www.pwc.se

Revisionsrapport

Granskning av IT-säkerhet och informationssäkerhet

Region Skåne

Projektledare:
Magnus Karmborg
Mats Malmberg

Maj 2017

pwc

Innehåll

Sammanfattning

- **Kort om bakgrund**

Revisorerna i Region Skåne har gett PwC i uppdrag att granska hur Region Skåne arbetar med IT- och informationssäkerhet.

Det övergripande syftet med informationssäkerhet är att säkerställa att information hanteras med utgångspunkt i sekretess, integritet och tillgänglighet till information för medarbetare och intressenter till Region Skåne. IT-säkerhet ligger till grund för att, där det är möjligt, tillhandahålla ändamålsenliga tekniska kontroller för att möjliggöra hantering av krav på informationssäkerheten.

Region Skåne är beroende av fungerande IT-system för att kunna bedriva verksamheten med hög patientsäkerhet, med god effektivitet och hög servicenivå mot medborgarna. Den förväntade utvecklingen av nya e-tjänster inom vården kommer att ytterligare öka detta beroende av säkra IT-system.

Region Skåne arbetar idag med digitalisering och teknologi för att optimera och effektivisera interna rutiner och arbetssätt, men även för att öppna upp tjänster för medborgare. Med den ökade graden av digitalisering tillkommer även andra typer av risker att beakta i hanteringen av den information som hanteras och lagras. Digitala e-tjänster medför att verksamheter öppnar upp och exponerar sin interna IT-miljö, och information där i, mot det publika Internet.

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda nyckelpersoner för olika verksamhetsområden kopplat till IT- och informationssäkerhet samt granskat styrande dokument för området.

- **Revisionell bedömning**

Uppdragets revisionsfråga är:

Har Region Skåne på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet?

Vår bedömning är att Region Skåne inte har ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet. De bedömningar som vi lämnar för kontrollmål 1-11 visar att det inte finns en fungerande styrmodell implementerad, inte heller tillräcklig omfattning av resurser, styrande dokument och rutiner till grund för att säkerställa ändamålsenlig hantering av informationstillgångar inom Region Skåne.

Vår uppfattning är att en del brister som vi noterat i samband med den utförda granskningen är kända av Region Skåne och att flertalet initiativ har påbörjats för att hantera dessa. Region Skåne arbetar med att upprätta och komplettera nuvarande struktur för styrande dokument inom informationssäkerhet. Vi har noterat att det även pågår en process för att omorganisera området för IT.

Utifrån genomförd granskning har vi redogjort för rekommenderade aktiviteter till grund för att hantera de brister vi identifierat för respektive kontrollfråga.

- **Bedömning av kontrollmålen som ligger till grund för svaret på revisionsfrågan**

De noterade bristerna är primärt relaterade till följande områden:

- *Styrande dokument:* Det saknas en övergripande struktur som beskriver relationen mellan olika styrande dokument. Vidare har vi noterat att det saknas väsentliga styrdokument inom IT- och informationssäkerhet. Som exempel kan nämnas instruktion för informationsklassificering, vilket utgör en väsentlig komponent i en effektiv styrning av det granskade området.

- *Definitioner av incidenter:* Processen för incidenthantering saknar en tillräckligt specifik definition av IT-säkerhets- och informationssäkerhetsrelaterade incidenter, vilket leder till svårighet att följa upp incidenter och säkerställa att kontrollmiljön är relevant utifrån aktuella risker och brister.

- *Organisation, roll och ansvarsfördelning:* Organisation, roller och ansvar kopplat till IT- och informationssäkerhetsområdet är inte tydligt definierade. De roller som vi identifierat för område IT- och informationssäkerhet förefaller även vara underdimensionerade beaktat Region Skånes storlek på verksamhet och den typ av informationstillgångar som hanteras i verksamheten. Kommunikationsvägar och mötesstrukturer internt inom Region Skåne och mot externa leverantörer är inte tydligt definierade.

- *Rutiner och arbetssätt:* Vi har noterat att det saknas dokumenterade rutiner för väsentliga processer såsom till exempel inventering och kartläggning av information till grund för informationsklassificering samt för genomförande av riskanalyser med viss periodicitet.

- *Uppföljning och utvärdering av kontroller och process för kontinuerlig förbättring:* Det saknas relevanta och tydligt definierade nyckeltal för styrning och uppföljning av området med syfte att säkerställa god IT- och informationssäkerhet samt kontinuerlig förbättring av kontrollmiljön, internt men även hos externa leverantörer. Vidare noterar vi att övervakningen av området för IT- och informationssäkerhet i dagsläget är i grunden mer reaktiv än proaktiv.

Vi har i rapporten valt att beskriva vårt arbete och iakttagelser för respektive kontrollfråga. Då kontrollfrågorna vid vissa tillfällen har beröringspunkter, kan effekten bli att viss upprepning är ofrånkomlig.

Rekommendationer

- Region Skåne rekommenderas att utvärdera behovet av att upprätta en särskild budget för respektive område för IT-säkerhet och informationssäkerhet med budgetansvar hos respektive ansvarig. I samband med budgetarbetet bör även en utvärdering av behovet av antalet resurser inom respektive område utföras.

- Region Skåne rekommenderas att inventera styrande dokument för området, identifiera och upprätta de dokument som saknas, såsom riktlinjer för rutin för riskanalys och informationsklassificering. Etablera en överskådlig modell över dokumentstrukturen, som tydliggör logisk tillhörighet och samband mellan dokument.

- Region Skåne rekommenderas att definiera och dokumentera organisation, roller och ansvar för området ner på verksamhetsnivå. Definiera struktur för möte och kommunikationsvägar för området, både internt inom Region Skåne men också för kommunikation med leverantörer. Ansvar för kontroller för efterlevnad bör förankras i definierade roller för området.

- Region Skåne rekommenderas att implementera rutiner för riskanalys och informationsklassificering samt kontroller för regelbunden efterlevnad av respektive område. Ansvar för kontroller för efterlevnad bör förankras i definierade roller för området.

- Region Skåne rekommenderas att öka graden av detaljer i att definiera och dokumentera vilken typ av händelser, både inom området för IT-säkerhet och inom området för informationssäkerhet, som utgör incidenter mot området. Dokumenterade definitioner av incidenter bör kommuniceras till medarbetare inom Region Skåne samt till externa leverantörer för att säkerställa att berörda parter förstår när en incident inträffat till grund för rapportering.

- Region Skåne rekommenderas att definiera relevanta nyckeltal, både inom området för IT-säkerhet och området för informationssäkerhet, till grund för styrning och kontinuerlig förbättring av området. Ägandeskap och uppföljning av nyckeltal bör förankras i definierade roller för området.

1. Inledning

1.1. Bakgrund

Revisorerna i Region Skåne har gett PwC i uppdrag att granska hur Region Skåne arbetar med IT-säkerhet och informationssäkerhet.

Det övergripande syftet med informationssäkerhet är att säkerställa att information hanteras med utgångspunkt i sekretess, integritet och tillgänglighet till information för medarbetare och intressenter till Region Skåne. IT-säkerhet ligger till grund för att, där det är möjligt, tillhandahålla ändamålsenliga tekniska kontroller för att möjliggöra hantering av krav på informationssäkerheten.

Region Skåne är beroende av fungerande IT-system för att kunna bedriva verksamheten med hög patientsäkerhet, med god effektivitet och hög servicenivå mot medborgarna. Den förväntade utvecklingen av nya e-tjänster inom vården kommer att ytterligare öka detta beroende av säkra IT-system. Med den ökade graden av digitalisering tillkommer även andra typer av risker att beakta i hanteringen av den information som hanteras och lagras. Digitala e-tjänster medför att verksamheter öppnar upp och exponerar sin interna IT-miljö, och information där i, mot det publika Internet.

Ett annat område som driver utveckling av området är nya lagar och förordningar kopplade till hantering av information. Ett exempel på en sådan förordning är EU:s dataskyddsreform (EU 2016/679). Den nya förordningen kommer att innebära att verksamheter är skyldiga att hantera personuppgifter enligt förordningen, vilket kommer att påverka organisation, roller och kontroller i den tekniska miljön av en verksamhet.

I samband med granskningen har det noterats att Region Skåne är i en process att etablera en ny organisationsstruktur för IT, vilket kan komma att medföra förändringar för området IT- och informationssäkerhet. I dagsläget är det oklart vilka typer av förändringar som kommer att implementeras. Vidare har det noterats att det pågår ett arbete med att revidera styrande dokument för området IT- och informationssäkerhet där en del av våra iakttagelser och bedömningar kommer att hanteras.

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda nyckelpersoner för olika verksamhetsområden kopplat till IT- och informationssäkerhet.

Vi har i rapporten valt att beskriva vårt arbete och iakttagelser för respektive kontrollfråga. Då kontrollfrågorna vid vissa tillfällen har beröringspunkter kan effekten bli att viss upprepning är ofrånkomlig.

1.2. Syfte och Revisionsfråga

Syftet med granskningen är att ge revisorerna i Region Skåne ett underlag för att kunna bedöma om Region Skånes arbete med IT- och informationssäkerhet bedrivs på ett systematiskt och effektivt sätt utifrån medborgare och patienters behov.

