionens organisation och interna kontroll är ändamålsenlig gällande IT-säkerhet.

Granskningen har besvarat följande revisionsfrågor:

- Finns det en övergripande styrning av informations-och IT-säkerhet inklusive styrande dokument?
- Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?
- Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?
- Sker säkerhetsklassning av funktioner och tjänster?
- Finns ändamålsenliga rutiner för behörigheter och lösenord? Inkluderar även leverantörer av enskilda system.
- Har regionen en ändamålsenlig incidenthanteringsprocess?

  - Upptäcks och hanteras icke önskvärda incidenter både internt och externt?
  - Finns det rutiner för att säkerställa att nya risker och hot identifieras och hanteras?

- Är medborgarnas integritet säkerställd (patientdatalagen) och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?
- Är känsliga patientdata lagrade på ett säkert sätt, till exempel genom kryptering?
- Är det säkerställt att personal som hanterar lagring och hantering av känsliga uppgifter om enskilda patienter har den utbildning i informationssäkerhet som behövs utifrån tilldelade arbetsuppgifter?
- Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Granskningen omfattar regionstyrelsen för revisionsåret 2020.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen (2017:725)
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2013)
- Internationella standarder enligt COBIT (Control Objective for Information and Related Technology Standards) avseende informationssäkerhet.

2.3 Metod

Granskningen har genomförts genom dokumentgranskning, intervjuer samt kartläggning av arbetsprocesser och rutiner för ett systematiskt informations-och IT-säkerhetsarbete.

Intervjuer har genomförts med:

- Regiondirektör
- Stabschef
- Beredskapschef
- IT-chef, IT och e-hälsoavdelningen
- Enhetschef e-hälsoavdelningen
- Enhetschef IT-enheten
- Kommunjurist tillika dataskyddsombud
- Kvalitetsstrateg

- Informationssäkerhetssamordnare
- IT-säkerhetsansvarig
- Förvaltningsledare IT Cosmic

Dokument som granskats anges löpande i rapporten och återfinns även i bilaga 1.

Bedömning av arbetet bygger på KPMG:s beprövade informationssäkerhetsramverk, *Cyber Maturity Assessment* (CMA) vilken utgår från IS27001. Analysen omfattar sex områden:

- Ledarskap och styrning
- Mänskliga faktorer
- Information och riskhantering
- Kontinuitetshantering
- Drift och teknik
- Regelefterlevnad.

Granskningen har genomförts av Jenny Thörn, kommunal revisor, Uppdragsledare har Sara Linge, certifierad kommunal revisor varit och Veronica Hedlund Lundgren, certifierad kommunal revisor har deltagit i sin roll som kvalitetssäkrare.

3 Lagrum

I arbetet med informations- och IT-säkerhet finns ett antal lagar som behöver beaktas. Vi redogör kort för den som en bakgrund till resultatet då hänvisningar finns till dessa i rapporten.

3.1.1 Dataskyddsförordningen (The General Data Protection Regulation)

Dataskyddsförordningen (GDPR, The General Data Protection Regulation) trädde i kraft den 25 maj 2018 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.

3.1.2 Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

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.

3.1.3 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.

3.1.4 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:

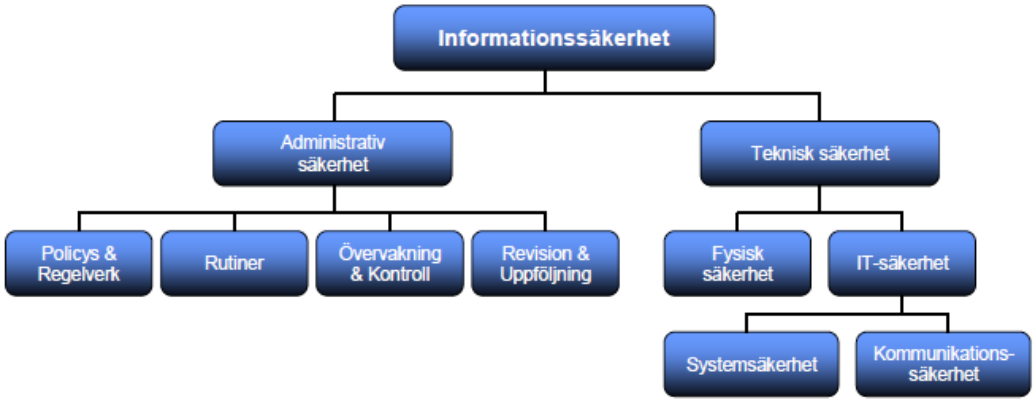
- Inre sekretess – en reglering som innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter. Detta förtydligas genom att det i lagen ställs krav på behörighetstilldelning och åtkomstkontroll.
- Sammanhållen journalföring, vilket innebär att 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.

4 Resultat av granskningen

4.1 Ledarskap och styrning

4.1.1 Policy och styrande dokument

IT-säkerhet är underordnat informationssäkerhet enligt nedan. Av detta följer att beslut om IT-säkerhet styrs av beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter eller liknande styrdokument.



Informationssäkerhetsarbetet styrs av regionens ledningssystem för informationssäkerhet utformat utifrån ISO/IEC 27000 och organisationens verksamhetskrav samt gällande författningar. Det finns en processbeskrivning av *Ledningssystem för Informationssäkerhet*[1] i vilken det framgår att inriktning och övergripande mål för regionens informationssäkerhetsarbete finns i *Policy för informationssäkerhet*[2].

Enligt policyn är mål för informationssäkerheten:

- Säker och riskbaserad informationshantering
- God informationssäkerhetskultur
- Effektiv incidenthantering
- Robust informationshantering
- Informationssäkerhetsberättelse och handlingsplan.

Inspektionen för vård och omsorg (IVO) som är tillsynsmyndighet för samhällsviktig verksamhet inom vård- och omsorg, genomförde under våren 2019 en inspektion av ledningssystemet för informationssäkerhet utifrån NIS-direktivet och motsvarande svensk lagstiftning (lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster). IVO identifierade inte några brister i regionens informationssäkerhetsarbete.

[1] Godkänd av Mikael Ferm, giltigt fr.o.m. 2020-07-20.
[2] Fastställd av Regionfullmäktige 2020-11-24 – 25§ 124

Informationssäkerhetspolicyn gäller för regionens bolag, stiftelser och för de som arbetar på uppdrag av regionen. Externa utförares ansvar styrs genom avtal. Vidare framgår att det övergripande ansvaret för informationssäkerhet inom de olika förvaltningsområdena vilar på den nämnd och styrelse som ansvarar för området. Det beskrivs även som viktigt att utse ansvariga informationsägare som bland annat ska klassificera informationen, ställa säkerhetskrav och bedöma risker.

Det finns upprättade *Informationssäkerhetsregler för anställda* som beskriver medarbetarnas ansvar för att skydda informationstillgångarna. Bland annat finns beskrivningar av ansvar för hantering av lösenord och när det behövs hjälpmedel för autentisering (flerfaktorsinloggning som en säkerhetsåtgärd). Det framgår vidare att medarbetarna ansvarar för att datorer eller andra informationsbärare som har använts inte lämnas utan att patientuppgifterna, sekretessklassade uppgifter eller annan känslig information är skyddade från obehörig åtkomst. Men också att medarbetarna endast tar del av den patientinformation/övrig sekretessklassad och känslig information som behövs för att utföra sitt arbete.

Begreppet IT-säkerhet nämns inte i policyn. I processbeskrivningen definieras begreppet IT-säkerhet som ”IT-stödets förmåga att tillgodose de krav på skyddsnivåer som verksamheten ställer”.

Det finns utkast till *Riktlinjer för IT-säkerhet* daterade 2020-10-15. Syftet med riktlinjerna anges vara att bidra till att upprätthålla ett grundläggande skydd av regionens digitala informationstillgångar, tillhörande system och enheter. Ansvarig för dokumentet är IT-säkerhetsansvarig. I intervjuer beskrivs att planen var att dokumentet skulle fastställas i januari 2021 men att arbetet är något fördröjt. Dokumentet följer i stora delar MSB:s föreskrift (2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Det finns beslutade *Regler för säkerhet IT-infrastruktur*[3]. Syftet med dokumentet anges vara att ge målgrupperna stöd och vägledning i det praktiska IT-säkerhetsarbetet kring IT-infrastrukturen. Målgrupp för dokumentet är regionens IT-personal, extern IT-driftsleverantör, tredjepartsleverantörer samt regionens systemägare och systemansvariga. Det framgår vidare att respektive verksamhetssystems säkerhetsnivåer ska beskrivas i en systemsäkerhetsplan för varje system.

