Revisionskontoret 2016-12-09 Dnr: REV 16/2016

Ulf Rubensson
Certifierad kommunal revisor
Tfn: 063-147529

Rapport från förstudie avseende granskning av IT-säkerheten/ informationssäkerheten

SAMMANFATTNING

Vårt samlade intryck är att det pågår ett aktivt arbete mot målet att säkerställa informationssäkerheten. Det finns dock en mängd kända brister av varierande allvarlighetsgrad. Åtgärder vidtas löpande, men inte i tillräcklig takt.

Det finns enligt vår mening några mycket angelägna förbättringsområden som vi vill rekommendera styrelsen att särskilt bevaka.

Dessa är främst:

- Bevaka att informationsklassning genomförs och hålls aktuell
- Bevaka att systemförvaltningsmodellen utvecklas eller byts
- Bevaka att uppföljningen av standarden ISO27001, så långt möjligt, finner ändamålsenliga former.
- Se till att användarna har de kunskaper som behövs ur ett säkerhetsperspektiv.
- Säkerställ och tydliggör resurser för åtgärder som bedömts vara nödvändiga att genomföra.

BAKGRUND

En förutsättning för att Region Jämtland Härjedalen ska kunna bedriva en effektiv och säker verksamhet är fungerande och säkra IT-system. Det är viktigt att informationen i systemen inte kan bli manipulerade utan är korrekt och riktig, tillgänglig för personal och patienter samt att ingen obehörig får tillgång till informationen. Det är också viktigt att det finns en spårbarhet som gör att man i efterhand kan identifiera vem som har gjort vad och när.

Det har tidigare framkommit vissa brister inom regionens informationssäkerhet. Bl.a. inom områden som ansvarsfördelning och otillräckliga förutsättningar för systemägare att leva upp till de krav som ställs. Vidare har revisorerna i tidigare granskningar noterat brister vad avser förekomsten av systematiska genomgångar av säkerheten i IT-system samt brister i förmåga/resurser att åtgärda det som bedömts behöver åtgärdas.

Ett eftersatt säkerhetsarbete kan innebära risk för att t ex sekretess inte upprätthålls, att patientuppgifter förvanskas eller att dokumentation inte är tillgänglig för behöriga användare.

Enligt informationssäkerhetspolicyn[1] ska informationssäkerhetsarbetet bedrivas på ett formaliserat och riskorienterat sätt och ta sin utgångspunkt i den internationella ledningssystemstandarden för informationssäkerhet, ISO/IEC SS 27001:2014.

Regionens revisorer har mot bakgrund av ovanstående i sin risk- och väsentlighetsanalys bedömt det angeläget att granska informationssäkerheten och har därför tagit med en förstudie av området i revisionsplanen för 2016, med syfte att ge underlag för bedömning av om det finns anledning till en fördjupad granskning avseende informationssäkerhetsarbetet.

AVGRÄNSNING

Förstudien är avgränsad till åtgärder inom områdena IT och informationssäkerheten på övergripande ledningsnivå inom Region Jämtland Härjedalen.

ANSVARIG NÄMND/STYRELSE

Ansvarig nämnd är styrelsen för Region Jämtland Härjedalen.

REVISIONSKRITERIER

Revisionskriterierna utgår, i tillämpliga delar, främst från krav i:

- Kommunallagen
- Patientdatalagen
- Socialstyrelsens föreskrifter om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården (SOFS 2011:9 och föreskrift en om informationshantering och journalföring i hälso- och sjukvården (2008:14)
- Region Jämtland Härjedalens policy för informationssäkerhet
- ISO 27001

METODER

Förstudien har utförs genom dokumentstudier och intervjuer. Intervjuade: Beredskapschef, informationssäkerhetssamordnare, IT Säkerhetsansvarig, och IT-chef.

De intervjuade har faktagranskat rapporten och synpunkter tillvaratagits.

