Västerbottens läns landsting

2017-11-09 REV 26:3–2017

Landstingsstyrelsen och
Hälso- och sjukvårdsnämnden

Granskning av IT-systemens robusthet

Landstingets revisorer har i flera granskningar uppmärksammat brister i kontrollen av landstingets IT- och informationssäkerhet (nr 23/2010, 17/2014, 22/2014 och 18/2015). En uppföljande granskning visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har vidtagit tillräckliga åtgärder med anledning av revisorernas rekommendationer. Endast fyra av 20 lämnade rekommendationer har blivit helt genomförda.

En slutsats från den uppföljande granskningen är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en tillräcklig styrning, uppföljning och kontroll av IT- och informationssäkerheten inom deras ansvarsområden:

- Fullmäktige har inte givits möjlighet att ta ställning till en policy för arbetet med informationssäkerhet i landstinget. I landstinget saknas en sådan policy.
- Det finns inga landstings- och nämndsövergripande riskanalyser inom området för informationssäkerhet.
- Riktlinjer och regler för informationssäkerhet har inte kommuniceras till berörda medarbetare i landstinget.
- Det saknas en tillräcklig uppföljning och kontroll av att verksamheterna följer riktlinjer och regler för informationssäkerhetsarbetet.

Nedan återger vi några konkreta brister som granskningsrapporten identifierat:

- Det saknas en komplett förteckning över landstingets informationssystem.
- För samtliga av landstingets verksamhetskritiska system finns det inte informationsklassning och beslut om längsta acceptabla tid som systemen kan få vara ur funktion. Det saknas också beslut om vilken prioriteringsordning som ska gälla vid återstart i händelse av IT-avbrott.
- Det saknas systematik som säkerställer att det görs regelbundna kontroller över anställdas behörigheter till IT-system.

Västerbottens läns landsting
Landstingshuset, Köksvägen 11, 901 89 Umeå
Telefon: 090-785 00 00, telefax: 090-13 68 82
E-post: landstinget@vll.se Org.nr: 232100-0222
VAT-nr: SE232100022201 Bankgiro 5728-3061

- Det saknas beslut om vilka kriterier som ska gälla för serverhallarnas fysiska säkerhet. Det saknas också periodiska kontroller av tillträde till serverhallar och servrar och inloggningar i databaser.
- Det har under en lång tid inte genomförts några penetrationstester av landstingets IT-system.
- Landstingets personuppgiftsombud och informationssäkerhetsstrateg saknar dokumenterade uppdragsbeskrivningar.

Rekommendationer

Med anledning av granskningens iakttagelser rekommenderar vi landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa:

- Att fullmäktige får ta ställning till ett förslag på informationssäkerhetspolicy för landstinget. Förslaget till policyn bör bland annat inkludera styrelser och nämnders ansvar för informationssäkerhet, inriktning och övergripande mål för informationssäkerhet samt struktur för riskbedömning och riskhantering.
- Att det på landstings- och nämndsövergripande nivå och bland verksamheterna finns riskanalyser för informationssäkerhetsområdet.
- Att riktlinjer och regler för informationssäkerhet är väl kända bland berörda medarbetare i landstinget.
- En tillräcklig uppföljning av informationssäkerhetsarbetet inom sina ansvarsområden.
- Att tidigare lämnade rekommendationer blir genomförda. Exempelvis:
    - Att det genomförs regelbundna kontroller av anställdas behörigheter.
    - Att det fattas beslut om vilken prioritetsordning som ska gälla vid återstart i händelse av avbrott i IT-systemen.
    - Att det finns en förteckning över landstingets samtliga informationssystem där det framgår vilka av dessa som är att betrakta som kritiska för verksamheten.
    - Att det finns beslut om vilka kriterier landstingets serverhallar ska uppfylla avseende fysisk säkerhet men även att säkerheten i de befintliga hallarna höjs till dess att andra lokaler finns tillgängliga.

- Att övriga i granskningen uppmärksammade brister blir åtgärdade. Exempelvis:
    - Att beslut om längsta acceptabla tid som informationssystem kan vara ur funktion fattas för alla verksamhetskritiska system.
    - Att kontroller av programförändringar i IT-systemen genomförs.
    - Att periodiska kontroller av användare med access till servrar och databaser genomförs.

- Att det görs kontroller av inloggning till och aktivitet i servrar och databaser.
- Att det genomförs penetrationstester.
- Att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar.

Vid revisorernas överläggning den 9 november 2017 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 3/2017) lämnar revisorerna för yttrande till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 2 mars 2018.