En *IT-säkerhetsplan* finns, daterad 2020-12-07 som IT-säkerhetsansvarig ansvarar för. Planens syfte är att regionen systematiskt ska kunna planera för IT-säkerhetshöjande åtgärder, såväl tekniska som organisatoriska. Planen sträcker sig över tre år och baseras på en självskattning för cybersäkerhetskontroller. I planen återfinns de områden som regionen behöver fokusera på under åren 2021–2023.

I *Riktlinjer digitalisering*[4] återfinns en kortare hänvisning till informationssäkerhet och IT-säkerhet. Det framgår att informationssäkerhet utgår från verksamhetens krav på säker informationshantering baserat på verksamhetens mål. Vidare framgår vikten av att berörda (patienter, brukare, medarbetare och invånare) ska kunna lita på informationen som avser dem och att den informationen hanteras säkert, är korrekt och att den personliga integriteten inte kränks. Att patientinformationen dessutom måste skyddas mot förlust, obehörig åtkomst och oönskad förändring står också utskrivet där

[3] Godkänd av Thomas Nesterud och giltig from. 2015-03-09.
[4] Beslutad av Regiondirektör 2019-11-06

IT-säkerhet är de tekniska lösningar som krävs för att de krav på skyddsnivåer som verksamheten ställer ska tillgodoses.

De dokument som betraktas som de mest väsentliga enligt intervjupersonerna är framförallt informationssäkerhetspolicyn och de som berör ansvar och befogenhet samt informationssäkerhetsregler för anställda.

Som komplement till ovan nämnda styrande dokument finns ett stort antal styrande och stödjande dokument avseende dataskyddsarbetet, hantering och krav för mobila enheter, molnbaserad lagring mm.

Registerkoodinatorerna används som informationskanal för att till exempel sprida styrdokumenten. Det sker en viss uppföljning av styrdokumenten och ansvaret beskrivs ligga på ledningssystemet och till stor del inom ordinarie verksamhetsansvar.

4.1.2 Roller och ansvar

I intervjuerna beskrivs säkerhetsarbetet (dataskydd och informationssäkerhet) som ett regionövergripande uppdrag. I uppdraget ingår att ansvara för att styrdokument finns på plats samt stödja, samordna och leda arbetet.

Det styrande dokumentet *Fördelning av ansvar för informationssäkerhet*[5] anger hur det organisatoriska ansvaret ser ut. I dokumentet beskrivs ansvarsfördelning mellan regionfullmäktige, regionstyrelsen och nämnderna, regiondirektören, hälso- och sjukvårdsdirektör, regional utvecklingsdirektör, regionstabschef, avdelningschef och områdeschef, enhetschef samt bland medarbetare. Vidare beskrivs övriga ansvarsroller och stödjande funktioner med specialistkompetens inom informationssäkerhet. Rollerna dataskyddsombud (DSO), biträdande DSO samt registerkoordinatorer (RK), systemägare, registerägare (RÄ) samt informationsägare förtydligas.

En stor del av informationssäkerhetsansvaret återfinns i linjeorganisationen som informationsägare för den information som hanteras. Av ansvarsdokumentet framgår att Områdeschef/Avdelningschef ansvarar för informationssäkerheten samt att organisera arbetet inom den egna verksamheten. I praktiken innebär det att linjecheferna ansvarar för att:

- informationsklassning/riskanalys genomförs för information som hanteras i gemensamma IT- system eller när nya IT system/tjänster ska införas
- i samverkan med andra områden vara kravställare mot berörda systemägare/registerägare så att systemen/registren uppfyller informationssäkerhets- och dataskyddskraven.
- kontinuitetsplaner för informationssäkerhet upprättas och kommuniceras
- underställda chefer och medarbetare får nödvändig information och utbildning i informationssäkerhet
- utse en registerkoordinator (RK) för sitt område/avdelning.

[5] Beslutad av Regionstabschef 2018-06-01

Registerkoordinatorerna uppdrag är att löpande uppdatera och hantera verksamhetens personuppgiftsbehandlingar, bistå vid begäran om registerutdrag samt bistå med grundläggande stöd och vägledning till sin avdelning i frågor om dataskydd.

Att införa registerkoordinatorer var ett beslut som fattades utifrån tidigare uppföljningsarbete för informationssäkerhet och dataskydd där behovet av detta identifierats. I intervjuer beskrivs att det inte i nuläget finns någon motsvarande roll som samordnar områdets/avdelningens informationssäkerhetsarbete. Av intervjuer och dokumentation vid uppföljning för 2020 framgår att rollen som informationsägare behöver tydliggöras och definieras. Det finns beskrivet att rollen, när detta är gjort, ska införas under 2021.

Informationssäkerhetsarbetet är organiserat inom enheten för krisberedskap, säkerhet och miljö, som tillhör samordningskansliet på Regionstaben. Ansvarig för staben är stabschef som rapporterar till regiondirektören. Vid intervjuer framkommer att det finns möjlighet att lyfta frågor till regiondirektör via regionens säkerhetsråd som är ett rådgivande organ.

Informationssäkerhetssamordnare finns som resurs i arbetet. Enligt *Fördelning av ansvar för informationssäkerhet* har informationssäkerhetssamordnaren i uppdrag av regiondirektören att ansvara för att:

- samordna regionens strategiska informationssäkerhetsarbete i enlighet med regionens policy för informationssäkerhet och dataskydd.
- utarbeta årlig plan för aktiviteter inom informationssäkerhetsarbetet.
- utarbeta årlig informationssäkerhetsrapport till vårdgivaren avseende riskanalyser, incidenter, uppföljningar samt förbättringsåtgärder.
- ta initiativ till arbete med att arbeta fram policy, regler och rutiner inom området
- ta initiativ till att utbildning tas fram och genomförs inom organisationen
- ta initiativ till och genomföra säkerhetsrevisioner
- bevaka och sammanställa informationssäkerhetsincidenter
- följa upp att föreskrifter för informationssäkerhet efterlevs
- omvärldsbevaka informationssäkerhetsområdet
- bistå informationsägare med stöd att genomföra informationsklassningar och riskanalyser inom informationssäkerhetsområdet
- i samverkan med IT-säkerhetsansvarig samordna informationssäkerhetsarbetet gentemot regionens systemägare för att få enhetlig utformning och nivå på de olika verksamhetssystemens säkerhetsåtgärder/-funktioner
- bistå DSO samt verksamhet med kompetens inom dataskydd till exempel att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen, bistå registerägare och informationsägare med att identifiera rätt skyddsåtgärder för personuppgifter baserat på informationsklassning samt ge råd vid genomförande av konsekvensbedömning för dataskydd.
- vara sammankallande i informationssäkerhetsrådet.

Intervjupersoner beskriver att rollen väl stämmer överens med den beskrivning som finns i dokumentet. Det finns dock delar av uppdraget som är svåra att genomföra då det till viss del saknas resurser i linjeverksamheten för att genomföra de uppdrag och ansvar som beskrivs för avdelningschefer/områdeschefer. Då det inte finns några utsedda representanter som kan utgöra ett stöd till cheferna i det systematiska informationssäkerhetsarbetet så sker i nuläget en stor del av arbetet både på strategisk och operativ nivå av informationssäkerhetssamordnaren.

Avdelningen för IT och e-hälsa är också organiserade under Regionstaben och leds av en IT-chef. Det finns enhetschefer för respektive enhet, för e-hälsa och för IT. På IT-enheten finns en IT-säkerhetsansvarig som enligt *Fördelning av ansvar för informationssäkerhet* har till uppgift att införa förebyggande skyddsåtgärder för att undvika IT-säkerhetsincidenter som hotar verksamhetens informationshantering.

I uppgifterna ingår att:

- löpande initiera och genomföra säkerhetshöjande förbättringsåtgärder för IT-infrastrukturen, baserat på kraven för regionens verksamhetssystem
- handlägga auktorisationer av nya och uppgraderade IT-system för godkännande innan de anskaffas och införs i IT-miljön
- genomföra risk- och sårbarhetsanalyser av specifika delar i IT-miljön utifrån bland annat ställda verksamhetskrav på informationssäkerhet
- löpande analysera och följa upp rapporterade IT-säkerhetsincidenter och utifrån dessa initiera säkerhetshöjande åtgärder
- vara konsultativ resurs för verksamheter som har behov av att utforma säkerhetshöjande åtgärder i IT-system
- agera kravställare säkerhet och säkerhetsrevisor på extern IT-driftleverantör som innehar avtal för regionens IT-drift
- samordna IT-säkerhetsarbetet gentemot regionens systemägare för att få enhetlig utformning och nivå på de olika verksamhetssystemens säkerhetsåtgärder/-funktioner
- bistå DSO med kompetens inom dataskydd till exempel att arbeta för att införa säkerhetsåtgärder enligt dataskyddslagstiftningen

IT-driften beskrivs i intervjuer vara mer eller mindre helt outsourcad och att regionen som kravställare därför behöver säkerställa att de externa IT-driftleverantörerna lever upp till en god informationssäkerhet enligt kraven i ISO27001/27002. Detta finns även dokumenterat i dokumentet *Regel för säkerhet IT-infrastruktur*. I intervjuer beskrivs att IT-säkerhetsansvarig har möten med leverantörer varje månad för genomgång och uppföljning.

