REGION SÖRMLAND

MISSIV

Revisionen

Datum
2022-03-31

Dokumentnummer
RE-REV22–0012

För kännedom
Enligt sändlista

Regionstyrelsen

Granskning av IT/informationssäkerhet

Revisorerna i Region Sörmland har gett KPMG i uppdrag att genomföra en granskning av regionens arbete med IT/informationssäkerhet. Syftet är att ge ett underlag för att bedöma om regionstyrelsen säkerställer en god intern styrning och kontroll av IT /informationssäkerhetsarbetet som ger en ändamålsenlig informationssäkerhet med god uppfyllelse av informationssäkerhetspolicyns mål.

Regionen bedriver verksamheter som ställer stora krav på välfungerande IT och där det är viktigt att den är stabil, säker och att informationen hanteras korrekt. Det är också viktigt att det finns kontinuitetsplaner som säkerställer att verksamheten kan upprätthållas om det sker en incident eller en störning i verksamheternas IT-miljö.

Den sammanfattande bedömningen är att regionstyrelsen delvis säkerställer en god intern styrning och kontroll av IT/informationssäkerhetsarbetet.

Regionstyrelsen har genom beslut om styrande dokument tydliggjort ansvarsfördelning och de aktiviteter som ingår i regionens ledningssystem för informationssäkerhet. Bedömningen är att regionens förvaltningsstyrningsmodell ytterligare har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation.

I nuvarande styrdokument ingår arbetet med IT-säkerhet endast på en övergripande nivå och bör kompletteras för att tydliggöra styrning och uppföljning av arbetet, särskilt då det finns en upplevd otydlighet mellan informationssäkerhetsenheten och IT-enheten.

Regionen har i stora delar etablerat metoder och stöd för att systematiskt identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering.

Nuvarande uppföljning av informationssäkerhetsarbetet är på en övergripande nivå och bör kompletteras med en stärkt intern kontroll avseende efterlevnad av de styrande dokumenten. I rapporten konstateras att brister i efterlevnad finns. Det avser bland annat att obligatoriska utbildningar i informationssäkerhet inte genomförs, att

Region Sörmland
Tel: 0155-24 50 00

Repslagaregatan 19
E-post: post@regionsormland.se

611 88 Nyköping
Org.nr: 232100 – 0032

samtliga informationstillgångar inte är klassade samt att kontinuitetsplaner saknas i stora delar.

Det är inte tydliggjort vilka krav som ställs på IT-säkerhetsåtgärder och hur uppföljning ska ske mer än på övergripande nivå. Vi noterar att det till viss del finns etablerade arbetssätt och funktioner för uppföljning av vidtagen IT-säkerhet för att upptäcka eventuella brister. Genom att de obligatoriska utbildningarna inte har genomförts av samtliga medarbetare är bedömningen att styrelsen inte har säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete. Det leder till att det finns en betydande risk att incidenter inte upptäcks och hanteras i tillräckligt hög grad trots att det finns etablerade rutiner för hantering av incidenter.

I rapporten lämnas ett antal rekommendationer som revisorerna ställer sig bakom. Rekommendationerna bedöms stärka den interna styrningen och kontrollen och i högre grad säkerställa ändamålsenligheten i informations-säkerhetsarbetet och god uppfyllelse av informationssäkerhetspolicyns mål.

Vi begär svar från regionstyrelsens med uppgifter om verkställda och planerade åtgärder senast den 23 juni 2022. Nämnderna får rapporten för kännedom då de bör stärka den interna kontrollen i sina respektive verksamheter kring bland annat loggkontroller och genomförda utbildningsinsatser på området.

Gustaf Wachtmeister
Ordförande

godkänt på distans
Torgerd Jansson
Vice ordförande

REGION SÖRMLAND

MISSIV

Revisionen

Datum
2022-03-31

Dokumentnummer
RE-REV22–0012

Sändlista
Regionala utvecklingsnämnden
Nämnden för kultur, utbildning och friluftsverksamhet
Nämnden för primärvård, rättspsykiatri och Dammsdalskolan
Nämnden för samverkan kring socialtjänst och vård
Inköpsnämnden
Gemensamma patientnämnden

Jan Grönlund, regiondirektör
Jonas Jensen, informationssäkerhetschef
Urban Petrén, IT-direktör
Sofia Stenlund Wretling, utvecklingschef
Kenneth Hagström, regional utvecklingsdirektör
Kajsa Fisk, HR-direktör

Region Sörmland
Tel: 0155-24 50 00

Repslagaregatan 19
E-post: post@regionsormland.se

611 88 Nyköping
Org.nr: 232100 – 0032

Granskning av IT/informationssäkerhet

Rapport

Region Sörmland

KPMG AB

2022-03-28

Antal sidor 22

Region Sörmland
Granskning av IT/informationssäkerhet

2022-03-28

Innehållsförteckning

1 Sammanfattning

Vi har av Region Sörmlands revisorer fått i uppdrag att granska rutinerna kring regionens arbete med IT- och informationssäkerhet.

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen delvis säkerställer en god intern styrning och kontroll av IT/informationssäkerhetsarbetet som ger en ändamålsenlig informationssäkerhet med god uppfyllelse av informationssäkerhetspolicyns mål.

Regionstyrelsen har genom beslut om styrande dokument tydliggjort ansvarsfördelning och de aktiviteter som ingår i regionens ledningssystem för informationssäkerhet. Vår bedömning är att regionens förvaltningsstyrningsmodell ytterligare har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation. I nuvarande styrdokument ingår arbetet med IT-säkerhet endast på en övergripande nivå och bör kompletteras för att tydliggöra styrning och uppföljning av arbetet, särskilt då det finns en upplevd otydlighet mellan informationssäkerhetsenheten och RSIT.

Regionen har i stora delar etablerat metoder och stöd för att systematiskt identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering. Nuvarande uppföljning av informationssäkerhetsarbetet är på en övergripande nivå och bör kompletteras med en stärkt intern kontroll avseende efterlevnad av de styrande dokumenten. Vi kan konstatera att brister i efterlevnad finns. Det avser bland annat att obligatoriska utbildningar i informationssäkerhet inte genomförs, att samtliga informationstillgångar inte är klassade samt att kontinuitetsplaner saknas i stora delar.

Det är inte tydliggjort vilka krav som ställs på IT-säkerhetsåtgärder och hur uppföljning ska ske mer än på övergripande nivå. Vi noterar att det till viss del finns etablerade arbetssätt och funktioner för uppföljning av vidtagen IT-säkerhet för att upptäcka eventuella brister.

Genom att de obligatoriska utbildningarna inte har genomförts av samtliga medarbetare är vår bedömning att styrelsen inte har säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete. Det leder till att det finns en betydande risk att incidenter inte upptäcks och hanteras i tillräckligt hög grad trots att det finns etablerade rutiner för hantering av incidenter. Vår bedömning är vidare att regionstyrelsen inte har säkerställt en ändamålsenlig kontinuitetshantering då dokumenterade planer saknas i stora delar.

