Granskning av informationssäkerhet

Region Västernorrland

November 2019

Linus Owman
Mattias Lööf
Fredrika Jönander

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av Region Västernorrlands förtroendevalda revisorer granskat regionens informationssäkerhet. Syftet med granskningen är att bedöma om Regionstyrelsen har tillsett att informationssäkerheten är tillräcklig. I granskningen ingår även en uppföljning av den granskning som genomfördes 2017 avseende IT-säkerhet.

Revisionsfrågorna har varit:

- Har ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning?
- Finns en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten?

Efter genomförd granskning bedömer vi att Regionstyrelsen **inte** säkerställt att ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning samt att regionstyrelsen **inte** säkerställt en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten. Vår bedömning är grundad i:

- regionens avsaknad av ett gediget ledningssystem för informationssäkerhet och tillhörande organisatorisk struktur och dokumentation; regionen saknar i nuläget en organisation som kan införa och motta ett ledningssystem för informationssäkerhet
- avsaknad av regelbundna rapporteringsrutiner avseende informationssäkerhetsarbetet;
- brister i regionens uppföljning och vidtagande av ändamålsenliga åtgärder som följd av iakttagelserna från 2017 års granskning.

Rekommendationer

Utifrån våra iakttagelser bör nämnas att ett flertal åtgärder identifierats av Region Västernorrland och eventuellt redan påbörjats avseende de förbättringsområden som uppmärksammats i granskningen. Beaktat detta och i enlighet med ovan nämnda bedömning har vi följande rekommendationer som Regionstyrelsen bör ge verksamheterna i uppdrag att utföra inom informationssäkerhetsarbetet:

Människor och processer:

- ➢ Regionen bör fastställa en färdplan för införandet av ett ledningssystem för informationssäkerhet. En sådan färdplan bör innehålla tydliga målsättningar, ansvarsbeskrivningar för medverkande resurser, samt en konkret tidsram som arbetet för framtagning av ett ledningssystem ska förhålla sig till.
- ➢ Regionen bör utreda möjligheten att upprätta en arbetsgrupp för informationssäkerhet som sammanträder regelbundet och inkluderar nyckel-personer för arbetet - exempelvis informationssäkerhetssamordnaren, IT-chef och/eller IT-säkerhetsansvarig, Administrativ chef, säkerhetssamordnare samt representanter från samtliga fackförvaltningar. Denna grupp bör ha ansvar för förvaltning av Ledningssystemet för informationssäkerhet och bör ha som uppgift att styra och samordna informationssäkerhetsarbetet inom hela regionen.

Arbetsgruppen bör vidare ha ett övergripande ansvar för omvärldsbevakning inom informationssäkerhetsområdet.

- Inom ramen för ledningssystemet för informationssäkerhet bör regionen upprätta ett aggregerat riskregister med regionövergripande informationssäkerhetsrisker. Ett sådant register bör uppdateras regelbundet samt användas för åtgärdsplanering, och bör utgöra grunden till en reguljär rapportering till regionstyrelsen eller regionens ledning. Riskregistret bör vara framtaget med regionens huvudsakliga samhällsfunktion och leverans i åtanke.

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation som tillhör ledningssystemet ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.

- Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhetspolicyn till riktlinjer.

- Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Västernorrland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.

- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör även genomföra systematiska uppföljningar av utbildningsverksamheten.

- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.

- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

- Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Västernorrland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

- Regionen bör se över förvaltningsmodellen för verksamhetssystem och utreda möjligheter till att förstärka ansvaret som systemägare har för tillämpning av informationssäkerhetsåtgärder.

Teknik:

- Utred möjligheterna till att införskaffa en central behörighetshantering som integreras med övriga verksamhetssystem (i synnerhet HR systemet som regionen använder). Ett sådant system bör till stor del automatisera processer för tilldelning, förändring, och borttagning av behörigheter. Utifrån ett sådant system bör behörighetstilldelning och behörighetsgrupper framtas som baseras på i

förväg bestämda roller. I synnerhet bör regionens tilldelning av behörigheter till fysiska lokaler ses över, särskilt med hänsyn till känsliga rum som serverhallar.

- Utred möjlighet till att införskaffa en SIEM-lösning som samlar in och aggregerar säkerhetsloggar från väsentliga nätverkskällor, exempelvis de virtuella brandväggar som i nuläget är placerade mellan nätverkssegment. Införskaffandet av en dedikerad loggserver bör även utredas med krav på bibehållen lagring på minst 180 dagar.

- Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans.

1. Inledning

1.1 Bakgrund

Under det senaste årtiondet har en snabb utveckling inom datakommunikation och teknik ägt rum. Digitaliseringen påverkar många olika delar av samhället, exempelvis har IT gått från att stödja affärsprocesser till att driva verksamheter. Detta medför att det är viktigt att identifiera och adressera cyberhot och risker. Allt fler allvarliga cybersäkerhetsincidenter har drabbat såväl privat som offentlig sektor de senaste åren. En gemensam beståndsdel i flera av de allvarligaste händelserna är information som på ett eller annat sätt kommit obehörig tillhanda, antingen genom bristande rutiner och hantering eller genom yttre påverkan, och i vissa fall en kombination av båda dessa. I det moderna samhället har så gott som all brottslighet en IT-koppling. I *Informationssäkerhet – trender 2015* skriver Myndigheten för samhällsskydd och beredskap (MSB) att *”Informationssäkerhet kommer framöver att allt mera betraktas som en fråga om att skydda hela samhället och dess välstånd snarare än bara teknik.”*. Att regionens informationssäkerhet är essentiell för ett välfungerande samhälle råder det inget tvivel om.

Som ett led i att förhindra cybersäkerhetsincidenter och upprätthålla samhällsviktig verksamhet behöver en region bedriva ett ändamålsenligt informationssäkerhetsarbete. Information som finns i regionen skall klassas, rutiner och riktlinjer ska finnas på plats och arbetet ska regelbundet följas upp. Detta kräver också ett säkerhetsmedvetande hos dem som hanterar informationen på daglig basis. Informationssäkerhet regleras inte i en sammanhållande lag utan genom bestämmelser i flera olika regelverk. Det finns även i lagstiftning, föreskrifter och rekommendationer inom hälso- och sjukvård etc.

Informationssäkerhet innebär en rutin och/eller process som tillämpas för att skydda information och mildra informationsrisker. En sådan process har som syfte att säkerställa att *konfidentialiteten*, *integriteten*, och *tillgängligheten* av information inte röjs. För att åstadkomma detta kan flera säkerhetsåtgärder tillämpas. Dessa säkerhetsåtgärder kan huvudsakligen sägas falla inom tre kategorier; administrativa, tekniska, och åtgärder som riktar sig till att skapa en säkerhetskultur anpassad till att skydda information. Ändamålsenlig och uppdaterad dokumentation är således väsentlig för att samtliga informationssäkerhetsåtgärder ska kunna tillämpas och efterföljas (se också avsnitt 2.1).