Substansgranskning har gjorts för att i erforderlig omfattning verifiera gjorda utsagor.

[1] Informationssäkerhetspolicy: Diarienummer RS/775/2116

SYFTE OCH SAMMANFATTANDE SVAR PÅ REVISIONSFRÅGORNA:

Syftet med förstudien har varit att kartlägga och bedöma om det finns anledning till en fördjupad granskning avseende hur informationssäkerhetsarbetet organiserats och bedrivs.

Nedan framgår ställda revisionsfrågor och svaren på dessa i sammanfattning:

Revisionsfråga:
Sker arbetet med informationssäkerhet med en systematik som ger förutsättningar för att en tillräcklig säkerhet uppnås?

Svar: **Nej, inte ännu.** Utveckling av systematik för informationssäkerhetsarbetet pågår, men det saknas ännu viktiga åtgärder inom en del områden. Det finns, vilket vi återkommer till i rapporten, stora brister i arbetet med klassning av informationen, problem med den systemförvaltningsmodell som tillämpas och kunskaper hos användarna.

Revisionsfråga:
Sker en planering och uppföljning av att standarden ISO 27001, så långt möjligt, följs?

Svar: **Ja,** ett arbete har påbörjats. En GAP-analys har gjorts och utveckling av formerna för uppföljning pågår. Med detta inte sagt att den nämnda standarden uppfylls.

Revisionsfråga:
Finns en tillräcklig kontroll över att inventeringen av säkerhetsproblem sker på ett ändamålsenligt sätt?

Svar: **Nej**, inte fullt ut. Det finns brister i klassningen av informationen och i systemägarnas förutsättningar att klara sin roll och att uppfylla det ansvar den innefattar.

Revisionsfråga:
Har det säkerställts att prioriterade åtgärder vidtas?

Svar: **Nej**, det har vidtagits en rad positiva åtgärder men vi anser inte att det ännu är säkerställt att prioriterade åtgärder kommer att vidtas. Huvudsakligen beror detta på att informationsklassning inte är genomförd i tillräcklig utsträckning och därmed kan det finnas ett mörkertal av viktiga åtgärder som borde lyfts upp för prioritering och att det saknas tydlig budget för att vidta åtgärder.

IAKTTAGELSER OCH BEDÖMNINGAR

Revisionsfråga:
Sker arbetet med informationssäkerhet med en systematik som ger förutsättningar för att en tillräcklig säkerhet uppnås?

Iakttagelser

Ett antal viktiga styrdokument finns framtagna:

- **Policy för informationssäkerhet** (RS/775/2016)
  Alla vårdgivare är enligt Socialstyrelsens föreskrifter skyldiga att ha en informationssäkerhetspolicy.

  Revidering av informationssäkerhetspolicyn har gjorts och den har fastställas under 2016.

- **Fastställd standard ISO 27001:2014** I informationssäkerhetspolicyn finns angivet att informationssäkerhetsarbetet ska ta sin utgångspunkt i den internationella ledningssystemstandarden för informationssäkerhet, ISO/IEC SS 27001:2014.

- **Informationssäkerhetsberättelse**
  Enligt SOSFS 2008:14 ska vårdgivaren utse en eller flera personer som ska ansvara för informationssäkerhetsarbetet. Den eller de som har fått denna uppgift ska minst en gång om året till vårdgivaren rapportera vilka

  1. granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med informationssäkerhetspolicyn,

  2. riskanalyser som har utförts avseende informationssäkerheten, och

  3. förbättringsåtgärder som har vidtagits.

  Informationssäkerhetsberättelse 2015 har behandlades av styrelsen i februari 2016 § 36.

