REGION
JÄMTLAND
HÄRJEDALEN
Regionens revisorer

Leif Gabrielsson
Revisionsdirektör
Tfn: 063-147528

SKRIVELSE

2024-02-28

REV/6/2023

Regionstyrelsen

Uppföljande granskning av IT-säkerhet

På vårt uppdrag har revisionskontoret tillsammans med upphandlad konsult genomfört en uppföljande granskning av regionens IT-säkerhetsarbete.

Granskningens syfte har varit att ta reda på om brister som framkom i den tidigare granskningen (2020) blivit åtgärdade.

Resultatet av granskningen redovisas i bifogad revisionsrapport.

- Under föregående granskning bedömdes hanteringen av den interna kontrollen vara bristfällig. Bristerna har delvis blivit åtgärdade men en internkontroll baserad på en riskanalys saknas.
- I föregående granskning framkom en avsaknad av tillräckliga och adekvata resurser i förvaltningarna som kan ta arbetet från den strategiska nivån till den praktiska nivån. Resurser har tillförts och bristerna bedöms ha blivit åtgärdade.
- I den tidigare granskningen framkom att det inte pågick något systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar, dock gjordes riskanalyser inom IT-säkerhet på ett tillfredsställande sätt. Vid den uppföljande granskningen uppges att det implementerats en systematisk metod för säkerhetsklassificering av funktioner och tjänster.
- Den tidigare granskningen visade att regionens rutiner för behörigheter och lösenord var bristfälliga. Regionen har genomfört vissa åtgärder för att förbättra hanteringen av behörigheter. Under 2024 planeras en genomgripande förändring av lösenordskraven vilket är en positiv åtgärd för att stärka behörighetshanteringen och därigenom öka den övergripande säkerheten. Utifrån ett tekniskt säkerhetsperspektiv görs bedömningen att skyddsnivån för patientinformation är tillräcklig.
- I den tidigare granskningen noterades att regionen saknade en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter. Vi anser att åtgärder vidtagits och regionens incidenthanteringsprocess bedöms vara utformad enligt god praxis och är välfungerande.
- I den tidigare granskningen bedömdes att medarbetare inte erhöll tillräcklig utbildning som krävdes för att efterleva de lagkrav och interna regler som finns för hantering av patientuppgifter. I den uppföljande granskningen bedöms bristerna kvarstå på grund av att endast hälften av personalen som genomgått den utbildning i informationssäkerhet som samtliga anställda ska genomgå i regionens kompetensportal.
- I den tidigare granskningen bedömdes att regionens riskanalysarbete kunde utvecklas för att kunna göra rätt prioriteringar. I den uppföljande granskningen bedöms bristerna delvis kvarstå.

Vi rekommenderar Regionstyrelsen att:

- Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.
- Säkerställa att en systematisk och fullständig process för informationsklassning etableras.
- Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.
- Implementera ett automatiserat identitets- och åtkomstverktyg för att adressera sårbarheter som kan uppstå genom manuell hantering. Olämpliga behörigheter och inaktuella användarkonton innebär ökad risk för obehörig åtkomst. En automatiserad metod för hantering av behörigheter kan mitigera risken för obehörig åtkomst, samtidigt som användarupplevelsen förbättras.
- Införa ett obligatoriskt krav för medarbetare att fullfölja utbildning inom informations-/IT-säkerhet inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten.
- Säkerställa att medarbetarna kontinuerligt utbildas inom området. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område.
- Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.
- Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noteras att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.
- Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser.

Vi emotser senast den 10:e september 2024 en redovisning av vilka åtgärder som regionstyrelsen vidtagit eller avser vidta med anledning av granskningsresultatet samt en tidplan för åtgärderna.

För Region Jämtland Härjedalens revisorer

Jan Rönngren
Ordförande

Viveca Asproth
Vice ordförande

Bilaga
Revisionsrapport – Uppföljande granskning av IT-säkerhetsarbetet Rev/6/2023
Rapportsammandrag – Uppföljande granskning av IT-säkerhetsarbetet Rev/6/2023

Kopia till
Regiondirektören
Regionstabschef
IT-säkerhetsansvarig

Region Jämtland Härjedalen

Uppföljande granskning av IT-säkerhet

Februari 2024

pwc

Innehållsförteckning

Förklaring till begrepp och förkortningar

CIS18-kontroller	CIS-ramverket är formulerade av en grupp it-experter som använder information som samlats in från faktiska attacker och deras effektiva försvar. Dessa 18 rekommendationer utvecklas, prioriteras och valideras varje år. Kontrollerna består av 18 rekommendationer för cybersäkerhet och defensiva åtgärder som kan hjälpa till att förhindra de mest genomgripande och farliga attackerna och stödja efterlevnad. CIS-kontrollerna ger specifik vägledning och en tydlig väg för verksamheter att uppnå de mål som beskrivs av flera juridiska, regulatoriska och policy-ramar.
GDPR	Förordning (EU) 2016/679 – om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Även kallad den allmänna dataskyddsförordningen
OSL	Offentlighet- och sekretesslagen (2009:400)
SOC-tjänst	Security Operations Center (SOC) är en säkerhetsavdelning, med ansvar för att identifiera, analysera och motverka alla digitala hot mot en organisation eller ett företag. Avdelningen kan vara en del av en organisation, men den kn också upphandlas som tjänst. SOC-teamet arbetar dygnet runt med att övervaka och analysera data från olika säkerhetsenheter, som till exempel brandväggar, intrångsförebyggande system och användarloggar. När ett hot eller en attack upptäcks, genomför teamet åtgärder för att skydda organisationen och förhindra ytterligare skador.

1. Sammanfattning

Region Jämtland Härjedalens revisorer, med stöd av KPMG, genomförde 2020 en granskning av regionens IT-säkerhet. Syftet med denna granskning är primärt att bedöma om regionstyrelsen vidtagit åtgärder för att åtgärda de brister som framkom vid den tidigare granskningen. Syftet är också att bedöma (utifrån de aktuella revsionsfrågorna) om regionens arbete med IT-säkerhet är ändamålsenligt.

Den övergripande bedömningen är att regionstyrelsen i Region Jämtland Härjedalen delvis har åtgärdat de brister som framkom vid den tidigare granskningen, och delvis bedriver ett ändamålsenligt IT-säkerhetsarbete.

Under granskningen har vi identifierat ett antal områden som tydligt återspeglar regionens ambition och målsättning med att förbättra IT-säkerheten. Dessa åtgärder inkluderar bland annat:

- Förstärkning av regionens monitorering- och responderingsförmåga genom upphandlad SOC-tjänst,
- Förbättrad intern kontroll avseende IT-säkerhet,
- Investeringar i både personella resurser och förbättrad infrastruktur,
- En välfungerande incidenthanteringsprocess.

Dessa förmågor utgör centrala aspekter som regionen bör sträva efter att behålla och bygga vidare på. Därtill är det värdefullt att konsolidera dessa styrkor över de olika verksamhetsområdena när det är möjligt, samtidigt som regionen aktivt bör mäta och kontinuerligt förbättra dessa styrkor.

Under granskningen har vi också noterat ett antal brister och utvecklingsområden, varav de viktigaste är nedan;

- Behov av att utveckla internkontrollplanens riskbaserade ansats.
- En manuell behörighetshantering.
- Avsaknad av kontroll eller säkerställande av medarbetares kunskapsnivå.
- Avsaknad av ändamålsenlig informationsklassning.
- Avsaknad av systematik kopplat till identifiering av verksamhetskritiska system.

Sammantaget gör vi bedömningen att ovan brister och utvecklingsområden innebär att regionen har ett återstående arbete att göra för att helt nå upp till en ändamålsenlig nivå på IT-säkerhetsarbetet. Regionstyrelsen behöver också stärka sitt arbete med att säkerställa att planerade mål och åtgärder verkligen slutförs inom givna tidsramar.

Dock vill vi poängtera den positiva förändring som skett sedan den föregående granskningen, och understryka att en tydlig förbättring har skett.

1. Samlad bedömning

Revisionsfrågor	Bedömning
1. Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?	**Delvis**
2. Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?	**Ja**
3. Sker säkerhetsklassning av funktioner och tjänster?	**Delvis**
4. Finns ändamålsenliga rutiner för behörigheter och lösenord (med inriktning på den interna hanteringen)?	**Delvis**
5. Har regionen en ändamålsenlig incidenthanteringsprocess?	**Ja**
6. Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?	**Delvis**
7. 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?	**Nej**
8. Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?	**Delvis**

3. Samlade rekommendationer

Efter genomförd granskning rekommenderar vi regionstyrelsen att vidta följande åtgärder för att stärka regionens IT-säkerhet.

Nedanstående lista är en sammanfattning av de viktigaste rekommendationerna. Fullständiga rekommendationer finns under respektive revisionsfråga.

- Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.
- Säkerställa att en systematisk och fullständig process för informationsklassning etableras.
- Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.
- Implementera ett automatiserat identitets- och åtkomstverktyg för att adressera sårbarheter som kan uppstå genom manuell hantering. Olämpliga behörigheter och inaktuella användarkonton innebär ökad risk för obehörig åtkomst. En automatiserad metod för hantering av behörigheter kan mitigera risken för obehörig åtkomst, samtidigt som användarupplevelsen förbättras.
- Införa ett obligatoriskt krav för medarbetare att fullfölja utbildning inom informations-/IT-säkerhet inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten.
- Säkerställa att medarbetarna utbildas inom området kontinuerligt. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område.
- Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.
- Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noteras att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.
- Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser.

