REGION VÄSTMANLAND
ANKOM
2018 -03- 08
Dnr. RV/80445-1

Region Västmanland
Regionens revisorer

2018-03-02

Hans Strandlund

Till
Regionstyrelsen för svar
Regionfullmäktige för kännedom

Granskning av informationssäkerhet

PwC har på uppdrag av Region Västmanlands förtroendevalda revisorer granskat regionen informationssäkerhet. Den övergripande revisionsfrågan har varit: Har regionstyrelsen på övergripande nivå ett ändamålsenligt arbete med informationssäkerhet?

Efter genomförd granskning bedömer vi att regionstyrelsen till viss del har uppfyllt kontrollmålen. Sammantaget bedöms regionen aktivt arbeta med informationssäkerhet, men att förbättringsmöjligheter finns för att nå ett fullt ut tillfredsställande och ändamålsenligt arbete. Därtill bör regionstyrelsen följa de rekommendationer som läggs fram i rapporten för att säkerställa ett fortsatt effektivt arbete inom regionen.

Det har identifierats att regionen brister i implementeringen av styrande dokumentation och riktlinjer. I granskningen har det även framkommit att regionen saknar en tidsplan för implementering för införandet av ett informationssäkerhetsarbete i enlighet med ISO 27001. En informationsklassning har genomförts för att säkerställa rätt nivå av säkerhet. Däremot framkommer det ingen dokumenterad riktlinje för implementering av informationsklassning. En förteckning på genomförda riskanalyser har tillhandahållits, vilket styrker regionens aktiva arbete inom området. Däremot framhölls det en osäkerhet kring uppföljning och säkerhetsställande av dessa riskanalyser och dess implementering. I regionens arbete för att öka medvetenheten kring informationssäkerheten ute i verksamheten genomförs olika aktiviteter. Det har framkommit att uppföljning sker, men detta har däremot inte kunnat styrkas i en systematisk genomförandeplan.

Utifrån våra iakttagelser bör nämnas att många åtgärder redan identifierats och eventuellt påbörjats av regionen avseende de utvecklingsområden som uppmärksammats i granskningen. Beaktat detta rekommenderar vi regionstyrelsen att uppmärksamma följande i kommande arbete gällande informationssäkerhet:

- För att uppnå certifieringsbarhet bör Region Västmanland i högre utsträckning ansluta till åtgärdsmålen definierade i ISO 27001. Granskningen har identifierat brister inom exempelvis; personalsäkerhet och styrning av all information inom regionen.
- 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.
- Säkerställ att informationssäkerhetspolicyn 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.

Region Västmanlands revisorer
c/o PwC
Box 885
721 23 VÄSTERÅS
Telefon: 010-212 61 18

Region Västmanland
Regionens revisorer

2018-03-02

Hans Strandlund

- 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.
- Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten
- Inför kriterier för när en incident ska klassas som en större incident.
- Med hänsyn till ny lagstiftning inom säkerhetsskydd bör Region Västmanland genomföra en djupare analys av regionens kritiska informationstillgångar för rikets säkerhet. Därtill bör regionen i metoden för informationsklassning införa en analys av om det förekommer uppgifter av betydelse för rikets säkerhet eller skyddet mot terrorism.
- Vi rekommenderar att krisberedskapssamordnaren specificerar vilka system som behövs vid en allvarlig eller extraordinär händelse samt att klassningen överensstämmer med rådande behov.

Iakttagelser och bedömningar framgår i bifogad rapport. Revisorerna önskar svar från regionstyrelsen senast 2018-06-04.

FÖR REGIONENS REVISORER

Hans Strandlund
Ordförande

Elisabeth Löf
Revisor

Region Västmanlands revisorer
c/o PwC
Box 885
721 23 VÄSTERÅS

Telefon: 010-212 61 18

www.pwc.se

Revisionsrapport

Granskning av informationssäkerhet

Region Västmanland

Martin Bernhardtz
Jaak Akker
Catharina Ankre
Louisa Rabaeus

Februari 2018

pwc

Innehåll

Sammanfattning och rekommendationer

PwC har på uppdrag av Region Västmanlands förtroendevalda revisorer granskat regionen informationssäkerhet. Den övergripande revisionsfrågan har varit: Har regionstyrelsen på övergripande nivå ett ändamålsenligt arbete med informationssäkerhet?

Efter genomförd granskning bedömer vi att regionstyrelsen till viss del har uppfyllt kontrollmålen. Sammantaget bedöms regionen aktivt arbeta med informationssäkerhet, men att förbättringsmöjligheter finns för att nå ett fullt ut tillfredsställande och ändamålsenligt arbete. Därtill bör regionstyrelsen följa de rekommendationer som läggs fram i rapporten för att säkerställa ett fortsatt effektivt arbete inom regionen.

Det har identifierats att regionen brister i implementeringen av styrande dokumentation och riktlinjer. I granskningen har det även framkommit att regionen saknar en tidsplan för implementering för införandet av ett informationssäkerhetsarbete i enlighet med ISO 27001. En informationsklassning har genomförts för att säkerställa rätt nivå av säkerhet. Däremot framkommer det ingen dokumenterad riktlinje för implementering av informationsklassning. En förteckning på genomförda riskanalyser har tillhandahållits, vilket styrker regionens aktiva arbete inom området. Däremot framhölls det en osäkerhet kring uppföljning och säkerhetsställande av dessa riskanalyser och dess implementering. I regionens arbete för att öka medvetenheten kring informationssäkerheten ute i verksamheten genomförs olika aktiviteter, så som obligatoriska kurser. Det har framkommit att uppföljning sker, men detta har däremot inte kunnat styrkas i en systematisk genomförandeplan.