- **Övergripande handlingsplan informationssäkerhet 2016-2017**, fastställd av regiondirektören (RS/1444/2015)
  ”Syftet med handlingsplanen är att med ledningens stöd på ett strukturerat sätt arbeta med informationssäkerhetsfrågor så att styrande lagar och beslutad policy efterlevs. Handlingsplanen syftar också till att vara ett övergripande styrdokument för de närmaste årens inriktning och prioritering av regionens informationssäkerhetsarbete. Då informationssäkerhet är komplext och involverar ett flertal staber samt all verksamhet är det nödvändigt att skapa en gemensam bild av ansvars- och rollfördelning inom området.”

  Handlingsplanens mål:

  - Tydliggöra ansvar och roller avseende informations- och it säkerhetsfrågor i Cosmic förvaltning
  - Öka kunskapsnivån avseende informationssäkerhet och öka säkerhetsmedvetande i organisationen
  - Säkerställa att regionens samhällsviktiga verksamheter har etablerade reservrutiner vid IT avbrott
  - Etablera regelverk för behörighetsstyrning samt förbättra uppföljningen av tilldelade behörigheter i verksamhetssystemen.
  - Riskbedöma och reglera användningen av verksamheternas externa molntjänster
  - Säkerställa att Region Jämtland Härjedalen lever upp till lagkrav om personuppgiftshantering

- **Fördelning av ansvar** för informationssäkerhet (RS/1978/2015)
  Beslutad av regiondirektören 27 juni 2016, med syfte att förtydliga roller och ansvar gällande informationssäkerhetsarbetet samt beskriva hur arbetet ska organiseras.

Bedömning:

Standarden ISO27001 har antagits och har, enl uppgift, implementerats i ledningssystemet. Även andra viktiga styrdokument finns framtagna.

Informationssäkerhetsberättelsen utgör en god källa till en översiktlig lägesinformation.

Informationssäkerhetsarbetet kan dock, enligt vår mening, inte ännu sägas ske med en systematik som ger förutsättningar att tillräcklig informationssäkerhet uppnås. Det finns, vilket vi återkommer till senare i denna rapport, stora brister i arbetet med klassning av informationen, och problem med den systemförvaltningsmodell som tillämpas.

Revisionsfråga:
Sker en planering och uppföljning av att standarden ISO 27001, så långt möjligt, följs?

Iakttagelse:

När revisionsfrågan formulerades gällde en tidigare version av informationssäkerhetspolicyn som angav att ISO 27001 skulle följas ”så långt möjligt”, men det var inte klargjort vad så långt möjligt innebar. Nu anges att planeringen ska ta sin utgångspunkt i denna standard.

Enligt beredskapschefen finns en planering av hur ledningssystemet ska följas upp med internrevision, egenkontroll samt ledningens genomgång. Ledningssystemet för informationssäkerheten sägs vara en del i det ”stora” ledningssystemet och följs därmed upp enligt planeringen.

ISO 27001 uppges vara implementerat i det ”stora” ledningssystemet. Standarden används dock utan att man haft ambition att certifieras.

I dokumentet ”Ansvarsfördelning informationssäkerhet” anges att det ingår i regiondirektörens ansvar att se till att regionens ledningssystem uppfyller kraven för ISO 27001.

Standarden är mycket omfattande och innehåller bland annat krav på att det görs övergripande riskanalyser som täcker standardens samtliga områden.

Det finns även en annan standard benämnd ISO 27002:2005 som används i informationssäkerhetsarbetet. Denna standard har beskrivits vara en sorts handbok som är mer detaljerad. Den är avsedd att användas som referens för val av säkerhetsåtgärder inom ramen för att införa ett ledningssystem för informationssäkerhet (LIS). Den kan även användas vägledning i införandet av informationssäkerhetsåtgärder.

En övergripande genomgång av nuläget har gjorts mot ISO 27002:2005 (GAP-analys), vilket innebär en betydligt mer omfattande genomgång än om den gjorts mot ISO 27001.

Vi har tagit del av arbetsmaterial från denna analys som visar på att det finns många åtgärder som vidtagits, många som pågår, men också att det finns många problem som återstår att lösa.