E-hälsoenheten ansvarar bland annat för vårdinformationssystemet Cosmic och en förvaltningsledare IT finns utsedd.

En arbetsgrupp för informationssäkerhet finns där IT-säkerhetsansvarig ingår. Ett tidigare informationssäkerhetsråd som bildades 2017 som finns beskrivet i dokumentet *Fördelning av ansvar för informationssäkerhet* ska enligt

informationssäkerhetsberättelse för 2019 avvecklas. Frågorna ska därefter fördelas i andra råd och grupperingar, däribland ett nyinrättat informationsförvaltningsråd.

Det framgår även av intervjuerna att det finns områden med utvecklingspotential. I dagsläget saknas en digitaliseringschef och en informationssäkerhetschef på motsvarande nivå som IT-chef. Vidare beskrivs att det finns behov av att arbeta mer med strategisk styrning av informationssäkerhet och IT-säkerhet då resurser inte är tillräckliga för de aktiviteter som det finns behov och ambition av att genomföra.

4.1.3 Informationssäkerhetsberättelse 2019

Informationssäkerhetsberättelse och övergripande handlingsplan för informationssäkerhet utgör delar av målen för regionens informationssäkerhetsarbete enligt beslutad policy.

Eventuellt verksamhetsspecifika styrande dokument ska enligt policyn utformas i enlighet med de regiongemensamma dokumenten. Organisationens verksamhetskrav samt gällande författningar är därtill styrande för arbetet enligt policyn.

Det framgår i intervjuer att informationsberättelsen för 2020 är under bearbetning. Vi har därför i granskningen tagit del av *Informationssäkerhetsberättelse 2019* [6]som ligger till grund för den övergripande handlingsplanen för 2020–2021.

4.1.4 Övergripande handlingsplan för informationssäkerhet 2020–2021

Övergripande handlingsplan för informationssäkerhet och dataskydd 2020–2021[7] har framställts av enheten för krisberedskap, säkerhet och miljö. Syftet med handlingsplanen beskrivs vara att säkerställa ett systematiskt informationssäkerhetsarbete och handlingsplanen tillsammans med informationssäkerhetsberättelsen utgör mål i informationssäkerhetspolicyn.

Arbetet ska bidra till att uppnå en ökad robusthet och förmåga i regionens informationshantering.

I handlingsplanen utrycks att:

> *”Det finns allvarliga risker förknippat med ett bristande informationssäkerhetsarbete. Detta gäller inte minst inom hälso- och sjukvården där känsliga personuppgifter hanteras. Dataskyddslagstiftningen är numera mycket långtgående i sina krav på att personuppgifter kan hanteras på rätt sätt. Om så inte sker kan höga viten utdömas och skadeståndsanspråk kan ställas från enskilda personer mot regionen.”*

Handlingsplanen inbegriper mål och de aktiviteter som ska möjliggöra att målen uppfylls i regionens tre förvaltningsområden. Det är vardera förvaltningschef som bär ansvar för att informationen i handlingsplanen beaktas i förvaltningsområdenas verksamhetsplanering.

Av handlingsplanen för åren 2020–2021 finns ett antal förbättringsåtgärder presenterade i syfte att utveckla regionens informationssäkerhetsarbete. Bland annat beskrivs behov av att utveckla styrning och kontroll över behörigheter till kritiska IT-

[6] Beslutad av Regionstyrelsen § 59 2020-04-29
[7] Beslutad 2020-01-14, RS/697/2019

system och till känslig information, att chefer ska få ett utökat stöd för att klara sina ansvarsområden för informationssäkerhet samt att regionens samhällsviktiga verksamheter har en fungerande avbrottshantering för sina kritiska IT-system. Vad gäller IT-säkerhet framgår av handlingsplan för regionstabens mål och aktiviteter att krav på skydd mot cyberattacker ska finnas etablerade 2021.

Handlingsplanen följs enligt dokumentets beskrivning upp kontinuerligt via tertialrapport, delårsrapport och årsbokslut. Regionstabschef bär ansvaret för uppföljningen med stöd av ansvarig verksamhetsstrateg för respektive handlingsplan, för informationssäkerhet är det informationssäkerhetssamordnaren som bistår regionstabschef.

4.1.5 Bedömning

Vår bedömning är att det finns en övergripande styrning genom ett implementerat ledningssystem för informationssäkerhet. I ledningssystemet finns en dokumenterad ansvarsfördelning och organisation för arbetet som tillsammans med styrande dokument har tydliggjort hur arbetet ska bedrivas.

Det finns beslutade regler för IT-infrastruktur och det pågår ett arbete för att uppdatera styrande dokument avseende IT-säkerhet i form av en ny riktlinje. Av det utkast vi tagit del av är dessa framtagna i enlighet med den av MSB nyligen beslutade föreskriften som gäller för säkerhetsåtgärder. Vi anser att dokumentet, när det fastställs, ytterligare tydliggör hur arbetet med IT-säkerhet är tänkt att bedrivas i regionen.

Vi noterar att det finns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som utpekas i dokumenterad ansvarsfördelning inte uppfylls av avdelnings- och områdeschefer. Vi konstaterar att det till stor del beror på att det upplevs saknas resurser som kan utgöra ett stöd till cheferna för det praktiska arbete som behöver ske i respektive förvaltning och enhet. Vi ser det som positivt att det finns upptaget i ”handlingsplan för åtgärder” att säkerställa ett utökat stöd till cheferna för att de ska få bättre förutsättningar för sitt informationssäkerhetsarbete. Vår bedömning är därtill att det finns risk att organisationen är sårbar då det i nuläget vilar ett stort ansvar för både det strategiska och operativa arbetet på de nyckelpersoner som leder arbetet med informationssäkerhet och IT-säkerhet. Vid eventuella personal- eller organisationsförändringar kan det leda till kontinuitet och kunskap går förlorad.

En informationssäkerhetsberättelse tas fram som underlag för beslut om åtgärder och prioriteringar för att förbättra informations- och IT-säkerhetsarbetet. Åtgärder samlas i en övergripande handlingsplan där mål, ansvar och tid för genomförande anges. Handlingsplanen beskriver på ett tydligt sätt vad respektive förvaltning behöver arbeta med under en kommande tvåårsperiod för att utveckla regionens informations- och IT-säkerhetsarbete.

4.2 Mänskliga faktorer

En viktig del i ett systematiskt informations- och IT-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till regionens information. I regionen är detta bland annat förtroendevalda, medarbetare, patienter, medborgare och externa konsulter.

4.2.1 Medarbetarnas kunskap och medvetenhet

I arbetet med behandling av personuppgifter har regionen utfört ett antal insatser för att säkerställa att medarbetare har kunskaper för att till exempel hantera känslig information. Det framgår i en av intervjuerna att medarbetare ska gå den obligatoriska utbildningen i kompetensplattformen ”SABA” och att uppföljning sker av vilka som har genomfört den.

Under intervjuerna framgår dock att deltagandet varit mycket lågt vilket ledningsgruppen har informerats om i december 2020.

Behov av utbildningsinsatser finns upptaget i den övergripande handlingsplanen och gäller för alla förvaltningar under åren 2020–2021. Som mål anges att e-utbildning för medarbetare i informationssäkerhet ska ha fullföljts av 80 % av medarbetarna 2020-12-31. I uppföljningen i december 2020 framgår att endast 21 % inom Regionala utvecklingsnämnden genomfört utbildningen och 26 % i övriga regionens verksamheter. Målet som anges ska uppnås fram till 2021-12-31 är 95 %. För nya medarbetare är målet att de ska ha genomgått e-utbildningen senast 3 månader efter att de påbörjat sin tjänst inom regionen. Det lyfts även att det skulle behövas ytterligare utbildning för utsedda registerkoodinatorer, för förvaltningsansvariga (inom systemförvaltningen) och för chefer specifikt.

Vid behov har information givits till medarbetare och förtroendevalda om risker i form av e-post med uppsåt att ta del av användaruppgifter eller med innehåll som kan skada regionens IT-miljö. Det har även tagits fram regler för hantering av lagring i molntjänster för att tydliggöra en korrekt informationshantering men det går inte att fastställa i hur hög grad medarbetare har tagit del av information och regler.