Rekommendationer

Utifrån våra iakttagelser bör nämnas att många åtgärder redan identifierats och eventuellt påbörjats av regionen avseende de utvecklingsområden som uppmärksammats i granskningen. Beaktat detta rekommenderar vi regionstyrelsen att uppmärksamma följande i kommande arbete gällande informationssäkerhet:

- För att uppnå certifieringsbarhet bör Region Västmanland i högre utsträckning ansluta till åtgärdsmålen definierade i ISO 27001. Granskningen har identifierat brister inom exempelvis; personalsäkerhet och styrning av all information inom regionen.

- 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.

- Säkerställ att informationssäkerhetspolicyn 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.

- 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.

- Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten

- Inför kriterier för när en incident ska klassas som en större incident.

- Med hänsyn till ny lagstiftning inom säkerhetsskydd bör Region Västmanland genomföra en djupare analys av regionens kritiska informationstillgångar för rikets säkerhet. Därtill bör regionen i metoden för informationsklassning införa en analys av om det förekommer uppgifter av betydelse för rikets säkerhet eller skyddet mot terrorism.

- Vi rekommenderar att krisberedskapssamordnaren specificerar vilka system som behövs vid en allvarlig eller extraordinär händelse samt att klassningen överensstämmer med rådande behov.

1. Inledning

1.1. Bakgrund

Allt fler allvarliga cybersäkerhetsincidenter har drabbat såväl privat- som offentlig sektor de senaste åren. En gemensam beståndsdel i flera av de allvarligaste händelser är information som på ett eller annat sätt kommit obehörig tillhanda, antingen genom bristande rutiner och hantering eller genom yttre påverkan, i vissa fall en kombination av bägge delarna. 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, men det kräver också ett säkerhetsmedvetande hos de som hanterar informationen på daglig basis. Informationssäkerhet regleras inte genom en sammanhållande lag utan genombestämmelser i flera olika regelverk. Det finns även i lagstiftning, föreskrifter och rekommendationer inom hälso- och sjukvård med flera områden varför ett ledningssystem för informationssäkerhet rekommenderas.

Under våren 2017 genomfördes en granskning av IT-säkerhet i Region Västmanland, och 2015 granskades även regionens fysiska säkerhet av verksamhetskritisk digital information. I denna konstaterades det bland annat att regionen förvisso har ett implementerat ledningssystem för informationssäkerhet men ett antal förbättringspunkter identifierades. Bland annat pågick arbetet med att ta fram en modell för informationsklassning. Det framkom även att det saknades dokumentation för bedömning av två av de viktigaste informationssäkerhetskomponenterna; krav på sekretess och riktighet.

Denna granskning tar vid och fördjupar hur väl ledningssystemet tillämpas i verksamheten och om det uppnår det som det är tänkt att stödja. Granskning tar även vara på en av de viktigaste aspekterna i ett väl fungerande informationssäkerhetsarbete; en god säkerhetskultur, något som inte berörts i tidigare granskningar.

En effektiv och säker användning av information är en förutsättning för regionens verksamhet och för förtroendet för förmågan att leverera service till medborgarna, detta gäller även vid en samhällskris. Informationshanteringen i samhällsviktiga funktioner inom vård och omsorg ska kunna upprätthållas även i krisläge.

Under 2015 granskades krisberedskapen i regionen där en ny systematiska säkerhetsorganisation just tagits i bruk. Vid granskningen pågick ett arbete med risk- och sårbarhetsanalys. Färdigställdes denna och ligger den till grund för arbetet med informationssäkerhet i regionen? För att ytterligare bygga på krisberedskapsgranskningen kommer denna

granskning undersöka om regionen arbetar med informationssäkerhet som en integrerad del av regionens krisberedskap. Revisorerna har med utgångspunkt i väsentlighet och risk beslutat att granska regionens informationssäkerhet.

1.2. *Syfte och Revisionsfråga*

Granskningen har inneburit att inom ramen för revisionsarbetet inom Region Västmanland genomföra en övergripande granskning av informationssäkerhet för att analysera huruvida verksamheten på en övergripande nivå har ändamålsenliga arbete med informationssäkerhet. Granskningen har översiktligt fokuserat på styrning och ledning av informationssäkerhet, uppföljning, säkerhetskultur, informationssäkerhetsincidenter, krisberedskap och informationsklassning. Syftet med granskningen är att klargöra vilka områden som Region Västmanland behöver arbeta vidare med och utveckla för att uppnå ett ändamålsenliga arbete för att hantera informationssäkerhet på ett lämpligt sätt.

Revisionsfrågan som har legat till grund för granskningen lyder:

- Har regionstyrelsen på övergripande nivå ett ändamålsenligt arbete med informationssäkerhet?

1.3. *Revisionskriterier*

- Offentlighets- och sekretesslag (2009:400)
- Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om landstings och kommuners risk- och sårbarhetsanalyser (MSBFS 2015:4 & 2015:5).
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)
- Patientdatalag (2008:355)
- Säkerhetsskyddslag (1996:627)
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
- Regionens regler, policys och riktlinjer motsvarande informationssäkerhet
- MSB Strategi för stärkt informationssäkerhet inom vård och omsorg

1.4. Kontrollmål

- Regionen har aktuella och ändamålsenliga styrande dokument och riktlinjer
- De styrande dokumenten och riktlinjerna är implementerade i verksamheten
- Regionens ledningssystem för informationssäkerhet är implementerat och fungerar ändamålsenligt
- Regionen arbetar ändamålsenligt med uppföljning kring efterlevnad av informationssäkerhet.
- Det finns en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet.
- Regionen arbetar aktivt för att främja en god säkerhetskultur inom informationssäkerhetsområdet.
- Regionen har förmåga att hantera informationssäkerhetsincidenter
- Informationstillgångar som kan vara kritisk för rikets säkerhet och omfattas av reglerna i Säkerhetsskyddslagen är identifierade och omhändertagna
- Regionen arbetar systematiskt med informationssäkerhet ur ett krisberedskapsperspektiv
- Det finns en implementerad modell för informationsklassning

1.5. Avgränsning

Granskningen betonar regionens övergripande informationssäkerhetsarbete under regionstyrelsen. Granskningen kommer att beröra men i mindre utsträckning beakta övriga nämnders och förvaltningars informationssäkerhet.