För landstingets revisorer

Christer Fessé
Ordförande

Bert Öhlund
Vice Ordförande

LANDSTINGSREVISIONEN

Granskning av IT-systemens robusthet

Rapport nr 03/2017

Västerbottens läns landsting

November 2017

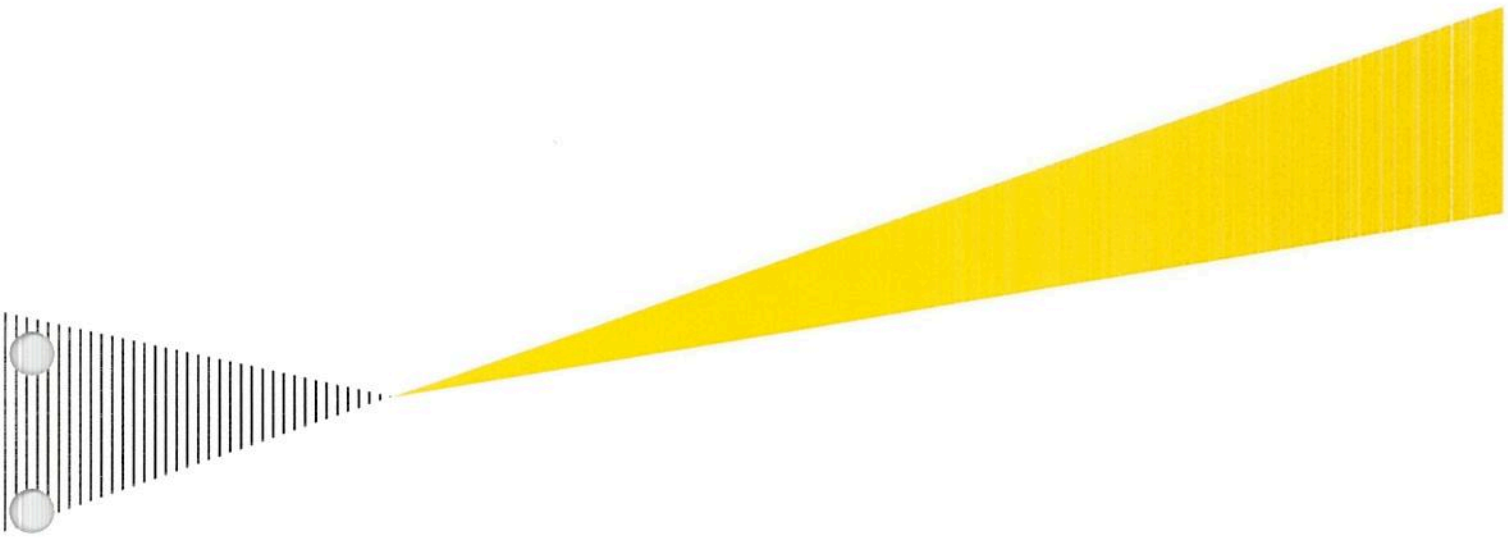
Hardik Patel, Ann-Mari Ek, Markus Bruus och Rebecka Arén, EY

Diarienummer: REV 26:2–2017

Building a better working world

2017-11-02

Granskning av IT-systemens robusthet – Västerbottens läns landsting



Building a better working world

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Västerbottens läns landsting genomfört en granskning av IT-systemens robusthet. Syftet med granskningen är att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer en tillräcklig styrning, uppföljning och kontroll av IT-systemen så att en säker hälso- och sjukvård kan bedrivas.

Bedömningen är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en tillräcklig styrning, uppföljning och kontroll av IT-systemen. Bedömningen grundas på att landstingsstyrelsen och hälso- och sjukvårdsnämnden ***inte*** har säkerställt:

- tillräcklig styrning, uppföljning och kontroll av informations-säkerhetsarbetet,
- ändamålsenlig rapportering för arbetet med informationssäkerhet,
- ändamålsenlig kommunikation och utbildning gällande riktlinjer för informationssäkerhet,
- att det finns en övergripande informationssäkerhetspolicy,
- att informationsklassning genomförts för system som bedöms som verksamhetskritiska,
- implementering av de rekommendationer som getts i tidigare granskningar (av 20 lämnade rekommendationer i tidigare revisionsrapporter inom området har fyra implementerats, sju delvis implementerats och nio ej implementerats),
- att det bedrivs ett systematiskt övergripande arbete med riskanalyser,
- att kontroll av programförändringar genomförs,
- att förteckning över landstingets samtliga informationssystem upprättats,
- att det genomförs en periodisk kontroll av användare med access till servrar och databaser,
- att det genomförs någon kontroll av inloggning till och aktivitet i servrar och databaser,
- att det är tillräcklig fysisk säkerhet till serverhallar och att beslut fattats för vilka kriterier serverhallar ska uppfylla avseende fysisk säkerhet,
- att beslut fattats för längsta acceptabla tid som informationssystem bedöms kunna vara ur funktion för alla verksamhetskritiska system,
- att externa och interna penetrationstester genomförts, samt
- att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar.