Den övergripande revisionsfrågan är formulerad enligt följande: *Har Region Skåne (Regionstyrelsen) på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet?*

1.3. Revisionskriterier

Gällande lagstiftning inom området. Relevanta styrdokument inom området. Delar av granskningen kommer att ta utgångspunkt i befintligt IT-säkerhets- och informationssäkerhetsarbete mot relevanta delar från rådande standarder, så som ISO 27001:2013, NIST 800-53, samt legala krav som EU:s dataskyddsförordning och patientdatalagen.

1.4. Kontrollmål

1. Bedriver Region Skåne ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för informationstillgångarna utifrån dagens krav?
2. Finns erforderliga resurser och är arbetet med informationssäkerhet tillräckligt prioriterat i förhållande till de risker som finns?
3. Hur säkerställs medborgarens integritet (patientdatalagen) och hur skyddas patientinformation i journalsystem mot obehöriga?
4. Har Region Skåne ett godtagbart skydd för sina databaser och system mot utomstående intressen som antingen vill komma åt information eller skada verksamheten genom att slå ut systemen eller göra dem otillgängliga på annat sätt?
5. Hur hanteras avvikelser i form av avbrott och säkerhetsintrång på system och data och vilken beredskap och resurser finns för omedelbara åtgärder vid allvarliga incidenter?
6. Hur hanteras IT-säkerheten då tjänster är outsourcade och system och applikationer drivs av extern part? Beaktas informationssäkerhetskrav vid upphandlingar, t ex av tjänster och programvaror?
7. Hur hanterar Region Skåne s.k. molntjänster för lagring av data och vilka riskanalyser, rutiner och regler finns inom detta område för att hantera information som innehåller sekretess eller patientuppgifter?
8. Hur säkerställs att medborgare får relevant, korrekt och säker information via hemsida och nya appar för e-hälsa m m?
9. Hur hanterar Region Skåne riskbedömningar, informationsklassificering, uppföljning och dokumentation av informationssystem med tillhörande skyddsåtgärder?
10. Vilka riskanalyser genomförs inom området informationssäkerhet och vem ansvarar för att de genomförs?
11. Vilken grad av utbildning genomförs av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter?

1.5. Metod och avgränsning

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda nyckelpersoner inom Region Skåne samt tagit del av och genomfört granskning av styrande dokument för verksamhetsområdet.

En sammanställning över granskade dokument samt intervjupersoner återfinns i bilaga 1 och 2. Kontaktpersoner från revisorskollegiet har varit Michael Michelsen och projektledare från Region Skånes revisionskontor har varit Fredrik Ljunggren. Granskningen har genomförts av Magnus Karmborg och Mats Malmberg PwC.

2. Iakttagelser och bedömningar

2.1. Bedriver Region Skåne ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för informationstillgångarna utifrån dagens krav?

2.1.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.1.1.1. Analys av styrande dokument till grund för styrmodell för informationssäkerhet

För att implementera en ändamålsenlig styrmodell för ett verksamhetsområde krävs att det finns en dokumentstruktur implementerad för att tydliggöra hur styrning av verksamhetsområdet ska genomföras. Styrande dokument bör löpande uppdateras för att säkerställa riktlinjer i förhållande till lagar och förordningar samt efter uppdaterade förutsättningar i verksamhetens interna och externa omvärld.

Det saknas en tydlig struktur för styrande dokument till grund för att beskriva hur Region Skåne operativt leder och styr IT- och informationssäkerhetsområdet. Det existerar delar av ett ramverk med styrande dokument, dock framstår dokumentationen i ramverket delvis som fristående delar utan en högre grad av integration, vilket försvårar förutsättningarna för implementation och efterlevnad av området i verksamheten.

2.1.1.2. Riskanalys

Det saknas dokumenterade riktlinjer för hur riskanalyser ska genomföras för område IT-säkerhet och informationssäkerhet. I dagsläget saknar Region Skåne en tydligt definierad styrmodell för riskanalys med utgångspunkt i ett riskbaserat förhållningssätt utifrån hantering av informationstillgångar.

Vidare saknas dokumenterade riktlinjer för hur riskanalys ska genomföras för att säkerställa ändamålsenlig hantering av informationstillgångar i förhållande till EU:s dataskyddsreform (EU 2016/679).

2.1.1.3. Kontroller för IT-säkerhet hos leverantörer

Granskningen har påvisat att det inte sker någon mätbar uppföljning över hur effektiva leverantörers kontroller för IT-säkerhet är. Det saknas en sammanställning över vilka tekniska skydd som finns hos leverantörer samt definierade nyckeltal till grund för styrning av kontrollmiljön hos leverantörer.

Granskningen har inte heller påvisat att det finns rutiner och mötesstrukturer för rapportering av incidenter och aktiviteter för kontinuerlig förbättring av kontrollmiljön för IT-säkerhet från leverantörer till Region Skåne.

Med utgångspunkt i befintliga historiska avtal med leverantörer, är det inte tydligt definierat vilket ansvar leverantörer har i att löpande investera i område för IT-säkerhet för att proaktivt kunna hantera nya typer av risker och hot mot teknologi och informationstillgångar.

2.1.1.4. Avsaknad av riktlinjer för löpande tekniska sårbarhetsanalyser

Det saknas dokumenterade riktlinjer för hur tekniska sårbarhetsanalyser ska genomföras för att över tiden säkerställa att sårbarheter i ny teknologi och mjukvara hanteras.

Vidare har granskningen påvisat att det inte genomförs återkommande sårbarhetsanalyser av den övergripande IT-miljön samt underliggande journalsystem med syfte att identifiera tekniska brister som kan utgöra hot för obehörig åtkomst till information.

2.1.2. Bedömning

Vi bedömer att Region Skåne inte bedriver ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för verksamhetens informationstillgångar utifrån dagens krav. Bedömningen baseras på följande:

- Det saknas en tydlig struktur för styrande dokument till grund för att beskriva hur Region Skåne operativt leder och styr IT- och informationssäkerhetsområdet. Det existerar delar av ett ramverk med styrande dokument, dock framstår dokumentationen i ramverket delvis som fristående delar utan en högre grad av integration.

- Rutiner för riskanalys är inte implementerade för att säkerställa ändamålsenlig hantering av informationstillgångar i förhållande till lagar och förordningar såsom EU:s dataskyddsreform (EU 2016/679).

- Det saknas riktlinjer för hur incidenter kopplade till IT-säkerhet rapporteras från leverantörer till ansvariga inom Region Skåne, mötesstrukturer och kommunikationsvägar är inte tydligt definierade. Om inte incidenter rapporteras på ett ändamålsenligt sätt till ansvariga inom Region Skåne finns det en risk att beslut, investeringar och prioriteringar görs baserat på felaktiga grunder.

- Det saknas dokumenterade riktlinjer för hur analyser ska genomföras för att identifiera tekniska sårbarheter i IT-miljön. Resultat av analyser och utförda åtgärder bör rapporteras tillbaka till ansvarig person inom Region Skåne samt följas upp över tiden med leverantörer för att säkerställa kontinuerlig förbättring i hantering av risker.

2.2. Finns erforderliga resurser och är arbetet med informationssäkerhet tillräckligt prioriterat i förhållande till de risker som finns?

2.2.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.2.1.1. Organisation för verksamhetsområde IT-säkerhet

Vid tidpunkten för den utförda granskningen genomgick Region Skåne en större omorganisation inom IT-verksamheten. Antalet befintliga resurser inom området för IT-säkerhet uppgick innan omorganisationen till två stycken utsedda resurser; IT-säkerhetsansvarig samt IT-säkerhetsarkitekt. IT-säkerhetsansvarig arbetar i en heltidsanställd tjänst. Vi har noterat att tjänsten i nuläget är vakant men att en process för att rekrytera en ersättare är initierad.

För verksamhetsområdet IT-säkerhet har vi inte kunnat identifiera några dokumenterade formella rollbeskrivningar.

När antalet resurser utvärderas för att driva ett verksamhetsområde bör det även beaktas hur komplex och stor den operativa verksamhetsmodellen är samt vilka informationstillgångar som hanteras i verksamheten. I Region Skånes fall finns det ett strategiskt beslut att operativt ansvar för IT-drift och kontroller för IT-säkerhet administreras och förvaltas av tredjepartsleverantörer i en outsourcad verksamhetsmodell. Modellen medför att Region Skåne inte behöver ha interna operativa resurser för att driva området, utan i stället fokuserar på resurser som utgör beställare och kravställare mot leverantörer för området.

Ansvar för kontrollmiljön för IT-säkerhet regleras enligt avtal med följande leverantörer:

- Telia (Cygate som underkonsult), som ansvarar för drift, underhåll och övervakning av nätverk samt brandväggar.
- Tieto ansvarar för område serverdrift och drift av applikation i utsedda datacenter samt tjänster för AIT (Användarnära IT).
- EMC, som ansvarar för tjänster för lagring i den interna IT-miljön.
- Ett stort antal systemleverantörer som ansvarar för att upprätthålla aspekter av IT-säkerhet på system och databasnivå för olika verksamhetssystem.

Tieto är samordnande part med ett ansvar för att registrera incidenter mot IT-säkerhet vilka ska rapporteras till Tieto helpdesk för hantering.

Givet ovanstående förutsättningar, med ett distribuerat ansvar av kontroller för IT-drift och IT-säkerhet, krävs det en intern organisation som kan ställa krav och säkerställa efterlevnad av området för IT- och informationssäkerhet mot externa leverantörer.