1.6. Metod

Arbetet har genomförts genom granskning av relevant dokumentation som reglementen, planer, policy, riskanalyser. Se bilaga 1 för specifikation.

Intervjuer har inom ramen för granskningen genomförts med:

- Administrativ direktör
- Informationssäkerhetssamordnare
- IT- direktör
- IT- chef
- RSA- handläggare

2. Iakttagelser och bedömningar

2.1. Styrande dokumentation och riktlinjer

Kontrollmål: Regionen har aktuella och ändamålsenliga styrande dokument och riktlinjer.

Regionen har tagit fram flertalet styrdokument, se specifikation enligt bilaga 1. Det framgår att samtliga riktlinjer är giltiga samt att dokumentationen är utfärdade och godkända. Dokumentationen utgörs av åtta riktlinjer, en verksamhetsplan, en kravspecifikation för inköp (ej fastställd), normskala vid informationsklassning samt tre dokument som beskriver incidenter. Det framgår inte hur prioriteringen gjorts för att skapa just dessa dokument. Flera av riktlinjerna har skapats efter definition i verksamhetsplanen för informationssäkerhet.

I regionens verksamhetsplan för informationssäkerhetsarbetet 2016 (giltig från och med 2015-10-23) utgår regionen från informationssäkerhetspolicyn för Landstinget Västmanland. Utgångspunkten i policyn är att arbeta systematiskt med riskanalyser och förbättringsarbete i frågor gällande informationssäkerhet. I verksamhetsplanen beskrivs framtagande av metod och riktlinjer kring riskanalyser, informationsklassning, incidenthantering och behörighetshantering.

I Region Västmanlands informationspolicy (giltig från 2014-09-24) beskrivs tio principer som ska styra regionens arbete med informationssäkerhet. Av de tio principer som nämns i informationspolicy har fem implementerats i riktlinjer. Dessa är riktlinjerna för riskanalys, informationsklassning, medarbetarinformation, drift och förvaltning av IT-miljö och krav på spårbarhet, dock endast för patientuppgifter. Enligt inriktning i informationssäkerhetpolicyn ska regionen följa SS-ISO/IEC 27001. De fjorton åtgärdsmål som specificerats i ISO 27001 har inte systematiskt omsatts i riktlinjer.

I granskningen har fem riktlinjer ingått, som redovisas kortfattat härnäst. Regionen har en riktlinje för riskanalys som anger omfattningen och principer för med vilken frekvens dessa ska genomföras. I granskningen har dokumentation på genomförda riskanalyser presenterats.

Riktlinjen för loggranskning avser åtkomst till patienters journalhandlingar med refereringar till instruktioner och blanketter Därtill är ansvar och befogenheter angivet för loggranskningar. Även i riktlinjen för IT- säkerhet i drift och förvaltning omnämns granskning av loggar, men däremot inte ansvarige för granskning och dokumentation av rutinerna. I den sistnämnda riktlinjen definieras mål, omfattning, ansvar och roller på ett tydligt sätt och riktlinjen bedöms vara omfattande. Däremot framgår inte syftet med urvalet av delrubriker och var dessa är hämtade ifrån.

Regionen har en riktlinje gällande åtkomst till patientuppgifter, som beskriver när åtkomst är tillåten respektive förbjuden. Det är en begränsning att endast åtkomst till patientuppgifter redogörs och att det inte finns en riktlinje för annan typ av åtkomst till information i regionen. I riktlinjen för utlämnande av journalhandlingar beskrivs utifrån flertalet aspekter när journalhandlingar får lämnas ut och även när detta inte får göras, vilket belyser problemet att göra klara gränsdragningar. I regionens riktlinje gällande sekretess och tystnadsplikt beskrivs grundprinciperna för offentlighet och sekretess. Det framgår inte om regionens har utfärdat instruktioner med anledning av denna riktlinje.

I riktlinje informationsklassning beskrivs principerna för informationsklassningsgenomförandet, men däremot framgår det inte vem som ansvarar för verkställandet av en informationsklassning. Detta framgår däremot i dokumentet "Region Västmanlands Organisation för systematiskt säkerhetsarbete" som specificerar att Riskrådet är beslutande vid initierande av analyser.

Samtliga riktlinjerna utom de som reglerar hanteringen av sekretess har förankring i informationssäkerhetspolicyn. De riktlinjer som gäller hantering av sekretess har istället sitt ursprung i svensk lagstiftning och inte i ledningssystem för informationssäkerhet.

2.1.1. Vår bedömning

Samtlig dokumentation är aktuell och giltig. Sammantaget har hälften av principerna beskrivna i informationssäkerhetspolicyn täckning i riktlinjer. Att det endast finns en riktlinje för åtkomst till patientuppgifter och inte en för annan information bedöms vara en begränsning för regionen. De fjorton åtgärdsmål som specificeras i ISO 27001 har inte tillämpats. Innehållet i riktlinje informationssäkerhet för medarbetare är högst relevant. Eftersom dess innehåll är konkret och tydligt bör denna snarare rubriceras som en instruktion än riktlinje. Kontrollmålet bedöms därmed vara delvis uppfyllt.

2.2. Implementation av styrande dokument och riktlinjer

Kontrollmål: De styrande dokumenten och riktlinjerna är implementerade i verksamheten.