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att:

- stärka den landstings- och nämndsövergripande styrningen och införa fler kontrollrutiner,
- aktivt följa upp arbetet med informationssäkerheten alternativt besluta om utökad intern kontroll inom området och öka kraven på återrapportering i patientsäkerhetsberättelsen,
- säkerställa att utbildning inom informationssäkerhet för medarbetare inom respektive styrelse/nämnds ansvarsområden koordineras på landstings- och nämndsövergripande nivå och görs obligatorisk, samt att deltagandet följs upp,
- säkerställa att relevanta styrdokument kommuniceras ut till alla berörda anställda,
- tillse att en informationssäkerhetspolicy arbetas fram för landstingsfullmäktiges beslut (policyn bör inkludera minst styrelse och nämnders ansvar, inriktning och övergripande mål, befogenheter, betydelsen av informationssäkerhet samt struktur för riskbedömning och riskhantering),
- genomföra informationsklassning,
- implementera rekommendationer från tidigare granskningar. Av de 16 rekommendationerna som inte eller delvis implementerats och som inte lyfts separat i denna granskning anses följande vara av särskild vikt:
    - Det bör genomföras regelbundna kontroller av anställdas behörigheter
    - Det bör fattas beslut om vilken prioritetsordning som ska gälla vid återstart i händelse av avbrott för IT-system,
- utarbeta landstingsövergripande riktlinjer för riskidentifiering och riskhantering, särskilt kartläggning av kritisk information, IT-system och hårdvara samt att det utförs riskanalyser för dessa,
- tillse att arbetet med riskanalyser utförs regelbundet och vid större verksamhetsförändringar,
- säkerställa att kontroll av programförändringar i verksamhetskritiska system genomförs,
- säkerställa att en inventering av landstingets informationssystem genomförs och att en förteckning över samtliga system sammanställs, där det framgår vilka av dessa som är att betrakta som kritiska för verksamheten,
- säkerställa att periodisk kontroll av fysisk tillgång till servrar och databaser genomförs,
- säkerställa att inloggning till servrar och databaser kontrolleras och att implementering av revisionsloggar för aktivitet i kritiska databaser och servrar genomförs,
- säkerställa att beslut tas om kriterier för vad en serverhall inom landstinget ska uppnå med avseende på fysisk säkerhet, att säkerheten i de befintliga hallarna höjs till dess att andra lokaler finns tillgängliga samt att en tidsplan för att flyta servrarna fastställs,
- säkerställa att längsta acceptabla tid verksamhetskritiska system kan vara ur funktion fastställs,
- säkerställa att det genomförs interna och externa penetrationstester i syfte att identifiera brister i IT-miljön, samt

- säkerställa att personuppgiftsombudet och informations-säkerhetsstrategen har dokumenterade uppdragsbeskrivningar.

Building a better working world

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Landstingets revisorer har baserat på tidigare granskningar samt genomförd riskanalys beslutat att genomföra en granskning av IT- och informationssäkerhetsarbetet inom Västerbottens läns landsting (VLL). Intrång i IT- och informationssystem blir allt mer vanligt och utgör därför en central risk för en offentlig verksamhet, vilken handhar en mängd känslig information. Vidare föreligger risk att fel uppstår i kritiska processer om information inte är tillförlitlig eller saknas. Brister i det systematiska IT- och informationssäkerhetsarbetet innebär därmed risk för att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte kan efterleva gällande lagkrav och således bedriva en säker hälso- och sjukvård.

1.2. Syfte

Syftet med granskningen är att ge landstingets revisorer underlag för att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer en tillräcklig styrning, uppföljning och kontroll av IT-systemen så att en säker hälso- och sjukvård kan bedrivas.

1.3. Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom granskning av erhållna dokument, såsom riktlinjer, rutiner och tidigare granskningsrapporter.

1.4. Revisionsfrågor

Granskningen beaktar följande revisionsfrågor:

- Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en ändamålsenlig organisation med tydlig ansvarsfördelning avseende IT- och informationssäkerhetsarbetet?
- Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att det finns riskanalyser gällande informationssäkerhet dokumenterade och uppdateras denna dokumentation löpande?
- Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig styrning av drift- och kontinuitetsfrågor?
- Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att drift- och kontinuitetsplanering genomförs på ett ändamålsenligt sätt utifrån de behov av informationssäkerhet som verksamheterna har?
- Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig fysisk säkerhet till serverhallar?

- Hur väl har landstingsstyrelsen och hälso- och sjukvårdsnämnden implementerat rekommendationerna för att minska de brister i informationssäkerheten som lyfts i tidigare granskningar?
- Säkerställer landstingsstyrelsen och hälso- och sjukvårdsnämnden en tillräcklig uppföljning och kontroll av arbetet med informationssäkerhet?

1.5. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. Revisionskriterier kan ofta hämtas från lagar och förarbeten, föreskrifter och interna regelverk, policys och fullmäktigebeslut.