För att stärka den interna styrningen och kontrollen och i högre grad säkerställa ändamålsenligheten i Informationssäkerhetsarbetet och god uppfyllelse av informationssäkerhetspolicyns mål rekommenderar vi regionstyrelsen att:

- Utvärdera om befintliga resurser för informationssäkerhetsarbetet är tillräckliga för att möta nya hot och risker samt de interna krav och lagkrav som finns.
- Stärka den interna kontrollen avseende efterlevnad av styrande dokument inom informationssäkerhet. Samt säkerställa att informationssäkerhetschef har mandat att genomföra interna revisioner där brister kan identifieras och påtalas för ansvariga.
- Fastställa styrande dokument för IT-säkerhetsarbetet som bland annat kan tydliggöra ansvar, krav på åtgärder samt uppföljning av vidtagna åtgärder.
- Säkerställa att de obligatoriska utbildningarna inom informationssäkerhet genomförs regelbundet för samtlig personal och förtroendevalda.
- Skyndsamt upprätta kontinuitetsplaner och regelbundet testa rutiner så att verksamheter, IT-infrastruktur och kommunikation kan fortgå/återgå med minimerad skadeverkan i händelse av avbrott eller allvarlig störning inom IT.

2 Bakgrund

I regionfullmäktiges budget för 2021 finns det politiska målet ”Region Sörmland tar tillvara digitaliseringens möjligheter”. Där anges att Region Sörmland bedriver verksamheter som ställer stora krav på en väl fungerande IT, det gäller allt från vård av människor till att förse länets invånare med kultur och utbildning samt att stödja det demokratiska arbetet i regionens olika politiska församlingar.

Regionens verksamhet förväntas fungera även i olika krissituationer och det finns stora krav på kontinuitet i verksamheten. Därför är det viktigt att regionens IT är stabil och säker och att informationen hanteras korrekt.

Regionfullmäktige antog 2019 en informationssäkerhetspolicy (RF117/19). Enligt den ska regionens informationssäkerhetsarbete skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för regionens verksamheter att uppnå sina mål.

Sex målområden anges i policyn som styrande:

- ✓ Säker och riskbaserad informationshantering
- ✓ God informationssäkerhetskultur
- ✓ Effektiv incidenthantering
- ✓ Robust informationshantering
- ✓ Informationssäkerhetsberättelse

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen är att bedöma om regionstyrelsen säkerställer en god intern styrning och kontroll av IT/informationssäkerhetsarbetet som ger en ändamålsenlig informationssäkerhet med god uppfyllelse av informationssäkerhetspolicyns mål.

Granskningen avser att besvara följande revisionsfrågor:

- Finns aktuella och ändamålsenliga styrande dokument som tydliggör krav och hur arbetet ska bedrivas?
- Är roller och ansvar tydliggjorda och uppfattade mellan regionstyrelse, nämnder, verksamhet, informationssäkerhetsenhet och IT-organisation?
- Finns systematiskt arbete för att identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering?
- Genomförs systematiska uppföljningar av vidtagna IT-säkerhetsåtgärder för att upptäcka eventuella brister?
- Har styrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete?
- Har styrelsen säkerställt en ändamålsenlig incident-och kontinuitetshantering?

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Kommunallagen 6 kap § 6

— Tillämpbara interna regelverk och policys

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Reglemente kommunstyrelsen
- Informationssäkerhetspolicy
- Riktlinje för informationssäkerhet
- Anvisningar inom informationssäkerhet
- Roller förvaltningsobjekt
- Underlag för informationsklassning och riskbedömning
- Handlingsplan för informationssäkerhet 2021-2024
- Informationssäkerhetsberättelse 2021

Intervjuer har genomförts med informationssäkerhetschef, IT-direktör, IT-säkerhetschef, gruppchef supportcenter IT/Supportteknik IT (innehar även rollen incident manager) samt objektägare och andra representanter från tre av regionens förvaltningsobjekt.

Rapporten är faktakontrollerad av verksamhetsföreträdare som deltagit i granskningen.

3 Resultat av granskningen

3.1 Styrande dokument

3.1.1 Informationssäkerhetspolicy

Regionfullmäktige i Region Sörmland har antagit en *informationssäkerhetspolicy*[1] som beskriver principerna för regionens informationssäkerhetsarbete. Policyn gäller för all information i regionen, samt för de bolag och stiftelser som arbetar på uppdrag av regionen.

Enligt policyn ska regionens informationssäkerhetsarbete skydda informationen inom verksamheten mot yttre och inre hot. Skyddet ska vara anpassat till skyddsvärdet, risk och lagkrav och därigenom möjliggöra för regionens verksamheter att uppnå sina mål.

Sex målområden anges i policyn som styrande:

- ✓ Säker och riskbaserad informationshantering
- ✓ God informationssäkerhetskultur
- ✓ Effektiv incidenthantering
- ✓ Robust informationshantering
- ✓ Informationssäkerhetsberättelse

Av policyn framgår att regionens informationssäkerhetsarbete styrs av ledningssystemet för informationssäkerhet. Ledningssystemet består av policyn med tillhörande riktlinjer och tillämpningsanvisningar.

3.1.2 Riktlinjer för informationssäkerhet

Regionstyrelsen har antagit R*iktlinjer för informationssäkerhet*[2] som ska styra regionens informationssäkerhets- och dataskyddsarbete. Riktlinjerna syftar till att förtydliga ansvaret för informationssäkerhetsarbetet i regionens linjeorganisation och för andra väsentliga roller.

Riktlinjen beskriver hur arbetet ska bedrivas och vilka krav som ställs på olika aktiviteter. Bland annat finns anvisningar över hur informationstillgångar ska kartläggas och hur personuppgifter ska behandlas. Det finns beskrivet hur personalsäkerhet och medarbetares ansvar är utformat och hur styrningen av åtkomst till regionens informationstillgångar ska hanteras. Det finns även tydliggjort hur incidenter ska hanteras.

Riktlinjerna inkluderar beskrivningar om krav och förfarande för arbetet med IT-säkerhet.

[1] Antagen 11 juni 2019, reviderad 23 november 2021
[2] Antagen den 4 juni 2019

3.1.3 Övriga styrande och stödjande dokument

Utöver ovan beskrivna styrande dokument finns även anvisningar för att ytterligare konkretisera arbetet med informationssäkerhet, exempelvis för incidenthantering, styrning av åtkomst och särskilda rutiner för att hantera skyddade personuppgifter.

I samband med intervjuer har sidor på regionens intranät visats. Där finns information för hantering av informationssäkerhet med instruktioner över vad som behöver göras i varje steg. Länkar till styrande dokument, rutiner och metoder finns även samlat under dessa sidor.

3.1.4 Bedömning

Finns aktuella och ändamålsenliga styrande dokument som tydliggör krav och hur arbetet ska bedrivas?

Vår bedömning är att det finns aktuella och ändamålsenliga styrande dokument. Dessa beskriver väl hur ansvaret är fördelat, vilka krav som ställs och hur arbetet ska bedrivas. De har nyligen reviderats och följer därigenom MSB:s rekommendation om att informationssäkerhetspolicy inte bör vara mer än tre till fem år gammal. Detta då informationssäkerhetsfrågorna är i snabb utveckling och styrningen därigenom behöver uppdateras med en viss frekvens för att inte riskera att bli föråldrad.