4.2.2 Bedömning

Vår bedömning är att det inte är säkerställt att medarbetare har fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar generellt.

De utbildningsinsatser som avser informationssäkerhet och GDPR har endast givits till en mindre andel av regionens medarbetare för att vi ska anse att det finns en etablerad säkerhetsmedvetenhet. Förutom de lagkrav som finns att efterleva introduceras även nya risker i form av nya arbetssätt och möjligheter till lagring i molntjänster. Detta leder till ökade risker att information hanteras felaktigt och det ställer ytterligare krav på att etablera en tillräcklig medvetenhet och mognad av informationssäkerhetsarbetet.

Vi noterar att den plan för introduktion av nya medarbetare som avses användas vid nyanställningar innehåller moment för att medarbetarna ska få information om regler och utbildning i informationssäkerhet och personuppgiftshantering. Ansvaret för att

detta ska genomföras finns hos ansvarig chef och det sker i nuläget inte någon uppföljning av hur introduktionsprogrammet genomförs. De utbildningsinsatser som avser informationssäkerhet och GDPR har dock endast genomförts av ca 25 % av det totala antalet medarbetare i regionen.

4.3 Information och riskhantering

4.3.1 Informationsklassning

Regionen har beslutat om *Regel för informations- och systemklassificering*[8]. Denna regel beskriver modell för informationsklassificering samt när och hur modellen ska tillämpas. Den beskriver även modell för klassning av IT-system och tjänster (baserat på systemets informationsinnehåll).

Det framgår av regeldokumentet att informationsklassificering tillsammans med risk- och konsekvensanalyser ska genomföras för att relevanta beslut om hanteringsregler (skyddsnivåer) för informationstillgångar och system/tjänst ska kunna fattas.

Konkreta användningsområden för informations- och systemklassificering är;

- Vid kravställning/kravspecificering inför anskaffning/utveckling av IT-system/IT-tjänst
- Vid framtagning och efterlevnad av kontinuitetsplaner för verksamheten – där tillgång till information är avgörande för verksamhetens kontinuitet
- Vid genomförande av riskanalyser av enskilt IT-system
- Vid genomförande av riskanalyser avseende informationsflöden
- Vid framtagning av hanteringsregler för information, till exempel avseende krav på kryptering av e-post, regler för och eventuell märkning av intern och extern post, kommunikation via mobiltelefon mm.

Vidare beskrivs i reglerna att det är viktigt att fastställa ansvaret för informationstillgångarna eftersom informationen hanteras på en mängd olika sätt idag via olika aktörer, till exempel via avtal om outsourcing eller via olika typer av molntjänster. I den typen av lösningar måste det vara klarlagt för alla parter vem som äger informationen och därmed är kravställare på leverantören. Informationsägare ska vara utsedda för informationstillgångar och ska ansvara för att information klassificeras enligt den modell som regionen beslutat.

Informationsklassificeringen ska leda till att informationsägaren får möjlighet att ställa säkerhetskrav på IT-system/IT-tjänster. Alla IT-system och tjänster (till exempel applikationer och molntjänster) ska enligt reglerna för klassning klassificeras innan införande.

Det framgår av intervjuerna att det finns utmaningar i arbetet med informationssäkerhetsklassningar och att det i dagsläget inte bedrivs något aktivt klassningsarbete. Det framgår att ansvaret för informationsklassning ligger i linjen vilket även framgår av ansvarsfördelningen i styrande dokument. Utmaningen beskrivs bero

[8] Fastställd av Mikael Ferm, samordningskansliet 2015-08-13 (arbetsversion enligt dokumentet)

på dels en resursbrist dels en kompetensbrist men framförallt sägs det vara en organisatorisk utmaning som tycks bero på otydligt mandat och bristande stöd.

Utifrån intervjuer noterar vi att det vid sidan om arbetet med informationssäkerhet finns stora behov av att utveckla regionens systematiska systemförvaltning där införande av en ny systemförvaltningsmodell pågår. Av presentationen ledningens genomgång som genomfördes för regionledningen i december 2020 framgår att arbetet är alltför personberoende för nyckelroller samt att en ansvarig förvaltare för systemförvaltningsmodellen behöver utses för att säkerställa vidareutveckling och utbildning inom systemförvaltningen. Arbetet har påbörjats men är i en uppstartsfas och har inte ännu gett någon effekt. Även bristen på detta anges som en orsak för att inte systemsäkerhetsplaner finns framtagna där klassning och riskanalyser kan utgöra en viktig del.

I informationssäkerhetsberättelsen 2019 framgår att en prioriterad åtgärd är att revidera regionens informationsklassningsmodell inklusive hanteringsregler genom att arbeta enligt MSB:s metodstöd för informationssäkerhet samt att regionen behöver etablera arbetssättet med informationsklassning och hanteringsregler i verksamheterna genom utbildning.

4.3.2 Riskanalyser

Intervjupersoner uttrycker att det inte finns rutiner att upprätta riskanalys för nya system. De som genomförs sker uteslutande vid stora införanden, till exempel vid implementeringen av Office 365. Vid intervjuer framkommer också att riskanalyser skulle behöva utföras men att det inte finns tillräckligt med personella resurser.

Regionen har genomfört ett antal riskanalyser för IT-infrastrukturen med hjälp av externa konsulter.

- Under 2018 genomfördes en riskanalys avseende säkerhet i regionens externa webbservrar, brandväggslösning och nätverk för att bedöma nuvarande uppsättning och hur eventuella intrång skulle kunna ta sig vidare i nätverk och system och utgöra ett hot mot driften eller informationstillgångarna. Ett antal åtgärdsförslag presenterades i rapporten.
- Under 2019 genomförde en extern konsult en riskanalys gällande regionens riskexponering för IT- och informationssäkerhetsrisker från leverantörer.
- Under 2019 gjordes en nulägesanalys med riskidentifiering utifrån regionens följsamhet till NIS-direktivet. Analysen baserades på en vedertagen modell Cyber Assessment Framework som är framtagen av Brittiska NCSC[9]. Analysen bestod av ca 40 utvärderingsområden med följande huvudområden:
    - Hantering av säkerhetsrisker
    - Försvar mot cyberattacker
    - Detektering av cybersäkerhetsevent
    - Minimera effekterna av cybersäkerhetsincidenter

[9] National Cyber Security (https://sv.qaz.wiki/wiki/National_Cyber_Security_Centre_(United_Kingdom))

Utifrån analysen har ett antal åtgärdsförslag tagits fram. Dessa har bedömts omfattas av sekretess vilket innebär att vi inte har tagit del av denna information. Enligt intervjupersoner pågår arbetet för att möta de risker som identifierats vilket även framgår av informationssäkerhetsberättelsen 2019 som en prioriterad åtgärd.

4.3.3 Åtkomsthantering och behörigheter

I *Regler för behörighetshantering IT-system*[10] beskrivs att behörighetsprocessen innefattar följande delar:

- Åtkomst
- Beställning och attest
- Tilldelning/borttag
- Kontroll

Regelverket lyfter även målgrupper, begreppsdefinitioner, roller, grundprinciper för behörighetshantering och principer för hantering av behörigheter. Regeln ska ses som övergripande för regionens samtliga IT-system.

Det framgår av reglerna att roller ska separeras i de sammanhang där det är möjligt (utifrån tillgänglig personal) för att undvika fel och otillåten manipulation. Det innebär att behörighetsbeställare inte får vara samma person som behörighetsgodkännare. Vidare finns ett antal grundprinciper fastlagda för att säkerställa att hög säkerhet uppnås i behörighetshanteringen.

Ett flertal bilagor återfinns också, däribland två checklistor avsedda för behörighetstilldelning och för uppföljning av tilldelade behörigheter.

Behörighet för åtkomst i regionens IT-infrastruktur beskrivs i intervjuer. Kontroll och information om höga behörigheter finns i regionens Active Directory[11]. Active Directory följer *The Administrative Tier Model* avseende administrativa behörigheter i domänen. Det innebär en skiktad modell i tre lager för administrativa behörigheter. Detta gäller samtliga administrativa användare oavsett dessa är anställda eller externa leverantörer. De högsta behörigheterna innehas av ett fåtal personer. Loggar från Active Directory, servrar, klienter och nätverkskomponenter skickas till regionens centrala SIEM[12] för analys och larmhantering.

Tredjepartsrisker är de risker som verksamheten exponeras mot eller kan exponeras mot som ett resultat av ett avtal med en annan part. Ofta benämns tredjepartsrisker i samband med utkontraktering eller outsourcing, det vill säga när en region sluter avtal med en leverantör om att utföra (helt eller delvis) en process, tjänst eller annan aktivitet som regionen i annat fall själv skulle utföra. Vi har i granskningen inte tagit del av avdelningarna och områdenas hantering av behörigheter för externa leverantörer för enskilda verksamhetssystem.