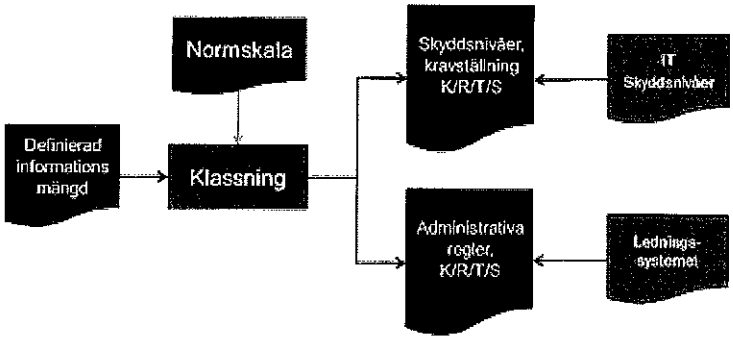
Regionen har sett till att implementera metoder för riskanalys och informationsklassning.

De senaste genomförda riskanalyserna med koppling till informationssäkerhet vars dokument som granskningen har utgått ifrån är följande:

- Ambulansdirigering
- Endobase
- IdP Autentiseringstjänst
- IT-systemet Privera

I verksamhetsplanen för 2016-2018 framkom ambitionen att införa riskanalyser som en naturlig del i verksamheternas informationshantering. Baserat på erhållna dokument samt förteckningen på genomförda riskanalyser under de senaste åren bedöms regionen arbeta aktivt för att nå denna ambition. I intervjusvar uppmärksammas det att regionen för tillfället genomför fler riskanalyser med anledning av att GDPR snart träder i kraft. Däremot framhölls en osäkerhet kring uppföljning och säkerhetsställande av dessa riskanalyser samt om de i själva verket implementerats. I granskningen har det inte framkommit några dokumenterade riktlinjer på implementering av informationsklassning.

Under granskningen tillhandahölls regionens genomförda informationsklassning över IT-komponenter samt en instruktion för normskala vid informationsklassning. För utförligare beskrivning av informationsklassning återges i avsnitt 2.10 Modell för informationsklassning.



Figur 1

Regionens riktlinjer är antagna och dokumenten är fullständiga, då samtliga riktlinjer har datum, utfärdare och godkännande.

Utöver regionens risk- och sårbarhetsanalys och informationsklassning är det inte dokumenterat att övriga dokument har implementerats. Regionen upplevs arbeta aktivt med att implementera dokument genom exempelvis att utbilda personal ute i verksamheten. Det har även tagits fram utbildningar och därtill planeras även framtagandet av nya utbildningar. Detta beskrivs närmare i avsnitt 2.6 Säkerhetskultur. Enligt "Verksamhetsplanen informationssäkerhet 2016-2018" skulle regionen ta fram en särskild utbildningsinsats med uppföljning under 2016. Dokumentation för att styrka denna uppföljning har inte tillhandahållits under denna granskning.

I intervjusvar framkom önskan om att ha informationssäkerhetsombud ute i verksamheten. Detta för att möjliggöra en högre efterlevnadsgrad av styrande dokument, då det upplevs att tid och engagemang är bristfälligt gällande frågor kopplade till informationssäkerhet. Det framkom även i intervjusvar att det har upplevts som att IT och informationssäkerhet har arbetat på varsina håll, vilket resulterat i ett glapp i informationskedjan.

2.2.1. *Vår bedömning*

I granskningen har det blivit tydligt att regionen inte har dokumenterat implementationen av regionens dokument utöver risk- och sårbarhetsanalys och informationsklassningen. Därtill har det inte framkommit några dokumenterade riktlinjer på implementering av informationsklassning. På dessa grunder bedöms Region Västmanlands delvis uppfylla kontrollmålet för implementering av styrande dokument och riktlinjer.

2.3. *Ledningssystem för informationssäkerhet*

Kontrollmål: Regionens ledningssystem för informationssäkerhet är implementerat och fungerar ändamålsenligt

I 2018 års verksamhetsplan för informationssäkerhet för Region Västmanland är målsättningen att regionen ska vara certifieringsbar enligt SS-ISO/IEC 27001:2014. I verksamhetsplanen framgår det att det ska tas fram metoder och riktlinjer med ett fokus på följande aktiviteter:

- Framtagande av metod och riktlinjer kring riskanalyser
- Framtagande av metod och riktlinjer kring informationsklassning
- Behörighetshantering
- Framtagande av metod och riktlinjer kring incidenthantering
- Informationssäkerhet i upphandling

Regionens arbete med implementeringen av ett ledningssystem för informationssäkerhet grundar sig i utfärdandet av framtagna dokument som policy och riktlinjer, där det uttalats att regionen ska bedriva ett systematiskt arbete med informationssäkerhet och att dessa ska bygga på riskanalyser och ständiga förbättringar. Styrning av säkerhetsarbetet ska därmed leda till att informationsklassningar görs och att rätt skyddsåtgärder vidtas. I riktlinjen dokumentkategorier och regler för dokumentstyrning finns det en förteckning över vilka styrande och redovisande dokumentation som organisationen har fastställt och som är nödvändiga för att säkerställa att processer planeras, genomförs och styrs på ett verkningsfullt sätt.

I enlighet med intervjusvar ska ett ledningssystem finnas men det är ännu inte certifierat. Ambitionen tycks inte vara att bli certifierade utan endast att uppnå en nivå av certifieringsbarhet.

I verksamhetsplanen för systematiskt säkerhetsarbete sammanträder ledningen minst en gång per år. Det har tillhandahållits dokumentation kring ledningens genomgång 2016 i "Sakområdets/verksamhetens underlag för ledningens genomgång – Sak/verksamhetsområde: Informationssäkerhet" och minnesanteckningar från kommitté samt råd. I verksamhetsplanen saknas det en tidsplan för implementering samt tillräcklig mängd åtgärder för att införa ett informationssäkerhetsarbete i enlighet med ISO 27001 de närmsta åren. Se avsnitt 2.4 Uppföljning.