Vi anser att de nuvarande styrande dokumenten bör kompletteras med styrande dokument avseende IT-säkerhet då detta i nuläget endast är beskrivet på en övergripande nivå. Detta skulle bidra i en tydlighet över vilka krav som ställs på IT-säkerhetsåtgärder och hur dessa ska följas upp.

3.2 Organisation

I *Reglemente för regionstyrelsen*[3] framgår att styrelsen har det övergripande ansvaret för informationssäkerhet, säkerhets- och trygghetsarbetet i Region Sörmland. Det åligger styrelsen att styrande dokument inom området utarbetas och hålls aktuella. Regionstyrelsen har därtill ett uppföljningsansvar för arbetet med informationssäkerhet på regionövergripande nivå.

I *Informationssäkerhetspolicyn* framgår att varje nämnd och styrelse är ansvarig för informationssäkerhet och personuppgiftshantering inom sina respektive verksamhetsområden. I ansvaret ingår att årligen följa upp informationssäkerheten och personuppgiftshanteringen. I intervjuer beskrivs nämndernas roll som något otydlig vad gäller styrning och uppföljning av informationssäkerhetsarbetet.

I *Riktlinjer för informationssäkerhet* finns angivet att regiondirektören ansvarar för att informationssäkerhet bedrivs i linje med styrande dokument för informationssäkerhet. Informationssäkerhetsansvaret följer i övrigt det delegerade verksamhetsansvaret på tjänstemannanivå vilket innebär att ansvariga för verksamhet även har ansvar för informationssäkerhetsfrågorna. Ansvaret kan inte delegeras men arbetsuppgifter kan

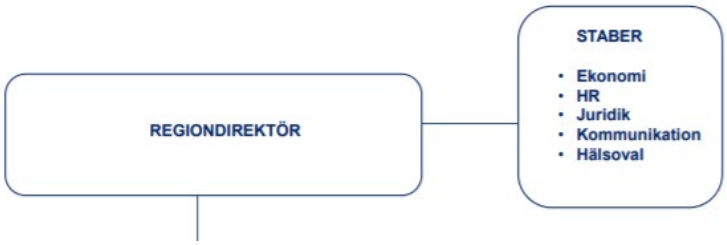
[3] Beslutat av regionfullmäktige 2021-04-27 § 14/21

fördelas. Av riktlinjerna framgår att regionen ska säkerställa att objektägare eller motsvarande stödjer informationsägaren i skyddet av informationstillgångarna.

Informationssäkerhetsarbetet där även IT-säkerhet ingår på övergripande nivå leds från informationssäkerhetsenheten. Region Sörmland IT ansvarar för det tekniska IT-säkerhetsarbetet. En definition av IT-säkerhet finns i *Riktlinjer för informationssäkerhet* ”Säkerhet i systemstöd för att uppnå och upprätthålla informationssäkerhet”.

3.2.1 Informationssäkerhetsenheten

Informationssäkerhetsenheten har i ansvar att skapa förutsättningarna för regionens systematiska informationssäkerhetsarbete. Informationssäkerhetsenheten ingår i regionens juridiska stab, som är en av regiondirektörens staber.



Inom enheten arbetar en informationssäkerhetschef och en handläggare. Informationssäkerhetschefen lyder direkt under chefsjuristen.

Enligt styrande dokument ingår bland annat följande i informationssäkerhetschefs ansvar:

- sammanställning och analys till regionen av regionens informationssäkerhetsarbetsberättelse.
- följa upp utbildningsnivån på regionövergripande nivå och rapportera genom ledningens genomgång.
- rapporterar händelser som har påverkat personuppgiftsbehandlingen till dataskyddsombud.
- årligen följa upp efterlevnaden av informationssäkerhetspolicy och riktlinje för informationssäkerhet.

I informationssäkerhetsenhetens uppdrag ingår att ge stöd till *processägarna* genom att ta fram styrdokument och metoder för att arbeta med informationssäkerhetsfrågor. Enheten ansvarar även för säkerhetsskyddet, samt för att ta fram utbildningsprogram och anordna utbildningar om informationssäkerhet.

Även det övergripande ansvaret för IT-säkerhet åligger informationssäkerhetsenheten.

3.2.2 Region Sörmland IT

Verksamhetsområde Region Sörmland IT (RSIT) ansvarar för regionens operativa IT-verksamhet. I uppdraget ingår bland annat att sköta IT-driften, arbeta med IT-arkitektur och IT-support samt projektledning. Verksamhetsområdet leds av en IT-direktör.

Inom verksamhetsområdet finns en IT-säkerhetschef som ansvarar för regionens IT-säkerhetsarbete. I *Riktlinjer för informationssäkerhet* framgår att ”regionen ska ha en utsedd ansvarig för att samordna och upprätthålla en teknisk säkerhetsnivå som motsvarar kraven för informationshanteringen och verksamheten som ska stödjas”. En hänvisning finns till NIS-direktivet[4], vilket regionen omfattas av som samhällsviktig verksamhet.

IT-säkerhetsansvarig har enligt riktlinjerna ansvar för att samordna arbetet inom enheten och se till att en tillräcklig teknisk säkerhetsnivå upprätthålls för IT-drift och IT-infrastruktur. Ansvarig har därtill i ansvar att samverka med nationella aktörer inom området, exempelvis Inera, MSB:s CERT[5] och Sveriges kommuner och regioner.

Inom IT-säkerhetsområdet finns det enligt uppgift även andra funktioner som genomför delar av IT-säkerhetsarbetet, däribland arkitekter. Konsulter nyttjas även vid behov av förstärkning av resurser.

Det finns inom organisationen ett supportcenter IT och supportteknik IT som leds av regionens incident manager tillika processledare för incidentprocessen. Servicedesk hanterar det vardagliga IT-flödet och hanterar IT-problem som anmäls av regionens användare.

3.2.3 Verksamhetsansvar och objektsförvaltning

Som vi beskrivit ovan följer informationssäkerhetsansvaret linjeansvaret, vilket innebär att alla verksamhetsområden behöver säkerställa att de har en organisation för att bedriva arbetet men även kännedom om hur dess ansvar ska upprätthållas och vilka aktiviteter som behöver genomföras. Linjeansvariga chefer är därmed informationsägare för information som hanteras inom sina respektive verksamhetsansvar. Vissa uppgifter har informationsägaren möjlighet att tilldela men ansvaret kan inte delegeras.

I linjeansvaret ingår bland annat att säkerställa att medarbetare har tillräckliga kunskaper för att upprätthålla informationssäkerheten samt att följa upp arbetet. Intervjupersoner uppger att det finns behov av att ytterligare tydliggöra ansvaret för informationssäkerhet i linjen. Vikten av att ytterligare tydliggöra inom respektive verksamhet hur information ska hanteras och vad som får dokumenteras i olika system och lagringsenheter som finns tillgängliga lyfts i intervjuer. Detta stärks av ytterligare uppgifter från intervjuer där en beskrivning ges att risker inom informations- och IT-säkerhet i nuläget inte ingår i verksamheternas ordinarie processer med riskanalyser.