I denna granskning har revisionskriterierna utgjorts av:

- Kommunallagen, 6 kap. § 7
  - Nämnder och styrelser ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de föreskrifter som gäller för verksamheten. Nämnder och styrelser ska också se till att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.
- Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården
  - Enligt 7 kap 1 § ska patientsäkerhetsberättelsen, utöver vad som framgår av patientsäkerhetslagen och ledningsföreskriften (SOSFS 2011:9), innehålla uppgifter om uppföljningar av informationssäkerheten, riskanalys enligt föreskriften, åtgärder av större betydelse som har vidtagits för förbättring av informationssäkerheten, utvärdering av skydd mot obehörig åtkomst samt granskning av personalens journalföring. Föreskrifterna kompletterar patientdatalagen och ska tillämpas då vårdgivare behandlar patienters personuppgifter inom hälso- och sjukvården.
- Etablerad praxis inom IT- och informationssäkerhetsområdet som bygger på internationella standarder.

1.6. Metod

Revisionsfrågorna har besvarats genom en granskning som utförts mot etablerad praxis inom IT- och informationssäkerhetsområdet vilken bygger på ISO27000. Granskningen har genomförts genom en dokumentstudie av styrdokument, samt genom att intervjua berörda funktioner (se bilaga 1). Samtliga intervjuade har beretts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Granskningen har även kvalitetssäkrats.

1.7. Definitioner

Attack- och penetrationstester: Test av informationssystem, nätverk eller webbapplikationer för att identifiera sårbarheter vilka kan utnyttjas av angripare.

Avbrottsplan: Dokumentation av de återstarts- och reservrutiner för datadriften som ska vidtas inom ramen för ordinarie drift för att informationssystemen ska kunna återstartas inom fastställd tid.

Batchjobb: Schemalagd överföring av data i ett program eller dator utan manuell intervention.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Informationsägare: Ansvarar för den verksamhet vars information ska hanteras. Äger och ansvarar för att informationen är riktig och tillförlitlig.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer. Planeringen bör också innefatta framtagande av avbrotts- och katastrofplan.

MIM: Major Incident Management är en process som följs av informatiken vid större incidenter/avbrott.

Patchning: Rutin för uppdatering av skydd mot skadlig programkod.

Patientsäkerhetsberättelse: Lagstadgad, årligen avlagd rapport vilken redovisar för vårdgivarens strategi, mål och resultat av dess arbete med patientsäkerhet.

Personuppgiftsombud: Särskilt utsedd person vilken tillser att personuppgifter behandlas på korrekt och lagenligt sätt inom organisationen.

Programförändring: Förändring av källkod i en applikation

Systemsäkerhetsanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Systemägare: Organisationens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.

2. Analys

2.1. Organisation och ansvarsfördelning

Inom Västerbottens Läns Landsting (VLL) innehas det övergripande ansvaret för informationssäkerhetsarbetet av landstingsfullmäktige, vilka enligt landstingets ledningssystem bär ansvar för att fastställa landstingets informationssäkerhetspolicy. Av reglementet för landstingsstyrelsen framgår att styrelsen ansvarar för de informationssystem som stödjer landstingets verksamhet. Landstingsstyrelsen ska även säkerställa att riktlinjer för informationssäkerhet finns och att dessa efterlevs. Enligt hälso- och sjukvårdsnämndens reglemente är nämnden ansvarig vårdgivare för sjukhusvården och tandvården. Av kommunallagen framgår att nämnden har ansvar att verksamheterna inom nämndens ansvarsområden genomförs på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Nämnden har ansvar att se till att vården genomförs i enlighet med patientsäkerhetslagen (2010:659), patientdatalagen (2008:355), personuppgiftslagen (1998:204) och annan lagstiftning samt förordningar och föreskrifter som gäller för vårdgivare. Styrelsen och hälso- och sjukvårdsnämnden har således ansvar för att tillse och följa upp att informationssäkerhetsarbetet i landstinget sker på ändamålsenligt sätt, och att nödvändiga resurser finns för att upprätthålla detta arbete.

Informationsägare

Roller och ansvar för informationssäkerhetsarbetets olika delar är fördelat på olika funktioner inom organisationen. I organisationen är respektive verksamhetschef informationsägare inom sitt verksamhetsområde vilket innebär att denne också ansvarar för att medarbetarna erhåller den information och utbildning som krävs gällande de policys, riktlinjer och instruktioner som beslutats. Verksamhetschefen ansvarar även för att årligen genom patientsäkerhetsberättelsen återrapportera till ledningen gällande de risker, analyser och genomförda åtgärder som vidtagits i verksamheten utifrån dess informationsansvar.

IT-säkerhetsansvar

Basenhet informatik Västerbotten, organiserat under verksamhetsområde Digitalisering och Medicinteknik, ansvarar för den tekniska IT-säkerheten. I detta ansvar ingår att upprätthålla en adekvat säkerhet inom nät, klientplattformar, servrar och lagring samt drift av system.

Alla IT-system i landstinget ska ha en utsedd systemägare, vilken ansvarar för det avsedda IT-systemets säkerhet och för att detta fungerar på avsett sätt. Systemägarna har i majoriteten av fallen sin organisatoriska tillhörighet utanför Informatik Västerbotten. Utav IT-systemen har ett 50-tal bedömts som verksamhetskritiska och driftas hos informatik Västerbotten. Denna lista beslutades i samråd mellan leveransansvariga på informatik Västerbotten och respektive systemägare. Tjänsteman i Beredskap och chefsläkargruppen har också har varit informerad i beslutet och getts tillfälle att påverka beslutet. Beslutet togs för ca 10 år sedan.