Mot bakgrund av detta har PwC på uppdrag av Region Västernorrlands förtroendevalda revisorer genomfört en granskning av regionens informationssäkerhet. Revisorerna granskade år 2017 regionens informationssäkerhet. I granskningen konstaterades bland annat brister i styrdokumenten. Revisorerna har bedömt att det finns en risk för att tillräckliga åtgärder inte har vidtagits för att säkerställa efterlevnad av fullmäktiges informationssäkerhetspolicy samt de nya bestämmelser som tillkommit efter föregående granskning. Bland annat har kraven kring informationssäkerheten skärpts genom dataskyddsförordningen, NIS-direktivet och den nya säkerhetsskyddslagen. Vidare har olika rättsliga uttalanden gjorts avseende så kallade molntjänster.

1.2 Syfte och Revisionsfrågor

Syftet med granskningen är att bedöma om Regionstyrelsen har tillsett att informationssäkerheten är tillräcklig.

Nedan framgår de revisionsfrågor som granskningen ska besvara:

1. Finns en tillfredsställande styrning, uppföljning och kontroll av informations-säkerheten?

Denna revisionsfråga besvaras utifrån dimensionerna ändamålsenlig

   a. organisation,
   b. dokumentation och
   c. uppföljning och kontroll

2. Har ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning?

1.3 Avgränsning

Granskningen avgränsas till att gälla informationssäkerhet inom Region Västernorrland 2019 samt uppföljning av den tidigare granskningen som genomfördes 2017.

1.4 Metod

Granskningen har genomförts med hjälp av ramverket NIST Cyber Security Framework. Ramverket utvärderar en organisations förmåga att genomföra handlingar kopplade till de fem domänerna: **Identifiera**, **Skydda**, **Upptäcka**, **Respondera** och **Återställa** utifrån ett människo-, process- och teknikperspektiv. Varje område innehåller ett antal kontrollmål vars grad av uppfyllnad poängsätts på en skala från 1 till 5. Ramverket har anpassats efter Region Västernorrlands förutsättningar och verksamhet. Vi har utvärderat Region Västernorrlands mognadsgrad beträffande följande funktioner:

Identifiera: Området täcker Region Västernorrlands 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 har vi bland annat sett till processer kopplade till riskhantering samt klassificering av tillgångar.

Skydda: Området fokuserar på Region Västernorrlands nuvarande tillstånd när det kommer till att skydda regionens information samt att avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörighetskonton samt säkerhet kopplad till data.

Upptäcka: Området inkluderar bland annat Region Västernorrlands förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, samt sökning efter skadlig kod och sårbarheter.

Respondera: Området täcker Region Västernorrlands rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat forensik (kriminalteknik) och incidenthantering.

Återställa: Området relaterar till Region Västernorrlands processer för kontinuitetshantering och förmågor relaterade till resiliens och återhämtning efter hantering av incidenter. Kommunikation och publika relationer (PR) inkluderas också i denna kategori.

Granskningen baserar sig på tre kvalitativa workshops/gruppintervjuer tillsammans med nyckelfunktioner inom Region Västernorrlands samt en efterföljande intervju med regiondirektören. Region Västernorrland har ombetts att, utifrån granskningsområdet, identifiera relevanta personer för intervjuerna. Dessa personer har sammantaget gedigen kunskap om, samt erfarenhet av, verksamheten och dess informations- och cybersäkerhet. Informationen har sedan värderats och på så sätt har en mognadsgrad kunnat tas fram. Vidare har granskningen inkluderat analys och genomläsning av rutiner, policyer och strategier. Granskningen har genomförts från september till november 2019. En lista över den dokumentation som vi tagit del av återfinns som bilaga. Workshops/gruppintervjuer inom ramen för granskningen har genomförts med följande personer/funktioner:

- Redovisningschef Ekonomi och planering
- Områdesdirektör HR
- Chefläkare Kvalitet- och patientsäkerhet
- Samordnare intern kontroll
- Verksamhetschef Administration/Dataskyddsföreträdare
- Regionstyrelsens ordförande
- Regionstyrelsens vice ordförande
- Samordnare informationssäkerhet
- Enhetschef för arkitektur och metodstöd, IT
- Säkerhetschef
- Systemförvaltare

2. Övergripande resultat - NIST

2.1 Inledning

NIST cybersäkerhetsramverk omfattar en riskbaserad sammanställning av riktlinjer som syftar till att hjälpa organisationer att identifiera, genomföra och förbättra säkerhetspraxis och skapa ett gemensamt språk för intern och extern kommunikation av säkerhetsproblem. Ramverket är en iterativ process utformad för att utvecklas i synkronisering med förändringar när det kommer till säkerhetshot, processer och lösningar. Detta innebär i klartext att givet den konsekventa metodologin kan mätningen återupprepas för att kartlägga hur organisationen förflyttat sig i mognadsgrad.

Ramverket tillhandahåller en utvärdering av mekanismer som möjliggör för verksamheten att klargöra nuvarande cybersäkerhetsförmåga, sätta individuella mål samt etablera en plan för åtgärder och upprätthållandet av cybersäkerhetsprogram. Detta innebär att resultatet nedan kan användas som utgångspunkt för ett systematiskt handlingsprogram framåt. Nivåerna varierar mellan 1 till 5, där 1 indikerar att medvetenheten om risker är låg, medan 5 indikerar att processer och program har etablerats och blivit väl implementerade i verksamheten.

Begreppet “cybersäkerhet” som används av NIST ramverket omfattar både informationssäkerhet och IT-säkerhet. Ramverket bygger på en indelning utifrån tre dimensioner - människor, processer, och tekniska verktyg - och berör därmed säkerhetskontroller som är administrativa, tekniska och kulturella. De fem funktioner som ramverket granskar täcker därmed in samtliga informationssäkerhetsprocesser.
Hantering av cybersäkerhetsrisker handlar i princip om hantering av interna och externa hot mot organisationskritiska informationstillgångar och IT-tjänster. Detta uppnås genom att tillämpa en strukturerad strategi (styrnings- eller förvaltningsmodell) för att arbeta med IT- och informationssäkerhetsaktiviteter i en organisation. Den strukturerade strategin inom detta område riktar sig ofta till de IT- och informationssäkerhetsansvariga delarna av organisationen, därmed är det fokus på dessa delar i vår nuvarande rapport.

Enligt vår uppfattning behöver organisationer en större grad av kontroll över sina IT- och informationssäkerhetsfunktioner än vad som tidigare varit fallet. I en era av digitalisering *stöder* IT och teknik inte längre produktionsprocesser utan *driver* dem. Underlåtenhet att hantera IT- eller informationssäkerhetskrav leder omedelbart till brist i funktionalitet och (i värsta fall) förlorat förtroende från medborgare i regionen. En strukturerad strategi för IT- och informationssäkerhet innebär att regionen har kunskap om:

- Regionens **IT-infrastruktur och applikationer** (hårdvara och mjukvara), förstår vilken av dessa som är känsliga / kritiska och därmed särskilt värda att skydda.
- Regionens **informationstillgångar**, var de befinner sig, och vilken information som är känslig / kritisk och därmed särskilt värdefull.
- **Risklandskapet** i regionen, baserat på förståelsen för regionens kritiska IT-infrastrukturkomponenter och applikationer samt kritiska informationstillgångar, dvs var regionens risker finns ur ett IT- och

informationssäkerhetsperspektiv. Regionen bestämmer sedan vilka av dessa risker som kan accepteras och vilka de vill minimera och hur detta görs, av vem, på vilken nivå och var i organisationen. Det strukturerade tillvägagångssättet betyder inte att man tar upp alla risker, utan om att göra ett informerat val av vilka risker man ska ta itu med, hur man gör det och vem som är ansvarig.