[4] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster syftar till att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga verksamheter. Hälso- och sjukvård är identifierad som en samhällsviktig verksamhet.
[5] CERT-SE är Sveriges nationella Computer Emergency Response Team med uppgift att stötta samhället i arbetet med att hantera och förebygga It-incidenter.

Regionen har sedan 2016 en förvaltningsstyrningsmodell som utgår från modellen pm3. I modellen finns ett dokument som vi tagit del av som tydliggör olika ansvar och roller både på strategisk och operativ nivå. Modellen bygger på att det ska finnas representation från verksamhet och IT i arbetet med förvaltning och utveckling av de system som används inom respektive verksamhet. En viktig roll är förvaltningsledare vilket är en funktion som leder det verksamhetsnära förvaltningsarbetet och förvaltningsledare IT som leder det IT-nära förvaltningsarbetet. I uppgifterna för dessa roller ingår hantering av informationssäkerhetsfrågor för den information som hanteras i IT-komponenter (system, funktioner och applikationer).

Förvaltningsorganisationen har ofta kontakt med informationssäkerhetsenheten för att få stöd i arbetet. I intervjuer beskrivs att behovet av stöd är större än informationssäkerhetsenheten har möjlighet att bistå med. Det har dock skett en förstärkning som upplevs positiv och varit viktig för förvaltarnas arbete med informationssäkerhet. Trots förstärkningen uppger intervjuade från verksamhetsområden att förutsättningarna för att uppfylla krav i interna styrdokument och lagkrav skulle stärkas om ytterligare stöd fanns att tillgå.

3.2.4 Samordning mellan verksamhet och centrala funktioner

I intervjuer framkommer att ansvarsfördelningen mellan framför allt informationssäkerhetsenheten och RSIT uppfattas som något oklar. Enligt uppgift pågår en dialog om gränsdragning mellan enheterna. På övergripande nivå styrs arbetet med IT-säkerhet genom de beslutade styrdokumenten inom informationssäkerhet. Det är dock inte tydliggjort vilka krav som ställs på infrastruktur och drift samt hur detta arbete ska genomföras i praktiken. Det finns inte några kompletterande styrdokument vid sidan om *Riktlinjer för informationssäkerhet* specifikt för IT-säkerhetsarbetet.

Verksamhetsföreträdare betonar vikten av att skapa ett gemensamt synsätt i hela verksamheten så att arbetet kan ske i samverkan mellan RSIT, informationssäkerhetsenheten och samtliga verksamheter i regionen.

I regionen finns ett antal forum med representation från olika verksamheter och funktioner där informationssäkerhetsfrågor diskuteras. Dessa beskrivs även i riktlinjer för informationssäkerhet. I intervjuer lyfts dock att befintliga grupperingar för närvarande utvärderas för att hitta en form och representation som kan få arbetet att utvecklas vidare.

Utöver de grupper som nämns i styrande dokument arrangeras gemensamma möten från förvaltningskontoret där objektsförvaltare träffas. Enligt intervjupersoner innehåller dessa möten i stora delar frågor som rör informationssäkerhet och dataskyddsarbetet.

På regionledningsnivå finns ett IT-råd som utgörs av koncernledningen där ledningsgruppen övergår till IT-råd del av sina möten. Vid dessa tillfällen är förvaltningskontoret föredragande tillsammans med RSIT.

3.2.5 Bedömning

Är roller och ansvar tydliggjorda och uppfattade mellan regionstyrelse, nämnder, verksamhet, informationssäkerhetsenhet och IT-organisation?

Regionstyrelsen har genom beslut om styrande dokument tydliggjort ansvarsfördelning och de aktiviteter som ingår i regionens ledningssystem för informationssäkerhet. Vår bedömning är att regionens förvaltningsstyrningsmodell har bidragit till att etablera en tydlig roll- och ansvarsfördelning mellan verksamhet och IT-organisation.

Stora delar av verksamheternas informationssäkerhets- och dataskyddsarbete har inkluderats i arbetet med förvaltningsobjekten och de roller som finns tillsatta i det arbetet. Med den ansvarsfördelning som finns i nuläget ser vi en risk att vissa delar av informationssäkerhetsansvaret inte upprätthålls då arbetet i nuläget har stort fokus på system och teknik. Exempelvis vill vi lyfta det viktiga linjeansvaret att medarbetare har tillräckliga kunskaper om informationssäkerhet och hanterar information på ett korrekt sätt. Samt att verksamheten inkluderar risker för informationssäkerhet i verksamhetens ordinarie riskanalysarbete.

Vår bedömning är att roll- och ansvarsfördelning mellan informationssäkerhetsenheten och RSIT bör tydliggöras ytterligare.

Därtill anser vi att informationssäkerhetschefens roll bör utvärderas för att säkerställa att denna har mandat att följa upp verksamheternas arbete och ställa krav om efterlevnad av interna styrdokument.

För att möjliggöra en utveckling av informationssäkerhetsarbetet som står i relation till nya hot och risker anser vi att regionstyrelsen bör se över om nuvarande resurser är tillräckliga i förhållande till de krav som ställs. Vi avser här resurser inom förvaltningsobjekten, informationssäkerhetsenheten samt RSIT.

3.3 Regionens mål för informationssäkerhetsarbetet och våra iakttagelser

3.3.1 Säker och riskbaserad informationshantering

”Informationstillgångar klassificeras och riskbedöms samt hanteras utifrån dess skyddsbehov, så att den är riktig och tillgänglig när den behövs och skyddas mot obehörig åtkomst. Detta för att värna verksamhetens förmåga att utföra sitt uppdrag och skydda individer mot skada. Lika viktigt är att värna integriteten för medborgarna. Medborgarna ska känna trygghet i att regionen omhändertar deras intressen avseende integritet och säkerhet i behandlingen av deras uppgifter”.

Informationssäkerhetsanalys

Enligt *Riktlinje för informationssäkerhet* ska samtliga informationstillgångar (system, datorer, nätverkskomponenter etc.) i regionen analyseras i form av en rättslig analys, en risk- och informationsklassning och en riskanalys. Analyserna ska genomföras för att bedöma informationens skyddsnivå. Skyddsnivån ska således baseras på de risker en informationstillgång kan utsättas för. De risker som identifieras i riskanalysen ska enligt riktlinjen dokumenteras. Vidare ska ett riskhanteringsbeslut tas, vilket redogör för om risken accepteras eller om risken behöver minskas.

För att fånga det praktiska arbetet med informationssäkerhet i regionen har vi i granskningen valt ut tre förvaltningsområden för att inhämta information om hur arbetet bedrivs i praktiken för de objekt som ingår i respektive förvaltningsområde. De förvaltningsområden som valts ut är: Vård och hälsa, Personal och Personresor.