Övriga ansvarsområden

Inom landstinget finns sedan 2015 ett personuppgiftsombud, vilken även fått bistå organisationen i frågor rörande informationssäkerhet då ingen dedikerad funktion har funnits för detta. Vid tidpunkten för granskningen har en informationssäkerhetsstrateg nyligen tillträtt. Varken personuppgiftsombudet eller informationssäkerhetsstrategen innehar i nuläget någon formell, dokumenterad uppdragsbeskrivning. Informationssäkerhetsstrategen rekryterades med syfte att koordinera och systematisera arbetet med informationssäkerhet inom landstinget, agera som länk mellan verksamhetens olika funktioner med informationssäkerhetsansvar samt vidareutveckla rutiner för rapportering till landstingsstyrelsen och hälso- och sjukvårdsnämnden.

Styrdokument

Landstingsstyrelsen har utfärdat två styrande dokument för arbetet med informationssäkerhet; riktlinje för informationssäkerhet förvaltning och drift, samt riktlinje för informationssäkerhet användare. Dessa dokument beskriver övergripande det ansvar och de befogenheter som råder inom organisationen. Det finns inte någon separat informationssäkerhetspolicy. Det finns en övergripande kvalitet- och säkerhetspolicy (187886), men denna behandlar dock inte explicit informationssäkerhet.

Uppföljning och utbildning

Det systematiska arbetet med att tillse att verksamhetscheferna, som innehar informationsansvaret, har erforderlig kunskap om informationssäkerhet är bristfälligt. Detta då avsaknad av landstingsövergripande koordinering, uppföljning och utbildning av arbetet kan noteras. Tidigare granskningar har rekommenderat landstinget att undersöka huruvida basenhet informatik Västerbotten, vilka besitter den tekniska kompetensen, kan bistå verksamheterna i arbetet med att upprätthålla en god informationssäkerhet. Något sådant systematiskt arbete förekommer inte i nuläget.

Informatik Västerbotten har skapat en e-kurs i informationssäkerhet riktad till användare av informationssystem inom landstinget. Denna utbildning är inte obligatorisk och det sker ingen uppföljning eller kontroll av att användare deltagit. Det kan inte heller klargöras huruvida den riktlinje för informationssäkerhet som riktar sig till användare har kommunicerats ut till anställda eller om anställda erhållit någon utbildning i relation till denna på annat håll. Av intervjuer framgår att det finns verksamhetschefer som inte har kännedom om riktlinjen och som inte vet om de anställda har fått någon utbildning inom området.

Patientsäkerhetsberättelse

Tidigare granskningar har påvisat att landstingsstyrelsen och hälso- och sjukvårdsnämnden ej erhållit tillfredställande återrapportering i relation till arbetet med informationssäkerhet i landstinget, vilket lett till att de inte haft en helhetsbild av informationssäkerheten i organisationen. Vid tidpunkten för granskningen har arbetet initierats genom att inkludera en informationssäkerhetsberättelse i den årliga patientsäkerhetsberättelsen. Denna skall enligt de riktlinjer som ges i landstingets styrdokument och i HSLF-SF 2016:40 7 kap 1 § behandla risker, analyser och genomförda åtgärder som vidtagits i verksamheten utifrån dess informationssäkerhetsansvar. Information till grund för detta har inhämtats från verksamhetschefer, informatik Västerbotten, personuppgiftsombud samt e-

hälsoenheten. I egenskap av informationsägare är verksamhetscheferna en viktig källa till insyn i detta arbete. Verksamhetschefernas bidrag till 2016 års Patientsäkerhetsberättelse gällande informationssäkerhet var dels att sammanställa information kring avbrott, dels att svara på frågan huruvida loggkontroller genomförs i journalsystemet. Enligt patientsäkerhetsberättelsen genomförde 21 procent av slutenvården inte loggkontroller alls eller genom egna varianter, såsom vid behov eller kvartalsvis. Inom primärvården uppgav fyra av femton verksamheter att de inte har genomfört loggkontroller och två av femton lämnade inget svar på frågan. Landstingsstyrelsen tog 2017-04-04/§50 del av patientsäkerhetsberättelsen. Hälso- och sjukvårdsnämnden tog del av patientsäkerhetsberättelsen 2017-04-12/§38.

Internkontroll

Landstingsstyrelsen beslutade 2016-12-13/§256 om internkontrollplan för 2017, i vilken följande kontrollområden ingår:

- *Risk för att avbrottsplanering/reservrutiner inte finns i verksamheten.*

  Kontroll av antal basenheter inom styrelsens ansvarsområde vilka har en avbrottsplan/reservrutin för IT, telefoni, elförsörjning, vattenleverans och värmebölja. En fullständig kontroll av inskickade planer/rutiner ska genomföras av beredskapssamordnare i november och återrapporteras till landstingsstyrelsen i årsrapporten. Vid tidpunkten för granskningen (oktober 2017) var denna kontroll ännu inte genomförd.