- Vilka formella **roller och ansvarsområden** som måste finnas på plats för att säkerställa att informationssäkerhetsarbetet går i önskad riktning, med tydliga rollbeskrivningar och förväntningar samt med en struktur som möjliggör kontroll från toppen och ner i organisationen utan att misslyckas på olika nivåer. Helst på ett sätt där det är möjligt att utöva tydlig kontroll inom IT- och informationssäkerhetsområdet på ett konsekvent sätt i hela organisationen. Dessa roller måste vara välkända och kommuniceras.

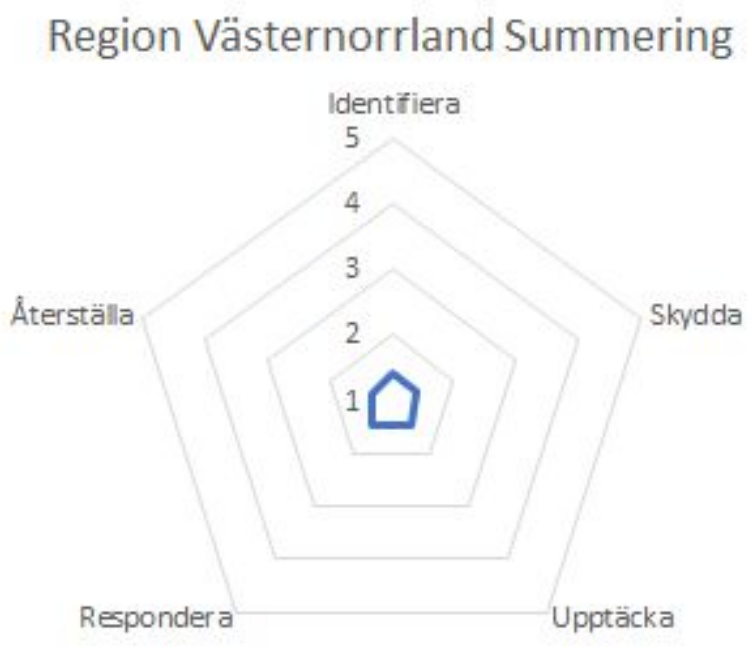
- **Dokumentation**; vilket innebär att för detta ändamål finns det tydlig dokumentation i form av policyer, riktlinjer och instruktioner som säkerställer att ledningens kontrollsignaler upprätthålls i hela beslutskedjan och kan följas upp med regelbundenhet.

2.2 Resultat NIST

Det har utifrån en informationsinsamling, som bygger på dokumentationsgranskning och intervjuer, framkommit att det finns utrymme för förbättringar när det kommer till regionstyrelsens styrning och uppföljning av informationssäkerhetsarbetet. De främsta bristerna berör Region Västernorrlands avsaknad av dokumenterade processer och ansvarsroller gällande ett flertal informations- och cybersäkerhetsområden. Vi har noterat att Regionen ofta utför flera viktiga processer och rutiner inom informationssäkerhet, men att dessa utförs utan systematik.

Det område som påvisar störst brister är avsaknaden av formaliserade och strukturerade rutiner och processer, vilket främst visar sig genom avsaknad av aktuell och uppdaterad dokumentation som faktiskt används i Region Västernorrlands arbete. Vidare genomförs varken utbildning eller övning i en ändamålsenlig utsträckning och det saknas strukturerade rutiner och processer för kontroll och uppföljning.

Givet att Region Västernorrland är en leverantör av samhällskritiska tjänster, och givet att organisationer i allmänhet bör sträva efter formella och dokumenterade processer inom samtliga informationssäkerhetsområden, vilket en bedömning på minst tre avspeglar, får regionens resultat inom de fem domänerna anses vara lågt.



Identifiera: 1.4
Respondera: 1.4
Skydda: 1.5
Återställa: 1.5
Upptäcka: 1.3

3. Iakttagelser och bedömningar

3.1 Finns en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten?

Denna revisionsfråga besvaras utifrån dimensionerna ändamålsenlig

a) organisation,
b) dokumentation och
c) uppföljning och kontroll

3.1.1 Iakttagelser organisation

Region Västernorrland är uppdelat i kärnverksamhet och serviceverksamhet. Regionens verksamhet består av sex förvaltningar:

1. Regionledningsförvaltningen
2. Folktandvården
3. Primärvården
4. Specialistvården
5. Rättspsykiatriska regionkliniken
6. Regional utveckling

Det är Regionledningsförvaltningen som denna informationssäkerhetsgranskning fokuserar på. Denna består i sin tur av ett antal avdelningar vilka framgår i bild 1 nedan. Utöver dessa områden ingår även Fastighet och Service, där frågor om exempelvis skalskydd och serverplacering ingår.

Bild 1. Organisationskarta Regionledningsförvaltningen[1]

Den nuvarande Regionledningsförvaltningen är ett resultat av sammanslagningen i samband med regionbildningen. Flertalet områden är självfinansierade, medan andra får

[1] https://www.rvn.se/sv/Om-regionen/regionens-organisation/regionledningsforvaltningen/

regionbidrag. Region Västernorrlands IT-avdelning är en del av Forskning, Utbildning och Innovation (FUI) och är intäktsfinansierat via interndebitering. Detta innebär att IT ses som en kostnad i andra delar av verksamheten. Området FUI samordnar även regionens digitaliseringsarbete.

Vi har iakttagit en bristande samordning mellan informationssäkerhetsansvariga och IT-säkerhetsansvariga. Avsaknaden av samordningsforum eller styrgrupper med förvaltnings- och regionövergripande representation resulterar i ett fragmenterat informationssäkerhetsarbete utan översyn. Detta kan exemplifieras genom att informationssäkerhet ligger under administration och it-säkerhet ligger under FUI samt att säkerhetschefen är lokaliserad under administration. Det framkommer under intervjuer att den nuvarande organisationen är en sammanslagning mellan landstingsservice och kansli. Ur ett informationssäkerhetsperspektiv kan det fragmenterade arbetet exemplifieras genom att det saknas en dedikerad grupp som endast arbetar och styr *asset management,* det vill säga tillgångshantering för hårdvaror. Att det finns en utpekad grupp som är ansvarig för detta är i detta exempel viktigt eftersom organisationen då minimerar risken för introduktion av icke godkända komponenter inom regionens IT-infrastruktur och i dess nät. En följd av detta är vidare avsaknaden av ett centralt inventarie för samtliga system och fysiska enheter som finns inom regionens IT-miljö. Utöver det så är arbetet med informationsklassning inte heller förankrat bland regionstyrelseförvaltningens ledning, vilket innebär att arbetet inte utförs konsekvent för samtlig information som behandlas inom verksamhetssystem. Det är däremot förankrat i GDPR-projektets styrgrupp. Att tillägga är dock att Region Västernorrland, som tidigare nämnt, under ett antal år använt sig av styr- och samverkansmodellen PM3 som används för förvaltning och verksamhetsutveckling i stort. Uppföljningen av aktiviteter och genomförda projekt sker dock inte kontinuerligt i verksamheterna i enlighet med PM3-modellen.