I intervjuer beskriver representanter från förvaltningsobjekten att det ingår i deras uppgifter att göra en informationssäkerhetsanalys för de system som de förvaltar. Sedan januari 2021 har regionen använt sig av systemet ISMS[6] som systemstöd i sina informationssäkerhetsanalyser. I samband med implementeringen av systemstödet har det genomförts lärarledda utbildningar om hur informationssäkerhetsanalyserna ska genomföras och hur systemet fungerar. Utbildningarna är inspelade och vid behov kan förvaltare ta del av dessa upprepade gånger. Informationssäkerhetsenheten finns som stöd i arbetet, dock poängteras det i intervjuer att enheten pga. få resurser inte alltid kunnat vara tillgängliga i den mån som det funnits behov av. Representanter från förvaltningsobjekten framför att stödet från informationssäkerhetsenheten kan utvecklas, men att det finns en förståelse för den begränsade resurstillgången.

I arbetet med systemstödet är det ansvarig för respektive IT-komponents som sätter ihop en grupp som genomför analysen. Enligt uppgift är det oftast de funktioner som har till uppgift att förvalta IT-system i förvaltningsobjekten som genomför analyserna. I intervjuer framförs att informationstillgångarna läggs in manuellt i ISMS. Vidare görs en kartläggning av informationen, en rättslig analys och sedan en informationsklassning utifrån konfidentialitet, riktighet och tillgänglighet. ISMS sammanställer sedan informationen och presenterar krav för informationstillgången utifrån olika områden.

[6] Information Security Management System, ett systemstöd för att stödja verksamheter i efterlevnad av GDPR och certifiering av informationssäkerhetsarbete i enlighet med ISO 27001.

Vidare görs en riskanalys där risker fastställs och åtgärder sedan tas fram för respektive riskområde.

I intervjuer påpekas att frågeställningarna som ska besvaras i ISMS är många till antalet, vissa frågeställningar uppges även vara relativt lika varandra. Detta bidrar enligt *verksamhetsföreträdare* (syftar på förvaltningsobjekten här) till att arbetet ofta blir väldigt tidskrävande och administrativt tungt. En annan synpunkt som lyfts är att språket i systemet ibland är avancerat och att svårförståeliga juridiska termer ofta förekommer, vilket kan leda till svårigheter att tolka och bedöma frågeställningen.

I intervjuar poängteras att förvaltningsobjekten kommit olika långt med antalet informationstillgångar som analyserats. Informationssäkerhetsenheten har möjlighet att följa upp antalet informationsklassningar då dessa dokumenteras i systemstödet.

Arbetet är fortfarande i en uppstartsfas och enligt intervjupersoner så har det hittills behövt fokuseras på att genomföra klassningar. Därför har inte processen för att vidta åtgärder kommit i gång på ett strukturerat sätt. De informationssäkerhetsanalyser som gjorts har främst visat på risker med åtkomst till information vilket gett en indikation på att behörigheter behöver ses över. Utifrån det har vissa åtgärder vidtagits för att möta risker.

Arbetet med att ompröva riskanalyser och informationsklassningar uppges inte prioriteras. Omprövningar ska enligt verksamhetsföreträdare ske vid större förändringar.

Åtkomst och behörigheter

Regler för åtkomst och behörighet till regionens informationstillgångar stadgas i *”Riktlinje för informationssäkerhet”*. Det finns även kompletterande anvisningar inom åtkomsthantering. Det framgår att åtkomsten till informationstillgångar ska analyseras utifrån behov, uppdrag, legitimation, delegation, kategori av medarbetare och andra eventuella omständigheter. Enligt riktlinjen ska åtkomsten till IT-stöd och nätverk begränsas och grundregeln är att neka åtkomst. System har olika identifieringskrav utifrån skyddsvärde.

Enligt *Riktlinjen för informationssäkerhet* är det verksamhetschef för respektive verksamhet som är ytterst ansvarig för att godkänna behörigheterna till medarbetare med stöd av IT. Enligt uppgifter förekommer det att ansvaret inom vissa verksamheter delegerats. Det ska göras en risk- och sårbarhetsanalys inför varje tilldelning, vilket är i enlighet med regionens riktlinjer för informationssäkerhetsarbete. I intervjuer konstateras det vara oklart i vilken utsträckning dessa analyser genomförs.

Inom supportcenter finns en administrativ gruppering som arbetar med behörighetstilldelning till regionens IT-system där dessa driftas lokalt. I dagsläget sker hanteringen av behörigheter till stor del manuellt. Beställning sker via självserviceportalen och ett ärende skapas. Den enda automatiserade processen som finns idag är då medarbetare anställs i regionen och HR-systemet automatiskt ger en signal så att det skapas ett konto och en e-postadress i Windows.

Det uppges i intervjuer finnas vissa brister i uppföljningen av behörigheter. Det pågår enligt uppgift ett arbete med att göra återkommande revision för att följa upp tilldelade

behörigheter och dess aktualitet. IT-säkerhetschefen har fått uppdraget att genomföra ett arbeta avseende regionens digitala arbetsplats med fokus på åtkomsthantering och behörighet. Projektet ska inbegripa en förstudie som ska vara färdigställd i slutet av mars år 2022. Projektet genomförs genom en GAP-analys med beskrivningar om nuläget och framtida behov. Utifrån projektet ska regionen fastställa mål och en strategi för arbetet med åtkomstantering.

I dagsläget saknas struktur för loggkontroller och logganalyser på regionövergripande nivå för användare och trafik på nätverket. Det betonas i intervjuer att det saknas resurser för att arbeta aktivt med denna fråga. Det framhålls att ett SOC-team[7] planeras att etableras inom RSIT så att ett mer aktivt arbete kan genomföras med bland annat loggar.

Supportcenter tilldelar inte behörigheter till journalsystem och IT-komponenter inom Personresor. Inom Personresor hanteras behörigheter av objektspecialister. IT-komponenter som ingår inom förvaltningsområde Personresor och Vård och hälsa är stöd till samhällsviktig verksamhet där förstärkta krav finns i enlighet med NIS-direktivet[8].

Inom förvaltningsobjektet Vård och hälsa finns krav att loggkontroller ska göras. I intervjuer framhålls att det enligt rutiner ska göras loggkontroller en gång i månaden och att ansvar för att dessa görs och följs upp åligger verksamhetschefer. Enligt uppgift finns idag inget system för hur loggkontrollerna ska genomföras men rutiner finns framtagna. Resultatet av kontroller ska rapporteras vidare till hälso- och sjukvårdsledningen.

3.3.2 God informationssäkerhetskultur

Behovet av skydd av information bedöms och är en central del i arbetet på alla nivåer i verksamheten utifrån de risker och hot som finns mot informationen och medarbetare är medvetna om sitt ansvar som användare.

Som beskrivits i avsnitt 3.3.1 så pågår ett arbete med att upprätta informationssäkerhetsanalyser för den information som hanteras i verksamheternas informationssystem. Resultatet av analyserna presenteras i form av en handlingsplan för att möta de risker som identifierats.