- *Risk för att verksamhetsstörning sker till följd av att drift för patientkritiska IT-system inte kan säkerställas.*

  Kontroll av antal större IT-störningar som lett till händelseanalys och som påverkat användning av verksamhetskritiska system inom primärvården. Fullständig kontroll av alla större IT-störningar under perioden februari till maj ska göras av verksamhetschef informatik och återrapporteras till landstingsstyrelsen vid delårsrapport per augusti. Under 2017 har det skett två driftstörningar varpå händelserapporter upprättats och redovisats genom internkontrollplanen.

- *Risk för att behörighet till administrativa system inte avslutas vid avslutad anställning.*

  Kontroll att attestregistret för beslutsattestanter i Agresso är korrekt avseende att rätt personer har behörighet och att behörighet är avslutad för medarbetare som har avslutat sin anställning. Detta kontrolleras via stickprov under februari och september av ekonomidirektör och avrapporteras till landstingsstyrelsen vid delårsrapport per april och augusti samt årsrapport.

Samma kontrollområden fanns med i 2016 års interna kontrollplan. Revisorernas granskning av internkontrollarbetet (rapport 18/2016) visade att rapportering av kontroll av att basenheter har avbrottsplaner saknades. Kontroll av större IT-störningar hade genomförts men på ett otydligt sätt. Kontroll av behörighet till administrativa system hade genomförts, dock bedömdes rapporteringen som bristfällig.

Hälso- och sjukvårdsnämnden beslutade 2016-09-29/§131 om intern kontrollplan för 2017, i vilken följande kontrollområden ingår:

- *Risk att avbrottsplaner/reservrutiner inte finns bland nämndens basenheter*

  Kontroll av antal basenheter inom nämndens ansvarsområde som har en avbrottsplan/reservrutin för IT, telefoni, elförsörjning, vattenleverans och värmebölja. En fullständig kontroll av inskickade planer/rutiner ska genomföras av beredskapssamordnare i november och återrapporteras till landstingsstyrelsen i årsrapporten.

- *Risk att verksamhetsstörning sker till följd av att drift för patientkritiska IT-system inte kan säkerställas*

  Kontroll av antal större IT-störningar som lett till händelseanalys och som påverkat användning av verksamhetskritiska system inom sjukhusvård och tandvård. Fullständig kontroll av alla större IT-störningar under perioden februari till maj ska göras av verksamhetschef informatik och återrapporteras till hälso- och sjukvårdsnämnden vid delårsrapport per augusti. Under 2017 har det skett två driftstörningar varpå händelserapporter upprättats och redovisats genom internkontrollplanen.

- *Risk för att behörighet till administrativa system inte avslutas vid avslutad anställning.*

  Kontroll att attestregistret för beslutsattestanter i Agresso är korrekt avseende att rätt personer har behörighet och att behörighet är avslutad för medarbetare som har avslutat sin anställning. Detta ska kontrolleras via stickprov under februari och september av redovisningschef och avrapporteras till hälso- och sjukvårdsnämnden vid delårsrapport per april samt årsrapport.

Samma kontrollområden fanns med i 2016 års interna kontrollplan. Revisorernas granskning av internkontrollarbetet (rapport 18/2016) visade att kontroll av att basenheter har avbrottsplaner hade genomförts men på ett bristfälligt sätt, och att kontroll av större IT-störningar hade genomförts på ett otydligt sätt. Kontroll av behörigheten till administrativa system hade genomförts men rapporteringen bedömdes som bristfällig. Hälso- och sjukvårdsnämnden fick 2017-02-16/§4 återrapportering på internkontrollarbetet 2016. Hälso- och sjukvårdsnämnden beslutade då att uppdra till hälso- och sjukvårdsdirektören att tillse att reservrutiner finns och är kända på alla basenheter. Under granskningen uppgav fyra av fyra intervjuade verksamhetschefer inom vården att reservrutiner finns och är kända.

Övrig rapportering

I landstingsstyrelsens yttrande till revisorerna med anledning av granskningen (nr 18/2015) av behörigheter till journalsystem meddelades att en förstudie om informationssäkerhet skulle påbörjas och slutföras under 2016. Landstingsstyrelsen behandlade 2017-02-01/§17 förstudien av vilken det framgår att det måste vidtas åtgärder inom områdena organisation, ramverk, riskhantering, informations-klassificering och styrning av åtgärder. Bedömningar som görs i förstudien är att det inte bedrivs något sammanhållet strategiskt informationssäkerhetsarbete, att det saknas en ledare för informationssäkerhetsarbetet, att det inte förekommer någon riskhantering inom informationssäkerhetsområdet och att det inte finns någon informationsklassificeringsmetod. Det lämnades en rad rekommendationer, bland annat att förbereda införandet av den nya dataskyddsförordningen. Landstingsstyrelsen beslutade att ge landstingsdirektören i uppdrag att i april återkomma till landstingsstyrelsen med en handlingsplan utifrån genomförd studie.