2.2.1.2. Organisation för verksamhetsområde informationssäkerhet

Organisationen för informationssäkerhet inom Region Skåne bestod vid tiden för vår granskning av en utsedd resurs i form av en informationssäkerhetschef som stöds av sex informationssäkerhetssamordnare fördelat på lika många förvaltningar vilka arbetar deltid inom området för informationssäkerhet. Informationssäkerhetschef och informationssäkerhetssamordnare har möten en gång per månad.

För verksamhetsområdet informationssäkerhet finns en samlad rollbeskrivning i dokumentet ”Förslag till organisation för informationssäkerhetsarbetet i Region Skåne”. Den samlade rollbeskrivningen beskriver tre personer för utförande av uppdraget; en informationssäkerhetschef, ett personuppgiftsombud samt en medarbetare med inriktning mot patientdatalagen och relaterade föreskrifter. Sedan 2012 har området för informationssäkerhet organisatoriskt minskat från fyra heltidsanställda resurser till en heltidsanställd

person i rollen som informationssäkerhetschef, samt en person i rollen som personuppgiftsombud på del av tjänst.

Rollbeskrivning för informationssäkerhetsamordnare återfinns i dokumentet *Förtydligande av organisation för Informationssäkerhet*.

Personuppgiftsombudet har enligt personuppgiftlagen (PuL 1998:204) uppgiften att kontrollera att personuppgifter hanteras på ett lagligt och korrekt sätt och i enlighet med god sed. Personuppgiftsombudet har också en roll som regionsjurist varför uppdraget som personuppgiftsombud inte är på heltid. Personuppgiftsombudet har stöd av 10 utsedda personuppgiftsföreträdare, på del av tjänster, inom respektive förvaltning. För rollen personuppgiftsombud finns en rollbeskrivning daterad 1998-11-16 som beskriver formell ställning och dennes uppgifter.

2.2.1.3. Budget för IT- och informationssäkerhet

Det noterades även att verksamhetsområdena för IT- och informationssäkerhet inte har en egen budget per verksamhetsområde. Kostnaden för att investera i IT-säkerhetslösningar är distribuerad och inkluderad i den totala IT-budgeten för respektive verksamhetsområde. Avseende kostnader för att investera i området för informationssäkerhet har granskningen inte identifierat hur denna typ av investeringar hanteras och fördelas budgetmässigt. Vid identifierade behov av investeringar i området har IT-säkerhetsansvarig respektive informationssäkerhetschef historiskt behövt förhandla fram medel från budgetansvarig på verksamhetsnivå. Det faktum att budget för IT-säkerhet och informationssäkerhet är inkluderad i budgeten för de olika verksamheterna bidrar till en komplicerad process i att investera i områdena, där det slutliga beslutet om en investering inte fullt ut ligger hos IT-säkerhetsansvarig eller informationssäkerhetschef.

2.2.2. Bedömning

Vi bedömer att Region Skåne inte har erforderliga resurser och inte arbetar med informationssäkerhet tillräckligt prioriterat i förhållande till de risker som finns. Bedömningen baseras på följande:

- Nuvarande storlek på organisation kopplat till ett ansvar för IT-säkerhet och informationssäkerhet bedöms inte vara tillräcklig för att hantera kraven på området beaktat verksamhetens storlek och typ av informationstillgångar som existerar inom Region Skåne. Utvecklingen de senaste åren är att antalet resurser inom området för informationssäkerhet minskat. Samtidigt har det skett en ökad grad av digitalisering av verksamhetstjänster vilket föranlett en förhöjd riskbild i hanteringen av informationstillgångar.

- Roller och ansvarsområden är inte tydligt dokumenterade ned på verksamhetsnivå. Formellt dokumenterade rollbeskrivningar med tillhörande ansvarsområden är en nyckelkomponent i att implementera en fungerande styrmodell för ett verksamhetsområde. Avsaknad av en formell rollstruktur kan medföra risker i hantering av kritiska informationstillgångar och efterlevnad av kontrollmiljön.

- Det saknas i dagsläget en särskilt beslutad budget till grund för att utveckla område för IT- och informationssäkerhet, vilket innebär att den lång- och kortsiktiga

planeringen och utvecklingen av område för IT- och informationssäkerhet blir eftersatt.

2.3. Hur säkerställs medborgarens integritet (patientdatalagen) och hur skyddas patientinformation i journalsystem mot obehöriga?

2.3.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.3.1.1. Tekniska kontroller för att säkerställa krav på informationssäkerhet i journalsystem

Nedan följer en sammanställning över vilka tekniska kontroller som finns implementerade i IT-miljön hos Region Skåne för att säkerställa obehörig åtkomst till patientinformation i journalsystem. När det gäller kontroller i applikation har granskningen fokuserat på kontroller relaterade till journalsystemet Melior för att upprätthålla krav på informationssäkerhet i applikationen.

2.3.1.2. Externt perimeterskydd – brandvägg

Region Skånes interna IT-miljö skyddas av en brandvägg. Brandväggen är en form av tekniskt skydd för att säkerställa kommunikation mellan Region Skånes interna IT-miljö och internet. Brandväggen består av ett antal regler som ligger till grund för att medge olika typer av externa IT-tjänster åtkomst till Region Skånes interna IT-miljö.

2.3.1.3. Segmentering av Region Skånes interna nätverk

Region Skånes interna nätverksmiljö saknar till stora delar segmentering (uppdelning av det interna nätverket med syfte att skydda kritisk infrastruktur från obehörig åtkomst). Granskningen har påvisat att det finns ett pågående projekt för att applicera aspekter av segmentering till nätverksmiljön.

2.3.1.4. Antivirus

Det finns tekniskt skydd implementerat i form av antivirusskydd. Skyddet används för att förhindra att, och övervaka om, olika typer av skadlig kods installeras och sprids i Region Skånes interna IT-miljö. Installation av skadlig kod i en IT-miljö kan medföra en risk för obehörig åtkomst till informationstillgångar eller att system och IT-tjänster som innehåller för verksamheten kritisk information blir otillgängliga på grund av skadlig kod.

2.3.1.5. Loggning och övervakning av kritiska IT-tjänster

Det finns kontroller för loggövervakning implementerade i den tekniska IT-miljön med syfte att övervaka kritiska komponenter av IT-miljön samt avvikande mönster i nätverkstrafiken. Eventuella larm i övervakningen som är relaterade till driften av IT-tjänster hanteras av Tieto helpdesk.

Granskningen har inte påvisat att det finns riktlinjer för att upprätta kontroller för att proaktivt analysera innehåll från systemloggar utifrån risk, för att fånga pågående aktiviteter i IT-miljön som kan utgöra hot mot informationssäkerheten. Uppföljning och analys av innehåll i systemloggar utförs i dagsläget reaktivt efter att händelser har rapporterats i form av incidenter mot informationssäkerheten.

2.3.1.6. Extern inloggning via RSVPN

All extern inloggning till den interna IT-miljön hos Region Skåne hanteras via RSVPN. RSVPN är en tjänst för säker extern åtkomst till Region Skånes nät. Den tekniska lösningen innebär att säker kommunikationsförbindelse upprättas mellan den externa datorn och Region Skånes interna IT-miljö vid anslutning. Ansökan om tillgång till RSVPN görs enligt Region Skånes interna rutin för tilldelning av RSVPN behörighet.

2.3.1.7. Tekniska kontroller för inloggning i journalsystem

Det finns tekniska förutsättningar för att logga in i IT-miljön och journalsystem med hjälp av stark autentisering. Stark autentisering innebär att flera identifieringsfaktorer kombineras för att öka säkerheten. Det innefattar tekniker som är säkrare än ett vanligt användarnamn och lösenord för att säkerställa att det är rätt person som loggar in. Det kan till exempel vara RS-kort (e-id kort), e-legitimation eller en dosa som genererar ett engångslösenord.

I Region Skånes fall finns tekniska möjligheter att använda ett personligt användarkonto och lösenord samt ett personligt magnetkort vid inloggning för att säkerställa behörig åtkomst till information.

2.3.1.8. Behörighetsstruktur och roller i system

Den inbyggda rollstrukturen i systemet medför att användare med en viss roll i systemet medges åtkomst till viss information. Vi har noterat att de uppsatta behörigheterna i Melior är breda, varför kompenserande kontroller i form av loggövervakning är implementerade för att säkerställa behörig åtkomst till information.

2.3.1.9. Loggfunktion i system

Kritiska aktiviteter och uppdatering av fast data loggas automatiskt i applikationen Melior, t ex loggas det vilka anställda som har läst en viss journal i systemet. Innehåll i loggar används även som grund för att säkerställa behörig åtkomst till patientinformation i form av sticksprovstestning vid årliga kontroller. Innehåll i loggar ligger även till grund för detaljuppföljning av aktiviteter i applikationen vid behov.

2.3.1.10. Rutin för administration av behörigheter

Det finns en dokumenterad rutin för att säkerställa ändamålsenlig hantering av administration av behörigheter till medarbetare inom Region Skåne (*Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter*). Som en del av rutinen ingår att utföra en behovs- och riskanalys av medarbetaren i relation till den efterfrågade behörigheten till systemmiljön. Det är verksamhetschef som är ytterst ansvarig för att behörigheter hanteras enligt rutinen.