2 Inledning

2. Inledning

Bakgrund

Regionens revisorer granskade 2020 regionens IT-säkerhet. Granskningen genomfördes av KPMG. I granskningen framkom bland annat att det fanns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som pekades ut i dokumenterad ansvarsfördelning inte uppfylls av avdelnings- och områdeschefer. Vidare framkom att det fanns risk att organisationen 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. Granskningen visade att medarbetare 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.

Det noterades att det saknades ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar samt att det saknades ändamålsenliga rutiner för behörigheter och lösenord. Det saknades också en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter och befintlig kontinuitetsplan avseende IT-drift var inte uppdaterad. I granskningen noterades att det inte fanns kontrollområden avseende information- eller IT-säkerhet i internkontrollplaner.

Syfte

Granskningens primära syfte är att svara på om regionstyrelsen har vidtagit åtgärder utifrån de brister som framkom i granskningen 2020. Efter dialog med revisionskontoret har det uppföljande perspektivet kompletterats med att också innehålla en granskning avseende de revisionsfrågorna som där brister identifierades vid den tidigare granskningen. Denna kompletterande del avser då en bedömning (utifrån de aktuella revsionsfrågorna) om regionens organisation och interna kontroll är ändamålsenlig avseende IT-säkerhet.

Metod

Granskningen är genomförd i enlighet med den projektplan som fastställs av regionens revisorer. Den har genomförts genom studier av styrdokument, beslut och beslutsunderlag samt intervjuer med nyckelpersoner. Primärt har granskningen genomförts genom tillämpning av det så kallade NIST-ramverket. Se bilaga för en fördjupad redovisning av metoden.

Granskningen redovisas genom en genomgång av den föregående rapportens iakttagelser, bedömningar och rekommendationer. Avseende några av revisionsfrågorna har vi inte kunnat identifiera tydliga rekommendationer eller iakttagelser, vilket också redovisas för de specifika revisionsfrågorna. Därefter redovisar vi de iakttagelser och bedömningar vi gör i denna granskning, utifrån ett uppföljande perspektiv. Därefter lämnar vi våra rekommendationer, utifrån en samlad bedömning avseende både uppföljning av tidigare rekommendationer samt de iakttagelser som görs i denna granskning.

De funktioner som intervjuats inom ramen för granskningen är följande:

- Regiondirektör
- Regionstabchef
- Säkerhetsskyddschef
- IT-säkerhetsansvarig
- IT-chef
- IT-strateg
- Enhetschef/IT-strateg

De intervjuade har getts möjlighet att faktagranska denna rapport.
Kvalitetssäkring har skett av Marie Lindblad, certifierad kommunal revisor, PwC.

2. Inledning

Avgränsningar

Granskningen avser regionstyrelsen i Region Jämtland Härjedalen. Primärt besvaras revisionsfrågorna utifrån ett uppföljande perspektiv men de bedöms även självständigt utifrån denna granskning.

Revisionskriterier

- Kommunallag (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,
- Relevanta interna styrdokument.

Revisionsfrågor

Vidstående revisionsfrågor är samma frågor som vid den föregående granskningen. Två frågor har tagits bort då hanteringen av dessa bedömdes vara ändamålsenlig vid föregående granskning. De borttagna frågorna är: *Finns det en övergripande styrning av informations- och IT-säkerhet inklusive styrande dokument?*, samt, *Är känsliga patientdata lagrade på ett säkert sätt, till exempel genom kryptering?*.

Revisionsfrågor, forts.

1. Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?
2. Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?
3. Sker säkerhetsklassning av funktioner och tjänster?
4. Finns ändamålsenliga rutiner för behörigheter och lösenord? Med inriktning på den interna hanteringen.
5. Har regionen en ändamålsenlig incidenthanteringsprocess?
6. Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?
7. 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?
8. Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

3

Granskningsresultat

Revisionsfråga 1: Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

Iakttagelser och bedömning föregående granskning

Under föregående granskning bedömdes hanteringen av den interna kontrollen avseende lagar, förordningar och interna regelverk kopplat till IT-säkerhet bristfällig. Granskningen framförde att regelbunden och systematisk uppföljning av informationssäkerhetsarbetet genomförs som en del av internrevisionen för det övergripande ledningssystemet, där IT-säkerhet ingår till viss del. Resultaten presenteras i form av en informationssäkerhetsberättelse, återrapportering av denna sker två gånger per år. Beslut om prioriterade åtgärder dokumenteras i en övergripande handlingsplan. Granskningen noterade även att avvikelser gås igenom i samband med utförda interna revisioner, dock noterades en avsaknad av kontroll över i hur stor grad åtgärder vidtas utifrån noterade iakttagelser.

Vidare noterades att uppföljning och rapportering av informationssäkerhetsarbetet presenteras årligen för regionstyrelsen enligt styrande dokument och regionstyrelsens uppföljningsplan. Samtidigt noterades en avsaknad av kontrollområden relaterade till informationssäkerhet eller IT-säkerhet i internkontrollplanerna för 2020. Detta ansågs vara en brist, särskilt med tanke på att detta utgör en betydande aspekt av uppföljningen för att bedöma hur verksamhetsansvariga har säkerställt överensstämmelse med lagar, regler och interna styrdokument inom sina respektive avdelningar och områden.

I den tidigare granskningen konstaterades även att de identifierade bristerna i det systematiska informationssäkerhetsarbetet potentiellt kan påverka regionens efterlevnad av exempelvis NIS-direktivet.

Rekommendationer föregående rapport

- Säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.

Revisionsfråga 1: Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

Uppföljande iakttagelser

Regionen har utvecklat den interna kontrollen avseende IT-säkerhet sedan föregående granskning. IT-säkerhetsfrågor har inkluderats i regionens övergripande internkontrollplan både 2021 och 2022, dock inte 2023. Inom ramen för det operativa IT-säkerhetsarbetet finns en ny IT-säkerhetsplan, som är direkt kopplad till målsättningen inom området för IT-säkerhet.

Vid intervju framgår att IT-säkerhetsenheten genomför systematiska genomgångar av säkerhetsåtgärder baserat på CIS18-kontrollerna (Center for Internet Security). Utvärderingen av dessa åtgärder utgör sedan grund för utformningen av nästa års IT-säkerhetsplan och därmed skapas grunden för ett kontinuerligt förbättringsarbete.

För att ytterligare förstärka den interna kontrollen planerar regionen att göra internkontrollarbetet mer riskbaserat. Som del av detta arbete har en särskild riskgrupp tillsatts som har i uppgift att hantera och adressera dessa frågor på ett mer strukturerat sätt. Riskgruppen agerar på koncernnivå och befinner sig för närvarande i uppstartsfasen.

IT-säkerhetsansvarig uppger att regelbundna föredragningar inom området har hållits för både krisledningsnämnd och regionfullmäktige. För 2022 finns även en så kallad informationssäkerhetsberättelse som återrapporterar regionens status inom området till regionstyrelsen.

Bedömning

Delvis

Bedömningen baseras på att:

- Sedan föregående granskning har en mer omfattande intern kontroll avseende IT-säkerhet införts, och därmed har regionstyrelsen uppnått en ökad grad av intern kontroll i dessa frågor.
- Arbetssättet att utgå från CIS18-kontrollerna och utifrån status på dessa utforma kommande års IT-säkerhetsplan är ett ändamålsenligt arbetssätt för att systematiskt skapa ett bättre resultat.
- Den interna kontrollen bör vara riskbaserad för att vara ändamålsenlig och effektiv, och än så länge är arbetet inte strukturerat utifrån ett riskbaserat perspektiv.
- En grundläggande förutsättning för att säkerställa en effektiv internkontroll är en väl genomförd riskanalys. För att internkontrollen ska vara ändamålsenlig krävs därför en prioritering av processer, vilket bör baseras på slutsatser från en tillförlitlig riskanalys. Etablerandet av en fungerande riskhanteringsprocess blir därmed avgörande för att stödja den övergripande interna kontrollen och skapa av en robust grund för målinriktade åtgärder inom IT-säkerhet.

Revisionsfråga 1: Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

Rekommendationer

PwC rekommenderar regionstyrelsen att:

- Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.
- Säkerställa att det arbete som påbörjats för att göra den interna kontrollen mer riskbaserad slutförs.
- Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noterar vi att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.
- Fortsätta prioritera området IT-säkerhet och följa upp att önskade resultat och effekter uppnås. Större delen av en regions verksamhet är i dag beroende av IT-system och digitala verktyg. Det innebär i sin tur att funktionalitet, kontinuitet och säkerhet i dessa system och verktyg utgör en grundläggande förmåga för att regionen ska kunna leva upp till sitt lagstadgade åtagande (exempelvis hälso- och sjukvård).

Revisionsfråga 2: Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?

Iakttagelser och bedömning föregående rapport

I föregående granskning framkom en avsaknad av tillräckliga och adekvata 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.

Rekommendationer föregående rapport

- Säkerställa att avdelningar och områden tillsätter resurser och tar sitt ansvar för det systematiska informationssäkerhetsarbetet i enlighet med ledningssystemet för informationssäkerhet.

Revisionsfråga 2: Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?

Uppföljande iakttagelser

Sedan den tidigare granskningen har ett flertal förändringar avseende IT-säkerhetsarbetet i regionen genomförts. Enligt medarbetare har resurser tillförts, både genom fler personella resurser men även genom infrastrukturella investeringar, exempelvis SOC-tjänsten för att monitorera risker och sårbarheter.