Landstingsstyrelsen fick 2017-04-04/§52 ta del av handlingsplanen som tagits fram utifrån förstudien. Av handlingsplanen framgår att rekrytering av informationssäkerhetsstrateg pågår och att föreslagna åtgärder i förstudien kommer att påbörjas när denne har tillträtt sin tjänst. Landstingsstyrelsen beslutade att godkänna handlingsplanen och att ge landstingsdirektören i uppdrag att lämna en lägesbeskrivning av informationssäkerhetsarbetet vid landstingsstyrelsens sammanträde i december.

Inspektionen för vård och omsorg (IVO) genomförde 2016 en tillsyn av informationssäkerhetsarbetet som visade att en person inte utsetts att ansvara för informationssäkerhet och att rapporter om informationssäkerhet därför hade uteblivit. IVO begärde att detta skulle åtgärdas och återrapporteras. Landstingsstyrelsen informerades 2017-02-01/§17 om att förvaltningen påbörjat rekrytering av informationssäkerhetsstrateg och att detta hade meddelats IVO.

2.2. Riskanalyser

Övergripande riskanalyser

Landstingsstyrelsen har inte säkerställt ett systematiskt och heltäckande arbete med att genomföra riskanalyser inom landstinget. Det finns inte några riskanalyser för drift, förvaltning eller hantering av information i landstinget.

Informatik Västerbotten använder sig dock av riskanalyser inom förändringsprocessen för IT-system, där det finns dokumenterat i process och styrdokument vad som bör föregå olika typer av systemändringar. Dessa riskanalyser följer miniriskmetoden, där ett riskvärde beräknas genom uppskattning av sannolikheten för att något ska inträffa multiplicerat med konsekvensen det ger. Även anskaffning av informationssystem inom informatik Västerbotten föregås av sådana riskanalyser. För de system vilka ej förvaltas inom informatik Västerbotten finns dock inga formaliserade riktlinjer för huruvida riskanalyser som ska föregå anskaffning och ändring följs upp.

Informationsklassning

Informationsklassning av information som finns i landstingens IT-system har inte genomförts och det finns ingen definitiv plan med tydlig deadline att genomföra det. En informationsklassning bör göras av information i system för att bedöma hur kritisk informationen är i termer av konfidentialitet, riktighet och tillgänglighet.

2.3. IT-drift och kontinuitetsplanering

Styrning av drift- och kontinuitetsplanering

Ansvaret för IT-drift och kontinuitetsplanering, vilket innefattar rutiner och processer för att upprätthålla kontinuitet i landstingets IT-system, är ålagt informatik Västerbotten. Planering för att landstingets verksamheter ska kunna upprätthålla produktionen vid driftstörningar sker inom respektive verksamhetsområde. Systemägaren ska besluta om längsta tid ett IT-system får ligga nere, något som inte skett för 30 av 50 verksamhetskritiska system.

Incidenthantering

Informatik Västerbotten innehar ansvaret för att hantera incidenter, där de processer och rutiner som följs för incidenthantering bygger på Information Technology

Infrastructure Library (ITIL)-ramverket och är dokumenterade i ledningssystemet. ITIL-ramverket är vedertagen internationell praxis och beskriver processer och rutiner för exempelvis incidenthantering. Användare och anställda inom informatik Västerbotten vänder sig alltid till första linjens support, Servicedesk, vid händelse av en incident. Efter en initial bedömning hos Servicedesk eskaleras incidenten till andra linjens support vilken i sin tur vid behov kan eskalera incidenten till leveransansvarig. Leveransansvarig tar sedan beslut om huruvida MIM-processen (Major Incident Management) ska initieras. MIM-processen initieras vid större avbrott i IT-system av särskild vikt för verksamheternas funktion. Vid MIM samlas ledningsgruppen (enhetschef, avdelningschefer samt leveransansvariga) för basenhet informatik Västerbotten, vilka leder det fortsatta arbetet enligt en fastställd process så att incidenten kan hanteras och lösas utan dröjsmål. Ledningsgruppen för informatik Västerbotten för också en dialog med Tjänsteman i Beredskap (TIB) för att bedöma om den inträffade incidenten legitimerar stabsläge. Det finns i dagsläget inga riktlinjer eller rutiner för att göra tester av MIM-processer. Vid tillfällen då MIM används görs dock en utvärdering och uppföljning i efterhand för att identifiera förbättringsmöjligheter.

Vid större incidenter där samtliga eller ett flertal verksamhetskritiska IT-system är ur funktion måste informatik Västerbotten prioritera vilka IT-system som ska startas upp först. Beredskapssamordnaren inom landstinget har i samråd med chefsläkargruppen arbetat med att ta fram en prioriteringslista över IT-system som bör startas upp först. Slutsatsen var att det är svårt att ha en statisk prioriteringslista då det kan skilja beroende på tid på dygnet och vilka anställda som finns på plats etc. Arbetet med att ta fram en ny prioriteringslista baserat på verksamheternas behov pågår, ansvaret är ålagt chefsläkargruppen men det finns ingen definitivt tidsplan.