Däremot finns det en beskriven process för tillgångshantering på Region Västernorrland, men majoriteten av arbetet kring tillgångshantering sköts av leverantör och det tydliggörs i det SLA (Service Level Agreement) som tagits fram.

I granskningen framkommer att det i Region Västernorrlands arbete med riskhantering i dagsläget saknas en dedikerad roll med ansvar för riskkontroll. Det har tidigare funnits en anställd med informellt ansvar som samordnare för riskarbetet. Region Västernorrland har inte en definierad riskaptit eller risktolerans kopplat till informationssäkerhetsarbetet.

Regionen har tagit fram en tydlig organisatorisk struktur inom arbetet för anpassning till dataskyddsförordningen (GDPR). I denna gruppering finns det en tydlig ansvars och rollfördelning, tydliga incidenthanteringsprocess och rapporteringsrutiner. Däremot saknas det motsvarande organisation för IT och Informationssäkerhet.

Det finns en nyligen framtagen samverkansmodell[2] som syftar till att säkerställa att Region Västernorrlands IT-tjänster som levereras styrs på ett effektivt och säkert sätt. I

[2] Samverkansmodell för IT-tjänstestyrning, 2019-08-16

den framgår organisation och roller mellan Region Västernorrland och Leverantören i form av nyckelpersoner på tre nivåer; strategisk nivå, taktisk nivå samt operativ nivå.

Det saknas kontroll över systemägare och det framkommer att det finns ett flertal system utan objektfamiljsstruktur. Vidare kan det konstateras att många system ligger utanför förvaltningsmodellen och det saknas etablerade tillvägagångssätt för upphandlingar, främst för IT. Det framkommer även att det finns en tydlig kompetensbrist kopplat till objektägarskap och den tekniska aspekten av organisationen. Medarbetare med ansvar för verksamhetssystem utifrån Regionens förvaltningsmodell anses inte att ha förutsättningar för att kunna arbete effektivt och strukturerat med informationssäkerhet för deras system. Kopplat till detta saknar systemägare även tydlighet avseende deras ansvar för informationssäkerhetsåtgärder inom verksamhets-system som de förvaltar.

Region Västernorrlands rapporteringsvägar vid händelse av en incident beskrivs som otydliga såtillvida att de inte tycks vara kända i organisationen. Det framkommer att Regionstyrelsen är otydlig i sin styrning gällande vilken sorts information som efterfrågas vid inträffade händelser, i vilka forum samt i vilken form. Region Västernorrlands beredskapsfunktion tar ej hänsyn till informations- säkerhets- eller it-relaterade incidenter.

3.1.2 Iakttagelser dokumentation

Granskningen visar att Region Västernorrland har dokumentation inom vissa områden, men att det saknas processer för regelbunden revision och uppdatering av dessa. Det finns en dokumentationshierarki, som dock inte fungerar till följd av brist på dokument. Ett systematiskt och kontinuerligt revideringsarbete kring dokumentationen på IT- och informationssäkerhetsområdet är ännu inte på plats och dokumentationen revideras endast sporadiskt. I intervjuer framkommer det vidare att det saknas efterfrågan på styrande dokumentation från ledningen. Region Västernorrland har ett dokumenterat Ledningssystem för Informationssäkerhet som framtogs 2010-10-12. Detta dokument beskriver flera processer som ska utföras och i sin tur dokumenteras. Utifrån intervjuer har det dock framkommit att det är flera områden som benämns inom ledningssystemet som inte utförs enligt beskrivning. Exempelvis så benämner regionens ledningssystem vikten av regelbundna riskbedömningar och riskanalyser avseende informationssäkerhet och förvaltning, och att dessa bedömningar och analyser ska dokumenteras. Vi har inte fått del av några dokumenterade riskbedömningar och det har även framkommit under intervjuer att detta inte är en process som utförs regelbundet.

Region Västernorrland har endast en begränsad mängd dokumentation på plats för flera områden som berör informationssäkerhet, exempelvis är regionens Informations-säkerhetspolicy från 2008-06-25 och är i väldigt begränsat utförande. Det framgår att informationssäkerhetsarbetet ska bedrivas i enlighet med standardserien SS-ISO/IEC 27000, men varken syfte, mål eller tillvägagångssätt framgår. Även dokumentation underordnad Informationssäkerhetspolicyn saknar regelbunden revision och uppdatering. Granskningen visar vidare på en otydlighet kring huruvida nuvarande dokumentation hör samman med varandra då många dokument saknar hänvisningar till övrig dokumentation.

Under granskningen noterades att ett flertal av planerna och dokumenten varken är beslutade eller har diarienummer, se Bilaga 1 för lista över dokumentation. Vidare framkom det under intervjuer att det övergripande saknas vetskap om styrdokument och rutiner gällande informationssäkerhet, såväl hos tjänstemän som hos politiker. Slutligen framkom det att regionen saknar ett arbete för dokumenthantering samt rutiner för hur dokument ska implementeras när de väl är beslutade. Diariesystemet Platina används för förvaltning och hantering av den styrande dokumentationen.

Vi har vidare iakttagit att flera väsentliga informationssäkerhetsprocesser saknar dokumentation, antingen i form av processbeskrivningar, rutiner eller instruktioner, vilket kan kopplas till avsaknaden av en tydligt tillämpad dokumentationsstruktur.

Nedanstående bild visar en vanligt förekommande struktur på en dokumentations-hierarki inom ett ledningssystem för informationssäkerhet:

Bild 2: Exempel på dokumentationshierarki inom ett ledningssystem för informationssäkerhet

Vi har iakttagit att Regionen har delar av denna dokumentationsstruktur på plats, med flera beskrivna instruktioner och rutiner, exempelvis Hantering av informationssäkerhets-incidenter - Personuppgiftsincident[3]. I flera fall finns det tydliga kopplingar mellan rutiner och riktlinjer. Noterat är vidare att Region Västernorrland har dokumentation för styrning av behörigheter och åtkomst till verksamhetskritiska system inom hälso- och sjukvården på plats.

Under intervjuer framkom att Region Västernorrland har som ambition att arbeta framåt i enlighet med ett ledningssystem för informationssäkerhet (ISO 27000), vilket bland annat enligt intervjuer avspeglar sig i den dokumentation som är under utarbetning.

Region Västernorrland har också ett detaljerat SLA [4]på plats med leverantör, samt en dokumenterad samverkansmodell som styr och reglerar samverkansarbetet mellan regionen och leverantören. SLA:t innehåller flera bilagor med kravställning inom viktiga

[3] Hantering av informationssäkerhetsincidenter - Personuppgiftsincident, 2018-06-07
[4] Service Level Agreement

informationssäkerhetsområden. Regionen har inom avtalet med leverantör en bilaga med specificerade säkerhetskrav, vilken inkluderar en kravlista på 131 punkter som härstammar från ISO 27001-standarden. Ytterligare en bilaga fastställer servicenivåer på som leverantörer ska förhålla sig till avseende drift, säkerhetskopiering och återställning.