2.3.1.11. Rutin för återkommande granskning av behörigheter

Som en del av den dokumenterade rutinen för administration av behörigheter (*Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter*) ingår det även årliga kontroller av behörigheter för att säkerställa att varje medarbetares behörighet överensstämmer med arbetsuppgifter medarbetaren har.

2.3.1.12. Rutin för stickprovstestning av åtkomst till patientjournaler

Det finns en implementerad instruktion för att säkerställa efterlevnad i verksamheten att patientuppgifter hanteras av medarbetare enligt gällande lagar och förordningar för området *(Loggkontroll - granskning av åtkomst till patientuppgifter)*. Denna instruktion utgår från nationellt överenskommen vägledning för loggkontroll som antagits i Region Skåne där riktmärket för loggkontroll är 10 % av personalen månadsvis. Kontroll av loggar ska även utföras då det föreligger misstanke om obehörig åtkomst. Verksamhetschef har enligt instruktionen ansvar för kontroll av personalens åtkomst till patientdata.

Baserat på ett stickprovsurval av journaler i journalsystem utvärderas om medarbetare är behöriga att arbeta med journalen. Avvikelser ska rapporteras av verksamhetschef enligt vedertagen instruktion (*Dataintrång - åtgärder vid misstanke om olovlig åtkomst*).

Vi har noterat att det inte finns ett automatiserat verktyg implementerat för att underlätta granskning av loggar av åtkomst till patientuppgifter. Detta innebär att granskning måste utföras manuellt vilket kräver stora personella resurser i anspråk med tanke på Region Skånes storlek. Vidare kräver det individuellt tekniskt kunnande och bedömningar vilket medför att det förefaller orimligt att 10 % av personalen kan granskas med detta förfarande. Vi har noterat att omfattningen av loggkontrollen på 10 % inte efterlevs. Enligt inrapporteringsstatistik rapporterar inte samtliga verksamhetschefer in loggkontroller och loggkontroller förefaller inte utföras konsekvent under alla månader. För de månader där loggkontroller utförts efterlevs inte stickprovsgränsen om 10% konsekvent.

Under vår granskning har vi inte noterat någon förekomst av nyckeltalsrapportering för avvikelser gällande obehörig åtkomst till patientuppgifter samlat för Region Skåne.

2.3.2. Bedömning

Vi bedömer att Region Skåne endast delvis säkerställer medborgarens integritet (patientdatalagen) och skyddar patientinformation i journalsystem mot obehöriga. Bedömningen baseras på följande:

- Det finns inte kontroller implementerade för proaktiv/automatiserad övervakning av innehåll i systemloggar med syfte att identifiera pågående aktiviteter och händelser som kan utgöra risker mot informationssäkerheten. Övervakning av innehåll i systemloggar sker i dagsläget reaktivt, vilket kan medföra en förhöjd risk för obehörig åtkomst till patientinformation.

- Region Skånes interna nätverksmiljö saknar till stora delar segmentering. Att inte använda segmentering i större nätverksmiljöer kan innebära förhöjd risk av obehörig åtkomst till informationstillgångar. Granskningen har påvisat att det finns ett pågående projekt för att applicera aspekter av segmentering till nätverksmiljön.

- Granskning av loggar av åtkomst till patientuppgifter ska enligt riktlinjerna genomföras månatligen av riktmärket 10 % av personalstyrkan. Eftersom ett automatiserat verktyg inte finns implementerat och således granskning måste göras manuellt efterlevs denna riktlinje inte konsekvent på grund av den stora arbetsbelastning detta medför.

2.4. Har Region Skåne ett godtagbart skydd för sina databaser och system mot utomstående intressen som antingen vill komma åt information eller skada verksamheten genom att slå ut systemen eller göra dem otillgängliga på annat sätt?

2.4.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.4.1.1. Riktlinjer för administration och övervakning av aktiviteter utförda direkt mot databasen

Det saknas dokumenterade riktlinjer för administration och övervakning av aktiviteter utförda av databasadministratörer för databaser som hanterar patientinformation.

2.4.1.2. Riktlinjer för kryptering av information i databaser till journalsystem

Det saknas dokumenterade riktlinjer för hur tekniskt skydd i form av kryptering ska appliceras på databaser som hanterar patientinformation. Att inte applicera kryptering på en databas kan innebära förhöjda risker för obehörig åtkomst till information via direkt inloggning mot databasen eller i att återställa säkerhetskopior av databasen till en extern server.

Granskningen har inte påvisat att teknologi för kryptering operativt appliceras på databaser som hanterar patientinformation.

2.4.1.3. Riktlinjer för hantering av backupfiler av databaser för journalsystem

Det saknas riktlinjer för hur hantering av backupfiler från databaser för journalsystem ska hanteras för att säkerställa behörig åtkomst till information.

För att säkerställa integritet i data över tiden i en databas används backuprutiner för att skapa en säkerhetskopia av databasen och underliggande transaktionsloggar att använda till grund för att återskapa en databas om en incident inträffar mot driftsdatabasen. Säkerhetskopian kan då användas för att återställa databasen till befintligt läge (tidpunkt för senaste backup), innan den inträffade incidenten.

2.4.1.4. Tekniskt skydd för överbelastningsattacker (DDOS)

Det finns tekniskt skydd för överbelastningsattacker installerat i en del av den nätverkstjänst som Region Skåne köper från Telia. Tjänsten innebär att onaturligt hög datatrafik mot Region Skånes IT-miljö filtreras så att den interna IT-miljön och kritiska IT-tjänster

inte överbelastas och därmed blir otillgängliga för användning. Med det installerade skyddet för att hantera överbelastningsattacker minskar sannolikheten för externa överbelastningsattacker mot Region Skånes IT-miljö med risk för att otillgängliggöra kritiska IT-system och informationstillgångar.

2.4.2. Bedömning

Vi bedömer att Region Skåne endast delvis säkerställer ett godtagbart skydd för sina databaser och system mot utomstående intressen som antingen vill komma åt information eller skada verksamheten genom att slå ut systemen eller göra dem otillgängliga på annat sätt. Bedömningen baseras på följande:

- Det saknas dokumenterade riktlinjer för hur databaser som hanterar patientinformation ska administreras och konfigureras för att säkerställa behörig åtkomst till information. Avvikelser rörande obehörig aktivitet direkt mot databasen från databasadministratörer bör rapporteras enligt Region Skånes rutin för avvikelsehantering.

- Det saknas riktlinjer för ändamålsenlig konfiguration (standard för säkerhetskonfiguration) i syfte att tydliggöra hur databaser ska vara konfigurerade ur ett IT-säkerhetsperspektiv samt för att möjliggöra spårbarhet och loggning av aktiviteter utförda av databasadministratörer direkt mot databasen.

- Det saknas riktlinjer för kryptering av databaser som innehåller patientinformation varmed det föreligger risker kopplat till obehörig återläsning av säkerhetskopior (backup) från journalsystem. Innan krypteringsteknologi appliceras bör det genomföras en riskanalys för att kartlägga behovet i detalj, vidare bör det även som en del av riskanalysen utvärderas om nyttjande av teknologi för kryptering kan påverka den övergripande prestandan av systemet.

2.5. Hur hanteras avvikelser i form av avbrott och säkerhetsintrång på system och data och vilken beredskap och resurser finns för omedelbara åtgärder vid allvarliga incidenter?

2.5.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.5.1.1. Instruktion för hantering av informationssäkerhetshändelser- och incidenter

Granskningen har påvisat att det finns en övergripande instruktion *(Instruktion för hantering av informationssäkerhetshändelser- och incidenter)* med syfte att öka informationssäkerheten genom att tydliggöra processer och metoder för att på ett strukturerat sätt klassificera och hantera informationssäkerhetsincidenter. Målgrupp är alla medarbetare och externa leverantörer som hanterar Region Skånes informationstillgångar.

Efter en granskning av instruktionen identifieras ett antal områden vilka ytterligare kan förtydligas:

- I instruktionen är incidenter mot området för IT-säkerhet och informationssäkerhet generellt beskrivna vilket medför att mottagaren (målgruppen) inte vet när en händelse utgör en incident mot IT-säkerheten- och informationssäkerheten, vilket innebär att det finns en risk för att faktiska incidenter inte rapporteras.

- I instruktionen framgår det inte hur kommunikationsvägar för rapportering ser ut eller mötesstrukturer för rapportering av incidenter från leverantörer och ansvariga personer för området inom Region Skåne.

2.5.1.2. Instruktion Dataintrång – åtgärder vid misstanke om olovlig åtkomst

Det finns en instruktion *”Dataintrång – åtgärder vid misstanke om olovlig åtkomst”* vilken syftar till att dels beskriva rutinen för hantering vid misstanke om dataintrång och dels straff- och arbetsrättsligt förfarande när arbetsgivaren i sin utredning konstaterat att obehörig åtkomst till patientuppgifter, dataintrång, skett.

2.5.1.3. Instruktion för incidenthantering

Granskningen har påvisat att det finns en dokumenterad instruktion för incidenthantering inom Region Skåne, som i detalj beskriver processen samt associerade roller och ansvarsområden. Huvudsyftet med rutinen för incidenthanteringen är att på ett strukturerat sätt så effektivt som möjligt återställa tjänster till normal funktionalitet.

Incidenthantering ska ingå i grundavtalen med applikations- och driftleverantörer. Vid incidenter som omfattar flera leverantörer skall Region Skånes incidentprocess användas. Incidenten koordineras då av en leverantör med koordineringsansvar och övriga leverantörer bidrar med kunskap inom sitt område för att lösa incidenten. I dagsläget är Tieto den leverantör som har ett koordineringsansvar.