Vi har fått det beskrivet som att man för närvarande söker former för hur uppföljning mot normen ska ske.

Bedömning:

Den uppföljning som förvaltningen själv gjort i form av ovan nämnd GAP-analys medför att planeringsunderlag skapats för att uppfylla ISO27001 och utgör även ett led i att finna former för uppföljningen, men därmed inte sagt att den nämnda standarden uppfyllts i nödvändig utsträckning. Vad som är nödvändigt är inte fastlagt.

Enligt vår mening är det viktigt att regionledningen bevakar att formerna för uppföljningen av standarden ISO27001, så långt möjligt, finner ändamålsenliga former. För att nå dit kan det vara lämpligt att fastställa vad som ska uppfyllas eller inte.

Revisionsfråga:
Finns en tillräcklig kontroll över att inventeringen av säkerhetsproblem sker på ett ändamålsenligt sätt?

Iakttagelse

Informationsklassning och kompetens

Utdrag ur informationssäkerhetsberättelsen 2015 (RS/2129/2015):

> Ett relativt omfattande arbete har gjorts under ett par års tid för att utarbeta en modell och metod för informationsklassning. Modellen har under 2015 prövats vid ett flertal tillfällen under året inför behov av införande av nya IT tjänster eller system, vilket är en framgångsfaktor för att kunna ställa rätt krav redan vid en upphandling.
>
> Parallellt har enligt handlingsplanen gjorts försök att arbeta vidare med BITS som är ett verktyg för att arbeta med systemsäkerhet och fastställa basnivå för informationssäkerhet i IT system. BITS är sedan 2009 det verktyg som IT avdelningen har fastställt ska användas inom regionen, men börjar nu bli relativt gammalt och omodernt. Dock har inget bättre verktyg funnits till hands.
>
> Ett av handlingsplanens mål var att stödja systemägare med att genomföra BITS analyser och att 50% av de verksamhetskritiska systemen skulle vara analyserade 2015. Målet har inte uppnåtts, dels beroende på resursbrist i centrala stödfunktioner men också beroende på systemförvaltningsmodellen där hela ansvaret läggs på systemägaren.
>
> Många systemägare är chefer i vårdverksamheter som varken har kompetens eller resurser för att utföra BITS analys eller annat systemsäkerhetsarbete.
>
> Under året har ytterligare tre verksamhetskritiska system BITS analyserats och ca hälften av våra verksamhetskritiska system är ännu inte BITS analyserade.
>
> ”Med nuvarande situation finns det risk att det görs dubbel jobb eller att inget jobb alls utförs för säkerheten i många befintliga system. För att komma vidare med arbetet måste ett beslut fattas under 2016 angående vilken modell och metod som ska användas.”

Ett nytt verktyg, benämnt ”KLASSA”, har tagits fram av SKL för informationsklassning. Verktyget har testats under 2016 och inriktningen anges vara att byta från BITS till KLASSA då detta ”förhoppningsvis är enklare för systemägarna att använda”. Ett förslag om detta kommer att läggas fram till regionledningen inom kort.

Ca 40 av systemen bedöms vara verksamhetskritiska. Av de ca 20 system som klassats är det, enl uppgift, få som bedöms ha en klassning som kan betraktas som aktuell.

I riskanalysen av systemförvaltningen som gjordes 2013 framkom bl a att *”I nuvarande modell har systemägaren dubbla roller som systemägare och informationsägare. Det innebär i många fall att kraven på hur informationen ska skyddas ställs av samma person som ska uppfylla kraven”.* Efter den riskanalysen lades det fram ett förslag om att bl a:
- centralisera de verksamhetskritiska systemens IT-nära systemförvaltning till färre systemansvariga och systemägare än idag
- inför en obligatorisk, anpassad utbildning för systemägare.

Det har också framkommit att det finns ett stort behov av utbildning av användarna av systemen.