[10] Godkänd av Anna-Lena Alfreds, giltig fr.o.m. 2017-05-15
[11] En katalog för samlad information om IT-objekt i en miljö
[12] Security information and event management, en tjänst för att sammanställa och analysera information från IT-säkerhetssystem.

Det framkommer i intervjuer att IT-enheten har outsourcat hela IT-driften. Det innebär att de leverantörer som behöver tillgång till regionens IT-miljö behöver ha höga behörigheter. Som en säkerhetsåtgärd avseende åtkomst till datacenter samt känsliga uppgifter avseende IT-infrastrukturen har ett arbete skett för att begränsa dessa till ett fåtal.

Externa leverantörer får tillgång till det eller de system som de har i uppdrag genom avtal att arbeta med och tilldelning sker på liknande sätt som för regionens interna medarbetare på IT-enheten. De ansluter sedan via regionens VPN-lösning.

För åtkomsthantering för patienter som ska logga in i patientinformationssystem för att ta del av sina uppgifter används tvåfaktorsinloggning i COSMIC. Det är även ett krav vid inloggning via appen COSMIC NOVA. Inloggningen sker via plattformen för nationella journal via nätet-tjänsten 1177.

I rutinen *Linjechefs ansvar för behörighetshantering*[13] beskrivs det ansvar för behörighetshantering som faller på linjechef avseende behörigheterna som dess medarbetare tilldelas i regionens IT-system. Beroende på hur systemet förvaltas används begreppet IT-system respektive IT-objekt.

I rutinen framgår att linjechef för varje system/objekt behöver ha information om följande:

- Genomföra bedömning av behörighetsbehov
- Ansvara för att beställa behörigheter (om inte behörigheter tilldelas med automatik)
- Godkänna (attestera) behörigheter (då krav på attest finns)
- Följa upp och återgodkänna tilldelade behörigheter för aktuellt IT-system/IT-tjänst.
- Avsluta behörigheter. I rutinen framgår även en mer detaljerad förklaring till vad som ska göras inom varje ansvarsområde, hur ansvaret ska utövas samt rekommendationer till linjechef att upprätta en checklista.

Slutligen är det respektive systems/objekts informationsägare som ska tillhandahålla linjechef med aktuellt behörighetsregelverk.

Informationssäkerhetssamordnaren presenterade i december 2020 ”Ledningens genomgång” för regionstab och chefer. Avseende behörigheter framgår av informationen att regionen har brister i sin behörighetshantering. Den är enligt informationen ineffektiv och uppfyller inte gällande regelverk och krav enligt GDPR och Patientdatalagen. Vidare beskrivs att ansvariga chefer saknad stöd för uppföljning och kontroll av tilldelade behörigheter och att hanteringen i nuläget har låg grad av automation. Vilket leder till många manuella moment och en fördröjning vid förändringar hos medarbetare när de börjar, slutar eller byter arbetsuppgifter/avdelning. Det finns därtill en otydlighet i vem som har rättigheter att godkänna tilldelade behörigheter.

[13] Godkänd av Anna-Lena Alfreds, giltig fr.o.m. 2019-03-05

4.3.4 Loggkontroll

I *Förvaltningsorganisation logg- och åtkomstkontroll*[14] framgår att åtkomstkontroll infördes inom regionen under 2016–2017 via en så kallad central loggplattform. Som en del i arbetet bildades en organisation för loggkontroll under 2018 för att vidareutveckla och förvalta arbetssätt och verktyg för åtkomstkontrollen och loggplattformen. Åtkomstkontrollen beskrivs vara indelade i ett antal huvudprocesser:

- Regelverk för åtkomst
- Granskningsprocessen
- Överträdelseprocessen
- Uppföljningsprocessen
- Utlämningsprocessen – patientens loggutdrag

Vidare beskrivs den centrala loggfunktionen i förvaltningen där loggadministratörer ska finnas utsedda. Deras uppdrag innefattar logghantering vilket bland annat innefattar att stödja för att mäta efterlevnad i uppföljningsprocessen. Det framgår även vilka befattningar som ingår i förvaltningen av den centrala loggplattformen, däribland Hälso- och sjukvårdsdirektören. Utöver det beskrivs även vilket ansvar som faller under systemägarna vilket kretsar kring att det vårdadministrativa systemet kan anslutas till den centrala loggplattformen. Det är regionens hälso-och sjukvårdsdirektör som ansvarar för beslut om vilka vårdsystem som ska anslutas till central loggplattform och när detta ska ske.

I informationssäkerhetsberättelsen för 2019 framgår att det under 2019 har införts en ny version av loggverktyg för kontroll/uppföljning av åtkomster till det vårdadministrativa systemet COSMIC. Verktyget möjliggör en mer systematiserad och effektiviserad loggkontroll vilken ska bidra till högre efterlevnad av såväl GDPR som Patientdatalagen då det gäller att säkra rätt åtkomst till patientuppgifter.

I intervjuer beskrivs att loggkontroller och uppföljning sker var fjärde månad. Det rör sig om stickprov samt löpande loggranskning. Vid misstanke om obehörig åtkomst sker riktade kontroller. Beslut finns taget att 10 % av de anställda ska kontrolleras genom dessa stickprov. Uppföljningar dokumenteras i loggverktyget vilket innebär att de registreras direkt när de utförs. Vid avvikelser rapporteras dessa i avvikelsehanteringssystemet av respektive chef. Rör det sig om en större avvikelse kontaktas HR för stöd. Uppföljning att loggkontroller sker via årliga internkontroller.

I informationssäkerhetsberättelsen framgår att det under 2019 funnits tre fall av anmälda dataintrång i form av otillåten läsning av patientjournal. Ett av dessa ledde till polisanmälan men ärendet lades senare ner av polismyndigheten. I det andra fallet fanns inte bevis att fel begåtts och i det tredje var inte utredningen klar när rapporten vi tagit del av upprättades.

[14] Beslutad av regiondirektör 2018-04-11

4.3.5 Bedömning

Vår bedömning är att det inte pågår något systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar. Utifrån regionens definition av begreppet IT-säkerhet som ”IT-stödets förmåga att tillgodose de krav på skyddsnivåer som verksamheten ställer” så drar vi slutsatsen att den avsaknad av informationsklassning och riskhantering avseende verksamhetens information och system leder till att verksamheten inte i någon högre grad ställer egna krav på skyddsnivåer. IT-säkerhetsåtgärder inrättas därmed till stor del utifrån den kunskap och förutsättningar som IT-enheten har. Detta riskerar att införda säkerhetsåtgärder inte står i relation till hur skyddsvärd informationen som den avser att hantera är. För viss information kan vissa åtgärder vara för avancerade och därigenom kostnadsdrivande medan det för annan information inte kan fastställas att ett tillräckligt skydd finns då ingen klassning eller riskbedömning har gjorts av informationsägaren. De säkerhetsåtgärder som inrättats för IT-infrastrukturen ingår i regionens samlade skydd för information och IT utan att dessa utgår från kravställning från informationsägarna.

Vi bedömer att riskanalyser inom IT-säkerhet sker på ett delvis tillfredsställande sätt. Det finns ingen vedertagen modell för upprättande av riskanalys och i nuläget görs inte detta systematiskt för regionens IT-säkerhet. Det har upprättats analyser över sårbarheter för enskilda delar av IT-miljön för att identifiera brister som skulle kunna påverka kontinuiteten och förtroendet för regionens förmåga att skydda informationen. Vi anser dock att arbetet med riskanalyser kan utvecklas och utgöra ett underlag för prioritering av IT-säkerhetslösningar där dessa tar utgångspunkt från de mest väsentliga riskerna.

Vår bedömning är vidare att regionen inte har ändamålsenliga rutiner för behörigheter och lösenord. Det finns ett flertal styrande och stödjande dokument men vi noterar att dessa i praktiken inte får genomslag och att rutiner inte efterlevs i tillräckligt hög grad. Det är positivt att regionen själva identifierat detta och genomfört en förstudie samt återrapporterat till ledningen att detta behöver utvecklas för att uppnå en tillräcklig regelefterlevnad i enlighet med GDPR och Patientdatalagen. Den bristande behörighetshanteringen bedömer vi påverkar regionens förmåga att säkerställa medborgarnas integritet avseende patientinformation i journalsystem.

Vi bedömer hanteringen inom IT-enheten för behörigheter till externa leverantörer avseende IT-drift som ändamålsenliga. Relevanta åtgärder har vidtagits för att en högre säkerhet ska finnas. Det finns etablerade rutiner och processer för hanteringen och en tillräcklig loggkontroll som synliggör hur tilldelade behörigheter används. Vår bedömning har inte omfattat tilldelning av behörigheter för enskilda system där detta sker utifrån respektive verksamhets behov.