3.1.3 Iakttagelser uppföljning och kontroll

Det saknas rutiner för uppföljning av Region Västernorrlands framtagna och beslutade dokumentation på samtliga nivåer. Det framgår av intervjusvar att erfarenhetsåterföring, och utvärderingar, exempelvis i form av ny lagstiftning, incidenter, omvärldsbevakning eller i det löpande arbetet, inte genomförs i önskad utsträckning. Vidare saknas det rutiner för uppföljning för att säkerställa att identifierade förbättringar implementeras i verksamheten. Under intervjuer framkommer det att finns en tydlig avsaknad av dokumenterade processer och ansvarsroller gällande ett flertal informations- och cybersäkerhetsområden.

Region Västernorrland genomför inte uppföljning av de informationssäkerhetsdokument som ska upprättas på förvaltnings- och områdesnivå. Vidare framkom det att det saknas rutiner för uppföljning för att säkerställa att förbättringar som identifieras i verksamheten implementeras.

Då IT-driften bedrivs av leverantör har det skapats ett omfattande SLA med en tydlig kravställan gentemot leverantören. Det framkommer i intervjuer att det finns ett forum för att följa upp avtal med leverantör. Däremot sker det inte någon aktiv säkerhetsgranskning eller kontroll av att avtalet följs. Vidare kan det konstateras att Regionen saknar dokumenterade arbetsroller med fokus på IT-säkerhet som kan säkerställa efterlevnad av avtal med leverantör; IT-säkerhetsarbetet tillhör IT-grupperingen och utförs av medarbetare med flera andra ansvarsområden.

Utifrån intervjuer med ledande beslutsfattare inom regionen har det framkommit att rapportering till regionledningen och regionstyrelsen avseende informationssäkerhets-händelser, incidenter samt övriga områden som berör informationsförvaltning inte sker regelbundet. Rapportering som har skett har främst berört frågor kopplade till dataskyddsförordningen, men inte heller detta utförs reguljärt. Region Västernorrlands organisationsstruktur inom informationssäkerhetsområdet uppges i intervjuerna försvåra möjligheterna till reguljär rapportering och uppföljning. I nuläget saknas det formella samarbetsforum och rutiner inom informationssäkerhet, då informationssäkerhets-ansvariga och IT-säkerhetsansvariga saknar dokumenterade processer för informationsutbyte.

3.1.4 Bedömning (organisation, dokumentation, uppföljning och kontroll)

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är vår bedömning att revisionsfrågan **ej uppfylls**.

Organisation

När det gäller den generella bilden av Regionstyrelsens förmåga att styra och leda verksamheten, med bäring på IT- och informationssäkerhet, är vår bedömning att den

hittills inte varit ändamålsenlig. Regionen saknar i stora delar ett *systematiskt* arbete med IT- och informationssäkerhet. *Detta är dock inte detsamma som att säga att arbete relaterat till dessa frågor inte bedrivs.* Regionen har både en IT-avdelning (Region-IT) vilken numera sorterar direkt under FUI, och regionen har likaså ett informationssäkerhetssamordnare som sorterar under administrativa enheten, vilket innebär att det finns ett utpekat men spritt ansvar för dessa frågor i organisationen. Det pågår vidare en rad olika insatser och projekt inom ramen för dessa verksamheter.

Enligt vår bedömning är nuläget således att det saknas en formaliserad systematik i hur arbetet bedrivs och att det saknas en helhetsbild av vad som genomförs. Organisationen går inte i takt inte i alla delar vad gäller systematiken kring riskanalyser, informationsklassning och stödjande och styrande dokumentation, vilka alla utgör viktiga byggstenar i ett systematiskt IT- och informationssäkerhetsarbete. Ett flertal viktiga processer och rutiner inom informationssäkerhet utförs därmed ad hoc till följd av brist på styrning. Exempelvis saknas det en dedikerad grupp som endast arbetar och styr *asset management* (det vill säga tillgångshantering på hårdvarusidan och mjukvarusidan). En följd av detta är avsaknaden av ett centralt inventarie för samtliga system och fysiska enheter som finns inom regionens IT-miljö. Arbetet med informationsklassning är inte förankrat bland regionstyrelseförvaltningens ledning, vilket innebär att arbetet inte utförs konsekvent för samtlig information som behandlas inom verksamhetssystem. Att IT ses som en kostnad då det krävs interndebitering för assistans och IT-relaterade tjänster ses även som problematiskt och kan vara en grund till det icke-ändamålsenliga informationssäkerhetsarbetet.

Det påbörjade arbetet med att implementera ett ledningssystem för informationssäkerhet i enlighet med ISO27000 serien har pågått under en längre tid utan att färdigställas. Inom ett ledningssystem för informationssäkerhet bör den strategiska inriktningen för ett informationssäkerhetsarbete fastställas av en strategi och policy. En sådan strategi eller policy för informationssäkerhet bör ge en tydlig förklaring till syftet med ett gediget informationssäkerhetsarbete och bör även förstärkas av en underordnad standard som beskriver samtliga processer som informationssäkerhet omfattar. En sådan standard bör ge en inriktning för, och en beteckning av, samtliga processer som ska utföras och bör vidare hänvisa till underordnade dokument (processbeskrivningar och rutiner) som beskriver vem som ansvarar för utförandet av underordnade aktiviteter och hur det ska utföras. Processbeskrivningar bör i sin tur omfatta samtliga informationssäkerhets- åtgärder; administrativa, tekniska, och dem som riktar sig mot att skapa en ändamålsenlig säkerhetskultur.

Dokumentation

Region Västernorrland har en ändamålsenlig dokumentation inom vissa områden, men det saknas processer för regelbunden revision och uppdatering av dessa. Det finns en dokumentationshierarki, som dock inte fungerar ändamålsenligt till följd av brist på dokument. Regionen saknar således väsentlig formell dokumentation för att styra sitt IT- och informationssäkerhetsarbete på en strategisk nivå som förankrar arbetet med Regionens centrala roll som leverantör av samhällsviktiga tjänster.

Regionen saknar vidare dokumentation för flera processer med bäring på ett strukturerat informationssäkerhetsarbete. Avseende exempelvis *riskhantering* (som berör informa-

tionssäkerhet), har vi noterat att det saknas formell dokumentation. De processer som utförs inom riskhantering är varken dokumenterade eller formaliserade. Detta fastän den dokumenterade *Ledningssystemet för Informationssäkerhet* som antagits 2010 benämner en dokumenterad riskhantering och riskbedömning som en huvudsaklig komponent i informationssäkerhetsarbetet. Det saknas även dokumentation som fastställer regionens riskaptit eller risktolerans som eventuella riskhanteringsåtgärder bör förhålla sig till.