Det finns enligt uppgift en del övervakningsverktyg och tekniska säkerhetsskydd som kan stoppa olika former av intrång. Med hjälp av systemen loggas intrången, däremot konstateras det i intervju att loggarna inte läses i detalj och att regionen inte automatiskt får rapporter vid dessa händelser. RSIT genomför regelbundet sårbarhetsskanning för att identifiera eventuella sårbarheter i regionens IT-miljö och dess komponenter för att i förebyggande syfte minimera risker för att intrång ska ske på grund av bristande säkerhetsuppdateringar mm. I informationssäkerhetsberättelse 2021 beskrivs att regionens förmåga att upptäcka, identifiera och agera vid ett angrepp är begränsad och behöver stärkas.

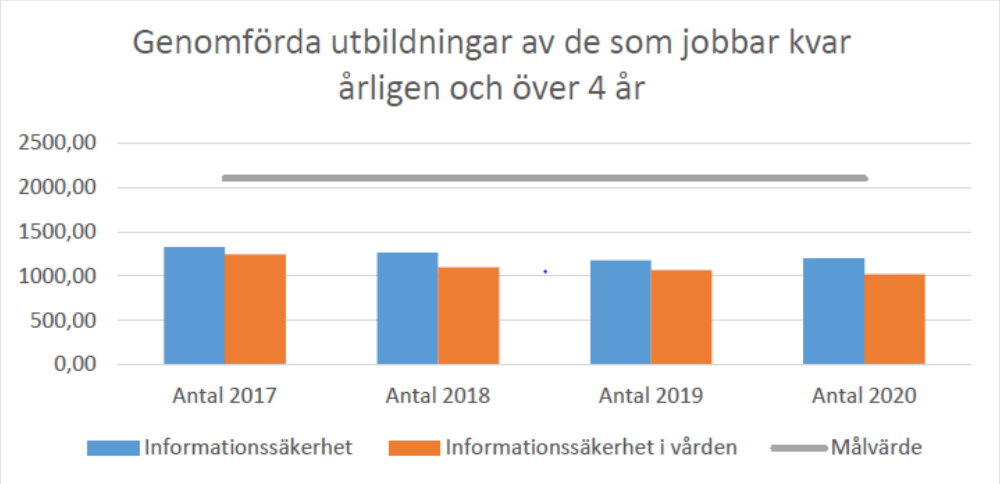
[7] Security Operations Center (SOC)
[8] The Directive on security of network and information systems. Direktivet kravställer åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom EU.

Av *Riktlinje för informationssäkerhet* framgår att regionen ska säkerställa att medarbetare och chefer har kännedom, kunskap och förmåga att agera säkert utifrån de risker och hot som finns med informationshanteringen. Verksamhetsansvarig ansvarar för att alla medarbetare ges introduktion i informationssäkerhet och följer regler, rutiner och har en tillräcklig nivå av kompetens.

I intervjuer beskrivs att utbildning i informationssäkerhet är obligatorisk och en del i introduktionen för alla regionens nyanställda. För vårdpersonal finns det även kompletterande utbildningar. Utbildningen finns på regionens kompetensportal och är en digital e-utbildning. Det är respektive chefs ansvar att följa upp att deras anställda genomfört utbildningen. Genom att utbildningen finns i kompetensportalen registreras genomförandet och det finns en bekräftelse på att utbildningen är genomförd, vilket medför en god möjlighet att följa upp andel som genomfört utbildning.

I nuläget uppger intervjupersoner att det saknas rutiner för återupprepade utbildningar inom informationssäkerhet. Det finns inte heller någon begränsning i exempelvis åtkomst till system och information beroende av om medarbetare genomfört utbildning eller ej.

I informationssäkerhetsberättelsen som årligen tas fram redovisas hur stor andel av medarbetarna som genomfört utbildning. Målvärdet är att 25 % ska genomföra utbildningen årligen för att det ska ske en regelbunden kompetensökning. I uppföljningen finns följande diagram presenterat, vilket visar att målvärdet för andel som genomfört utbildning årligen inte har nåtts de senaste fyra åren. Därtill beskrivs i berättelsen att närmare 20 % av de som genomfört utbildning 2020 varit tillfälliga medarbetare som inte längre finns kvar i verksamheten.



I intervjuer beskrivs att det inte finns en tillräckligt väl grundläggande förståelse för och kompetens inom informationssäkerhet bland regionens medarbetare. Det betonas även att det generellt är en utmaning att nå ut till medarbetare med information om de risker som finns i det vardagliga arbetet.

3.3.3 Robust informationshantering

Verksamheternas informationssystem och IT-infrastrukturen är riskbedömda och kontinuitetsplanerad där åtgärder som ska vidtas vid avbrott, störningar och kriser är planerade, testade och övade.

I *Riktlinje för informationssäkerhet* framgår att regionen ska planera för att kunna upprätthålla samhällsviktig verksamhet och viktiga funktioner för samhället vid bortfall av informationstillgångar och/eller informationssystem.

Riskanalys

I arbetet med informationssäkerhetsanalys ingår även en riskanalys. Arbetet genomförs inom ramen för förvaltningsobjekten. Enligt uppgift är det ett tidskrävande arbete, vilket medför att kraven på riskanalyser är ett pågående arbete och alla informationssystem är inte riskbedömda vid tiden för granskningen. Sedan införandet av ISMS finns systemstöd för genomförande och dokumentation vilket innebär att riskanalyser kommer finnas dokumenterade när arbetet är slutfört. De förvaltningsobjekt med stort antal system anger att de inte har resurser för att nå kraven inom överskådlig tid. För att klara det skulle det krävas att det ordinarie arbetet med systemförvaltning och utveckling skulle behöva läggas åt sidan.

RSIT genomför löpande riskanalyser utifrån olika komponenter. Nyligen har en riskanalys upprättats utifrån den förhöjda hotbilden i samhället och sett över hur det kan påverka regionens IT. Det har under året gjorts en säkerhetsanalys övergripande för IT-miljön med hjälp av en extern leverantör.

Därtill beskrivs i intervjuer att RSIT löpande vidtar säkerhetsåtgärder utifrån verksamheternas informationssäkerhetsanalyser och klassningar. Som vi beskrivit tidigare behöver dock processen etableras så att de genomförda klassningarna leder till kravställningar av IT-säkerhetsåtgärder när det finns behov av det, vilket enligt uppgift inte finns etablerat ännu i alla verksamheter. Fokus har varit att göra analyser och dokumentera i det nya systemstödet.

Intervjupersoner beskriver vidare att etableringen av en SOC-grupp syftar till att systematisera arbetet med risker och åtgärder. Det har även lyfts som en prioriterad åtgärd i verksamhetsplanen för IT och resurser för etableringen har äskats.

Kontinuitetsplanering

Det uppges i intervjuer att kontinuitetsplaner saknas i stora delar av organisationen. Det är verksamheterna som behöver bedöma behov av kontinuitetsplaner för att upprätthålla verksamhet om det sker en incident eller störning i IT-miljön som påverkar förmågan att leverera i kärnverksamheten. Inom förvaltningsobjekten ingår att bedöma hur kritiska systemen är och hur lång den acceptabla bortfallstiden är innan systemet måste vara i drift efter ett bortfall eller störning. Det framkommer i intervjuer att det skett en del allvarliga incidenter i regionen vilket lett till att reservrutiner har behövts i skarpt läge. I dessa fall hade inga tidigare tester genomförts under kontrollerade former för att bedöma om rutinerna var tillräckliga. Intervjupersoner menar att rutinerna fungerade i de fall som de behövdes.