Bedömning:

Vid såväl intervjuer som i informationssäkerhetsberättelsen har framkommit att många systemägare varken har kompetens eller resurser för att utföra BITS analyser eller annat systemsäkerhetsarbete. Situationen, vad gäller systemägarnas förutsättningar att klara sin roll

och att uppfylla det ansvar den innefattar, har trots att den varit känd ännu inte förbättrats. Vi bedömer detta som en allvarlig risk.

Bristerna i informationsklassningen innebär en säkerhetsrisk. I såväl dokumentation som vid intervjuer har det framkommit att det finns brister i informationsklassningen av system. Uppsatta mål för genomförd klassning är långt ifrån uppnådda. Förutom att en stor andel av de verksamhetskritiska systemen inte har en aktuell klassning är det också oklart i vilken utsträckning åtgärder som bedömts nödvändiga har vidtagits i de system som är klassade/riskbedömda. Utbildning har angivits som ett prioriterat område under 2016 och kan tillsammans med den rekrytering av en informationssäkerhetssammordnare som nyligen gjorts, möjligen bidra till en förbättring.

Vi rekommenderar styrelsen att särskilt bevaka att

- Organisationen och förutsättningarna för systemägandet skyndsamt utvecklas
- Klassningen av information når målen och att den hålls aktuell
- Användarna har de kunskaper som behövs ur ett säkerhetsperspektiv.

Revisionsfråga:
Har det säkerställts att prioriterade åtgärder vidtas?

Iakttagelser

Resursbrist

Utdrag ur informationssäkerhetsberättelsen 2015 *(RS/2129/2015):*

> ”Personalresurser har omfördelats internt inom Samordningskansliet och arbetet sker i allt högre grad i samarbete med IT. Handlingsplan för informationssäkerhet har funnits sedan 2014 och ett ledningssystem med regelverk för informationssäkerhet enligt standarden ISO 27001 har byggts upp och integrerats i Region Jämtland Härjedalens ledningssystem för kvalitet. ”
> …
> ”Avdelade resurser har dock inte motsvarat behovet och alla mål har inte uppnåtts, det finns fortfarande ingen avsatt budget för informationssäkerhet.”

Enligt informationssäkerhetspolicyn har regionstyrelsen ett ansvar att säkerställa att det finns ekonomiska och personella resurser för informationssäkerhetsarbetet.

Vid intervju har bl.a. framkommit att det upplevs som ett problem att det saknas budgeterade medel för informationssäkerhet.

Det uppges finnas en brist på personella resurser i organisationen sedan tidigare informationssäkerhetssamordnare beviljades särskild förtidspension. Rekrytering av ny en informationssäkerhetssammordnare har nyligen genomförts och tillträde kommer att ske i mars.

Organisation

Utdrag ur informationssäkerhetsberättelsen 2015 *(RS/2129/2015):*

> ”Fördelning av och gränsdragning för IT- och informationssäkerhetsfrågor behöver ses över framför allt inom områden som E-hälsa, COSMIC förvaltning samt molntjänster.
>
> **Cosmic**
> Datainspektionen gjorde en tillsyn 2013 avseende bl.a. om det fanns en dokumenterad behovs- och riskanalys för behörigheter i huvudjournalsystemet. Då en sådan inte fanns fick regionen ett föreläggande under våren 2015 om detta. Beredskapschefen fick i uppdrag att prioritera en sådan analys under 2015. En analysgrupp med deltagande från vårdverksamhet, chefläkare, IT och COSMIC förvaltning arbetade med risk- och behovsanalys för behörigheter i COSMIC under hösten 2015.
>
> Under 2015 förekom också problem med loggar i Cosmic. Loggarna beskrevs som

svårtolkade och att de krävde manuell bearbetning. Enligt informationssäkerhets-berättelsen har logghanteringen en hög prioritet.