Det kan vidare konstateras att Region Västernorrland inte arbetar aktivt med rutiner och processer med syfte att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle inkludera regelbunden revision och uppdatering av styrande dokument.

Bedömningen är sammanfattningsvis således grundad i avsaknaden av regelbunden revision, granskning och uppdatering av samtlig dokumentation, iakttagelsen att vissa processer saknar dokumentation, samt i iakttagelsen att det saknas ett strukturerat ledningsarbete som samordnar samtlig väsentlig dokumentation.

Uppföljning och kontroll

Sammanfattningsvis kan man säga att det genomförs arbetsinsatser inom både IT- och informationssäkerhet, men att den formella och systematiska sidan av detta arbete hittills tyngs av brister i form av tydliga rapporteringsvägar (framför allt på strategisk nivå), avsaknad av dokumentation, och delvis av avsaknad av riskanalyser och informationsklassning, vilket innebär att helheten uteblir.

Region Västernorrland har under ett antal år använt sig av styr- och samverkans-modellen PM3 som används för förvaltning och verksamhetsutveckling i stort. Uppföljningen av aktiviteter och genomförda projekt sker dock inte kontinuerligt i verksamheterna i enlighet med modellen.

Givet att Regionstyrelsen hittills inte regelbundet och med systematik efterfrågat återrapportering inom IT- och informationssäkerhetsområdet innebär detta att inte heller Regionstyrelsen kan sägas besitta den helhetsbild som krävs för att styra, leda eller ge direktiv gällande informationssäkerhetsarbetet. Det otydliga ägandeskapet av informationssäkerhetsfrågor kan vidare betraktas som en bidragande orsak till bristande rapportering. Ett exempel är det utspridda ägandeskapet av informationssäkerhetsfrågor samt säkerhetsfrågor. Informationssäkerhet förekommer som en del av ansvaret inom systemägarrollen utifrån förvaltningsmodellen, och är även placerad centralt inom regionstyrelseförvaltningens administrativa enhet. Det tekniska ansvaret för informationssäkerhet är placerat hos IT-organisationen, vilken tillhör en annan organisatorisk enhet. Vi har varken iakttagit några formella, dokumenterade eller informella samarbetsforum för att säkerställa samordning mellan dessa enheter. Denna situation accentueras ytterligare av avsaknaden av formaliserad och uppdaterad dokumentation av väsentliga styrdokument såsom IT- och informationssäkerhets-strategier. Det är inte klart huruvida avsaknaden av vissa centrala styrdokument har lett till att styrsignalerna varit svaga, eller om de svaga signalerna lett till att vissa styrande dokument inte kommit på plats.

3.2 Har ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning?

3.2.1 Inledning

Den tidigare granskningen från 2017[5] benämnde ett flertal brister avseende IT- och informationssäkerhetsarbetet. Granskningen betonade särskilt att:

- *"Styrelsen behöver säkerställa att det finns moderna, konkreta och väl kända styrmedel för IT-säkerheten. Att organisera informationssäkerhetsarbetet och ansvaret för IT-säkerheten i två olika ansvarsområden underlättar inte en effektiv hantering. Särskilt som det inte finns uttalat och dokumenterat hur det praktiskt ska åstadkommas. En väsentlig aktivitet i uppdateringen av styrdokumenten är att utföra analyser, få informationen klassad och tydliggöra för verksamhetens chefer att de har det yttersta praktiska ansvaret för informationssäkerheten och därmed vilken IT-säkerhet som kommer att behövas. Detta innebär ett behov av återkommande utbildning av och information till alla delar av verksamheten.*

- *Vi anser det oroande att anpassningen till nya förordningar, författningar och direktiv (bland annat dataskyddsförordningen, GDPR) inte kommit längre än vad som framkommer vid våra intervjuer. Verksamheten som bedrivs framförallt inom sjukvården omfattas i stor utsträckning och det är kort om tid för att få till stånd alla nödvändiga anpassningar. Eftersom styrningen av informationssäkerheten inte bedöms som utvecklad i en ändamålsenlig omfattning så ger det heller inget stöd för hur anpassningsarbetet ska bedrivas.*

- *Vi saknar att styrelsen genom åren inte säkerställt efterlevnaden av informationssäkerheten så att det påverkat hur internkontrollen inriktats och hanterats. Vi menar vidare att styrelsens uppfattning om efterlevnaden av informationssäkerheten ska framgå av centrala dokument som patientsäkerhetsberättelser och årsredovisningar.*

- *Vi anser att med underlag av våra iakttagelser det finns motiv för revisionen att fortsättningsvis på olika sätt omfatta informationssäkerhet i kommande granskningar."*[6]

Bedömningen utifrån revisionsfrågorna blev att Region Västernorrlands styrelse inte tillsett att det vid granskningstillfället funnits aktuella styrande dokument i en omfattning och konkretisering som tydliggör alla de krav som ställs på hur arbetet med informationssäkerhet och IT-säkerhet ska bedrivas. Vidare gjordes bedömningen att styrelsen inte tillsett att det funnits ett genomtänkt och strukturerat arbete för att säkerställa en ändamålsenlig IT-säkerhet som ansågs vara tillräcklig i förhållande till de utmaningar som framtiden skapar. Slutligen gjordes bedömningen att styrelsen inte hade former att säkerställa efterlevnad av informationssäkerhet och därigenom även IT-säkerheten.

[5] Revisionsrapport IT-säkerhet, Region Västernorrland, KPMG, 2017-12-13
[6] Revisionsrapport IT-säkerhet, Region Västernorrland, KPMG, 2017-12-13

3.2.2 Iakttagelser

Regionstyrelsen bedömde att den tidigare revisionens bedömningar och iakttagelser var en korrekt beskrivning av nuläget inom informationssäkerhet och IT-säkerhet. Vidare ansåg Regionstyrelsen det vara relevant och angeläget att åtgärda identifierade brister och att det systematiska informationssäkerhetsarbetet ska ske med stöd av ett ledningssystem, vilket ger ett sätt för organisationens ledning att styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering. Regionstyrelsen avsåg även, enligt Svar på revisionsrapport "IT-säkerhet"[7], att upprätta och införa ledningssystemet för informationssäkerhet enligt kraven i standarden ISO 27000 enligt tidigare beslutad policy och riktlinje. Ledningssystemet omfattar bland annat policy, organisation, ansvar, styrande dokument, resurser och efterlevnad. Detta har ännu inte slutförts. Slutligen konstaterade Regionstyrelsen att ett projekt skulle tillsättas i december 2017 för införande av åtgärder med syfte att säkerställa efterlevnad av Dataskyddsförordningen.

Vid svaret på granskningen framgick Regionstyrelsens planerade åtgärder att tillsätta en utredning inom ramen för implementerandet av ledningssystemet ISO 27000 för att bedöma omfattning, resurser/kostnader för ett projekt med målet att införa ledningssystemet ISO 27000. I detta skulle även kompetens och resurser analyseras till följd av att det vid granskningens svar ansågs vara en brist. Det kan konstateras att det från samtliga håll finns en stor förväntan på att ledningssystemet för informationssäkerhet kommer åtgärda en stor del av de problematiska områden som finns i dagsläget och som har iakttagits av föregående rapport. Det finns även en medvetenhet om att det återstår mycket arbete inom detta projekt och att det i nuläget saknas en mogen organisatorisk struktur som kan ta emot och förvalta ledningssystemet.