2.5.1.4. Instruktion för hantering av stor incident – IT, telefoni och MT

Det finns en instruktion framtagen för att beskriva hanteringen av stora incidenter som inträffar i Region Skånes leveranser av IT, telefoni och Medicinsk teknik. Instruktionen för hantering av stor incident är övergripande och förutsätter att leverantörer med operativt ansvar i sin tur har mer detaljerade arbetsbeskrivningar för hantering av incidenter. Som en del av dokumentet finns även beskrivning av eskalering och kommunikationsvägar.

2.5.1.5. Serviceavtal och servicenivåer

Granskningen har påvisat att det i nuvarande driftsavtal med Tieto finns definierat fyra olika typer av servicenivåer för IT-tjänster. Definierade servicenivåer ligger till grund för att säkerställa tillgänglighet till informationstillgångar.

2.5.1.6. Redundans i teknisk infrastruktur

Det finns en dokumentation som beskriver relation mellan hur servicenivåer är definierade och hur redundans i systemarkitektur är uppbyggd. (*Redundans innebär att flera servrar arbetar parallellt med samma uppgifter och speglar varandra, så att om en av dessa havererar så tar den andra över.*) Redundans i arkitektur ligger till grund för att upprätthålla tillgängligheten i IT-tjänster och tillgång till information enligt gällande servicenivåer enligt avtal.

2.5.1.7. Automatisk övervakning av kritiska IT-tjänster och övervakning av försök till obehörig åtkomst

Vid en granskning av rutinen för incidenthantering konstaterades det att incidenthantering bland annat sker med utgångspunkt i automatisk övervakning av kritiska IT-tjänster.

Kontroller för automatisk övervakning sker genom att använda specialmjukvaror som analyserar olika typer av systemloggar från kritiska IT-tjänster. Mjukvaran är konfigurerad för att fånga upp specifika detaljer i systemloggar, vilka utgör tröskelvärden för när en IT-tjänst börjar påverkas negativt i prestanda. När mjukvaran fångar upp en avvikelse i systemloggen genereras ett larm till helpdeskfunktionen i form av ett ärende, e-mail eller SMS till ansvariga personer.

Den utförda granskningen har inte påvisat att det finns några riktlinjer för hur kontroller för aktiv övervakning av innehåll i systemloggar i IT-miljö/journalsystem ska implementeras, däribland obehöriga intrångsförsök.

2.5.1.8. Backuprutin – Melior

Säkerhetskopiering av system och tillhörande databaser och underliggande information syftar till att kunna återställa en systemmiljö vid kritiska incidenter.

Det finns en dokumenterad backuprutin för Melior. Enligt den dokumenterade rutinen tas en full databasbackup en gång per dygn och en backup av databasens transaktionsloggar tas en gång var 10:e minut, vilket innebär att databasen går att återställa med en maximal dataförlust av transaktioner på 10 min.

2.5.1.9. Rutin för återställning av journalsystem Melior

Det finns en dokumenterad rutin för återställning av Melior vid tillfälle för kritiska incidenter. Rutinen beskriver systemmiljöns olika nivåer som ska kunna återställas. Primärt fokuserar rutinen på hur återställning av databasen ska genomföras baserat på olika typer av scenarion med utgångspunkt i olika typer av felmeddelande.

2.5.1.10. Testning av återställningsrutiner

Granskningen har påvisat att det saknas dokumenterade riktlinjer för hur leverantörer årligen ska säkerställa testning och effektivitet i återställningsrutiner.

2.5.2. Bedömning

Vi bedömer att Region Skåne delvis hanterar avvikelser i form av avbrott och säkerhetsintrång ändamålsenligt på system och data och att det delvis finns beredskap och resurser för omedelbara åtgärder vid allvarliga incidenter. Bedömningen baseras på att:

- Det finns existerande rutiner för incidenthantering, samt återställningsrutiner till grund för effektiv återställning av kritiska IT-tjänster.
- Rutin för incidenthantering inkluderar roller och ansvarsområden, samt kommunikationsvägar för hur incidenter ska hanteras.
- Det finns inbyggda kontroller för redundans i den tekniska miljön vilket ligger till grund för att den tekniska miljön är mindre utsatt för risker kopplat till driftsavbrott.

Bedömningen är också att det finns en övergripande risk att nuvarande kontrollmiljö och rutin för incidenthantering inte på ett effektivt sätt fångar händelser som kan utgöra incidenter i hanteringen av informationstillgångar. Bedömningen baseras på att:

- Det saknas detaljerade definitioner över vad som utgör en incident mot IT-säkerhet och informationssäkerhet vilket medför att det blir svårt att definiera olika typer av kontroller för övervakning av området. Iakttagelsen innebär att övervakning av risker kopplat till IT-säkerhet och informationssäkerhet tenderar att ske reaktivt istället för utifrån ett proaktivt förhållningssätt.

- Det saknas dokumenterade riktlinjer för hur kommunikationsvägar ser ut för rapportering av incidenter från leverantörer till ansvariga personer för området inom Region Skåne.

- Det saknas dokumenterade riktlinjer för hur leverantörer årligen ska säkerställa testning och effektivitet i återställningsrutiner. Utfall och resultat av utförda tester bör kommuniceras till beställare av IT-tjänsten. Eventuella avvikelser ska rapporteras som incidenter, åtgärder som leverantören initierat för att säkerställa att rutinen fungerar i framtiden ska presenteras och redovisas.

- Det saknas definierade nyckeltal relaterat till incidenthantering. Nyckeltal saknas i två nivåer:

    - Det saknas definierade nyckeltal för att följa upp och övervaka incidenter relaterade till IT- och informationssäkerhet. Övervakning av nyckeltal ligger till grund för att säkerställa att planerade och genomförda åtgärder i verksamheten får en förväntad effekt i form av färre antal rapporterade incidenter inom ett visst område.

    - Det saknas definierade nyckeltal för att säkerställa effektivitet i incidenthanteringsprocessen. Det är viktigt att övervaka effektiviteten i processer, för kontinuerlig förbättring av arbetssätt och rutiner. I en verksamhetsmodell där processer är outsourcade till externa leverantörer är det ytterst viktigt att verksamheten som beställare arbetar med relevanta nyckeltal för att säkerställa effektiva rutiner hos leverantörer.

2.6. *Hur hanteras IT-säkerheten då tjänster är outsourcade och system och applikationer drivs av extern part? Beaktas informationssäkerhetskrav vid upphandlingar, t ex av tjänster och programvaror?*

2.6.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.6.1.1. Styrning och övervakning av kontrollmiljön för IT-säkerhet

Granskningen har påvisat att det inte finns dokumenterade riktlinjer för hur Region Skåne ska säkerställa att leverantörer upprätthåller förväntade nivåer av IT-säkerhet uti-

från risker kopplade till hantering av informationstillgångar. Vidare saknas det relevanta nyckeltal för styrning av området med syfte att övervaka antalet incidenter kopplade till IT-säkerhet för att utvärdera åtgärder för kontinuerlig förbättring.

Det operativa ansvaret för IT-säkerhet inom Region Skåne hanteras i dagsläget av ett antal tredjepartsleverantörer. För IT-säkerhet i nätverket och brandväggar ansvarar Telia för tekniskt skydd. För området server och applikationsdrift är det Tieto som ansvarar för kontroller avseende IT-säkerhet. För enskilda verksamhetsapplikationer är det olika systemleverantörer som har ett ansvar för aspekter av IT-säkerhet kopplat till systemet.

I Region Skånes fall ökar komplexiteten i att övervaka kontrollmiljön för IT-säkerhet hos tredjepartsleverantörer då ansvaret för området är delat mellan ett antal parter. Det distribuerade ansvaret för kontrollmiljön ställer höga krav på Region Skånes interna organisation att både agera i rollen som kravställare av kontrollmiljön för IT-säkerhet och samtidigt agera i en övervakande roll för att säkerställa att förväntade skyddsnivåer levereras av leverantörer.

2.6.1.2. Kontinuerlig förbättring och utveckling av kontrollmiljön för IT-säkerhet

Det saknas dokumenterade riktlinjer för hur Region Skåne ska säkerställa att leverantörer med ett operativt ansvar över kontrollmiljön för IT-säkerhet kontinuerligt arbetar med att utveckla och förbättra kontrollmiljön för IT-säkerhet.

2.6.1.3. Intern granskning av kontrollmiljö för IT-säkerhet hos leverantörer

IT-säkerhetsansvarig har under år 2016 genomfört en intern granskning avseende IT-säkerhet hos tredjepartsleverantörer. Ett antal iakttagelser gjordes i samband med granskningen, bland annat noterades:

- Det finns avancerade tekniska lösningar för övervakning av IT-säkerhet hos tredjepartsleverantörer, teknologin utnyttjas inte till sin fulla potential i hur lösningar är implementerade och övervakade.
- Interna och externa hot mot IT-säkerheten är med dagens höga grad av digitalisering ett område i ständig förändring och utveckling. Det noterades att kontroller för IT-säkerhet hos tredjepartsleverantörer inte hanterar nya typer av hot och risker på ett ändamålsenligt sätt.
- Design av nuvarande nätverk har inte gjorts med utgångspunkt i att hantera risker kopplat till hantering och information och har en design som i princip saknar segmentering.