I den övergripande handlingsplanen för info-säkerhet ingår att ”klargöra ansvar och roller avseende informations- och IT säkerhetsfrågor inom Cosmic förvaltning samt nationella e-hälsotjänster” (Tidplan 2016). Aktiviteten i handlingsplanen har genomförts, men betecknas som ännu inte helt slutförd. Det finns en organisation och IT stöd för loggning. Pilotförsök pågår för närvarande inom två områden för att testa automatiserade loggkontroller. När detta är klart kan breddinförande till övrig verksamhet ske 2017.

Det finns en grupp benämnd informationssäkerhetsrådet som arbetar övergripande med informationssäkerhetsfrågor i regionsstaben. Inom gruppen finns kompetens inom områdena juridik, IT-säkerhet, arkiv och dokumenthantering, riskhantering, patientsäkerhet samt kvalitetsutveckling. Rådet samlar de ledande aktörerna vad avser att utveckla informationssäkerheten.

I dokumentet ”Ansvarsfördelning informationssäkerhet (RS/1978/2015), finns en närmare beskriv av vilka aktörerna är och deras ansvar.

Vid intervju har åsikter framkommit om att man upplever organisationen kring informations-säkerheten som något otydlig.

Det saknas nätverk/forum för systemförvaltarna. Att skapa sådant var bl a ett av de förslag till fortsatt arbete som framkom i samband med den riskanalys som gjordes 2013.

Behörighetshantering

Utdrag ur informationssäkerhetsberättelsen 2015 *(RS/2129/2015):*

> ”Resultatet av analysen är ännu inte helt slutförd men visar bl.a. på det finns ett antal generella risker i dagens behörighetshantering, främst kopplat till att alltför vida behörigheter tillämpas. Analysen kommer att innehålla åtgärdsförslag på kort och lång sikt utifrån förväntad nytta och effekt. Resultatet kan utgöra underlag för prioritering av åtgärder, men åtgärdsförslagen behöver kompletteras med kostnadsberäkningar.”
> ”Här krävs ett utvecklingsarbete både för att automatisera behörighetsbeställning i högre utsträckning men också för att säkerställa styrning av behörigheter och ge chefer möjlighet att kontrollera behörigheter”

I den övergripande handlingsplanen för info-säkerhet ingår bl a följande aktiviteter:

- *Regelverk behörighetsstyrning (Tidplan 2016)*
- *Minska andelen behörigheter som beställs och avbeställs manuellt i verksamhetssystem (Tidplan 2017)*
- *Förbättra möjligheter för chef att kontrollera behörigheter för användare inom en enhet (Tidplan 2017)*

Beredskapschefen ser en stor risk för att aktiviteterna för 2017 inte kommer att hinna genomföras då aktiviteterna 2016 redan är försenade.

Under 2016 har, i enlighet den övergripande handlingsplanen för info-säkerhet, en ”organisation och IT-stöd för effektiv loggkontroll”[2] etablerats.

Vad gäller integritetsfrågor har det uppgivits att verksamheten är medveten om att sekretess råder gällande patientuppgifter. Det pågår en översyn av hanteringen av personuppgifter inom regionen. Styrdokument för hanteringen finns, men de avses ses över och kompletteras i de delar de inte uppfyller dataskyddsförordningen.

Vi har dock också mött åsikten att integritetsfrågor har varit ett eftersatt område.

---

[2] Roller och ansvar loggkontroll vårdsystem (Centuri dok nr 32597-1),
Regel för loggkontroll i vårdadministrativa system (Dnr RS/1714/2015)

Nya EU regler kommer, enligt uppgift, medföra ny lagstiftning 2018. Anpassning till detta sägs komma att kräva ett omfattande arbete.