4.4 Kontinuitetshantering

I *Riktlinje för avbrottsplanering av kritiska aktiviteter och beroenden*[15] framgår syftet och målet med kontinuitetsplanering. I riktlinjen anges att ett oplanerat eller planerat avbrott med hjälp av reservrutiner i verksamheten ska:

- kunna upprätthålla verksamheten på en acceptabel nivå
- minimera avbrottstid och total störningstid
- mildra konsekvenser av avbrottet

Vidare beskrivs avbrottsplanering i riktlinjen som en planeringsprocess där robusthet i verksamheten skapas genom förebyggande arbete.

Dokumenten beskriver även processen för avbrottsplanering som bland annat inkluderar analyser av den ordinarie verksamheten. Vidare redogörs för organisationens uppdrag där det framgår att avbrottsplanering ska återfinnas i alla verksamheter.

Under en av intervjuerna framgår att regionen tidigare utförde ett antal övningar varje år men att så inte skett på senare tid. Det framgår vidare i intervjun att den nuvarande kontinuitetsplanen innehåller en prioriteringsordning med två återstartsgrupper. Det beskrivs dock att den samlade datan för IT-objekt som dokumenteras i regionens CMDB i nuläget inte är i tillräckligt bra skick för att kunna agera på.

Det framgår att det finns en bra systemdokumentation över datacenter och dess IT-komponenter men att flöden mellan system skulle behöva tydliggöras och dokumenteras för att fungera i tillräcklig grad om någon allvarlig störning skulle ske.

I intervjuer och i dokumentation som vi tagit del av framgår att avbrottsplanering och kontinuitetshanteringen behöver utvecklas inom vårdverksamheten för att säkerställa kontinuiteten för kritiska IT-stöd så att reservrutiner finns om oplanerade händelser sker som påverkar informationssystem eller IT-miljön i stort.

4.4.1 Kontinuitetsplan

I *Kontinuitetsplan för IT-infrastruktur*[16] beskrivs att planen ska tillämpas vid en uppkommen allvarlig störning som beträffar IT-infrastrukturen. Planen är avgränsad till att behandla IT-infrastrukturen vilket innebär att informationssystemen som är beroende av IT-infrastrukturen inte är inkluderade.

Planen är byggd på tre nivåer, vars nivåer är relaterade till varandra. Den övre nivån beskriver kraven på IT-infrastrukturen ställda av verksamheten och den andra nivån beskriver hur realiseringen av kraven går till genom framtagning av rutiner och metoder. Den tredje och sista nivån är mer operativ och består av diverse bilagor som till exempel behandlar aktuella rutiner och testplaner.

I avsnittet tillhörande organisation beskrivs bland annat roller, ansvar och befogenhet där det framgår att IT-säkerhetsansvarigs ansvar inkluderar samordning, styrning och uppföljning av landstingets (numera regionens) IT-miljö. Vidare fungerar denne som rådgivande till systemansvarig IT-infrastruktur.

[15] Godkänd av Mikael Ferm, giltig fr.o.m. 2020-10-03
[16] Godkänd av Thomas Nesterud, giltig fr.o.m. 2014-09-15

En powerpointpresentation finns framtagen som är döpt *Reservrutiner vid bortfall av IT-system*. Vi uppfattar att dokumentet är avsett för att utgöra ett stöd i verksamhetens upprättande av kontinuitetsplaner för sina verksamhetssystem och tillgång till verksamhetskritisk information. Men också hur IT-driftsleverantör och IT-enheten ska möta dessa i deras hantering för kontinuiteten på övergripande nivå.

I materialet anges två mål:

1. Skapa manuella reservrutiner för att kunna upprätthålla en fungerande verksamhet i händelse av IT-störningar, avbrott etc.

   Arbetet sker i tre steg:

   - Inventering av samtliga IT-system som finns i verksamheten inklusive alla redan existerande reservrutiner.
   - Värdering av vilka IT-system som är verksamhetskritiska. Samt fastställande av vilken den maximala tolererbara avbrottstiden är för samtliga av dessa.
   - Översyn befintliga reservrutiner samt, klargöra vilka som behöver skapas.

2. Hitta återstartsprioriteringar för IT-system hos vår driftleverantör.

I presentationen konkretiseras hur målen tillgodoses eller ska tillgodoses, bland annat återfinns en konsekvensmall för att avgöra graden av skada skedd, acceptabla avbrottstider samt en mall för att ta fram reservrutiner.

I intervjuer framkommer att nuvarande kontinuitetsplan är i behov av revidering och att systemdokumentationen i sin nuvarande form riskerar att vara otillräcklig vid en störning. Kontinuitetsplanen har inte testats de senaste åren.

4.4.2 Incidenthantering

Incidentrapportering är en mycket viktig del för såväl organisationens som samhällets informations- och cybersäkerhet. Att hantera, analysera och rapportera incidenter är en av grunderna för den ständiga förbättringen av organisationens informationssäkerhetsarbete. På samhällsnivå är kännedom om allvarliga incidenter avgörande för att kunna mildra konsekvenserna och identifiera sårbarheter.

Ett av målen i regionens informationssäkerhetspolicy är att ha en effektiv incidenthantering. Informationssäkerhetssamordnaren ansvarar enligt ansvarsdokumentet för att bevaka och sammanställa informationssäkerhetsincidenter. I *Processbeskrivning av ledningssystem för informationssäkerhet* framgår att en del i informationssäkerhetsprocessen utgörs av incidenthantering. Incidenthantering beskrivs som att hantera och följa upp incidenter inklusive att lära av inträffade incidenter syftande till att undvika att incident återupprepas.

I intervjuer framkommer dock att det inte finns någon beslutad rutin för hantering av informationssäkerhetsincidenter. Det finns en rutin för personuppgiftsincidenter vilken beskrivs till viss del i *Informationssäkerhetsberättelse 2019*. Regionen har rutiner för att rapportera personuppgiftsincidenter till Datainspektionen och att incidenter måste rapporteras inom 72 timmar. Under 2019 rapporterades tre incidenter i enlighet med lagkraven.

Inget av ovanstående dokument anger hur rutinen för incidenthantering fungerar eller ger en samlad bild av de incidenter som ev. har inträffat.

Vid intervjutillfälle beskrivs att alla medarbetare går en utbildning för att få kunskap om var de ska rapportera incidenter. När en avvikelse anmäls följs det upp genom avvikelsessystemet. Rutinen för hur det följs upp i systemet finns däremot inte dokumenterat. Det uttrycks även av en person i intervjuerna att incidenter håller sig inom sin förvaltning och att det därigenom inte finns någon övergripande information över inträffade incidenter. Det anges därtill vara en omfattande manuell hantering för att lokalisera och ta del av den avvikelserapportering som skett avseende incidenter.

IT-incidenter rapporteras via Helpdesk. Där finns framtagna rutiner för hur incidenter ska hanteras beroende på allvarsgrad och en riskbedömning sker utifrån en given mall. Det finns eskaleringsvägar angivna i rutinen. Bland annat finns en rutin framtagen vid misstanke om skadlig kod och hur detta ska hanteras initialt för att inte intrång ska leda till betydande skada för regionen.

Vidare beskrivs i intervjuerna att det inte har rapporterats om några allvarliga incidenter till tillsynsmyndigheterna.

4.4.3 Bedömning

Vår bedömning är att det inte finns en ändamålsenlig incidenthanteringsprocess för informationssäkerhetsincidenter. Det finns ingen dokumenterad och etablerad rutin för hur hanteringen ska gå till. Det sker i nuläget ingen övergripande sammanställning över inträffade incidenter så att dessa kan utvärderas och ligga till grund för regionens förbättringsarbete genom att de då kan vidta åtgärder så att dessa inte sker igen.

Det fåtal anmälda personuppgiftsincidenter som upptäckts och anmälts ger en signal om att det finns risk för ett mycket stort mörkertal gällande hur många incidenter som inträffar mot hur många som upptäcks, anmäls och i de fall det behövs rapporteras till tillsynsmyndigheterna.

Då inte utbildning har genomförts för så stor del av medarbetarna gör vi tolkningen att kunskapen och medvetenheten idag är alltför låg för att icke önskvärda incidenter både internt och externt upptäcks och hanteras.

Det finns till viss del rutiner för att säkerställa att nya risker och hot identifieras genom att regionen löpande får information från CERT, sina externa leverantörer samt genom de riskanalyser som genomförts med externa konsulter. De genomför därtill regelbundet sårbarhetsscanning av regionens IT-miljö och komponenter.