2.6.1.4. Styrande dokument och rutiner vid upphandlingar

Det finns styrande dokument på övergripande nivå i form av en Upphandlingspolicy, vilken inte berör Informationssäkerhet.

Vid upphandlingar och inköp har vi inte kunnat identifiera några gemensamma rutiner, riktlinjer eller formaliserade processer för Region Skåne som bestämmer något krav att informationssäkerhetskrav måste beaktas. Däremot tillsätts en expertgrupp i upphandlingar som stöd för beställaren, där IT-avdelningen är representerade när IT-system och

IT-tjänster berörs. Expertgruppens roll är att definiera behovet och kravställningen för upphandlingen vilket resulterar i förfrågningsunderlaget för upphandlingen. Vad gäller informationssäkerhetskrav så finns det endast informella riktlinjer där expertgrupp eller beställare vid behov rådfrågar juristavdelning, personuppgiftsombud eller informationssäkerhetschef.

2.6.1.5. Informationssäkerhetskrav vid upphandlingar

Vid upphandlingar av IT-tjänster som sker genom en behovsprocess i Region Skåne, sker kravställning med involvering av IT-säkerhetsarkitekt. Till grund för hur kravställning ska formuleras utgår kravställningsarbetet från riktlinjer enligt kravkatalog *”Kravkatalog för IT-stöd inom Region Skåne v.2.0”*.

Det finns även en kravkatalog med kravformuleringar som används vid upphandling och utveckling och är ett internt verktyg inom Region Skåne som används för att ta fram den kravmassa som är aktuell för respektive upphandling eller utvecklingsprojekt. Lösningsarkitekterna använder katalogen i samråd med domänarkitekter för att ta fram vilka krav som är relevanta för respektive upphandling.

Innehållet i kravkatalogen är baserat på olika standarder för informationssäkerhet, primärt ISO 27001:2014, och kan appliceras på olika typer av tjänster för upphandling. Kravkatalog finns att tillgå på Region Skånes intranät.

Dokumentet ” Kravspecifikation informationssäkerhet avseende upphandling av IT-tjänster” senast reviderad 2012-12-07 finns även som stöd vid upphandlingar av IT-tjänster. Kravspecifikationen fokuserar på legala och tekniska krav föranledda av främst Personuppgiftslagen och Patientdatalagen.

Granskningen har påvisat att IT-säkerhetsarkitekt inte konsekvent deltar i utvärderingsfasen av upphandlingsprocessen. IT-säkerhetsarkitekt ska med fördjupad kunskap om området säkerställa att detaljer i inkomna anbud möter krav på IT- och informationssäkerhet för den upphandlade tjänsten.

2.6.2. Bedömning

Vi bedömer att Region Skåne delvis bedriver ett ändamålsenligt informationssäkerhetsarbete, då tjänster är outsourcade och system och applikationer drivs av extern part, samt vid upphandlingar, t ex av tjänster och programvaror. Bedömningen baseras på att:

- Det saknas dokumenterade riktlinjer för hur Region Skåne ska säkerställa att leverantörer upprätthåller förväntade nivåer av IT-säkerhet utifrån risker kopplat till hantering av informationstillgångar. Kommunikationsvägar och mötesstrukturer mellan ansvariga inom Region Skåne och leverantörer är inte tydligt definierade.

- Region Skåne arbetar i dagsläget inte proaktivt med riskanalys och klassificering av informationstillgångar vilket medför att det inte finns ändamålsenliga förutsättningar att kravställa existerande kontrollmiljö för IT-säkerhet hos leverantörer.

- Region Skåne arbetar inte med definierade nyckeltal för styrning av området vilket innebär att det saknas mätbara förutsättningar att förstå hur leverantörer proak-

tivt övervakar och kontinuerligt förbättrar kontrollmiljön för IT-säkerhet över tiden.

- Processen för inköp och upphandling hanterar inte konsekvent frågor som berör informationssäkerhet och det är inte tydligt hur dessa beaktas när beslut fattas.

- IT-säkerhetsarkitekt är inte konsekvent involverad i utvärderingsfasen av upphandlingsprocessen för att säkerställa att inkomna anbud på ett ändamålsenligt sätt svarar till formulerade krav på IT- och informationssäkerhet.

2.7. Hur hanterar Region Skåne s.k. molntjänster för lagring av data och vilka riskanalyser, rutiner och regler finns inom detta område för att hantera information som innehåller sekretess eller patientuppgifter?

2.7.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.7.1.1. Styrande dokument och riktlinjer för nyttjande av molntjänster

Det saknas dokumenterade riktlinjer för hur molntjänster ska hanteras inom Region Skåne samt hur enskilda medarbetare får nyttja molntjänster. Vi har noterat att det finns visst stöd i styrande dokument för upphandling och inköp i form av en kravkatalog. Däremot är det inte tydligt i vilken utsträckning denna används. Vidare har vi inte kunnat identifiera något samlat register för vilka publika molntjänster som används.

Granskningen har inte påvisat förekomsten av riktlinjer för hur proaktiv övervakning av nyttjandet av molntjänster ska göras på regelbunden basis. Ett exempel på detta kan vara att man blockerar åtkomsten till vissa molntjänster inifrån Region Skånes IT-miljö.

2.7.1.2. Intern granskning av nyttjande av molntjänster

Enligt informationssäkerhetschefens årliga rapport till Regionstyrelsen om informationssäkerhetsarbetet, har en analys som gjorts under våren 2016 visat att 1 183 tjänster utnyttjats som molntjänster. Av dessa har 88 klassats som högrisktjänster. Då Region Skånes informationstillgångar inte inventerats och klassificerats utifrån risk, är det i nuläget oklart vilka risker som föreligger kopplat till denna iakttagelse.

2.7.2. Bedömning

Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete avseende molntjänster för lagring av data. Bedömningen baseras på att:

- Det saknas en samlad bild över de molntjänster som används och hur informationstillgångarna i dessa skyddas. Det finns inte etablerade rutiner och processer för att inventera och bedöma den information som används i alla publika molntjänster.

- Det saknas dokumenterade riktlinjer för hur molntjänster kan användas av medarbetare inom Region Skåne i det dagliga arbetet med hantering av information.

- Interna granskningar har påvisat att ett stort antal molntjänster används av medarbetare inom Region Skåne, det är oklart vilken typ av information som dessa tjänster hanterar. Iakttagelsen påvisar att det i nuläget inte finns en fungerande styrmodell för att säkerställa ändamålsenlig hantering av informationstillgångar vid nyttjande av molntjänster.

- Det saknas dokumenterade riktlinjer för att tydliggöra hur området framåt proaktivt ska övervakas för att säkerställa ändamålsenlig hantering av informationstillgångar vid nyttjande av molntjänster.

- Vid upphandling av systembaserade molntjänster ska en kravkatalog användas för att säkerställa ändamålsenlig kravställning på tjänsten utifrån krav på IT-säkerhet och informationssäkerhet. Det är i dagsläget oklart i vilken utsträckning kravkatalogen används vid upphandling av IT-stöd då det saknas kontroller för att säkerställa efterlevnad av området.

2.8. Hur säkerställs att medborgaren får relevant, korrekt och säker information via hemsida och nya appar för e-hälsa m m?

2.8.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.8.1.1. Styrande dokument och riktlinjer för information via hemsida och nya appar m m

Det finns styrande dokument och riktlinjer för hur information ska publiceras via publika e-tjänster. Riktlinjerna innehåller bland annat:

- Varumärkespolicy: Policyn beskriver Region Skånes identitet och önskade position samt dess uppdrag.

- Kommunikationspolicy: Policyn beskriver bland annat Region Skånes riktlinjer för kommunikation.

- Kommunikationsstrategin: Strategin anger Region Skånes kommunikationsmål, målgrupper, samt ansvarsområden.

- Medieanvisningar. Anvisningarna beskriver hur Region Skåne ska hantera sina kontakter med media.

- Regelverk för web-platser: Regelverket beskriver hur Region Skåne ska förhålla sig till publicering av information på web-platser och web-applikationer.

- Strategi för sociala medier: Strategin anger vilken information som får förekomma på sociala medier och hur den ska anges.

Granskningen har inte påvisat att det finns dokumenterade riktlinjer för att säkerställa att den information som publiceras via publika e-tjänster uppfyller krav på informationssäkerhet. Vidare har inte granskningen påvisat förekomsten av dokumenterade riktlinjer för att regelbundet genomföra tekniska analyser för att identifiera och åtgärda tekniska sårbarheter i publika e-tjänster.

2.8.2. Bedömning

Vi bedömer att Region Skåne delvis bedriver ett ändamålsenligt informationssäkerhetsarbete för att säkerställa att medborgaren får relevant, korrekt och säker information via hemsida och nya appar för e-hälsa m.m. Bedömningen baseras på att:

- Det saknas dokumenterade riktlinjer runt arbetssätt och kontrollaktiviteter för att säkerställa att information uppfyller krav på informationssäkerhet vid publicering av information på publika e-tjänster.

- Det saknas dokumenterade riktlinjer för hur tekniska sårbarhetsanalyser ska genomföras över tiden med syfte att identifiera och åtgärdshantera tekniska sårbarheter i publika e-tjänster.

2.9. Hur hanterar Region Skåne riskbedömningar, informationsklassificering, uppföljning och dokumentation av informationssystem med tillhörande skyddsåtgärder?