Inom RSIT har varje grupp fått i uppdrag att ta fram en plan. För närvarande finns ett utkast till en kontinuitetsplan inom Service Desk. Enligt uppgift ska kontinuitetsplanerna utgå ifrån krisberedskapsplanen. Kontinuitetsplaneringen uppges vara ett löpande arbete som sker i samverkan mellan krisberedskapsenheten och IT-direktören.

Det framförs i intervju att det saknas en övergripande kontinuitetsplan för hela regionen. Verksamhetsföreträdare menar att det inte är tydliggjort vad verksamheterna har för krav på sig vid stora avbrott och störningar och hur det kan påverka regionen som helhet.

3.3.4 Effektiv incidenthantering

Regionen har förmåga att hantera och lära av allvarliga informationssäkerhetsincidenter.

I *Riktlinje för informationssäkerhet* regleras regionens incidenthantering. Där framgår att regionen ska säkerställa att det finns processer, metoder och rapporteringsvägar för incidenter i informationssystem och informationstillgångar. Riktlinjerna anger även hur rapportering av olika incidenter ska göras utifrån vilken typ av incident som sker och till vilken myndighet dessa ska rapporteras utifrån olika lagar och direktiv.

Av informationssäkerhetsberättelse 2021 framgår att ett antal allvarliga incidenter har inträffat under 2020 som påverkat regionens möjligheter att bedriva en effektiv och god vård under kortare eller längre tid. Incidenter i regionens informationsstöd beror enligt berättelsen till stor del på misstag hos egen eller externa leverantörers personal. Även felkonfigureringar, brister i programvara eller uppdateringar är vanliga orsaker.

Flera personuppgiftsincidenter har rapporterats till Datainspektionen, ingen av dessa har dock lett till beslut om åtgärd från Datainspektionen. I handlingsprogram för informationssäkerhet 2021-2024 finns som särskilt viktig åtgärd att regionen behöver stärka incidentrapporteringen kring rapporteringsskyldiga incidenter och att detta ska ske genom en central hantering.

I intervjuer beskrivs regionens incidenthanteringsrutiner. Incidenter ska rapporteras till Servicedesk på RSIT via regionens självbetjäningsportal. Incidenterna dokumenteras därefter i ärendehanteringssystemet. Enligt uppgift går det även att ringa eller mejla Servicedesk för att upprätta ett ärende. Servicedesk gör vidare en bedömning av incidenten, om den är kritisk eller inte och sedan sker en kategorisering beroende på incidentens karaktär. I informationssäkerhetsberättelse 2021 framgår att kategoriseringen behöver utvecklas för att korrekta bedömningar och analyser ska kunna göras. En så kallad incident manager finns utsedd som hanterar anmälda incidenter utifrån interna rutiner och processer inom RSIT.

Beroende på allvarsgrad och komplexitet i händelser eskaleras ärendet vidare i regionen till berörda funktioner. I de fall en incident har direkt koppling till informationssäkerhet distribueras ärendet till informationssäkerhetschefen och/eller dataskyddsombudet. När en incident av allvarligare karaktär inträffar finns etablerade rutiner andra funktioner i regionen kopplas in, exempelvis tjänsteman i beredskap, chefen för patientsäkerhetsenheten, IT-direktör och andra kritiska kompetenser inom IT.

Verksamhetsföreträdare framhåller att uppföljning av inträffade incidenter är ett utvecklingsområde. Exempelvis så är incident manager endast inblandad inledningsvis men inte det fortsatta analys- och uppföljningsarbetet. Därtill finns en problematik utifrån det vi beskrivit tidigare, att en felaktig kategorisering eller bedömning inledningsvis i processen kan leda till att berörda funktioner inte blandas in i tillräckligt hög grad eller att samband missas i analyser på övergripande nivå.

3.3.5 Informationssäkerhetsberättelse och handlingsprogram

Ledningen och regionstyrelsen ska informeras av särskild utsedda roller om informationssäkerhetsläget och dataskydd i regionen samt om vilka åtgärder som bör vidtas.

I *Riktlinje för informationssäkerhet* fastslås att varje nämnd och styrelse ansvarar för att följa upp informationssäkerheten inom sitt verksamhetsområde. Det är informationssäkerhetschefen som ansvarar för sammanställning av uppföljning och för att göra en analys som presenteras i regionens informationssäkerhetsberättelse. Denna rapporteras till regionstyrelsen som samtidigt fattar beslut om ett handlingsprogram med viktiga förbättringsåtgärder för informationssäkerheten.

Enligt ärendet för den senaste rapporteringen till regionstyrelsen[9] baseras berättelsen på ett antal källor. Bland annat data från sårbarhetsscanning, incidentrapportering, uppföljning genom egenkontroll samt statistik avseende avvikelser, utbildningar och genomförda riskhanterande åtgärder.

Som vi beskrivit tidigare i rapporten är implementeringen av ISMS en del i att stärka möjligheten att följa upp informationssäkerhetsarbetet. Informationssäkerhetschef hämtar numera vissa uppgifter från systemstödet för att upprätta informationssäkerhetsberättelsen, exempelvis uppgifter om utbildning och antal genomförda informationssäkerhetsanalyser.

Handlingsprogrammet 2021-2024 förtydligar regionens övergripande mål för informationssäkerheten och syftar till att konkretisera och skapa tydligare uppföljning för kommande treårsperiod. Handlingsprogrammet ska revideras årligen utifrån det som framkommit i informationssäkerhetsberättelsen och anger på övergripande nivå de åtgärder som ska genomföras under 2021.

Informationssäkerhetschef har inte genomfört några interna revisioner för att säkerställa efterlevnad av styrande dokument. Vi kan dock notera av den uppföljning som sammanställts till informationssäkerhetsberättelsen och uppgifter som lämnats i intervjuer att det finns områden där inte riktlinjerna följs fullt ut.

Det pågår ett pilotprojekt om att inkludera informationssäkerhet i den egenkontroll som verksamheterna gör utifrån olika ledningssystem, detta som ett sätt att stärka uppföljningen av informationssäkerhet. Det är dock inte möjligt vid tiden för granskningen att bedöma detta då arbetet är i en uppstartsfas.

[9] Regionstyrelsen 2021-03-30 § 50/21 § 50/21 §

3.3.6 Bedömning

Finns systematiskt arbete för att identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering?

Vår bedömning är att regionen i stora delar har etablerat metoder och stöd för att systematiskt identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering. Krav är tydliggjorda i styrande dokument och vi bedömer att ansvaret för dessa aktiviteter är uppfattat i verksamheten.