2.3.1. *Vår bedömning*

Utifrån insamlat material framgår inte att en informationssäkerhetsmetodik systematiskt använts i verksamheten med undantag för risk- och sårbarhetsanalysen, incidentanalys, informationsklassning och loggning av patientjournaler. Därmed bedöms regionen delvis uppfylla kontrollmålet.

2.4. *Uppföljning*

Kontrollmål: Regionen arbetar ändamålsenligt med uppföljning kring efterlevnad av informationssäkerhet.

Efter fortsatt granskning utav Region Västmanlands arbete med uppföljning kring efterlevnad av informationssäkerhet har det kunnat styrkas att regionen arbetar aktivt med att ta fram riktlinjer för att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Detta har gjorts genom uppföljning av tidigare genomförda riskanalyser och informationsklassningar.

Ur riktlinjen gällande informationsklassning står det att: "Ansvaret för att ta fram och regelbundet uppdatera skyddsnivåer ligger hos Centrum för IT. Skyddsnivåerna ska också användas i avtal med utomstående leverantörer av system/tjänster och IT-drift". I informationssäkerhetspolicyn framkommer det att uppföljning ska ske på ett regelbundet och strukturerat sätt samt utföras genom interna kontroller och revisioner av oberoende part. Senaste tillfälle vid antagande var 2014. I riktlinjen loggranskning har Region Västmanland höga krav på sig enligt Patientdatalagen. Detta då regionen enligt lagen ska göra systematiska och återkommande kontroller om någon obehörig öppnat en patientjournal. Den ansvariga för att loggranskning utförs är verksamhetschefen. Loggkontrollen är en del av den interna kontrollen, se dokumentet "Rapport över uppföljning av internkontroll 2017". I dokumentet anges det att regionen årligen ska upprätta en särskild plan för granskning/uppföljning av den interna kontrollen. Logguppföljning sker systematiskt och resultatet från uppföljningen rapporteras sedan till regionstyrelsen. Under granskningen har inga statusrapporter gällande loggranskningen tillhandahållits.

I enlighet med intervjusvar finns det förvaltningsplaner som innehåller säkerhetsfrågor. I förvaltningsplanen läggs det in vilka riktlinjer, dokumentation eller arbetssätt som måste kontrolleras och följas upp. Allt eftersom efterlevnaden kontrolleras, stämmer den ansvarige av att det har gjorts.

På IT-sidan har det genomförts oberoende granskningar, både från PwCs sida men även internt då man valt att genomföra IT-penetrationstester. Tester genomförs löpande och finns med i verksamhetsplanen för 2018. Det har även skickats ut phishing-mail till anställda med en länk i syfte att öka medvetenheten. Det finns dock ingen processbeskrivning över detta i nuläget. Resultatet för uppföljning och efterlevnad delges sedan till ledningen.

2.4.1. *Vår bedömning*

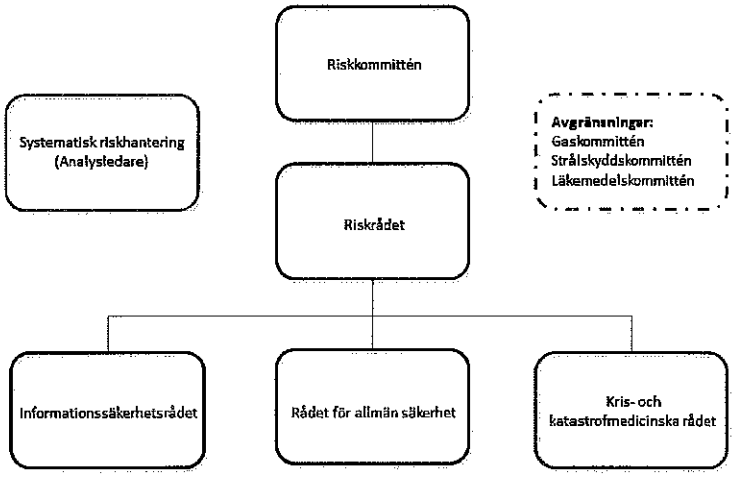
Regionen har genomfört ett antal åtgärder för att stärka uppföljningen, så som definition av roller och ansvar samt genomfört phising-kampanjer. Därtill har penetrationstester genomförts, men det finns ingen processbeskrivning. I enlighet med intervjusvar rapporteras efterlevnad till ledningen. Enligt regionens ledningssystem ska råden göra uppföljning av genomförda analyser samt föreslå områden för uppföljning och prioritering av åtgärder inför ledningens årliga genomgång. Någon dokumentation som styrker genomförandet har inte erhållits. Detta ligger till grunden för att regionen bedöms uppfylla kontrollmålet delvis.

2.5. *Organisation, roller och ansvar*

Kontrollmål: Det finns en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet

I Region Västmanlands organisation för systematiskt säkerhetsarbete (29043-2) beskrivs organisationens struktur och rollfördelning samt respektive ansvarsområden på ett tydligt sätt i enlighet med kapitel 6 ISO 27001. Därtill beskrivs även arbetsordningen och målet för säkerhetsorganisationen. Det systematiska säkerhetsarbetet är organiserat enligt figuren nedan. Det framgår även i intervjusvar att organisationen upplevs ha tydliga roller med tillhörande ansvarsområden.

Det framgår i informationssäkerhetspolicyn att regionsfullmäktiga har det yttersta ansvaret för regionens informationssäkerhetsarbete, vilket bland annat innebär beslutande av policyn och övergripande inriktning för arbetet.