Regionen har en kontinuitetsplan avseende IT-drift men den är inte uppdaterad sedan 2014. Planen har inte testats regelbundet så att regionen vet om den skulle uppfylla sitt syfte. Med den status som nuvarande dokumentation av IT-miljön och system har finns en risk att det inte finns tillräckliga underlag för att upprätthålla kontinuiteten i verksamheten vid större händelser i form av avbrott eller störning.

4.5 IT-säkerhetsåtgärder

I intervjuerna beskrivs hur regionen arbetar med drift och teknik. Granskningen har därigenom identifierat att det för nätverk, system och klienter finns ett flertal tekniska skydd inkluderande bland annat brandväggar, skydd mot skadlig kod, antivirusskydd, vitlistningsskydd för samtliga klientplattformar mm. Det finns i nuläget ingen SOC (Security Operations Centers) som löpande kan bevaka säkerhetsrelaterade händelser, hot och sårbarheter.

Omvärldsbevakning sker dagligen av IT-säkerhetsansvarig genom sociala medier, andra kända forum samt genom en löpande information från CERT-SE. CERT-SE utfärdar kontinuerligt varningar och råd om sårbarheter IT-system då de som organisation har i uppdrag att omvärldsbevaka hot och säkerhetsproblem på IT-området. Detta sker genom ett nära samarbete och informationsutbyte med liknande nationella och internationella organisationer. Det sker även en viss omvärldsbevakning genom de outsourcingleverantörer som regionen har för IT-driften.

Omfattande arbete har genomförts de senaste åren för att segmentera regionens nätverk (uppdelning av nätverket i mindre delar vilket ger ett bättre skydd) vilket den analys som genomfördes 2018 även pekade ut förbättringsåtgärder för.

Det finns rutiner och processer för uppdatering och säkerhetskonfigureringar för IT-komponenter som sker i olika steg för att minska risken att dessa ska innebära störningar i funktionaliteten i verksamhetens informationssystem.

Utifrån revisionsfrågan avseende kryptering för lagring av känsliga data har svar från enhetschef IT-enheten varit att detta inte har varit efterfrågat från informationsägare eller förvaltningsledare för vårdinformationssystem och patientdata. Däremot har det funnits en dialog mellan IT-säkerhetsansvarig och informationssäkerhetssamordnaren om att kryptering ses som önskvärt där det är praktiskt genomförbart. Intervjupersoner anger att de inte har en bild av att kryptering för lagring är en standard för regionerna utan att säkerhetsåtgärder av andra slag används. Bland annt beskrivs att den segmentering som gjorts av nätverk handlar om att säkerställa skyddet för känsliga patientdata då den lagring som sker finns på ett isolerat nät. Om det skulle ske ett intrångsförsök från extern part via extern webbserver eller liknande så är dessa nätverk åtskilda med flertal skyddsmekanismer som intrånget i sådana fall skulle behöva penetrera.

Regionen har infört krav på flerfaktorsautentisering i publikt nåbara tjänster, bland annat via VPN, Office 365 och webbtjänster.

En säkerhetsrisk som framkommer är att regionen i nuläget godkänner privata enheter som ansluter mot IT-miljön via fjärraccess. Införande av tvåfaktorautentisering är en del för att möta risker men det innebär ändå att det finns en hel del enheter i form av telefoner och datorer som används i arbetsrelaterade uppgifter som i nuläget inte kan övervakas, uppdateras eller anpassas till regionens krav på säkerhetsåtgärder. Det framgår i intervjuer att det är prioriterat att åtgärda detta men har under rådande pandemin bedömts svårt att genomföra. Detta då ett stort antal medarbetare som har behövt arbeta på distans inte i nuläget har utrustning som tillhandahålls av regionen. IT-enheten anger att de hittills inte har fått gehör för att vidta åtgärder så att det blir otillåtet att ansluta till IT-miljön från privata enheter. Regionledningen har dock under

2020 antagit en målsättning att *”varje enhet som tillåts att ansluta till regionens nätverk ska vara känd och betrodd”.*

Det finns till viss del funktioner för att upptäcka hot om intrång i nätverk där patientdata lagras genom IPS (Intrusion Prevention System som översatt betyder intrångsförhindrande system). I övrigt anges det i intervjuer finnas behov av ytterligare funktioner för att på strukturerat sätt få ett helhetsgrepp med övervakning och larm för regionens nätverk, trafik och klienter för att i tid kunna upptäcka och förhindra ev. intrångsförsök och hot mot IT-miljön.

Regionen genomför löpande sårbarhetsscanning och anser att de genom det arbetet har identifierat och getts möjlighet att genomföra ett stort antal förbättringsåtgärder i syfte att öka säkerheten. I dessa sker en genomgång av samtliga servrar och klienter och ger automatiskt en riskprioritering per sårbarhet. I intervju framgår att regionen inte genomfört några penetrationstester eftersom de först behöver åtgärda de problem som redan är kända för dem. Däremot anser de sig ha kommit så långt genom sina sårbarhetsscanningar och övriga externa riskanalyser att de skulle kunna komplettera sin uppföljning med hjälp av penetrationstester.

Det beskrivs i en av intervjuerna att en auktoriseringsprocess finns för att regionen inför upphandling och implementering av nya tjänster och system ska göra en analys av väsentliga aspekter. Exempelvis lyfts att säkerhet, juridik och funktionalitet till övriga redan implementerade system bedöms. I gruppen som utför auktorisationsprocessen ingår därför funktionsansvariga inom ovan nämnda aspekter som gemensamt kan göra bedömningar vid inköp av nya IT-stöd.

4.5.1 Bedömning

Vår bedömning är att regionen har ett aktivt arbete med IT-säkerhet genom vilket de har tillsett att det ska finnas säkerhetsåtgärder för att skydda regionens information inklusive lagrade patientdata. Det är dock inte säkerställt genom kryptering men genom andra åtgärder, exempelvis segmenterade nätverk, funktioner för övervakning, säkra inloggningsfunktioner samt en regelbunden sårbarhetsscanning för att upptäcka sårbarheter. Det har därtill genomförts en analys utifrån NIS-direktivets krav om säkerhet vilken ligger till grund för förbättringsarbete för IT-säkerheten.

Vi noterar att regionen tar en säkerhetsrisk genom att tillåta privat utrustning i form av datorer, mobiler och läsplattor som inte tillhandahålls av regionens IT-enhet. Vilket leder till att IT-säkerhetsansvaret inte kan upprätthållas fullt ut.

4.6 Uppföljning och intern kontroll

4.6.1 Uppföljning

I informationssäkerhetspolicyn framgår att uppföljning av följsamhet gentemot policy med tillhörande regler, rutiner och anvisningar ska kontrolleras årligen och rapporteras till regiondirektör och styrelser/nämnder.

Regionstyrelsen har en beslutad uppföljningsplan i vilken informationssäkerhet ingår. Beredskapschef har sedan 2017 genomfört denna rapportering vilken genomförts avseende år 2020 på regionstyrelsens sammanträde 2021-03-23. Rapporteringen består av en presentation i korthet av den framtagna informationssäkerhetsberättelsen med en beskrivning av de mest väsentliga riskerna och åtgärderna som genomförts under 2020.

Det finns en utsedd kvalitetsstrateg som samordnar arbetet med interrevisioner utifrån regionens ledningssystem. Med i arbetet finns utsedda specialister inom respektive område i ledningssystemet. Informationssäkerhetssamordnaren är specialist och den som ansvarar för uppföljningen inom informationssäkerhet. Det finns ingen specialist utsedd inom IT-säkerhet så inom det sker i nuläget ingen uppföljning i de interna revisionerna utifrån ledningssystemet.

De områden som omfattas är:

- Patientsäkerhet
- Miljö
- Kvalitetsstyrning
- Arbetsmiljö
- Styrning och ledning
- Informationssäkerhet

Som stöd i arbetet har egen-checklistor upprättats som avdelnings/områdes-chefer ska svara på två gånger per år. Resultatet presenteras i form av ”Ledningens genomgång” som genomförs i de tre förvaltningsledningarna två gånger per år. I intervjuer beskrivs att det inte är tillräckligt att presentationen sker i förvaltningsledningarna då många beslut om åtgärder och prioriteringar behöver tas av regionstyrelsen. I nuläget upplevs informationen stanna i tjänstepersonsorganisationen. Beslutsflödet skulle behöva utvecklas så att information kan ges i förvaltningarna men att de formella besluten fattas av regionstyrelsen.