Det har upprättats en virtuell dataskyddsorganisation inom ramen för det administrativa området. Det finns en utpekad dataskyddsjurist, ett dataskyddsombud samt kommunikatörer som fokuserar på personuppgiftsincidenter, frågor samt rekommendationer kring GDPR. Vidare har det upprättats en e-utbildning om dataskyddsförordningen för nyanställda och chefer, däremot sker ingen uppföljning eller kontroll av att denna görs och det sker inga utbildningar för informationssäkerhet. Det finns en påbörjad ansats för att utbilda TiB i att ta kontakt med Datainspektionen för att effektivisera processen.

Rutiner för informationsklassning och riskanalyser togs fram i samband med dataskyddsförordningen. Det är verktyget KLASSA som används som ramverk och det uttalade målet för Region Västernorrland är att samtliga system ska klassas, det har dock inte slutförts i dagsläget. Riskanalyser genomförs i samband med upphandlade system, dock endast utifrån KLASSA. Däremot samordnas inte riskanalyser med övrig verksamhet vilket tyder på ett fragmenterat arbete som inte styrs centralt.

Det tidigare Landstinget Västernorrland saknade ett formellt strukturerat arbete utifrån ISO 27000-standarden. Vidare tenderade informationssäkerhetsfrågor att ofta omprövas, vilket resulterade i ett bristande informationssäkerhetsarbete. Det

[7] Svar på revisionsrapport "IT-säkerhet", 2018-02-15

framåtsyftande arbetet med bland annat omarbetad dokumentation har som ambition att vara i linje med ISO 27000. Vid intervjuer framkommer att det generellt sett fortfarande saknas central styrning av informationssäkerhetsarbetet i Region Västernorrland, vilket även identifieras som en sårbarhet och svaghet i regionen av intervjudeltagare. Det framkommer under intervjuerna med både strategiska och operativa funktioner att det saknas en gemensam förståelse för nuläge, respektive önskat läge, gällande informationssäkerhet. Under intervjuer konstateras att det saknas bestämmelser och riktlinjer från Regionstyrelsen respektive ledning avseende efterlevnad av säkerhetsbestämmelser och grundläggande inställningar och krav.

Det framkommer under intervjuer att det inte finns ett etablerat mottagande av ett ledningssystem för informationssäkerhet. Som nämnt i avsnittet ovan anser vi att Region Västernorrland inte uppnår en ändamålsenlig mognadsnivå kopplat till informationssäkerhet i dagsläget. Givet organisationen är mottagandet av ett till fullo implementerat ledningssystem för informationssäkerhet eventuellt inte möjligt då det saknas mottagande struktur på plats som kan möjliggöra en ändamålsenlig implementering av ett ledningssystem.

Klassificering av IT-system med avseende på informationssäkerhet genomförs av regionen men samtliga verksamhetssystem har inte klassats utifrån informationssäkerhetskrav. Däremot har någon systematisk genomgång av övriga informationsklasser inte genomförts mer än sporadiskt. Det saknas dokumentation i form av exempelvis instruktioner för informationsklassning i regionen. Däremot finns rutiner och processer på plats för riskanalys i samband med upphandlingar och i samband med införandet av nya system.

Som konstaterats i iakttagelserna under den föregående revisionsfrågan noteras att någon särskild rapportering om status på IT- och informationssäkerheten ännu inte efterfrågas av Regionstyrelsen. Det sker ingen löpande rapportering, utöver den årliga rapporteringen, om informationssäkerhet till Regionstyrelsen i dagsläget.

3.2.3 Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är vår bedömning att revisionsfrågan **ej uppfylls**.

Utöver tydlig, beslutad och kommunicerad dokumentation kräver ett gediget informationssäkerhetsarbete tydliga processer och rutiner för att säkerställa styrning och ändamålsenlig uppföljning. En strukturerad uppföljning och rapportering av resultat och efterlevnad av styrande dokument är en förutsättning för att styrelse och nämnder ska kunna följa upp och utvärdera förvaltningarnas uppdrag och verksamheternas arbete. Uppföljning är viktig för att regionens invånare ska få en inblick i verksamheten och säkerställa att offentliga medel används effektivt. Bedömningen är grundad i avsaknaden på regelbunden revision, granskning och uppdatering av samtlig dokumentation samt att vissa processer saknar dokumentation. Att Regionstyrelsen sällan efterfrågar en rapportering resulterar i att medvetenheten om informationssäkerhet inte kan säkerställas.

De positiva effekterna av de riskanalyser som exempelvis genomförs i samband med upphandlingar uteblir om riskanalyserna inte kan sättas i relation till regionens totala

riskkarta, vilken i nuläget åtminstone delvis saknas. Risker tillhörande regionens kritiska IT-infrastrukturkomponenter och applikationer samt kritiska informationstillgångar, ur ett IT- och informationssäkerhetsperspektiv, finns inte samlade i ett centralt register. Regionen bestämmer vilka av dessa risker som kan accepteras och vilka de vill minimera och hur detta görs, av vem, på vilken nivå och var i organisationen. Det strukturerade tillvägagångssättet betyder inte att man tar upp alla risker, utan att göra ett informerat val av vilka risker man ska ta itu med, hur man gör det och vem som är ansvarig.

Bristen på systematisk informationsklassning resulterar i svårigheter för regionen att skapa en helhetsbild av hur IT- och informationssäkerhetsarbetet ska bedrivas för att adressera och minimera de risker som olika informationsklasser innebär. Samma sak gäller för ett systematiskt arbete med risker kopplat till IT- och informationssäkerhet.

4. Revisionell bedömning

De övergripande revisionsfrågorna för aktuell informationssäkerhetsgranskning är följande:

- *Finns en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten?*

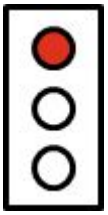
Nej. Vår bedömning är att Regionstyrelsen **inte** har säkerställt en styrning och uppföljning som ger en ändamålsenlig informationssäkerhet. Grunden till denna bedömning är den nuvarande avsaknaden av regelbunden revision, granskning och uppdatering av styrande dokumentation, avsaknaden av dokumentation för vissa väsentliga informationssäkerhetsprocesser, bristande kontinuerlig uppföljning och rapportering kring informationssäkerhetshändelser och incidenter till Regionstyrelsen, samt ineffektiva organisationsstrukturer avseende informationssäkerhetsarbetet.

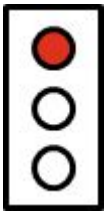
- *Har ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning?*

Nej. Vi bedömer vidare att Regionstyrelsen **inte** har vidtagit och kommit i mål med åtgärder med anledning av de brister och förbättringsförslag som framfördes i förstudien 2017. Denna bedömning bygger på den iakttagna avsaknaden av både systematisk informationsklassning av samtliga system samt regelbundna och dokumenterade riskanalyser, vilket är åtgärder som rekommenderades av 2017 års granskning. Den ovan nämnda punkten kring brister med styrningen och dokumentation påvisar således att det fortfarande finns ett förbättringsarbete som regionen bör utföra.