Figur 2. Organisationsstruktur

Riskkommittén har det strategiska och för de områden som organiseras under kommittén. Det innebär att kommittén är ett beslutande organ gällande förlag om åtgärder, planer och policys samt finansieringsprinciper. Ordförande för kommittén är regiondirektören. I bilaga 1 redogörs representanter i kommittén. Riskkommitténs beredande organ är

Riskrådet. Denna har även beslutanderätt i vissa frågor, så som vid initierandet av analyser. Riskrådet främsta uppgift är att vara ett forum för Informationssäkerhetsrådet, Rådet för allmän säkerhet och Kris- och katastrofmedicinska rådet samt analysledare. Riskrådet ska ta emot förslag, initiera utredningar, utvärdera och ge uppdragsdirektiv. I bilaga 2 framgår representanter samt behandlade ärenden i Riskrådet.

Under Riskrådet ligger Informationssäkerhetsrådet, Rådet för allmän säkerhet och Kris- och katastrofmedicinska rådet. Det förstnämnda är ansvarig för regionens informationssäkerhet med hänsyn tagen till kraven på konfidentialitet, riktighet, tillgänglighet och spårbarhet. Informationssäkerhetsrådets arbete utgår ifrån regionens informationssäkerhetspolicy och riktlinjer i ledningssystemet. Enligt Informationssäkerhetssamordnaden finns det verksamhetsrepresentanter i rådet. Övriga representanterna i Informationssäkerhetsrådet framgår i bilaga 3.

Regionens intresse i säkerhets- och trygghetsfrågor bevakas av Rådet för allmän säkerhet. Rådet följer även upp statistik i dessa frågor, initierar frågor inom säkerhetsområdet, lägger fram förslag och/eller bereder frågor som sedan tas upp för diskussion i Riskrådet. Representanterna är listade i bilaga 4.

Kris- och katastrofmedicinska rådet är ansvariga för upprättande av en god katastrofmedicinsk beredskap vid en allvarlig händelse. Rådet är även ett utbildningsråd som planerar och upprättar en utbildning och övningsplan. Likt övriga råd lägger Kris- och katastrofmedicinska rådet fram förslag och/eller bereder frågor till Riskrådet och Riskkommittén. I bilaga 5 finns förteckningen över representanterna i Kris- och katastrofmedicinska rådet.

Arbetet inom regionen med risk och kontinuitetshantering sker inom ramen för den systematiska riskhanteringen. Detta gäller regionens alla verksamheter då syftet är att samordna detta inom rammen för det systematiska säkerhetsarbetet. Detta innebär bland annat att upprätthålla en lägesbild, säkerställa kontinuitets- och riskhanteringsarbetet samt uppdatera och leverera processer för kontinuitets-/riskhantering.

2.5.1. Vår bedömning

Sammanfattningsvis bedöms organisationen för styrning och ledning vara väldefinierad men det framgår inte tydligt ansvar för genomförande av säkerhetsåtgärder. Med detta som bakgrund bedöms regionen delvis uppfylla kontrollmål gällande en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet.

2.6. Säkerhetskultur

Kontrollmål: Regionen arbetar aktivt för att främja en god säkerhetskultur inom informationssäkerhetsområdet.

I riktlinjerna för säkerhetsorganisationen ska regionen skapa en struktur och god kultur som stödjer styrning och uppföljning av regionens systematiska säkerhetsarbete. I intervjusvar framkommer att regionen arbetar med att främja en god säkerhetskultur genom bland annat. att informera personal i frågor rörande informationssäkerhet via intranätet och arbetsplatsträffar (ATP). Därtill används intranätet för att publicera informationssä-

kerhetssamordnarens bloggtexter vars syfte är att nå ut till personalen gällande aktuella frågor inom informationssäkerhet.

Utbildning av personalen inom informationssäkerhet sker via en obligatorisk EU- kurs. Beslut om kursen finns dokumenterat i minnesanteckningar från Riskrådet, (2017-11-30). Regionen arbetar med att ta fram flera utbildningar gällande informationssäkerhet med ambitionen att även dessa ska vara obligatoriska. I intervjusvar framkommer det att regionen skickar ut phising- mejl för att öka medvetenheten bland personalen.

I dokumentet "Region Västmanlands organisation för systematiskt säkerhetsarbete" specificeras att råden ska ta fram utbildnings- och övningsplaner utifrån inventering av utbildningsbehov avseende fortbildning och kompetensutveckling inom området.

För att bibehålla patientsekretessen, som är en del av en god säkerhetskultur, finns det inom regionen ett logguppföljningssystem. Detta specificeras i avsnitt 2.4 Uppföljning.

2.6.1. Vår bedömning

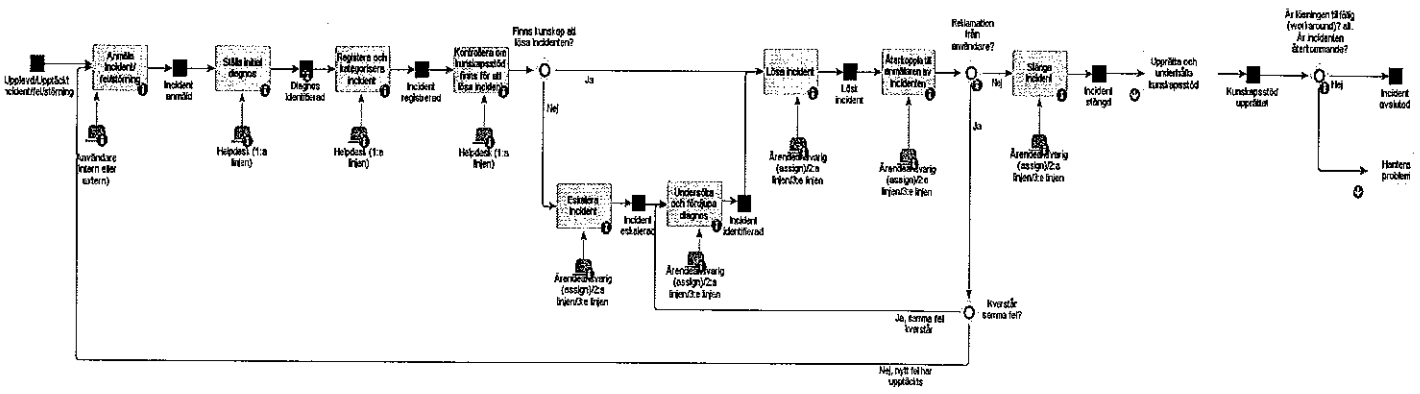
Främjandet av en god säkerhetskultur specificerades i intervjusvar, men det är inte dokumenterat i en systematisk genomförandeplan. Aktiviteterna är inte heller specificerade eller dokumenterade i verksamhetsplanen för 2018. Därmed bedöms regionen delvis uppfylla kontrollmålet gällande att aktivt arbeta för att främja en god säkerhetskultur inom informationssäkerhetsområdet.