I intervjuer beskrivs att det pågår ett utvecklingsarbete för att bättre följa upp arbetet och efterlevnad inom de fyra områdena och det nya arbetssättet bygger på en modul som implementerats i Stratsys i form av ett enkätsystem som blir uppföljningsbart. Tidigare har arbetet varit manuellt och till viss del på papper. Arbetet enligt det nya arbetssättet har inte kommit igång inom informationssäkerhet ännu men planeras att påbörjas.

Efterlevnad av styrande dokument är ett ansvar för linjen att följa upp och säkerställa att det finns. De interna revisionerna kan i samband med ledningens genomgång påtala avvikelser och föreslå förslag till förbättringar i efterlevnad men det är upp till

varje chef att genomföra arbetet. Det framkommer dock i intervju att det saknas resurser i förvaltningarna som kan ta arbetet från den strategiska nivån till den praktiska nivån. Resursbristen anges i intervjuer i hög grad påverka förutsättningarna att bedriva uppföljningsarbete och analyser för utveckling. Dessutom framhålls att regionens system inte har ett tillräckligt tydligt ägandeskap och hierarki sinsemellan för att informationen ska kunna bearbetas och presenteras som en helhet. Vilket försvårar nyttjande av beslutsstödsystem och andra analysverktyg som kan bidra i regionens uppföljnings- och förbättringsarbete.

4.6.2 Intern kontroll

Vi har i granskningen tagit del av Regionstyrelsens plan för intern kontroll 2020, Regionala utvecklingsnämndens plan för intern kontroll 2020 samt Hälso- och sjukvårdsnämndens plan för intern kontroll 2020. I dessa finns inga risker upptagna avseende informations- och/eller IT-säkerhet vilket innebär att inga kontrollområden finns i plan för 2020.

4.6.3 Bedömning

Vår bedömning är att den interna kontrollen avseende lagar, förordningar och interna regelverk för IT-säkerhet i vissa delar är tillräcklig. Det genomförs en regelbunden och systematisk uppföljning av informationssäkerhetsarbetet som en del i internrevisioner för det övergripande ledningssystemet. IT-säkerhet ingår till viss del i detta arbete. Resultatet presenteras i en informationssäkerhetsberättelse. En återrapportering sker två gånger per år och beslut om prioriterade åtgärder fattas som dokumenteras i en övergripande handlingsplan. Genom de interna revisionerna kan avvikelser påpekas men det sker i nuläget ingen kontroll över i hur stor grad åtgärder vidtas utifrån dessa påpekanden.

Vi noterar att uppföljning och rapportering av informationssäkerhetsarbetet sker årligen till regionstyrelsen i enlighet med styrande dokument och regionstyrelsens uppföljningsplan.

Det finns inga kontrollområden avseende information- eller IT-säkerhet i internkontrollplaner för 2020. Vi anser att det är en brist då den kan utgöra en viktig uppföljning över hur de verksamhetsansvariga har säkerställt att de lagar och regler samt interna styrdokument efterlevs i respektive avdelning/område. Särskilt utifrån den dokumentation som regionen har över identifierade brister i regelefterlevnad utifrån Patientdatalagen och GDPR. Vi har inte tagit del av den analys som genomförts utifrån NIS-direktivet (då den anses för känslig att dela) men noterar att det med de brister vi beskrivit avseende det systematiska informationssäkerhetsarbetet även kan finnas en risk för regionens efterlevnad i enlighet med NIS-direktivet.

5 Slutsats och rekommendationer

5.1 Slutsats

Vår sammanfattande bedömning är att regionen delvis har en ändamålsenlig organisation för arbetet med IT-säkerhet. Det finns en tydliggjord ansvarsfördelning avseende informationssäkerhetsarbetet och en utsedd ansvarig att leda IT-säkerhetsarbetet. En stor del av IT-verksamheten är outsourcad och vi konstaterar att det sker en regelbunden uppföljning för att säkerställa att regionen kravställer de säkerhetsåtgärder som det finns behov av för att skydda IT-infrastrukturen. Hantering av behörighet för externa leverantörer bedöms ske på ett ändamålsenligt sätt och loggkontroller görs regelbundet för att kontrollera hur behörigheterna nyttjas.

Det finns brister i förvaltningarnas informationssäkerhetsarbete vilket påverkar arbetet med IT-säkerhet. Det sker i nuläget inget systematiskt arbete med informationsklassning och riskanalyser för den information som hanteras i förvaltningarna. Det leder till att verksamheterna i nuläget inte är kravställare av IT-säkerhetsåtgärder som de bedömt att det finns behov av i förhållande till skyddsvärdet på informationen. Dessa upprättas därför utifrån ett tekniskt perspektiv och de förutsättningar kompetensmässigt och ekonomiskt som IT-enheten har för att implementera säkerhet för infrastrukturen. Det finns därtill brister i behörighetshanteringen vilken i nuläget inte möter de lagar och krav som finns enligt Patientdatalagen och GDPR.

Det finns till viss del styrande dokument som utgör ett stöd i arbetet och en ny riktlinje för IT-säkerhet ska inom kort fastställas. Vi ser att denna följer den nyligen beslutade föreskriften från MSB som avser att vara ett stöd i myndigheternas upprättande av IT-säkerhetsåtgärder. Dokumentation av IT-miljön behöver utvecklas så att dessa underlag är uppdaterade och tillgängliga för att det ska finnas förutsättningar att upprätthålla regionens kontinuitet vid händelse av störning eller avbrott.

Vår bedömning är att den interna kontrollen avseende efterlevnad av lagar, förordningar och interna regelverk för IT-säkerhet är bristfällig. Det genomförs en regelbunden och systematisk uppföljning av informationssäkerhetsarbetet som en del i internrevisioner för det övergripande ledningssystemet. Det finns inga kontrollområden avseende information- eller IT-säkerhet i internkontrollplaner för 2020. Vi anser att det är en brist då den kan utgöra en viktig uppföljning över hur de verksamhetsansvariga har säkerställt att de lagar och regler samt interna styrdokument efterlevs i respektive avdelning/område. Särskilt utifrån den dokumentation som regionen har över identifierade brister i regelefterlevnad utifrån Patientdatalagen och GDPR.

5.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen att:

- Säkerställa att avdelningar och områden tillsätter resurser och tar sitt ansvar för det systematiska informationssäkerhetsarbetet i enlighet med ledningssystemet för informationssäkerhet.
- Säkerställa att informationsklassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.
- Säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.
- Riskanalyser upprättas regelbundet för IT-infrastruktur och drift.
- Upprätta en riskanalys över att privata enheter kan ansluta via fjärraccess till regionens IT-miljö och utifrån dessa risker fatta beslut om relevanta åtgärder för att möta dessa.
- Uppdatera kontinuitetsplan för IT-driften.
- Besluta om regionövergripande rutin för incidenthantering och rapportering för informationssäkerhetsincidenter samt kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av samtliga inträffade incidenter så att dessa kan beaktas i förbättringsarbetet.
- Säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.

2021-03-25

KPMG AB

Jenny Thörn	Sara Linge	Veronica Hedlund Lundgren
Kommunal revisor	Certifierad kommunal revisor	Certifierad kommunal revisor, kvalitetssäkrare

Bilaga 1

Dokumentgranskning

Titel	Datum för fastställande	Ansvarig	Dokumenttyp
Ledningssystem för informationssäkerhet	2020-07-20	Mikael Ferm	Processbeskrivning
Policy för informationssäkerhet	2020-11-24	Regionfullmäktige	Policy
Riktlinjer för IT-säkerhet (Utkast)		Anders Lönn	Riktlinjer
Riktlinjer digitalisering	2019-11-06	Regiondirektör	Riktlinjer
Fördelning av ansvar för informationssäkerhet	2018-06-01	Regionstabschef	
Regler för säkerhet IT-infrastruktur	2015-03-09	Thomas Nesterud	
IT-säkerhetsplan	2020-12-07	Anders Lönn	Plan
Informationssäkerhetsberättelse 2019	2020-04-29	Regionstyrelsen	Berättelse
Övergripande handlingsplan för informationssäkerhet och dataskydd 2020–2021	2020-01-14	Enheten för krisberedskap, säkerhet och miljö	Handlingsplan
Regel för informations- och systemklassificering	2015-08-13	Mikael Ferm	Regler
Regler för behörighetshantering IT-system	2017-05-15	Anna-Lena Alfreds	Regler
Linjechefs ansvar för behörighetshantering	2019-03-05	Anna-Lena Alfreds	Rutin

Förvaltningsorganisation logg- och åtkomstkontroll	2018-04-11	Regiondirektör	
Riktlinje av avbrottsplanering av kritiska aktiviteter och beroende	2020-10-13	Mikael Ferm	Riktlinje
Kontinuitetsplan för IT-infrastruktur	2014-09-15	Thomas Nesterud	Kontinuitetsplan
Reservrutiner vid bortfall av IT-system			