2.9.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.9.1.1. Styrande dokument för riktlinjer kring rutin för informationsklassificering

Det saknas dokumenterade riktlinjer för hur inventering och klassificering av informationstillgångar ska genomföras utifrån risk.

För att kartlägga risker i hantering av informationstillgångar i en verksamhet behöver information som hanteras i verksamheten inventeras och kartläggas och därefter klassificeras utifrån risk. Inventering av information bör genomföras för samtliga informationstillgångar som existerar i en verksamhet oavsett om informationen existerar i digitalt format eller i analogt format.

Den utförda granskningen har dock påvisat att det som en del av riskanalysverktyget finns en definition för hur information inom Region Skåne ska klassificeras utifrån risk. Definition av hur information ska klassificeras utifrån risk i olika känslighetsnivåer behöver formuleras som en instruktion till verksamheten för att säkerställa ändamålsenlig hantering av information i verksamheten. Då en viss informationstillgång klassificeras utifrån risk ska risken bedömas utifrån negativ påverkan på verksamheten vid obehörig åtkomst,

bristande riktighet och bristande tillgänglighet till informationstillgången i verksamhetens dagliga arbete med informationen.

Klassificeringen av informationstillgångar utifrån risk utgör den logiska länken mellan områden för IT-säkerhet och informationssäkerhet och ligger till grund för att tydliggöra vilka krav på IT-säkerhet som bör implementeras för att upprätthålla krav på informationssäkerhet. Granskningen har inte påvisat att det finns dokumenterade riktlinjer för hur krav på IT-säkerhet i system och IT-tjänster samt supporterande infrastruktur (server, databas) ska implementeras i förhållande till den information som systemet/IT-tjänsten hanterar. Granskningen har inte heller påvisat att system och IT-tjänster klassificeras utifrån den information de hanterar, nuvarande klassificering av system är baserad på olika servicenivåer för IT-drift.

2.9.2. Bedömning

Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete med avseende på riskbedömningar, informationsklassificering, uppföljning och dokumentation av informationssystem med tillhörande skyddsåtgärder. Bedömningen baseras på att:

- Det saknas dokumenterade riktlinjer för hur informationstillgångar ska kartläggas och inventeras i verksamheten för att säkerställa att all information beaktas i arbetet med informationssäkerhet. Inventering av information kan göras utifrån verksamhetsprocesser eller informationsflöden i verksamheten.

- Det saknas dokumenterade riktlinjer i form av en instruktion för hur information ska klassificeras utifrån risk i olika känslighetsnivåer för att säkerställa ändamålsenlig hantering av information i verksamheten och hos leverantörer.

- Det saknas en dokumenterad sammanställning över system och IT-tjänster i vilken det tydliggörs risk klassificering utifrån vilken information som systemet och IT-tjänsten hanterar.

- Det saknas dokumenterade riktlinjer för hur krav på IT-säkerhet i informationssystem ska implementeras i förhållande till risk i informationstillgångar de hanterar. T ex bör system som hanterar patientinformation ha teknologi för kryptering implementerad på databasnivå.

2.10. Vilka riskanalyser genomförs inom området informationssäkerhet och vem ansvarar för att de genomförs?

2.10.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.10.1.1. Riskanalyser inom området för informationssäkerhet

Granskningen har påvisat att det utförs olika typer av riskanalyser inom området för informationssäkerhet inom Region Skåne. Det saknas däremot riktlinjer för vilka riskanalyser som ska genomföras inom området för att säkerställa ändamålsenlig hantering av informationstillgångar i verksamheten samt riktlinjer i form av med vilken frekvens riskanalyser ska genomföras.

Vi har under vår granskning tagit del av ett urval av genomförda riskanalyser som främst berör informationssäkerhet vad gäller inköp eller upphandlingar av IT-tjänster eller programvaror. Av dessa framgår det att riskanalysen genomförts vid olika tidpunkter, och i förekommande fall när beslut redan fattats och riskanalys således skett i efterhand.

2.10.1.2. Kontroller för efterlevnad avseende genomförda riskanalyser

Den utförda granskningen har inte kunnat påvisa att kontroller genomförts för att säkerställa att riskanalyser har utförts i verksamheten för de system som hanterar kritiska informationstillgångar. Riskanalyser som inte genomförs enligt riktlinjer i verksamheten bör rapporteras som incidenter kopplat till området och rapporteras som en del av rutinen för incidenthantering.

Vi har noterat att informationssäkerhetschef i sin årliga rapport till Regionstyrelsen om informationssäkerhetsarbetet, behandlar ett urval av de riskanalyser som genomförts i verksamheten. Däremot finns det i nuläget inte dokumenterade riktlinjer för insamling och aggregering av de riskanalyser som genomförts i verksamheterna.

2.10.1.3. Roller och ansvar kopplat till genomförande av riskanalys.

Det saknas dokumentation som beskriver roller och ansvarsområden för genomförande av riskanalyser i verksamheten. Vidare har vi inte identifierat en formell process för ansvarstilldelning och uppföljning av risker över tid.

2.10.2. Bedömning

Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete med avseende på vilka riskanalyser som genomförs inom området informationssäkerhet och vem som ansvarar för att de genomförs. Bedömningen baseras på följande:

- Det existerar riktlinjer för hur en enskild riskanalys ska genomföras inom området för informationssäkerhet men det är inte tydligt definierat vid vilka tillfällen riskanalys ska göras, vilket medför en risk för att inte alla risker i verksamheten identifieras och hanteras för åtgärd.

- Det saknas riktlinjer för hur verksamheten ska arbeta med riskanalyser inom området för informationssäkerhet. Det är oklart vilka riskanalyser som har gjorts inom området då det saknas en sammanställning över utförda analyser.

- Det saknas dokumenterade riktlinjer för uppföljning och bevakning av risker över tid liksom regelbunden riskanalys av informationstillgångar mot bakgrund av omvärldsfaktorer såsom gällande lagar och förordningar samt Region Skånes verksamhetsmål.

- Det saknas dokumenterade riktlinjer för roller och ansvar kopplat till riskanalyser i ett antal nivåer, det är oklart vem i verksamheten som har ett ansvar för att riskanalys ska utföras, hur risker ska ansvars tilldelas för åtgärdshantering, samt vem i verksamheten som har ett ansvar för att följa upp utvecklingen av åtgärder för att hantera identifierade risker.

- En förutsättning för att verksamheten ska kunna genomföra ändamålsenliga riskanalyser inom området informationssäkerhet är att rutin för informationsklassificering är definierad och implementerad, vilket inte är fallet i nuläget.

2.11. Vilken grad av utbildning genomförs av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter?

2.11.1. Iakttagelser

För att besvara kontrollfrågan har granskningen fokuserat på nedanstående områden.

2.11.1.1. Riktlinjer för utbildning inom område för informationssäkerhet

Det saknas dokumenterade riktlinjer för utbildning för Region Skånes medarbetare inom område för informationssäkerhet.

Vi har noterat att vid tillfället för vår granskning så finns en tillgänglig e-utbildning inom informationssäkerhet etablerad. Innehållet i utbildningen uppdateras inte löpande då nuvarande innehåll inte uppdaterats på 1,5 år. Utbildningen är inte obligatorisk.

Vi har noterat att det görs enskilda utbildningsinsatser inom informationssäkerhet, bland annat av informationssäkerhetssamordnare och personuppgiftsombud.

Vi har noterat att det saknas dokumenterade riktlinjer för hur information om risker och hot med informationshantering ska bevakas, samlas in och kommuniceras till medarbetarna i verksamheten.

Vi har även noterat att det i nuläget inte heller görs någon samlad uppföljning eller nyckeltalsrapportering av genomförda kurser och utbildning i informationssäkerhet på medarbetarnivå.

2.11.2. Bedömning

Vi bedömer att Region Skåne delvis bedriver ett ändamålsenligt informationssäkerhetsarbete med avseende på vilken grad av utbildning som genomförs av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter. Bedömningen baseras på följande:

- Det saknas dokumenterade riktlinjer för hur löpande information om nya risker och hot med informationshantering ska kommuniceras till medarbetare i verksamheten (t ex vid olika typer av riktade falska e-mail vilka skickas ut till anställda

inom Region Skåne). Det är även oklart var information ska publiceras samt vem inom Region Skåne som har till uppgift att publicera denna typ av information.

- Det finns e-utbildningar att tillgå för medarbetare inom Region Skåne för att informera om risker med informationshantering. Utbildningen är inte obligatorisk och det sker ingen aktiv uppföljning av vilka medarbetare som har genomgått utbildningen.

3. Revisionell bedömning

Uppdragets revisionsfråga är:

Har Region Skåne på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet?

Vår bedömning är att Region Skåne inte har ändamålsenliga rutiner och processer för att hantera IT-säkerhet och informationssäkerhet. De bedömningar som vi lämnar för kontrollmål 1-11 visar att det inte finns en fungerande styrmodell implementerad, inte heller tillräcklig omfattning av resurser, styrande dokument och rutiner till grund för att säkerställa ändamålsenlig hantering av informationstillgångar inom Region Skåne.