2.7. Informationssäkerhetsincidenter

Kontrollmål: Regionen har förmåga att hantera informationssäkerhetsincidenter.

I verksamhetsplanen för informationssäkerhet framgår att målsättningen för Region Västmanland är att ta fram en metod och riktlinjer för att kunna nå målet om ett konsekvent och effektivt tillvägagångssätt för incidenthantering. För att nå detta krävs framtagande av rutiner och riktlinjer som kan anpassas till befintliga lösningar för rapportering av avvikelser och incidenter.

Dokumentation för incidentrapportering samt åtgärdsförslag har tillhandahållits och informationssäkerhetsincidenter registreras och följs upp likt andra incidenter. I enlighet med intervjusvar finns det en process för incidentrapportering. Användare vet att rapportering av incidenter ska ske via Helpdesk, därefter bedömer Helpdesk själva vad felet kan bero på. En del incidenter kan hanteras direkt av Helpdesk men det kan även resultera i att incidenthanteringen delegeras till en tillgänglig chef.



Figur 3. Process för incidenthantering

Statistik över incidenter förs löpande och taggas utifrån vilket objekt som berörs. Det finns en tagg för informationssäkerhet/IT. En incident ska sedan enligt plan hanteras inom tre arbetsdagar och uppföljning ska ske löpande. I enlighet med intervjusvar sker veckovisa uppföljningar av rapporterade incidenter, både avslutade och kvarvarande incidenter.

2.7.1. Vår bedömning

Det framkommer statistisk som påvisar att regionen aktivt arbetar med incidenthantering. För att minska risken för framtida incidenter beskrivs i respektive statusrapport för en inträffad incident vad som kan göras annorlunda nästa gång en liknande incident inträffar samt vilka åtgärder som vidtagits för att det inte ska inträffa igen. Det framgår inte i dokumentation om dessa incidentrapporter följs upp. Inte heller framgår det i styrdokument kriterierna för när en incident kan klassas som "större incident" samt hur denna ska hanteras En instruktion benämnd "Rutin vid allvarlig händelse" har tillhandahållits, dock finns inga kriterier för när den ska tillämpas. Detta föranleder till att Region Västmanland bedöms uppfylla kontrollmålet delvis.

2.8. Kritiska informationstillgångar för rikets säkerhet

Kontrollmål: Informationstillgångar som kan vara kritisk för rikets säkerhet och omfattas av reglerna i Säkerhetsskyddslagen är identifierade och omhändertagna.

Frågan om kritiska informationstillgångar för rikets säkerhet har analyserats av Region Västmanland och enligt det senaste mötesprotokollet för Riskkommittén (2017-12-13) bedömdes det att regionen inte hanterar sådana tillgångar. I protokollet redogörs inte med vilken metodik som denna bedömning grundar sig i. I intervjusvar framgår det att regionen kommer att se över detta beslut, men inte när.

2.8.1. Vår bedömning

Värdering av om det finns informationstillgångar för rikets säkerhet bör vara en del av informationsklassningen vilket inte är fallet idag. Då denna granskning inte har fördjupat sig i huruvida säkerhetsskyddslagen följs samt på grund av den påbörjade nationella totalförsvarsplaneringen bör en djupare analys av informationstillgångar för rikets säkerhet genomföras. Likväl framgår det i granskningen att regionen har genomfört en analys, vilket föranleder att kontrollmålet bedöms vara uppfyllt.

2.9. *Krisberedskap och informationssäkerhet*

Kontrollmål: Regionen arbetar systematiskt med informationssäkerhet ur ett krisberedskapsperspektiv.

I risk- och sårbarhetsanalysen framkommer att informationssäkerhetsområdet kopplat till krisberedskap och kontinuitetshantering är på ett initieringsstadium och att fortsatt arbete krävs. Informationssäkerhetsområdet i form av kritiska beroenden av känslig informationshantering nämns inte heller i verksamhetsplanen för 2016. Inte heller i Region Västmanlands krisberedskapsplan framgår någonting om informationssäkerhet.

2.9.1. Vår bedömning

I Region Västmanlands dokument "Indikatorer för bedömning av Landstingets generella krisberedskap (MSBFS 2015:4)" finns frågan om att regionen har rutiner för att identifiera och hantera kritiska beroenden till system och tjänster för informationshantering som är av central betydelse för regionens verksamhet. I dokumentet besvaras frågan med att regionen har som avsikt att införa detta i samband med kontinuitetshantering under 2016. I verksamhetsplanen 2016 framgår det ingenting om uppfyllelse av detta. Region Västmanland bedöms inte arbeta systematiskt med informationssäkerhet utifrån ett krisberedskapsperspektiv, vilket ger anledning till att kontrollmålet inte bedöms vara uppfyllt

2.10. *Modell för informationsklassning*

Kontrollmål: Det finns en implementerad modell för informationsklassning

Regionen har tagit fram en instruktion för informationsklassning "Normskala vid informationsklassning" (2017-10-11). Instruktionen används vid all informationsklassning som genomförs utifrån tre konsekvensnivåer; lindriga, allvarliga och mycket allvarliga konsekvenser. Konsekvenserna bedöms utifrån konfidentialitet, tillgänglighet, riktighet och spårbarhet. Därtill bedöms de även utifrån sex olika konsekvensområden. Syftet med dokumentet är att uppnå en likvärdig informationsklassning för hela regionen oavsett utförare och information.