Systemförvaltningsmodell

Utdrag ur informationssäkerhetsberättelsen 2015 *(RS/2129/2015)*:

> ”IT chefen har tilldelats ett uppdrag att se över systemförvaltningsmodell för Region Jämtland Härjedalen under 2016 samt att i det arbetet beakta de risker, brister samt förbättringsförslag som framkom i analysen”
>
> ”Checklistan i ledningssystemet för egenkontroll av det systematiska kvalitetsarbetet har kompletterats med delar om informationssäkerhet. I de internrevisioner som har genomförts under 2015 har också frågor ställts angående informationssäkerhet.”

Vid intervju framkom att det upplevts ha funnits ett glapp mellan verksamheterna och IT-enhetens roll.

Någon ny övergripande systemförvaltningsmodell har ännu inte föreslagits, men en modell benämnd PM3 uppges ha använts för Cosmic och beslutsstöd/datalager. En utvärdering och analys av behov av förändrad organisation, kan enligt IT-chefen, innebära att PM3 förvaltningsmodell implementeras inom ytterligare förvaltningsobjekt. IT-chefen överväger om denna modell skall införas även för andra system.

På grund av hög arbetsbelastning uppgav IT-chefen att arbetet med att se över systemförvaltningsmodellen nedprioriterats.

Den handbok som finns för systemförvaltningen - den sk. Q-handboken är, enligt uppgift, inaktuell och i behov upp uppdatering

Regiondirektören fattade den 27 juni 2016 ett delegationsbeslut[3] om fördelningen av ansvar för informationssäkerhet med syfte att förtydliga roller och ansvar gällande informationssäkerhet samt att beskriva hur arbetet ska organiseras.

Reservrutiner

Utdrag ur informationssäkerhetsberättelsen 2015 (*RS/2129/2015)*:

> Under februari och mars inträffade tre omfattande IT driftstörningar på sjukhuset under 1,5-2 timmar. Då även intranätet påverkades framstod svårigheterna att kommunicera till och från vårdens verksamheter som ett tydligt problem. Händelserna visade på vikten av reservrutiner.
>
> Enheten för krisberedskap har haft i uppdrag att starta upp ett arbete med kontinuitetshantering i samhällsviktig verksamhet. Parallellt har också inom informationssäkerhet funnits ett uppdrag att upprätta kontinuitetsplaner i vården avseende informationssäkerhet d.v.s. planer för hur verksamheten ska bedrivas vid avsaknad av kritiska IT system samt hur återgång till normalläge ska ske.
>
> De båda arbetena har resulterat i att akutområdet under 2015 har arbetat med att identifiera vilka IT system som verksamheten är beroende av samt att fastställa en maximal tolerabel avbrottstid och bedöma konsekvenser av IT störningar ur ett patientsäkerhetsperspektiv. Befintliga reservrutiner har inventerats och behov har kartlagts av vad som återstår att utarbeta. Målbilden är att akutområdet under 2016 ska ha en färdig kontinuitetsplan för IT. Förhoppningsvis kan arbetet sedan spridas vidare till andra verksamheter inom regionen

I den övergripande handlingsplanen för info-säkerhet ingår att *upprätta kontinuitetsplaner* (Tidplan 2016-2017).

[3] Dnr: RS/1978/2015

Incidenter

Utdrag ur informationssäkerhetsberättelsen 2015 (*RS/2129/2015)*:

> En incidenttyp som blivit alltmer vanlig under året är angrepp av skadlig kod med s.k. ”ransomware”, vilket innebär att kod som laddas ner (utan att användaren upptäcker det) och låser filer som därmed blir oläsliga (förstörda). En lösensumma begärs för att göra filerna läsbara igen. Flera angrepp av denna typ har inträffat i regionens IT-miljö, med olika omfattning på antalet låsta filer. Angreppen har skapat merarbete i form av återskapande av filer från säkerhetskopior och det kan inte uteslutas att förlust av information/filer också har skett i vissa av fallen.