De tjänstepersoner vi intervjuat har också uttryckt att resurstilldelningen i dagsläget är tillräcklig. Man uppger också att det finns en lyhördhet för när man äskat om mer resurser, framförallt i form av investeringar eller inköp. Samtidigt uppger alla intervjuade att området är i ständig förändring, och därmed också resursbehovet. Det innebär att samtliga intervjuade också understryker vikten av att ha beredskap för ökade resursbehov.

Under intervjuerna förs även ett resonemang avseende regionens val att delvis förvalta IT-verksamheten genom outsourcing. Det beskrivs att man i dagsläget fortfarande prövar sig fram för att hitta den optimala modellen för driften av verksamheten, men att man i dagsläget ser en blandning av egen drift och outsourcing som den som kombinerar kvalité och kostnadseffektivitet på bästa sätt. En annan förändring som skett sedan förra granskningen är att specifika roller har etablerats och förstärkts för att mer effektivt hantera IT-säkerhetsaspekterna.

Bedömning

Ja

Bedömningen baseras på att:

- Sedan den tidigare granskningen har mer resurser tillförts, både personella och investeringar.
- Det förändrade arbetssättet med mer tydliga roller innebär sannolikt att de resurser som finns att tillgå (både avseende tid, kompetens och materiella resurser) utnyttjas bättre.
- Vi noterar att planerade åtgärder (beskrivs i regionstyrelsens verksamhetsplan för både 2022 och 2023) inte är helt genomförda. Dock kan vi inte styrka att det bristande genomförandet beror på avsaknad av resurser.

Revisionsfråga 2: Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?

Rekommendationer

För att fortsätta upprätthålla en god hantering i framtiden rekommenderas regionstyrelsen att:

- Utvärdera om den bristande måluppfyllelsen av relevanta aktiviteter i verksamhetsplanen beror på bristande resurser, och i så fall åtgärda den bristen.
- Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser.

Revisionsfråga 3: Sker säkerhetsklassning av funktioner och tjänster?

Iakttagelser och bedömning föregående rapport

Den tidigare rapporten saknade redovisade iakttagelser avseende denna revisionsfråga.

Rekommendationer föregående rapport

Den tidigare rapporten saknade redovisade rekommendationer avseende denna revisionsfråga.

Revisionsfråga 3: Sker säkerhetsklassning av funktioner och tjänster?

Uppföljande iakttagelser

Under denna granskning framkommer det i intervjuer att säkerhetsklassning genomförs av relevanta funktioner och tjänster inom regionen. Granskningen visar också att regionen har etablerat riktlinjer och rutiner för säkerhetsklassificering av olika funktioner och tjänster, vilket framgår i relevant dokumentation.

Vid intervju framgår att regionen utför regelbundna befattningsanalyser. Dessa analyser utförs systematiskt i syfte att säkerställa att personal som hanterar säkerhetsskyddad information har genomgått korrekt kontroll och att deras roller och ansvarsområden är i linje med regionens övergripande funktion. Befattningsanalyser genomförs enligt medarbetare med regelbundenhet, minst vartannat år, för att säkerställa en aktuell och korrekt bedömning av behörigheter och ansvarsområden.

För att ytterligare säkra och övervaka personalens lämplighet genomgår medarbetare som hanterar säkerhetsskyddad information säkerhetsprövningar. Regionen tillämpar också tillfälliga registerkontroller kopplade till säkerhetsskydd för att säkerställa att de anställda eller inblandade i vissa tjänster regelbundet genomgår granskning av sina registeruppgifter. Denna rutin bidrar till att identifiera och hantera eventuella säkerhetsrisker över tid.

Vi har inte haft tillgång till befattningsanalysen, eftersom den är baserad på säkerhetsskyddsanalysen och därmed klassificerad som säkerhetskänslig. Detta innebär att vi inte har kunnat styrka de uppgifter som lämnats vid intervju med dokumentation.

Bedömning

Delvis

Bedömningen baseras på att:

- Av intervjuerna framgår det att regionen har implementerat en systematisk metod för säkerhetsklassificering av funktioner och tjänster.
- De regelbundna befattningsanalyserna indikerar en ambition att upprätthålla aktuella och korrekta bedömningar av behörigheter och ansvarsområden.
- Regionen genomför säkerhetsprövningar för att bedöma personalens lämplighet över tid. Genomförandet av dessa är av avgörande betydelse för att säkerställa att endast personer med lämplig pålitlighet och behörighet involveras i arbetsuppgifter som rör känslig information.
- De angivna uppgifterna kan inte styrkas med tillgänglig dokumentation, vilket gör det svårt att verifiera att rutiner och åtgärder efterlevs.

Revisionsfråga 3: Sker säkerhetsklassning av funktioner och tjänster?

Rekommendationer

För att fortsätta upprätthålla en god hantering i framtiden rekommenderas regionstyrelsen att:

- Regelbundet utvärdera och uppdatera rutiner i linje med identifierade risker och förändrade lagkrav, för att säkerställa en anpassningsbar och effektiv hantering av säkerhetsskyddet.
- Säkerställa en korrekt hantering av säkerhetsklassning av leverantörer. Vid identifiering av eventuella nya risker bör regionen upprätthålla en korrekt hantering av säkerhetsklassning för funktioner och tjänster relaterade till leverantörer.

Revisionsfråga 4: Finns ändamålsenliga rutiner för behörigheter och lösenord? Med inriktning på den interna hanteringen.

Iakttagelser och bedömning föregående rapport

Den tidigare granskningen visade att regionens rutiner för behörigheter och lösenord var bristfälliga och att hanteringen påverkade regionens förmåga att säkerställa medborgarnas integritet avseende patientinformation i journalsystem. Det fanns styrande och stödjande dokumentation men dessa ansågs inte ha fått genomslag i praktiken. Det bedömdes också att rutiner inte efterlevdes i tillräckligt hög grad.

Det framkom även att regionen själva identifierade efterlevnad av styrande dokumentation som ett utvecklingsområde, och att regionen genomfört en förstudie samt återrapporterat till ledningen att detta behövde utvecklas för att uppnå en tillräcklig regelefterlevnad avseende integritetsskydd.

Däremot bedömdes hanteringen av behörigheter till externa leverantörer inom ramen för IT-drift som ändamålsenlig. Åtgärder hade vidtagits för att säkerställa en högre nivå av datasäkerhet jämfört med tidigare. Etablerade rutiner och processer för behörighetshantering samt en tillräcklig loggkontroll identifierades, vilka tydligt belyste hur tilldelade behörigheter användes.

Rekommendationer föregående rapport

- Säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.

Revisionsfråga 4: Finns ändamålsenliga rutiner för behörigheter och lösenord (med inriktning på den interna hanteringen)?

Uppföljande iakttagelser

Vid intervju uppges att regionen delvis använder ett automatiskt behörighetsverktyg i systemet Plexus. Verktyget möjliggör automatiserat skapande av användarkonton baserat på information från HR-systemet samt automatisk avveckling av användarkonton när en anställning avslutas. Den automatiska hanteringen omfattar dock endast ett begränsad antal verksamhetssystem som för närvarande är kopplade till Plexus. Det finns även en del begränsningar med Plexus och vissa system saknar stöd för automatiserad behörighetstilldelning.

För systemadministrativa och tekniska konton sker manuell tilldelning av behörigheter. Vid intervju uppges att det planeras för att knyta ägarskap av varje systemadministrativt eller tekniskt konto till en ägare i Plexus. Årligen ska alla chefer kontrollera behörigheterna för sina medarbetare och ändra vid behov. Detta är en säkerhetsåtgärd som tydligt beskrivs i riktlinjer för IT-säkerhet. Dock har vi inte kunnat styrka att det sker uppföljning om kontrollen sker, och hur utfallet dokumenteras och följs upp.

Regionen har implementerat larmsättning för användare med höga behörigheter, även kallade privilegierade användare, för att upptäcka avvikelser och att säkerställa att kritiska system övervakas. Systemet kan även varna om användare med höga behörigheter tilldelas för många behörigheter.

Regionen planerar för en genomgripande förändring av lösenordskraven. Syftet med åtgärden är att stärka användarnas autentiseringsmetoder och därmed öka säkerheten, samtidigt som risken för obehörig åtkomst minskas. För att ytterligare stärka integriteten i driftsystemen finns loggningsverktyg som hanterar leverantörer med behörighet till systemen för att minska risken för obehörig åtkomst.

Bedömning

Delvis

Bedömningen baseras på att:

- Från den tillhandahållna informationen framkommer det att regionen har genomfört vissa åtgärder för att förbättra hanteringen av behörigheter.
- Adekvat hantering av användares behörigheter är centralt för att skydda och bevara information. För närvarande används en manuell hantering av behörigheter vilket medför ökad risk för bedrägerier och obehörig åtkomst till känslig information.
- Larmsättningen för privilegerade användare stärker skyddet mot obehörig åtkomst och bidrar till en mer omfattande säkerhet för känslig information.
- Planen att genomföra en genomgripande förändring av lösenordskraven under 2024 är en positiv åtgärd för att stärka behörighetshanteringen och därigenom öka den övergripande säkerheten.
- Larmsättningen innebär ett ökat skydd för obehörig åtkomst och bidrar till att patientinformation hålls mer skyddad.

Revisionsfråga 4: Finns ändamålsenliga rutiner för behörigheter och lösenord(med inriktning på den interna hanteringen)?