2.10.1. Vår bedömning

Under granskningen har dokumentet "Informationsklassning av IT-komponenter" tillhandahållits där 298 komponenter har klassats. Av namnen att döma är det snarare IT-system än komponenter. I enlighet med intervjusvar har de 500 viktigaste datasystem informationsklassats. Detta ses som ett tecken på att modellen är implementerad och att regionen uppfyller kontrollmålet för informationsklassning.

Bilagor

Bilaga 1. Dokumentation som ingått i granskningen:

- Verksamhetsplan – Region Västmanlands systematiska säkerhetsorganisation (2017-11-23, utfärdat Michael Patricksson, Hans Löhman, Lena Lundgren, Birgitta Rasmussen)
- Kravspecifikation inköp (skapad av Cecilia Lundin Mellström)
- Informationssäkerhetspolicy (giltig från 2014-09-24, utfärdat Michael Patriksson, godkänd Marianne Bergendal)
- Riktlinje för riskanalys informationssäkerhet (giltig från 2017-08-28, utfärdat Michael Patricksson, godkänd Jan Hallberg)
- Riktlinje loggranskning (giltig från 2017-03-28, utfärdat Michael Patricksson, informationssäkerhetssamordnare, godkänd Jan Hallberg, administrativ direktör)
- Riktlinje åtkomst till patientuppgifter i journal (giltig från 2016-02-08, utfärdat Michael Patricksson, godkänd Jan Hallberg; Fastställd av Landstingsstyrelsen 2015-01-28)
- Riktlinje för informationsklassning (giltig från 2017-08-28, utfärdat Michael Patricksson, godkänd Jan Hallberg)
- Riktlinjer informationssäkerhet för medarbetare (giltig från 2016-12-05, utfärdat Michael Patricksson, godkänd Anders Åhlund, regiondirektör)
- Riktlinjer för IT-säkerhet i drift och förvaltning (giltig från 2015-11-13, utfärdat Michael Patricksson, godkänd Lars Öhman, IT direktör)
- Riktlinje utlämnande av journalhandlingar, kopplar mkt till PUL (giltig från 2016-03-15, utfärdat Åsa Ternström, landstingsjurist, godkänd Jan Hallberg)
- Riktlinje sekretess och tystnadsplikt, kopplar lite till PUL, offentlighets- och sekretesslagen (giltig från 2017-08-29, utfärdat Åsa Ternström, landstingsjurist, godkänd Jan Hallberg)
- Normskala vid informationsklassning (giltig från 2017-10-11, utfärdat Michael Patriksson, godkänd Jan Hallberg)
- Bilaga 1 - Incidentrapport - Nätverksstörningar 1.1
- Bilaga 2 - Incidentrapport_cosmic_ver2
- Bilaga 3 - Åtgärdsförslag händelseanalys nätverk och cosmicavbrott

Bilaga 2. Lista på representanter i Riskkomittén

- Regiondirektör (ordförande)
- Administrativ direktör (föredragande)
- IT-direktör
- Hälso-och sjukvårdsdirektör
- Kommunikationsdirektör
- Förvaltningsdirektör VS/bitr. förvaltningsdirektör
- Förvaltningsdirektör PPHV
- Förvaltningsdirektör Verksamhets och ledningsstöd
- Smittskyddsläkare
- Riskkommittén är ett beslutande organ som exempelvis kan besluta om förslag till åtgärder, planer och policys samt finansieringsprinciper för att genomföra beslutade åtgärder.

Bilaga 3. Lista på representanter i Riskrådet

- Administrativ direktör (ordförande)
- Ordförande i Informationssäkerhetsrådet
- Ordförande i Rådet för allmän säkerhet
- Ordförande i Kris- och katastrofmedicinska rådet
- Representant VS
- Representant PPHV
- Representant CIT
- Representant Kollektivtrafikförvaltningen
- Representant Fastighet
- Representant Centrum för Kommunikation
- Driftchef - regionservice
- Risksamordnare motsvarande
- Representant från patientsäkerhetsteamet

Bilaga 4. Lista på representanter i Informationssäkerhetsrådet

- Representanter ska utgöras av funktionerna:
- Informationssäkerhetssamordnare (ordförande)
- Regionsjurist
- IT-säkerhetsansvarig CIT
- Representant CIT
- Två representanter från systemförvaltningsorganisationen, en från objektfamiljen Hälso- och sjukvård och en från objektfamiljen Administrativt stöd
- Representant VS
- Representant PPHV

Bilaga 5. Lista på representanter i Råder för allmän säkerhet

- Säkerhetssamordnare VS
- Säkerhetssamordnare Primärvården
- Säkerhetssamordnare Psykiatrin
- Säkerhetssamordnare Rättspsykiatrin
- Säkerhetssamordnare Kollektivtrafiken
- Säkerhetssamordnare Länsmuseet
- Säkerhetssamordnare VLS
- Brandskyddsingenjör Fastighet

Bilaga 6. Lista på representanter i Kris- och Katastrofmedicinska rådet

- Katastrof- och beredskapsplanläggare (ordförande)
- Medicinskt ansvarig inom CBRNE
- Tre representanter från Akutkliniken
- Representant från kirurgen
- Representant operationskliniken
- PKL-samordnare
- RSA-ansvarig
- En eller två representanter för PPHV
- Beredskapshandläggare

2018-03-02		2018-03-02
Tobias Bjöörn		***Martin Bernhardtz***
Uppdragsledare		*Projektledare*