Vid intervjuer har framkommit att detta utgör en allvarlig risk för förlust av information. Vid de incidenter som drabbat regionen uppger IT-chefen att informationen kunnat återställas genom inläsning av backup.

Molntjänster

Utdrag ur informationssäkerhetsberättelsen 2015 (*RS/2129/2015)*:

> ”En ny version av auktorisation (godkännande) av IT-system som även täcker in molntjänster har utformats och införts”.
> ”Mycket arbete återstår kring att utarbeta regelverk för anskaffning av molntjänster. En risk- och behovs analys avseende användning av molntjänster bör också utföras.”

Vid intervju framkom att s.k. molntjänster är ett aktuellt och växande problem ur säkerhetssynpunkt. Risk finns för att känslig information kan spridas. Regler för nyttjandet mm behöver tas fram.

I den övergripande handlingsplanen för info-säkerhet ingår att:

- *Göra riskanalys (Tidplan 2016)*
- *Utarbeta regelverk (Tidplan 2016)*
- *Genomlysa stödprocess för verksamheten vid anskaffning av IT-system/molntjänster (Tidplan 2017)*

Enligt uppgift har dock arbetet med att styra upp nyttjandet av molntjänster bortprioriterats under 2016, men avses genomföras 2017.

Bedömning:

Revisionsfrågan som ska besvaras är ”Har det säkerställts att prioriterade åtgärder vidtas?”

Regionen använder, enligt uppgift, standarden ISO 27001 som utgångspunkt och den sägs ha inarbetats i regionens ledningssystem. Det har gjorts en GAP-analys. Det har gjorts en prioritering av kända problem. Det finns en övergripande handlingsplan för informationssäkerhet för åren 2016-2018. Detta lägger tillsammans en grund för att utveckla en systematisk uppföljning och att vidta nödvändiga åtgärder.

Iakttagelsen vad avser problemet med systemägarnas dubbla roller, och brist på kompetens för uppgiften ser ut att kvarstå.

Den framkomna bristen på personella resurser är, åtminstone delvis, på väg mot en lösning då rekrytering av en informationssäkerhetssamordnare pågår.

Regionstyrelsen bör på ett tydligare sätt säkerställa att det, i enlighet med informations-säkerhetspolicyn, finns ekonomiska och personella resurser för informationssäkerhetsarbetet.

Vårt samlade intryck är ändå att det pågår ett aktivt arbete mot målet att säkerställa informationssäkerheten. Åtgärder vidtas löpande.

Det finns dock mycket angelägna förbättringsområden, så som informationsklassning och utvecklande av eller ev, byte av systemförvaltningsmodell samt att säkerställa resurser för åtgärder som bedömts vara nödvändiga att genomföra.

Svaret på revisionsfrågan, "om det säkerställts att prioriterade åtgärder vidtas", är dock att vi ännu inte anser att det är säkerställt. Huvudsakligen beror detta på att informationsklassning inte är genomförd i tillräcklig utsträckning och därmed kan det finnas ett mörkertal av viktiga åtgärder som borde lyfts upp för prioritering och att det saknas tydlig budget för att vidta nödvändiga åtgärder.

KVALITETSSÄKRING

Revisionsdirektören har det övergripande ansvaret för att kontrollera om förstudien har en tillräcklig yrkesmässig och metodisk kvalitet samt att det finns en överensstämmelse mellan revisionsfrågorna/kontrollmålen, metoder, fakta, slutsatser/bedömningar och framförda förslag.

UNDERTECKNANDE OCH GODKÄNNANDE

Ansvarig projektledare vid regionens revisionskontor har varit Ulf Rubensson, certifierad kommunal revisor. En prövning av den sakkunniges oberoende och integritet har gjorts och finns dokumenterad i bilaga till projektplan.

Datum 2016-12-09
Ansvarig:

.....
Ulf Rubensson
Certifierad kommunal revisor

Datum 2016-12-09
Kvalitetsgranskare

.....
Revisionsdirektör