Rekommendationer

PwC rekommenderar regionstyrelsen att:

- Fullfölja den planerade revideringen av lösenordskraven.
- Effektivisera behörighetsstyrningen genom införandet av ett automatiserat verktyg. Ett verktyg såsom ett Identity and Access Management system (IAM) gör det enklare att hålla behörigheter aktuella, bevilja och begränsa åtkomst baserat på roll och upptäckta avvikelser.
- Upprätta en systematisk uppföljning för att kontinuerligt utvärdera efterlevnaden av lösenordskraven, i syfte att säkerställa att dessa upprätthålls över tiden.

Revisionsfråga 5: Har regionen en ändamålsenlig incidenthanteringsprocess?

Iakttagelser och bedömning föregående rapport

I den tidigare granskningen noterades att regionen saknade en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter. Granskningen visade också att regionen saknade en formaliserad process för en övergripande sammanställning över inträffade incidenter i syfte att dessa skulle kunna utvärderas och ligga till grund för regionens förbättringsarbete. Det bedömdes vara en omfattande manuell hantering för att lokalisera och ta del av den avvikelserapportering som skett avseende incidenter, vilket i sin tur också minskade förmågan till översikt och systematisk förbättring.

Däremot visade granskningen att framtagna rutiner fanns för hur olika incidenter skulle hanteras samt att riskbedömning skedde utifrån en given mall. Eskaleringsvägar fanns även angivna i rutinen. Vidare noterades att medarbetare genomgick utbildning för att få kunskap om hur incidenter skulle rapporteras.

Vidare beskrevs att det inte har rapporterats om några allvarliga incidenter till tillsynsmyndigheterna.

Rekommendationer föregående rapport

- 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.

Revisionsfråga 5: Har regionen en ändamålsenlig incidenthanteringsprocess?

Uppföljande iakttagelser

Under granskningen framkommer att regionens incidenthantering hanteras med stöd av framtagna processer och rutiner, exempelvis genom dokumenten “Fördelning av ansvar för Informationssäkerhet” och Eskalering av incidenter utanför kontorstid, utkast”. Den praktiska hanteringen sköts av en intern helpdeskfunktion tillsammans med extern driftsleverantör. I de fall incidenter hanteras av driftsleverantören samverkar den utpekade ansvarige med leverantören för att samordna och åtgärda incidenter som potentiellt kan påverka system och tjänster. Dessutom beskrivs under intervju med bland annat IT-chef att etablerandet av ett incident- och problemforum som fungerar som en gemensam plattform för regionen och driftsleverantören. Inom detta forum granskas och behandlas incidenter som uppstår. Forumet möjliggör en strukturerad och samordnad process för att hantera och lösa incidenter, vilket bidrar till att förbättra den övergripande incidenthanteringen.

Den externa SOC-tjänsten övervakar och analyserar även incidenter i realtid för att säkerställa proaktiv hantering av incidenter. För att hantera och lära av incidenter genomförs även regelbundna uppföljningar under ett månatligt forum. Under dessa möten utvärderas uppkomna incidenter i syfte att dra lärdomar för att förbättra organisationens övergripande säkerhetssituation. I de fall tekniska brister uppstår i samband med incidenterna tar IT-säkerhetsfunktionen initiativ till att utvärdera och analysera dessa brister. Denna utvärdering syftar till att identifiera eventuella sårbarheter i systemen och föreslå åtgärder för att förhindra liknande händelser i framtiden.

Under intervju beskrivs att efterkontroll av incidenter genomförs av it-säkerhetsfunktionen, dock dokumenteras dessa inte enligt ett på förhand bestämt protokoll. Processen för efterkontroll bedöms snarare ske ad hoc, vilket innebär att den genomförs i anpassning till varje specifik incident. Denna flexibilitet upplevs enligt medarbetare möjliggöra anpassning till de unika omständigheterna för varje incident och gör det möjligt för verksamheten att snabbt vidta åtgärder för att stärka säkerheten baserat på de lärdomar som dras från varje händelse.

Bedömning

Ja

Bedömningen baseras på att:

- Regionens incidenthanteringsprocess bedöms vara utformad enligt god praxis och är välfungerande.
- Det etablerade incident- och problemforumet ger effektiv styrning avseende uppkomna incidenter. Genom forumet kan incidenter noggrant granskas och analyseras, vilket möjliggör snabb och inriktad respons.
- Som en följd av rekommendationer från föregående granskning har regionen stärkt sin monitorering- och responderingsförmåga genom SOC-tjänsten som övervakar, analyserar och hanterar incidenter.

Revisionsfråga 5: Har regionen en ändamålsenlig incidenthanteringsprocess?

Rekommendationer

För ytterligare höjd kvalité rekommenderar PwC regionstyrelsen att:

- Säkerställa en hög rapporteringsfrekvens till ledningen avseende uppkomna incidenter och tillhörande lessons-learned dokumentation.
- Säkerställa tillgänglighet av rapporteringsformulär och rutiner. Formulär ska vara utformade så att samtliga anställda utan alltför stor tidsåtgång kan notera en avvikelse.
- Säkerställa effektiv informationsspridning kopplat till uppkomna och hanterade incidenter. Samtliga berörda av en incident bör erhålla information om denna, från att den hänt till beslut och genomförande av åtgärder.

Revisionsfråga 6: Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?

Iakttagelser och bedömning föregående rapport

Vid den tidigare granskningen gjordes bedömningen att regionen saknade ändamålsenliga rutiner för behörigheter och lösenordshantering. Trots att det fanns styrande och stödjande dokument, konstaterades att dessa inte efterlevdes i praktiken och att rutiner inte följdes i tillräcklig utsträckning. Denna bristande hantering av behörigheter bedömdes påverka regionens förmåga att säkerställa medborgarnas integritet, särskilt vad gäller patientinformation i journalsystem.

Rekommendationer föregående rapport

- Säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.

Revisionsfråga 6: Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?

Uppföljande iakttagelser

Under granskningen har vi noterat att regionen har implementerat ett flertal åtgärder för att säkerställa medborgarnas integritet och skydd för patientinformation i journalsystemen. Rutinen för behörighetshantering och skydd mot obehörig åtkomst beskrivs utförligt i dokumentet ”Mall för rutin behörighetshantering [systemnamn/namn på tjänst], och fungerar som ett stöd i arbetet med att fastställa gällande regelverk för behörighetshantering i aktuellt system/tjänst.

Under intervjuer beskrivs att en systemkartläggning har genomförts för att identifiera vilka system som innehåller personuppgifter och patientinformation. För att öka skyddet för dessa system och dess information har de segmenterats till unika kommunikationsnät.

Därtill framkommer i intervju att loggkontroller görs systematiskt samt uppdatering av samtliga användares behörigheter och för detta finns även en tydlig ansvarsfördelning genom Riktlinjer för IT-säkerhet.

Regionen har även implementerat larmsättning för användare med höga behörigheter, även kallade privilegierade användare, för att upptäcka avvikelser och att säkerställa att kritiska system övervakas. Systemet kan även varna om användare med höga behörigheter tilldelas för många behörigheter. Larmsättningen innebär att ett ökat skydd för obehörig åtkomst och bidrar till att patientinformation hålls mer skyddad.

Bedömning

Delvis

Bedömningen baseras på att:

- Utifrån ett strikt tekniskt säkerhetsperspektiv gör vi bedömningen att skyddsnivån för patientinformation är tillräcklig.
- Riktlinjerna för IT-säkerhet ger en god styrning. Dock behöver det följas upp att dess innehåll följs i praktiken, exempelvis att de system som bedöms ha behov av utökat skydd har flerfaktorsautentisering såsom riktlinjen föreskriver.
- Frågan är dock bred, och hänger ihop med flera av de andra revisionsfrågorna. Exempelvis krävs adekvat kunskapsnivå bland de som hanterar patientinformation. Eftersom flera av de revisionsfrågor som samverkar med denna inte är helt uppfyllda, gör vi bedömningen att det innebär inte heller denna kan bli helt uppfylld.

Revisionsfråga 6: Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?

Rekommendationer

PwC rekommenderar regionstyrelsen att:

- Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.
- Säkerställa att övriga rekommendationer i denna rapport implementeras, särskilt avseende uppföljning av behörigheter samt avseende utbildning inom området, eftersom dessa är två centrala aspekter för att säkerställa en adekvat hantering av patientinformation. En noggrann och regelbunden uppföljning av behörigheter är avgörande för att undvika obehörig åtkomst till känslig information. Kunskap och utbildning är även avgörande för dem som hanterar patientinformation. Bristande utbildning kan leda till felaktig hantering av information och att etablerade rutiner inte efterlevs.

Revisionsfråga 7: 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?

Iakttagelser och bedömning föregående rapport

I den tidigare granskningen bedömdes att medarbetare inte erhöll tillräcklig utbildning som krävdes för att efterleva de lagkrav och interna regler som finns för hantering av patientuppgifter.

Det noterades vidare att regionen vidtagit åtgärder för att säkerställa medarbetares kunskap i behandlingen av personuppgifter. Obligatorisk utbildning hade införts, dock ansågs deltagandet lågt och utbildningsbehov pekades ut som ett prioriterat område i den övergripande handlingsplanen för 2020–2021.

Vidare noterades att ytterligare utbildning krävs för registerkoodinatorer, förvaltningsansvariga och chefer. Information om risker, särskilt i e-post, hade delgetts medarbetare och förtroendevalda. Regler för molntjänster hade införts, men det var oklart i vilken utsträckning medarbetare hade följt dem.

Rekommendationer föregående rapport

- Den tidigare rapporten saknar redovisade rekommendationer för denna revisionsfråga.

Revisionsfråga 7: 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?