3.1. Bedömningar mot kontrollmål

Kontrollmål	Kommentar
Kontrollmål 1 Bedriver Region Skåne ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för informationstillgångarna utifrån dagens krav?	**Inte uppfyllt** Vi bedömer att Region Skåne inte bedriver ett informationssäkerhetsarbete som ger ett ändamålsenligt skydd för verksamhetens informationstillgångar utifrån dagens krav.
Kontrollmål 2 Finns erforderliga resurser och är arbetet med informationssäkerhet tillräckligt prioriterat i förhållande till de risker som finns?	**Inte uppfyllt** Vi bedömer att Region Skåne inte har erforderliga resurser och inte arbetar med informationssäkerhet tillräckligt prioriterat i förhållande till de risker som finns.
Kontrollmål 3 Hur säkerställs medborgarens integritet (patientdatalagen) och hur skyddas patientinformation i journalsystem mot obehöriga?	**Delvis uppfyllt** Vi bedömer att Region Skåne endast delvis säkerställer medborgarens integritet (patientdatalagen) och skyddar patientinformation i journalsystem mot obehöriga.
Kontrollmål 4 Har Region Skåne ett godtagbart skydd för sina databaser och system mot utomstående intressen som antingen vill komma åt information eller skada verksamheten genom att slå ut systemen eller göra dem otillgängliga på annat sätt?	**Delvis uppfyllt** Vi bedömer att Region Skåne endast delvis säkerställer ett godtagbart skydd för sina databaser och system mot utomstående intressen som antingen vill komma åt information eller skada verksamheten genom att slå ut systemen eller göra dem otillgängliga på annat sätt.

Kontrollmål 5 Hur hanteras avvikelser i form av avbrott och säkerhetsintrång på system och data och vilken beredskap och resurser finns för omedelbara åtgärder vid allvarliga incidenter?	**Delvis uppfyllt** Vi bedömer att Region Skåne delvis hanterar avvikelser i form av avbrott och säkerhetsintrång ändamålsenligt på system och data och att det delvis finns beredskap och resurser för omedelbara åtgärder vid allvarliga incidenter.
Kontrollmål 6 Hur hanteras IT-säkerheten då tjänster är outsourcade och system och applikationer drivs av extern part? Beaktas informationssäkerhetskrav vid upphandlingar, t ex av tjänster och programvaror?	**Delvis uppfyllt** Vi bedömer att Region Skåne delvis bedriver ett ändamålsenligt informationssäkerhetsarbete då tjänster är outsourcade och system och applikationer drivs av extern part, samt vid upphandlingar, t ex av tjänster och programvaror.
Kontrollmål 7 Hur hanterar Region Skåne så kallade molntjänster för lagring av data och vilka riskanalyser, rutiner och regler finns inom detta område för att hantera information som innehåller sekretess eller patientuppgifter?	**Inte uppfyllt** Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete avseende molntjänster för lagring av data.
Kontrollmål 8 Hur säkerställs att medborgaren får relevant, korrekt och säker information via hemsida och nya appar för e-hälsa m m?	**Delvis uppfyllt** Vi bedömer att Region Skåne delvis bedriver ett ändamålsenligt informationssäkerhetsarbete för att säkerställa att medborgaren får relevant, korrekt och säker information via hemsida och nya appar för e-hälsa m m.
Kontrollmål 9 Hur hanterar Region Skåne riskbedömningar, informationsklassificering, uppföljning och dokumentation av informationssystem med tillhörande skyddsåtgärder?	**Inte uppfyllt** Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete med avseende på riskbedömningar, informationsklassificering, uppföljning och dokumentation av informationssystem med tillhörande skyddsåtgärder.
Kontrollmål 10 Vilka riskanalyser genomförs inom området informationssäkerhet och vem ansvarar för att de genomförs?	**Inte uppfyllt** Vi bedömer att Region Skåne inte bedriver ett ändamålsenligt informationssäkerhetsarbete med avseende på vilka riskanalyser som genomförs inom området informationssäkerhet och vem som ansvarar för att de genomförs.
Kontrollmål 11 Vilken grad av utbildning genom-	**Delvis uppfyllt** Vi bedömer att Region Skåne delvis bedriver

förs av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter?	ett ändamålsenligt informationssäkerhetsarbete med avseende på vilken grad av utbildning som genomförs av Region Skånes personal kring informationssäkerhet vid t ex lagring och hantering av känsliga uppgifter om enskilda patienter.

4. Bilagor

Bilaga 1 – Intervjuade personer

- **Johan Reuterhäll**, Informationssäkerhetschef
- **Anders Roos,** Processansvarig Incident- och Problem Management samt Avvikelsehantering inom IT Processer & avtal, Avdelning för Digitalisering och IT
- **Per Bergstrand,** Personuppgiftsombud
- **Jonas Johansson,** Informationssäkerhetssamordnare SUS
- **Malin Nyman,** Informationssäkerhetssamordnare förvaltningen Kryh
- **Louise Strand**, Inköpsdirektör
- **Thomas Schuster,** IT-säkerhetsarkitekt
- **Stefan Schörling,** IT-säkerhetsansvarig
- **Pia Ferhm,** Systemansvarig för Melior, intyg, tillväxtjournalen, Support system, Avdelning för Digitalisering och IT
- **Marie Rosendal**, Enhetschef, Support system IT teknik och förvaltning, Avdelning för Digitalisering och IT

Bilaga 2 – Granskade dokument

- Instruktion för incidenthantering, *2016-09-07 (Arkiverad)*
- Dataintrång- åtgärder, *Beslutad 2013-10-09*
- Informationssäkerhetsincidenter Instruktion, *Beslutad 2017-03-03*
- Tillämpningsanvisning-skydd-mot-störningar & angrepp, *2011-04-19*
- Kravspecifikation-informationssäkerhet, *2012-12-07*
- Kravkatalog för IT-stöd inom Region Skåne v2.0, *2017-04-19*
- Förtydligande informationssäkerhet, *2016-06-23*
- Beslut ledningssystem informationssäkerhet, *Beslutad 2011-05-24*
- Kommunikationsstrategi Region Skåne- *Kommunikationsstrategin grundar sig på varumärkespolicyn och kommunikationspolicyn som är två av Region Skånes styrande dokument och beslutade av regionfullmäktige 2012-09-25*
- Patientuppgifter instruktion om styrning av åtkomst till patientuppgifter, *Beslutad 2017-03-01*
- Säkerhetspolicy, *Fastställd av Regionfullmäktige 2003-06-18*
- Kommunikationspolicy, *2012-09-25*
- Anvisningar för roller och ansvar på Skåne.se, *2015-01-28*

- Programvarutillgångars hantering från anskaffning till avveckling, *Beslutad 2011-09-06*
- Rf 136-11 Upphandlingspolicy, *Beslutad 2011-09-06*
- Region Skåne varumärkesguide 2013, *Beslutad i Regionfullmäktige 25 september 2012*
- Regelverk för användning av IT-baserade verktyg i Region Skåne, *Beslutad 2016-12-08*
- Införande av strategi sociala medier i Region Skåne, *Beslutad 2017-01-24*
- TCS 2.0 Riskanalys- Resultat och konsekvenser*, 2016-03-18*
- Riskanalys om sms-påminnelse och journaldokumentation inom barnsjukvård, *maj-juni 2016*
- Personuppgiftsbehandling i Region Skåne - Sammanställning av regler och krav, *Fastställt 2016-07-18*
- Loggkontroll - granskning av åtkomst till patientuppgifter, *Beslutad 2013-07-01*
- Bakgrund och beskrivning av informationssäkerhet, PDL och säkerhetstjänster i Region Skåne- *2012-12-07*
- Förslag till organisation för informationssäkerhetsarbetet i Region Skåne, *Fastställt 2009-12-21*
- PUO-regionstyrelsen, 1998-11-24
- Upphandlingspolicy Region Skåne, Region Skånes Upphandlingspolicy *beslutades av Regionfullmäktige 2011-11-28 samt Tillämpningsanvisningarna är godkända av Koncernledningen (KL) 2013-02-04.*
- Rapport om informationssäkerhetsarbetet, 2016-11-21
- ITMT organisationsskiss, 2016-01-27
- Yttrande HSM, 2016-07-15
- Ansvarsmodell
- Bakgrund och beskrivning av informationssäkerhet, PDL och säkerhetstjänster i Region Skåne, *2012-12-07*
- Definitioner SLA nivåer, *2015-11-12*
- Patientsäkerhetsberättelse, Medicinsk service 2016, *2017-02-12*
- Instruktioner om styrning av behörigheter för åtkomst till uppgifter om patienter, *Beslutad 2017-03-01*
- Hantering av patientuppgifter för kvalitetssäkring inom vård och behandling i Region Skåne, *Beslutad 2014-06-25*
- Anvisning- Säkerhetsuppdateringar för IT infrastruktur, *Fastställd 2011-06-29*

- Tillämpningsanvisning för skydd mot störningar och angrepp på IT-infrastrukturen, *2017-05-15*
- Riskanalys SG Melior Teknik, *2013-03-22 rev 2016-12-09*
- Systemkarta- Beskrivning av Infrastruktur
- Backuprutin- Melior, *2017-03-03 (skapat av Tieto)*
- Referensarkitektur, *2012-02-20 (skapat av Tieto)*
- Disaster Recovery Plan för Melior
- SLA-nivåer, *2016-01-16 (skapat av Tieto)*

Magnus Karmborg
(Projektledare)

Mats Malmberg
(Projektledare)

Pär Sturesson
(Kvalitetssäkrare)