Med hänvisning till de brister som identifierats följer här nedan en förteckning på rekommendationer som regionen bör ta i åtgärd.

4.1 Bedömningar mot revisionsfrågor

Revisionsfråga	Kommentar	
Finns en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten?	**Nej.** • Regionen saknar ett gediget ledningssystem för informationssäkerhet och tillhörande organisatorisk struktur och dokumentation • Regionen saknar regelbundna	

	rapporteringsrutiner avseende informationssäker-hetsarbetet	
Har ändamålsenliga åtgärder vidtagits med anledning av 2017 års granskning?	**Nej.** • Regionens har ej säkerställt en uppföljning och vidtagning av ändamålsenliga åtgärder som följd av iakttagelserna från 2017 års granskning.	

Rekommendationer

Människor och processer:

- Regionen bör fastställa en färdplan för införandet av ett ledningssystem för informationssäkerhet. En sådan färdplan bör innehålla tydliga målsättningar, ansvarsbeskrivningar för medverkande resurser, samt en konkret tidsram som arbetet för framtagning av ett ledningssystem ska förhålla sig till.

- Regionen bör utreda möjligheten att upprätta en arbetsgrupp för informationssäkerhet som sammanträder regelbundet och inkluderar nyckelpersoner för arbetet. Denna grupp bör ha ansvar för förvaltning av Ledningssystemet för informationssäkerhet och bör ha som uppgift att styra och samordna informationssäkerhetsarbetet inom hela regionen. Arbetsgruppen bör vidare ha ett övergripande ansvar för omvärldsbevakning inom informations-säkerhetsområdet.

- Inom ramen för ledningssystemet för informationssäkerhet bör regionen upprätta ett aggregerat riskregister med regionövergripande informationssäkerhetsrisker. Ett sådant register bör uppdateras regelbundet samt användas för åtgärdsplanering, och bör utgöra grunden till en reguljär rapportering till regionstyrelsen eller regionens ledning. Riskregistret bör vidare vara framtaget med regionens huvudsakliga samhällsfunktion och leverans i åtanke.

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation som tillhör ledningssystemet ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.

- Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhetspolicyn till riktlinjer.

- Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Västernorrland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.

- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör genomföra systematiska uppföljningar av utbildningsverksamheten.

- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.

- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

- Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Västernorrland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

- Regionen bör se över förvaltningsmodellen för verksamhetssystem och utreda möjligheter till att förstärka ansvaret som systemägare har för tillämpning av informationssäkerhetsåtgärder.

Teknik:

- Utred möjligheterna till att införskaffa en central behörighetshantering som integreras med övriga verksamhetssystem. Ett sådant system bör till stor del automatisera processer för tilldelning, förändring, och borttagning av behörigheter. Utifrån ett sådant system bör behörighetstilldelning och behörighetsgrupper framtas som baseras på i förväg bestämda roller. I synnerhet bör regionens tilldelning av behörigheter till fysiska lokaler ses över, särskilt med hänsyn till känsliga rum som serverhallar.

- Utred möjlighet till att införskaffa en SIEM-lösning som samlar in och aggregerar säkerhetsloggar från väsentliga nätverkskällor, exempelvis de virtuella brandväggar som i nuläget är placerade mellan nätverkssegment. Införskaffandet av en dedikerad loggserver bör även utredas med krav på bibehållen lagring på minst 180 dagar.

- Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans.

Bilaga

Dokumentationslista

Dokumentrubrik	Beslutat?	Fastställt	Giltigt t.o.m.	Dnr
Change Management	Ja	2019-05-28	2020-11-28	376007 / Version 1
Dataskyddsförordningen	Nej			
Informationssäkerhetsutbildning för alla användare	Nej			
Hantering av informationssäkerhetsincidenter - Personuppgiftsincident	Ja	2018-06-07	2019-12-07	327500 / Version 1
Hantering av tillgångar	Ja	2016-11-21	2020-01-04	231696 / Version 2
Informationsklassning - verktyget KLASSA	Ja	2017-12-20	2019-06-20	288149 / Version 1
Informationssäkerhet	Nej			
Informationssäkerhetspolicy	Ja	2008-06-25		
IT Incidentprocess	Ja	2019-05-28	2020-11-28	393051 / Version 1
Ledningsystem, informationssäkerhet	Ja	2010-10-12		
Reglemente för Regionstyrelsen, Nämnden för hållbar utveckling och Hälso- och sjukvårdsnämnden 2019-2022	Ja	2018-04-25		371678 / Version 1
Protokoll Regionledningsgruppen Region Västernorrland		2019-06-03		19-RS4
Styrning av åtkomst - op-konto för driftleverantör	Ja	2019-01-20	2020-07-20	361606 / Version 1
Systemdokumentation	Ja	2016-11-22	2020-02-27	231947 / Version 2
Systemförteckning	Ja	2016-11-21	2020-01-04	235331 / Version 2
Säkerhets- och krisberedskapsarbetet i Landstinget Västernorrland		2013-11-12		/92657 / Version 2
Krisberedskap och allmän säkerhet i Landstinget Västernorrland		2013-10-30		/92653 / Version 2
Kommunikationspolicy 2019-2022		2019-06-20		/40900 / Version 4
Region kris- och katastrofmedicinsk beredskapsplan		2017-10-25		/132212 / Version 3
Kriskommunikationsplan		2014-11-26		
Bilaga 6 - Servicenivåavtal	Ja			13LS1494
Samverkansmodell för IT-tjänstestyrning		2019-08-16		

Behörighetstilldelning Vårdsystem		2012-10-11		/73775 / Version 1
Avbrottsinstruktion – LVNHSAWS är inte tillgänglig!		2017-06-20		
Förvaltningsplan för Organisations- och behörighetsstyrning		2018-09-12	2021	
Bilaga 2 OBS – Servicefönster		2017-08-16		
Avbrottsplan OBS		2018-01-08		
Bilaga 1 OBS – SLA krav		2017-08-16		
Namnstandard organisatoriska enheter				317847 / Version A.K.
Behovs- och riskanalys vid behörighetstilldelning i vårdsystem				/109760 / Version A.K.
Stöd och beslutsprocess vid organisationsförändringar		2019-09-15	2021-03-15	426117 / Version 1
Bilaga 3 OBS – klassificering/prioritering		2017-08-16		
Tillgänglighetsplan OBS		2016-08-04		
Tilldelning av läsbehörigheter med medarbetaruppdrag		2014-06-25	2016-12-30	/127967 / Version 2
Laglig behandling OSL och GDPR	Nej			
Ställningstagande om informationshantering i vissa molntjänster		2019-04-12		Ärendenummer: 19/00087
Beslutsunderlag - Fortsatt upphandling av RIS/PACS till RVN		2019-01-15		
Protokoll §§ 102-104 Regionstyrelsens Finansutskott		2019-06-17		19RS1
Bilaga 9 - Säkerhet				13LS1494

2019-11-27

Marie Lindblad

Linus Owman