Uppföljande iakttagelser

I denna granskning har det framkommit att samtliga medarbetare förväntas genomgå en allmän informationssäkerhetsutbildning, inklusive grundläggande IT-säkerhet. Utbildningen finns tillgänglig i regionens kompetensportal. Hittills har totalt 2 768 medarbetare avslutat utbildningen, vilket motsvarar cirka hälften av antalet anställda i regionen. Informationssäkerhetssamordnare ansvarar för utbildningen tillsammans med kommunikationsavdelningen.

Medarbetare beskriver under intervju att utöver ovan nämnda utbildning finns spridd information tillgänglig på intranätet om aktuella områden inom IT-säkerhet, och det informeras även separat vid behov. Det framförs även att regionen planerar att övergå från enstaka anställningsbaserade utbildningar till årliga kampanjer med mikroutbildningar för samtliga medarbetare. Det kommer även att införas riktade utbildningar för chefer med informationsägarskap och systemförvaltare inom informationsförvaltningen. Dessa förändringar ingår som en del av en övergripande uppdatering av regionens ledningssystem för informationssäkerhet. Regionen avser aktivt mäta och följa upp resultaten av dessa insatser för att säkerställa en kontinuerlig förbättring av personalens kunskaper inom området.

Vi har inte kunnat styrka att någon form av kontroll av relevant personals kunskapsnivåer sker, eller att utbildningen är tvingande i någon form.

Bedömning

Nej

Bedömningen baseras på att:

- Utifrån att hälso- och sjukvårdsverksamhet i stor utsträckning präglas av hantering av känsliga personuppgifter, som dessutom till stor del omfattas av sekretess, anser vi att det är en låg andel av personalen som genomgått den förväntade utbildningen.
- Eftersom det saknas kontroll eller någon annan typ av säkerställande av kunskapsnivå finns en uppenbar risk för att medarbetare saknar adekvata kunskaper.

Revisionsfråga 7: 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?

Rekommendationer

PwC rekommenderar regionstyrelsen att:

- Införa ett obligatoriskt krav för medarbetare att fullfölja utbildningen inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten.
- Säkerställa en adekvat kunskapsnivå genom att relevant personal kunskapstestas på regelbunden basis.
- Säkerställa att medarbetarna utbildas inom området kontinuerligt. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område.
- Utvärdera möjligheten att införa en specifik IT-säkerhetsutbildning, särskilt riktad till medarbetare som arbetar med känsliga uppgifter.
- Säkerställa att det systematiskt utvärderas vilka kunskaper som medarbetarna behöver besitta, samt hur det aktuella kunskapsläget inklusive eventuella brister kan åtgärdas. Förändrade behov och identifierade brister bör därefter åtgärdas genom exempelvis utbildning, informationsinsatser och övningar.

Revisionsfråga 8: Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Iakttagelser och bedömning föregående rapport

I föregående granskning konstaterades att riskanalyser inom IT-säkerhet på regionen bedrevs på ett delvis tillfredsställande sätt. Det noterades att regionen hade upprättat analyser över sårbarheter för enskilda delar av IT-miljön i syfte att identifiera brister. Granskningens slutsats var dock att regionens arbete med riskanalyser kunde utvecklas och att området borde utgöra ett underlag för prioritering av IT-säkerhetslösningar där dessa tar utgångspunkt från de mest väsentliga riskerna.

Rekommendationer föregående rapport

- Upprätta riskanalyser 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.
- Säkerställa att informationsklassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.

Revisionsfråga 8: Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Uppföljande iakttagelser

Under granskningen framkommer att regionen arbetar aktivt med att implementera mer formella riskanalyser inom ramen för IT-säkerhet. Ett pågående arbete bedrivs i nuläget med att formalisera en tydlig ansvarsfördelning, genom att tjänsteansvariga (exempelvis ansvarig för datanätverk) ges det övergripande ansvaret för riskanalysen, med stöd från IT-säkerhetsenheten.

Identifiering av risker sker huvudsakligen genom rapporter och omvärldsbevakning som tillhandahålls av den inköpta SOC-tjänsten samt genom månatliga avstämningar i säkerhetsforum, där hotbilder och riskbedömningar diskuteras. Ansvaret för att omhänderta riskerna faller på systemägaren. Dock är denna ansvarsfördelning och riskhanteringen inte dokumenterad. Det är heller inte helt klarlagt hur systemen ska förvaltas (det vill säga hur systemägarskapet ska bedrivas) utan modellen för detta är under utredning.

Därtill noterar vi att det inte finns en systematisk metod eller riskhanteringsmodell för att identifiera och fastställa verksamhetskritiska system. Det saknas även en underliggande analys och resonemang som ligger till grund varför vissa system anses vara verksamhetskritiska. Istället har en bedömning gjorts baserat på en ad hoc bedömning.

Bedömning

Delvis

Bedömningen baseras på att:

- Även om riskanalyser regelbundet genomförs, finns inte ändamålsenliga informationsklassningar för den information som hanteras. Det innebär att även riskanalyserna blir något bristfälliga. Utan tydlig information om känslighetsgrad och adekvat skyddsnivå på den information som hanteras i de olika systemen blir det utmanande att korrekt bedöma och hantera riskerna. Detta har således skapat en osäkerhetsfaktor som begränsar regionens möjlighet att vidta åtgärder i linje med de faktiska riskerna som respektive system kan stå inför.
- I och med att omhändertagandet av risker inte är dokumenterat (både ansvar och processen för det), riskerar identifierade risker att inte bli åtgärdade på ett adekvat sätt.
- Frånvaron av en systematisk metod och riskhanteringsmodell för att identifiera veksamhetskritiska system resulterar i att regionen saknar en grund för att avgöra vilka system som kräver kontinuitetsplaner. Detta skapar en brist i förmågan att korrekt hantera och prioritera risker för de system som är av kritisk betydelse.

Revisionsfråga 8: Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Rekommendationer

PwC rekommenderar regionstyrelsen att:

- Säkerställa att en systematisk och fullständig process för informationsklassning etableras.
- Säkerställa att informationsklassningen hålls aktuell och systematiskt omprövas.
- Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.
- Säkerställa att en strukturerad och formell process för riskanalyser etableras. Den bör vara anpassad utifrån verksamhetens behov, krav och förutsättningar och innehålla en tydlig struktur för löpande styrning och uppföljning för att säkerställa att processen hålls uppdaterad efter förändrade behov. Det är även rekommenderat att verksamheten involverar samtliga relevanta intressenter i processen i syfte att bidra till ökad förståelse och samarbete kring riskanalysen.
- Säkerställa att arbetet med ett mer proaktivt riskarbete, som påbörjats, färdigställs.
- Införa en strukturerad metod för att identifiera och klassificera verksamhetskritiska system. Detta skapar en tydlig grund för att avgöra vilka system som kräver kontinuitetsplaner, förbättrar hanteringen och prioriteringen av risker samt säkerställer en effektiv beredskap.

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Jämtland Härjedalens förtroendevalda revisorer enligt de villkor och under de förutsättningar som framgår av avtal. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.

2024-02-19

Charlotte Arnell

Projektledare

2024-02-19

Marie Lindblad

Kvalitetssäkrare

4

Bilagor

Dokumentationslista

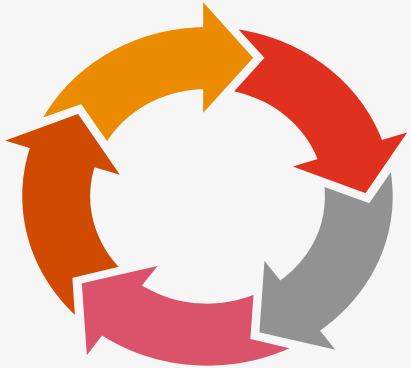
Dokument
Riktlinjer digitalisering
Fördelning av ansvar för Informationssäkerhet
Informationssäkerhetspolicy
Mall för rutin behörighetshantering
Regel för behörighetshantering IT-system
Regel för informations- och systemklassificering
Reglemente för intern kontroll och styrning
Riktlinje för intern styrning och kontroll
Ansvar och kontaktuppgifter kontinuitetsplanering
Eskalering av incidenter utanför kontorstid_utkast
Eskalering och återstartsprioritering IT-system
Kommunikationsplan
Tillgänglighetskrav
Ansvarsfördelning, övervakning och skydd för utrymmen central IT-drift
ATEA MIM process
Exempel DR, Kontinuitetsplan

Dokument
Initial hantering av befarat utbrott av skadlig kod - klient
IT-säkerhetsplan 24-26 Region Jämtland Härjedalen
Riktlinjer för IT-säkerhet
HLD Client flow
HLD segmentation
Handbok för loggkontroll
RJH processkarta incidentprocessen
Verksamhetsplan för regionstyrelsen, 2022 och 2023
Årsredovisning 2022 regionstyrelsens förvaltningsområde
Delårsrapport augusti 2023 regionstyrelsen
Informationssäkerhetsberättelse 2022
Internkontrollplan 2023
Uppföljning regionstyrelsens internkontrollplan 2022
Riktlinje säkerhetsskydd
Säkerhetsskyddsincident
Dokumenthanteringsplan säkerhetsskydd

Metod NIST CSF

Granskningen utfördes med hjälp av ramverket NIST CSF. Ramverket utvärderar en organisations förmåga att genomföra handlingar kopplade till förmågorna **Identifiera**, **Skydda**, **Upptäcka**, **Hantera** och **Återställa** från ett resurs-, process- och teknikperspektiv. Ramverket har anpassats efter Region Jämtland Härjedalens förutsättningar och verksamhet. PwC har utvärderat Region Jämtland Härjedalens mognadsgrad beträffande följande förmågor:

- **Identifiera**, täcker Regionstyrelsens förmåga att identifiera kritiska informationstillgångar och data, det nuvarande läget för styrning och övergripande riskhantering när det kommer till cybersäkerhet. Som ett led i detta undersöker PwC bland annat processer kopplade till riskhantering samt klassificering av informationstillgångar.
- **Skydda**, fokuserar på Regionstyrelsens nuvarande tillstånd när det kommer till att skydda information samt avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörigheter och konton samt säkerhet och skyddsåtgärder kopplad till data som lagras, transporteras och bearbetas.
- **Upptäcka**, inkluderar bland annat Regionstyrelsens förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, sökning efter skadlig kod och sårbarheter.
- **Hantera**, täcker Regionstyrelsens rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat forensik och incidenthantering.
- **Återställa**, relaterar till Regionstyrelsens processer för kontinuitetshantering och förmågor relaterade till resiliens och återhämtning efter hantering av incidenter.