Vi bedömer att efterlevnad av de krav som ställs i styrande dokument inte i tillräckligt hög grad kontrolleras. Vi kan därtill konstatera att de krav som ställs inte efterlevs fullt ut. Det avser bland annat att obligatoriska utbildningar i informationssäkerhet inte genomförs av medarbetare, att informationstillgångar inte är klassade och riskbedömda för samtliga informationssystem samt att kontinuitetsplaner saknas i stora delar. Vi noterar därtill att regionen behöver säkerställa att rutiner för och uppföljning av hantering av behörigheter och loggkontroll följs. Detta är en väsentlig del i en robust informationshantering där endast behöriga får tillgång till den information som de har behov av utifrån roll och uppgift.

Eftersom inga interna revisioner görs av verksamheternas informationssäkerhets-arbete finns risk att viktiga åtgärder för att säkerställa en robust informationshantering missas, vilket skulle kunna leda till både ekonomisk skada och förtroendeskada för regionen. Vi anser därför att den interna kontrollen bör stärkas samt att interna revisioner av informationssäkerhetsarbetet genomförs.

Har styrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete?

Genom att de obligatoriska utbildningarna inte har genomförts av samtliga medarbetare är vår bedömning att styrelsen inte har säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete. Utbildning är en väsentlig del för att etablera en grundläggande kunskap hos medarbetare. Den mänskliga faktorn utgör procentuellt sett den största risken för att informationstillgångar ska komma till skada på grund av bristande rutiner i informationshanteringen. Det är därför av stor vikt att rutiner för återkommande utbildning för nyanställda, befintliga anställda och förtroendevalda upprättas och sedan följs upp.

Genomförs systematiska uppföljningar av vidtagna IT-säkerhetsåtgärder för att upptäcka eventuella brister?

Då det inte är tydliggjort vilka krav som ställs på IT-säkerhetsåtgärder och hur uppföljning ska ske mer än på övergripande nivå kan vi inte uttala oss om arbetet är tillräckligt. Vi noterar att det delvis finns etablerade arbetssätt och funktioner för uppföljning av vidtagen IT-säkerhet för att upptäcka eventuella brister.

Vi ser positivt på att regionen avser att etablera arbetssätt för att strukturera säkerhetsarbetet organisatoriskt genom etableringen av SOC.

Den uppföljning i form av informationssäkerhetsberättelse som presenteras för regionstyrelsen ger en bra överblick av det regionövergripande arbetet. Vi noterar att åtgärder avseende IT-säkerhetsarbetet ingår som en del i detta.

Har styrelsen säkerställt en ändamålsenlig incident-och kontinuitetshantering?

Vår bedömning är att styrelsen i vissa delar har säkerställt en ändamålsenlig incidenthantering. Rutiner finns för att anmäla incidenter tillsammans med interna rutiner för hantering samt utsedd incident manager.

Med hänvisning till att det finns risk för att mognaden och medvetenheten om informationssäkerhet i verksamheten är alltför låg finns en betydande risk att incidenter inte upptäcks och hanteras i tillräckligt hög grad. Därav är utbildning dels i vad som är incidenter och hur dessa ska hanteras viktigt, dels att de som tar emot anmälningar har kunskap om allvarsgrad för att kategorisera incidenter tillsammans med god kännedom om rutiner i incidenthanteringsprocessen.

Vår bedömning är att styrelsen inte har säkerställt en ändamålsenlig kontinuitetshantering då dokumenterade planer saknas i stora delar. Dessa bör skyndsamt upprättas så att verksamheter kan fortgå samt återgå med så lite skadeverkan som möjligt om en attack eller annan störning sker.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen delvis säkerställer en god intern styrning och kontroll av IT/informationssäkerhetsarbetet som ger en ändamålsenlig informationssäkerhet med god uppfyllelse av informationssäkerhetspolicyns mål.

Genom styrande dokument har styrelsen tydliggjort ansvar och vilka krav som ställs på informationssäkerhetsarbetet. I nuläget saknas dock styrande dokument som tydliggör ansvar och krav inom IT-säkerhetsarbetet som endast beskrivs på övergripande nivå i riktlinjer.

I stora delar finns etablerade metoder och stöd för att systematiskt identifiera, hantera och åtgärda risker och behov för att säkerställa en robust informationshantering. Vi bedömer dock att efterlevnad av de krav som ställs i styrande dokument inte i tillräckligt hög grad kontrolleras. Inom vissa delar har vi i granskningen identifierat en bristande efterlevnad. Det är bland annat att obligatoriska utbildningar för medarbetare inte genomförs, att informationstillgångar endast delvis är klassade och riskbedömda samt att kontinuitetsplaner saknas i stora delar. Det är inte tydliggjort vilka krav som ställs på IT-säkerhetsåtgärder och hur uppföljning ska ske mer än på övergripande nivå vilket innebär att vi inte kan uttala oss om arbetet är tillräckligt. Vi noterar att det delvis finns etablerade arbetssätt och funktioner för uppföljning av vidtagen IT-säkerhet för att upptäcka eventuella brister.

Genom att de obligatoriska utbildningarna inte har genomförts av samtliga medarbetare är vår bedömning att styrelsen inte har säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete. Det leder till att det finns en betydande risk att incidenter inte upptäcks och hanteras i tillräckligt hög grad trots att det finns etablerade rutiner för hantering av incidenter. Vår bedömning är vidare att regionstyrelsen inte har säkerställt en ändamålsenlig kontinuitetshantering då dokumenterade planer saknas i stora delar.

En bedömning av resurser bör göras för att säkerställa att dessa står i relation till de krav som ställs i arbetet. I nuläget förklaras en bristande efterlevnad med att resurser inte räcker till för att prioritera aktiviteter inom informationssäkerhetsarbetet. Det påverkar därtill förutsättningar att följa upp det arbetet och identifiera förbättringsåtgärder för att säkerställa en robust informationshantering.

För att stärka den interna styrningen och kontrollen och i högre grad säkerställa ändamålsenligheten i Informationssäkerhetsarbetet och god uppfyllelse av informationssäkerhetspolicyns mål rekommenderar vi regionstyrelsen att:

- Utvärdera om befintliga resurser för informationssäkerhetsarbetet är tillräckliga för att möta nya hot och risker samt de interna krav och lagkrav som finns.
- Stärka den interna kontrollen avseende efterlevnad av styrande dokument inom informationssäkerhet. Samt säkerställa att informationssäkerhetschef har mandat att genomföra interna revisioner där brister kan identifieras och påtalas för ansvariga.
- Fastställa styrande dokument för IT-säkerhetsarbetet som bland annat kan tydliggöra ansvar, krav på åtgärder samt uppföljning av vidtagna åtgärder.
- Säkerställa att de obligatoriska utbildningarna inom informationssäkerhet genomförs regelbundet för samtlig personal och förtroendevalda.
- Skyndsamt upprätta kontinuitetsplaner och regelbundet testa rutiner så att verksamheter, IT-infrastruktur och kommunikation kan fortgå/återgå med minimerad skadeverkan i händelse av avbrott eller allvarlig störning inom IT.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Veronica Hedlund Lundgren
Certifierad kommunal revisor