Granskningen baserar sig på kvalitativa intervjuer tillsammans med nyckelfunktioner inom regionen. Personerna som deltagit har kunskap och erfarenhet av verksamheten samt dess IT-säkerhet. Vidare har granskningen inkluderat analys och genomläsning av regionens styrande dokument.

Särskild fråga avseende sekretess

Sekretess och IT-tjänster

Under intervjuer har frågan om sekretess och hantering av denna uppkommit. Eftersom offentlighets- och sekretessregelverket inte är ett revisionskriterium i denna granskning biläggs här nedan en kommentar avseende frågan.

En stor del av den information som regionen hanterar i IT-system utgörs av patientinformation, och är således sekretesskyddat. När sekretesskyddad information tillgängliggörs till personer eller organisationer utanför den egna myndigheten (i detta fall respektive nämnd inom region Jämtland Härjedalen), så som kan ske vid outsourcing av IT-tjänster/-drift och användning av externa konsulter, måste det antingen vara möjligt att tillämpa någon av de sekretessbrytande grunderna i offentlighets- och sekretesslagen (OSL), eller möjligt att de personer som tar del av uppgifterna omfattas av OSL. Risken annars är att uppgifter som ska skyddas av sekretess röjs till obehöriga personer. Det kan resultera i både att regionen gör sig skyldig till sekretessbrott men också till skada för enskilda som får sina uppgifter röjda.

För att följa regelverket krävs således en bedömning, innan beslut om outsourcing, tjänsteköp och liknande tas, om hur OSL-reglerna påverkar den planerade åtgärden. I första steget behövs kunskap/kartläggning om vilka uppgifter som den externa parten kan komma i kontakt med. I nästa steg behövs en bedömning om hur den planerade åtgärden kan efterleva kraven i OSL. I det fall man planerar att använda en IT-tjänst som innebär att sekretessbelagda uppgifter kan komma att hanteras av en extern leverantör kan detta vara tillåtet, men det krävs en föregående lämplighetsbedömning (OSL 10 kap. 2a §).

Ovan resonemang hindrar inte att olika typer av “sekretessavtal” används, det är till och med lämpligt i de allra flesta fall. Det är dock olika frågor och ersätter inte varandra. Ett sekretessavtal kan så att säga inte “läka” en brist avseende efterlevnad av OSL. Det innebär exempelvis att i det fall en IT-tjänst används, måste både en föregående analys göras, sedan behöver tjänsteavtalet anpassas, och dessutom behövs i de flesta fall även ett sekretessavtal, för att användningen av IT-tjänsten ska vara både lagenlig, lämplig och affärsmässigt adekvat.

Under intervjuerna har vi fått uppgiften att dessa analyser inte görs idag. Utifrån den bakgrunden rekommenderar vi regionen följer upp detta och eventuellt genomför ovan analyser och bedömningar.

§130

Svar på uppföljande granskning av IT-säkerhet (RS/237/2024)

Sammanfattning

På regionens revisorers uppdrag har revisionskontoret och upphandlad konsult genomfört en uppföljande granskning av regionens IT-säkerhetsarbete. Syftet har varit att bedöma om regionstyrelsen vidtagit åtgärder för att åtgärda de brister som framkom vid den tidigare granskningen. Syftet är också att bedöma om regionens arbete med IT-säkerhet är ändamålsenligt.

Revisorernas övergripande bedömning är att regionstyrelsen i Region Jämtland Härjedalen delvis har åtgärdat de brister som framkom vid den tidigare granskningen, och delvis bedriver ett ändamålsenligt IT-säkerhetsarbete.

Under granskningen noterades ett antal brister och utvecklingsområden:

- Behov av att utveckla internkontrollplanens riskbaserade ansats.
- En manuell behörighetshantering.
- Avsaknad av kontroll eller säkerställande av medarbetares kunskapsnivå.
- Avsaknad av ändamålsenlig informationsklassning.
- Avsaknad av systematik kopplat till identifiering av verksamhetskritiska system

Revisorerna vill att regionstyrelsen redovisar vilka åtgärder som vidtagits eller avses att vidtas med anledning av granskningsresultatet senast den 10 september 2024.

Ett förslag till svar har upprättats inom IT- och ehälsoavdelningen.

Förslag till beslut

Upprättat förslag till svar på uppföljande granskning av IT-säkerhet antas.

Beslut

Upprättat förslag till svar på uppföljande granskning av IT-säkerhet antas.

Expedieras till

Svar skickas till regionens revisorer
IT-chef
Regionstabschef

Beslutsunderlag

- Tjänsteskrivelse Svar på uppföljande granskning av IT-säkerhet

- Svar Granskning av IT-säkerhet_2024
- Skrivelse från regionens revisorer till regionstyrelsen om uppföljande granskning av IT-säkerhet
- Granskning av IT-säkerhet Region Jämtland Härjedalen

REGION JÄMTLAND HÄRJEDALEN

IT- och eHälsoavdelningen
Marit Nilsson
Tfn: 063-147677 (ank 27677)
E-post: marit.nilsson@regionjh.se

2024-08-27

RS/237/2024

Regionens revisorer

Svar på uppföljande granskning av IT-säkerhet 2024

Granskningsrapporten

Regionens revisorer granskade 2020 regionens IT-säkerhet (RS/338/2021). Granskningen genomfördes av KPMG. I granskningen framkom bland annat att det fanns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som pekades ut i dokumenterad ansvarsfördelning inte uppfylldes av avdelnings-och områdeschefer. Vidare framkom att det vilade ett stort ansvar för både det strategiska och operativa arbetet på nyckelpersoner inom informationssäkerhet och IT-säkerhet. Granskningen visade även att medarbetare 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.

Det noterades att det saknades ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar samt att det saknades ändamålsenliga rutiner för behörigheter och lösenord. Det saknades också en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter och befintlig kontinuitetsplan avseende IT-drift var inte uppdaterad. I granskningen noterades att det inte fanns kontrollområden avseende information-eller IT-säkerhet i internkontrollplaner.

Regionens revisorer har genomfört en uppföljande granskning av IT-säkerheten (RS/237/2024). Denna granskning genomfördes av PwC. Syftet var att bedöma om regionstyrelsen vidtagit åtgärder för att åtgärda de brister som framkom vid den tidigare granskningen. Syftet var också att bedöma om regionens arbete med IT-säkerhet är ändamålsenligt.

Revisorernas övergripande bedömningen är att regionstyrelsen i Region Jämtland Härjedalen delvis har åtgärdat de brister som framkom vid den tidigare granskningen, och delvis bedriver ett ändamålsenligt IT-säkerhetsarbete.

Under granskningen noterades ett antal brister och utvecklingsområden:

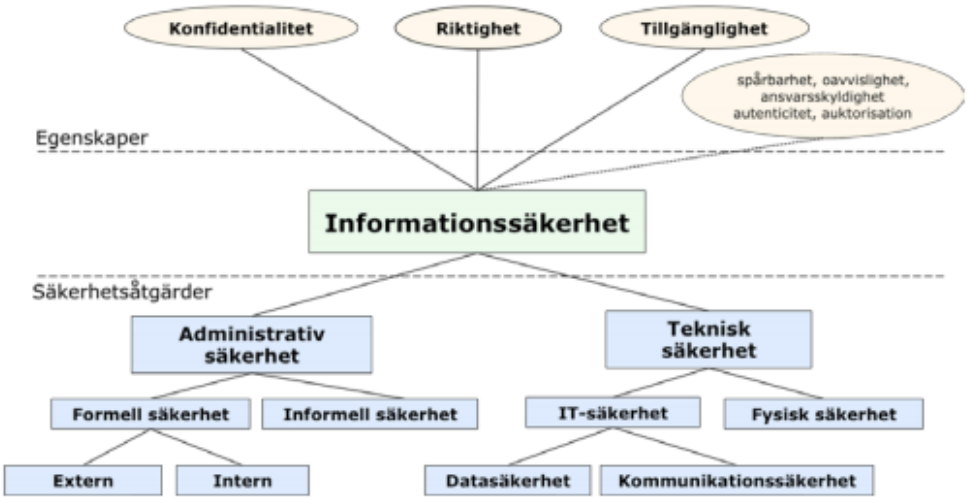
- Behov av att utveckla internkontrollplanens riskbaserade ansats.
- En manuell behörighetshantering.
- Avsaknad av kontroll eller säkerställande av medarbetares kunskapsnivå.
- Avsaknad av ändamålsenlig informationsklassning.
- Avsaknad av systematik kopplat till identifiering av verksamhetskritiska system.

Granskningen har genomförts genom studier av styrdokument, beslut och beslutsunderlag samt intervjuer med nyckelpersoner. Primärt har granskningen genomförts genom tillämpning av det så kallade NIST-ramverket.

Regionstyrelsens svar

Titeln på rapporten är Uppföljande granskning av IT-säkerhet. Liksom vid den tidigare granskningen speglar det inte helt rapportens innehåll. Informationssäkerhet är en kombination av administrativ och teknisk säkerhet, där fysisk och IT-säkerhet ingår i den tekniska säkerheten.

Bilden nedan från Teknisk rapport SIS-TR 50:2015 Terminologi för informationssäkerhet, illustrerar vad som omfattas av begreppet informationssäkerhet.



Figur 1 – Informationssäkerhetsmodell

Informationssäkerhet handlar om att förhindra att information läcker ut, förvanskas eller förstörs. Det handlar också om att göra information lättillgänglig när den behövs och för rätt person. Begreppet omfattar information tryckt på papper, lagrad elektroniskt, som överförs per mejl eller post, visas på film eller yttras i en konversation.

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, men även tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd.

IT-säkerhet handlar om skydd av IT-system och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid

databehandling samt dator- och telekommunikation. En viktig del av arbetet med IT-säkerhet handlar om att förstå olika hotbilder, hantera sannolikheter för att utsättas för skada samt att balansera kostnader för motmedel för skydd mot värdet av det man skyddar.

Rapporten innehåller 8 revisionsfrågor med revisorernas bedömning och rekommendationer till respektive fråga.

Revisionsfråga 1: Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

Revisorerna rekommenderar Regionstyrelsen att: Fullfölja arbetet med att utveckla internkontrollarbetets riskbaserade ansats, vilket innebär att etablerade kontrollaktiviteter bör stå i proportion till verksamhetens befintliga risker. Ett riskbaserat förhållningssätt syftar till att bidra till att regionens resurser och medel utnyttjas effektivt, vilket i sin tur möjliggör värdeskapande för regionens medborgare.

Regionstyrelsens svar: Politisk nivå**:** Internkontrollarbetet är indelat i nivåer där Politikens riskarbete finns i internkontrollplanen i Stratsys (i enlighet med kommunallagen). Här har målområde, nyckeltal och uppdrag riskbaserats. Det sker på styrelse och nämndnivå

Verksamhetsnivå**:** Arbetsmiljöarbetet i RISK hanteras i Stratsys där allt annat arbetsmiljöansvar också dokumenteras. Nytt sedan i maj är att HS också adderades till samma riskmodell med nya säkerhetsområden (miljö, informationssäkerhet, patientsäkerhet)

I höst kommer även arbetet starta med att sammanföra alla risker för att styra på risker. Regionen har då tillräckligt med material för att kunna göra ett bra arbete och också avgöra om det ska hanteras i Stratsys eller ej eftersom klassningen blir en annan.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att det arbete som påbörjats för att göra den interna kontrollen mer riskbaserad slutförs.

Regionstyrelsens svar: Föräldraledighet för medarbetare vid säkerhet och beredskap medför att arbetet inte kunnat starta.

Intern kontroll sker i Stratsys

1. Internrevisionen utvalda frågor att ställa till chefer och specialister.
2. Kontrollmoment lagefterlevnad med påståenden till chefer– Idag utför verksamheterna kontrollmoment på miljö, läkemedel och patientsäkerhet.
3. Checklistor – används framför allt i Arbetsgivaransvaret tex. skyddsrond.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att planerade aktiviteter och åtgärder inom området slutförs. Flera olika IT-säkerhetsrelaterade åtgärder tas upp i verksamhetsplan både för 2022 och 2023, exempelvis säkerheten i nätverksansluten hårdvara. Samtidigt noterar vi att aktiviteterna återkommande inte når den eftersträvade måluppfyllelsen.

Regionstyrelsens svar: IT-säkerhetsfunktionen genomför två gånger per år en övergripande analys baserade på CIS ramverket. De aktiviteter och åtgärder som hänvisas ovan är brister som identifierats i analyserna och ålagts IT-enheten och dess leverantörer att åtgärda. Planering och genomförande ligger utanför IT-säkerhetsfunktionens kontroll.

Revisorerna rekommenderar Regionstyrelsen att: Fortsätta prioritera området IT-säkerhet och följa upp att önskade resultat och effekter uppnås. Större delen av en regions verksamhet är i dag beroende av IT-system och digitala verktyg. Det innebär i sin tur att funktionalitet, kontinuitet och säkerhet i dessa system och verktyg utgör en grundläggande förmåga för att regionen ska kunna leva upp till sitt lagstadgade åtagande (exempelvis hälso- och sjukvård).

Regionstyrelsens svar: Säkerhetsläget har försämrats till följd av krig i världen och hotbilden i form av cyberattacker har ökat. Åtgärder för att stärka regionens IT-säkerhet är därför ett prioriterat område. Regionstyrelsen verksamhetsplan innehåller mål och uppdrag för att stärka regionens skydd och robusthet.

Security Operations Center (SOC) är i drift sedan juni 2022, för övervakning, analys och skydd från cyberattacker. Ett antal tekniska åtgärder har genomförts, pågår och planeras genomföras. Vad dessa åtgärder innebär kan av naturliga skäl inte beskrivas i detta dokument.

Revisionsfråga 2: Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?

Revisorerna rekommenderar Regionstyrelsen att: Utvärdera om den bristande måluppfyllelsen av relevanta aktiviteter i verksamhetsplanen beror på bristande resurser, och i så fall åtgärda den bristen.

Regionstyrelsens svar: Det är IT-enheten och dess leverantörer som ansvarar för att åtgärda de brister som identifierats av IT-säkerhetsfunktionen. Att identifiera brister är oftast den enkla biten. Det som tar tid och resurser är att åtgärda bristerna. En utvärdering bör därför riktas mot IT-enheten i stort och inte begränsas till IT-säkerhetsfunktionen.

Revisorerna rekommenderar Regionstyrelsen att: Fortsätta utvärdera och vara uppmärksam på behov av eventuella ytterligare resurser. Eventuella risker som ännu inte har identifierats kan medföra ett ökat behov av nya resurser och kompetenser .

Regionstyrelsens svar: Regionen instämmer med revisorernas rekommendation.

Revisionsfråga 3: Sker säkerhetsklassning av funktioner och tjänster?

Revisorerna rekommenderar Regionstyrelsen att: Regelbundet utvärdera och uppdatera rutiner i linje med identifierade risker och förändrade lagkrav, för att säkerställa en anpassningsbar och effektiv hantering av säkerhetsskyddet.

Regionstyrelsens svar: Utvärdering och uppdatering av rutiner görs fortlöpande genom regionens riktlinje för säkerhetsskydd och tillhörande rutiner, checklistor samt planer

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en korrekt hantering av säkerhetsklassning av leverantörer. Vid identifiering av eventuella nya risker bör regionen upprätthålla en korrekt hantering av säkerhetsklassning för funktioner och tjänster relaterade till leverantörer..

Regionstyrelsens svar: Regionen löser detta genom att teckna säkerhetsskyddsavtal med de entreprenörer som vistas eller kommer kontakt med våra säkerhetsklassade anläggningar och lokaler samt säkerhetskänsliga uppgifter och handlingar. Dessutom finns det en fastställd befattningsanalys över klassade befattning i regionen

Revisionsfråga 4: Finns ändamålsenliga rutiner för behörigheter och lösenord? Med inriktning på den interna hanteringen.

Revisorerna rekommenderar Regionstyrelsen att: Fullfölja den planerade revideringen av lösenordskraven.

Regionstyrelsens svar: Uppdraget är utlagt på driftleverantör och pågående.

Revisorerna rekommenderar Regionstyrelsen att: Effektivisera behörighetsstyrningen genom införandet av ett automatiserat verktyg. Ett verktyg såsom ett Identity and Access Management system (IAM) gör det enklare att hålla behörigheter aktuella, bevilja och begränsa åtkomst baserat på roll och upptäckta avvikelser.

Regionstyrelsens svar: Region Jämtland Härjedalen har sedan flera år ett IAM-system i drift. Vi ställer oss därför frågande till denna rekommendation.

Revisorerna rekommenderar Regionstyrelsen att: Upprätta en systematisk uppföljning för att kontinuerligt utvärdera efterlevnaden av lösenordskraven, i syfte att säkerställa att dessa upprätthålls över tiden.

Regionstyrelsens svar: Tekniska funktioner för att säkerställa att domänlösenord minst håller avsedd lägstanivå är redan införda. Under 2024 skall samtliga domänlösenord som inte bytts sedan de nya lösenordskraven infördes få ett tvingande lösenordsbyte för att säkerställa att samtliga domänlösenord uppfyller kraven. Funktionen för IT-säkerhet genomför återkommande säkerhetstester för att identifiera svaga lösenord.

Revisionsfråga 5: Har regionen en ändamålsenlig incidenthanteringsprocess?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en hög rapporteringsfrekvens till ledningen avseende uppkomna incidenter och tillhörande lessons-learned dokumentation

Regionstyrelsens svar: Regionens incidentprocess är utformad efter bästa praxis rekommendationer i ITILv4-ramverket, då incidenter med hög prioritet inträffar upprättas en incidentrapport till tjänsteägaren där bland annat ”lessons learned” dokumenteras.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa tillgänglighet av rapporteringsformulär och rutiner. Formulär ska vara utformade så att samtliga anställda utan alltför stor tidsåtgång kan notera en avvikelse.

Regionstyrelsens svar: I den mån avvikelse används som synonym till incident så finns en länk till rapporteringsformulär lätt tillgänglig direkt från skrivbordet i Citrix som är utformad för att vara så enkel som möjligt och ändå tillhandahålla relevant information för felsökning. Om begreppet avvikelse avser brister i processer etcetera så hanteras dessa i systemet Centuri.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa effektiv informationsspridning kopplat till uppkomna och hanterade incidenter. Samtliga berörda av en incident bör erhålla information om denna, från att den hänt till beslut och genomförande av åtgärder.

Regionstyrelsens svar: Vid incidenter som berör enskilda medarbetare kan denne enkelt följa dessa via självbetjäningsdelen av regionens ärendehanteringssystem. Incidenter med högre påverkan kommuniceras dessutom via driftinformation på regionens intranät och talsvarsmeddelande vid samtal till regionens helpdesk. Om intranätet och/eller telefonin skulle vara utslagna har helpdesk också möjlighet att skicka sms-meddelanden till berörda verksamheter via systemet Everbridge.

Revisionsfråga 6: Är medborgarnas integritet säkerställd och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att riktlinjerna för IT-säkerhet efterlevs i praktiken.

Regionstyrelsens svar: Regionstyrelsen instämmer i revisorernas rekommendation.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att övriga rekommendationer i denna rapport implementeras, särskilt avseende uppföljning av behörigheter samt avseende utbildning inom området, eftersom dessa är två centrala aspekter för att säkerställa en adekvat hantering av patientinformation. En noggrann och regelbunden uppföljning av behörigheter är avgörande för att undvika obehörig åtkomst till känslig information. Kunskap och utbildning är även avgörande för dem som hanterar patientinformation. Bristande utbildning kan leda till felaktig hantering av information och att etablerade rutiner inte efterlevs.

Regionstyrelsens svar: Informations- och IT-säkerhet är prioriterade områden i regionen. I Regionstyrelsen verksamhetsplan finns målen - “Hög säkerhet hos mjukvara som körs i regionens IT-miljö genom inventering och kontroll” samt “Hög säkerhet i nätverksansluten hårdvara"

Planen innehåller även uppdraget - “Vidta åtgärder för att öka Region Jämtland Härjedalens robusthet i händelse av olyckor, samhällsstörningar samt krig. Uppdraget omfattar försörjningsberedskap, cybersäkerhet, informationspåverkan och ett fortsatt arbete inom kontinuitetshantering”. I verksamhetsplan för IT- och eHälsoavdelningen finns flera aktiviteter kopplade till detta uppdrag.

Behörigheter till system hanteras i Plexus, med ett gränssnitt för chefer att beställa och följa upp medarbetare behörigheter. Enligt krav från IT-säkerhetsansvarig får ansvariga chefer i Plexus en uppmaning i Behörighetsportalen att revidera anställningsuppgifter när en anställd bytt arbetsplats eller fått ny befattning. Dessutom har chef alltid en möjlighet att enkelt få en överblick över alla anställdas verksamhetsroller genom menyvalet ’Mina medarbetare’ i Plexus. Alla aktiviteter i Plexus loggas i audit-logg.

Revisionsfråga 7: 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?

Revisorerna rekommenderar Regionstyrelsen att: Införa ett obligatoriskt krav för medarbetare att fullfölja utbildningen inom en given tidsram för att på så sätt öka deltagandet och stärka informationssäkerheten..

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa en adekvat kunskapsnivå genom att relevant personal kunskapstestas på regelbunden basis.

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informations-säkerhetsutbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Att uppnå en bra säkerhetskultur där alla medarbetare förstår sitt informations-säkerhetsansvar baseras ej på kunskapstester utan på regelbunden utbildning inom sakområdet, tillsammans med annan löpande information, riskarbete, etcetera. Rekommendationen är inte baserad på evidensbaserad forskning och regionen anser därmed att revisorernas rekommendation ej är ändamålsenlig.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att medarbetarna utbildas inom området kontinuerligt. Detta är viktigt både för att repetera kunskaperna men också för att kunskapskraven ändras relativt snabbt inom detta område..

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Revisorerna rekommenderar Regionstyrelsen att: Utvärdera möjligheten att införa en specifik IT-säkerhetsutbildning, särskilt riktad till medarbetare som arbetar med känsliga uppgifter.

Regionstyrelsens svar: Regionen instämmer med revisorernas rekommendation och skall utvärdera möjligheten.

Revisorerna rekommenderar Regionstyrelsen att: S. Säkerställa att det systematiskt utvärderas vilka kunskaper som medarbetarna behöver besitta, samt hur det aktuella kunskapsläget inklusive eventuella brister kan åtgärdas. Förändrade behov och identifierade brister bör därefter åtgärdas genom exempelvis utbildning, informationsinsatser och övningar.

Regionstyrelsens svar: Hösten 2024 inför regionen en ny årlig informationssäkerhets-utbildning som alla förväntas ta del av. Genomförande kommer att följas upp och återkopplas till respektive medarbetares chef vid ej genomförd utbildning.

Utöver detta får redan specifika roller såsom registerkoordinatorer regelbunden utbildning av regionens dataskyddsombud, riskombud regelbunden utbildning av brandansvarig, etcetera.

Rekommendationen bör formuleras så att samtliga roller med ett informationssäkerhets-ansvar är medvetna om det delegerade ansvaret för informationssäkerheten.

Revisionsfråga 8: Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att en systematisk och fullständig process för informationsklassning etableras.

Regionstyrelsens svar: En risk består av sannolikhet + konsekvens = risk. I en informationsklassning värderas informationen endast utifrån konsekvensen. Då sannolikheten inte tas i beaktande är detta inte en riskanalys.

Regionen har en dokumenterad regel med tillhörande rutiner och mallar för att kunna genomföra informationsklassningar. Det som saknas är den sista delen i att värderingen omsätts till organisatoriska och tekniska säkerhetsåtgärder där samma värdering genererar samma krav på åtgärder. Detta kommer att åtgärdas under hösten 2024.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att informationsklassningen hålls aktuell och systematiskt omprövas.

Regionstyrelsens svar: Regionen saknar en enhetligt implementerad styr- och förvaltningsmodell för IT och digitalisering. En extern genomlysning av IT-funktionen genomfördes 2019, som bl a resulterade i reviderad styr- och förvaltningsmodell för regionens informationssystem. Modellen baseras på tillämpbara delar av pm3. Förvaltningsdelarna har implementerats i ett fåtal system t ex vårdinformationsystemet

COSMIC. Förvaltningsstyrning enligt modell har inte påbörjats, vilket bl a innebär att inte samtliga informationssystem är identifierade eller identifierade med ägare.

Det saknas även en fullständig processkartläggning eller informationskartläggning så förutsättningarna för att uppfylla kravet att informationsklassa antingen genom informationsmängder eller informationssystem finns inte på plats.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att arbetet med att fastställa och etablera en systemförvaltningsmodell färdigställs.

Regionstyrelsens svar: Etablering av systemförvaltningsmodell enligt rekommendationer i ”Genomlysning av IT-funktionen”, behöver prioriteras och kommer att hanteras i någon form inom ramen för den nya organisationen för Utveckling och digitalisering.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att en strukturerad och formell process för riskanalyser etableras. Den bör vara anpassad utifrån verksamhetens behov, krav och förutsättningar och innehålla en tydlig struktur för löpande styrning och uppföljning för att säkerställa att processen hålls uppdaterad efter förändrade behov. Det är även rekommenderat att verksamheten involverar samtliga relevanta intressenter i processen i syfte att bidra till ökad förståelse och samarbete kring riskanalysen.

Regionstyrelsens svar: Regionens verksamheter ska samtliga arbeta strukturerat med analys och hantering av risker. I utvecklingsprojekt inom IT och digitalisering görs riskanalyser inför initiering och planering av aktiviteter. Omfattning och modell varierar beroende på projektets art. Projektil Riskanalys med handlingsplan är en modell som tillämpas.

Revisorerna rekommenderar Regionstyrelsen att: Säkerställa att arbetet med ett mer proaktivt riskarbete, som påbörjats, färdigställs.

Regionstyrelsens svar: Proaktivt riskarbetet sker inom en rad olika områden t ex patientsäkerhet, arbetsmiljö, IT och digitalisering. Regionen saknar ett enhetligt riskramverk, som kan vara tillämpbart för samtliga behov. Det finns inte heller en utpekad roll/ funktion som ansvarar för utforming av ramverk och verktyg för identifiering och hantering av risker. I Stratsys ISK Internkontroll finns identifierade processer kartlagda och stöd för riskhantering, dock har modulen inte ännu börjat tillämpas i någon större utsträckning.

Revisorerna rekommenderar Regionstyrelsen att: Införa en strukturerad metod för att identifiera och klassificera verksamhetskritiska system. Detta skapar en tydlig grund för att avgöra vilka system som kräver kontinuitetsplaner, förbättrar hanteringen och prioriteringen av risker samt säkerställer en effektiv beredskap.

Regionstyrelsens svar: I kontinuitetsplan för oplanerade avbrott i regionens IT-miljö, finns verksamhetskritiska system identifierade med en fastställd prioriteringsordning vid återstart.

REGIONSTYRELSEN

Bengt Bergqvist (S)
Regionstyrelsens ordförande

Sara Lewerentz
Regiondirektör

Yttrandet är fastställt av regionstyrelsen 2024-08-27 § 130