Kontinuitetsplanering

Kontinuitetsplanering kan innefatta både planering för att upprätthålla kontinuitet i verksamheten trots att IT-system inte är tillgängliga och att det finns avbrotts- och återstartsrutiner för IT-system, databaser och servrar. Enligt de riktlinjer för informationssäkerhet som upprättats av landstingsstyrelsen ska varje IT-system inom landstinget ha en kontinuitetsplan, och ansvaret för att tillse att sådana finns och efterlevs ligger på respektive systemägare. Vid tidpunkten för granskningen kunde det noteras att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte säkerställt att det finns en tillräcklig styrning, uppföljning och kontroll av arbetet med kontinuitetsplaner. Detta då det inte finns riktlinjer för hur ofta de ska testas och revideras. Informatik Västerbotten har dock dokumenterade rutiner i databasen Lotus Notes vilka redogör för hur man ska starta upp de system som informatik Västerbotten driftar vid avbrott.

Drift

Inom landstinget finns teknik för att upptäcka intrång och det interna nätverket är segmenterat, vilket betyder att nätverket är uppdelat i olika delar. För de system som driftas inom basenheten informatik Västerbotten finns en process för programförändringar vilken är beskriven i rutiner och styrdokument. Ändringsprocessen ska gälla för alla ändringar om inget annat reglerats i ändringsöverenskommelsen, dock sker det i nuläget ingen uppföljning av programförändringar i syfte att säkerställa att processen för programförändring följs.

Backuper på servrar tas en gång per dygn och sparas i minst 14 dagar. Backuper på databaser tas en gång per dygn och frekvensen på transaktionsloggar varierar per system men i regel sker detta var 10:e och 60:e minut. Om en full backup fallerar väntar informatik Västerbotten till dagen efter för att undersöka om nästa backup fullföljs. Om backupen nästa dag också fallerar vidtas relevanta åtgärder. Säkerhetskopior sparas på servrar i en hall som är separerad från övriga servrar. Enligt rutinen för säkerhetskopiering (178868) ansvarar förvaltningen för respektive system inom informatik Västerbotten beställa återläsningstester.

Batchjob beställs av förvaltningen för respektive system. Övervakning av batchjob sker via mail eller whatsapp, där servicedesk får notifikationer om ett batchjob har fallerat under dagstid. Vid nattetid får även tekniker i beredskap en notifikation.

Access till och kontroll av aktivitet i känslig utrustning

Inom informatik Västerbotten har driftgruppen och ett fåtal andra tekniker inom basenheten access till att logga in på servrar och databaser, enligt leveransansvarig för infrastruktur och systemdrift. Det finns ingen periodisk genomgång av användare som har access till servrar och databaser för att säkerställa att endast behörig personal har access.

All inloggning till servrar och databaser loggas men det genomförs ingen uppföljning på vilka tekniker som loggat in. Det sker heller ingen övervakning av aktivitet på servrarna och databaserna. Inom informatik Västerbotten har det diskuterats att installera en revisionslogg på aktivitet i servrar och databaser, men är enligt leveransansvarig för infrastruktur och systemdrift för kostsamt.

2.4. Fysisk säkerhet till serverhallar

Serverhallar

VLL nyttjar tre olika serverhallar, där en av serverhallarna är dedikerad till säkerhetskopierad data. Samtliga serverhallar är försedda med avbrottsfri kraft, både via batterier och diselgeneratorer. Inom VLL finns inga dokumenterade riktlinjer kring vilka säkerhetskriterier en serverhall bör uppfylla, något som även påvisats i den tidigare granskningen "Landstingets styrning och kontroll av IT-avbrottsplaner" (17/2014). Under granskningen har det framkommit att säkerheten i framförallt de två äldre hallarna ännu ej anses vara tillräckligt god. Ett behov av nya hallar är väl känt hos informatik Västerbotten, dock uppskattas att investeringen för att bygga serverhallar vilka uppfyller kraven på god säkerhet är mycket hög och att en adekvat nivå på säkerhet i serverhallar inte är möjlig att uppnå hos serverhallar förlagda vid nuvarande läge. Det beslutades därför av dåvarande direktör för Service[1] om att undersöka möjligheten att hyra andra lokaler för att placera servrarna i. Detta beslut gäller i nuläget endast driften av lokalerna och således omfattas inte driften av servrarna, för vilka ansvaret bibehålls internt.

Landstingsstyrelsen fick 2016-10-25/§214 en återrapport av ett uppdrag lämnat till Verksamhetsområde Service vilket syftade till att göra en genomlysning av landstingets serverhallar. Uppdraget inkluderade även en genomlysning av landstingets hela nät för data- och telekommunikation mellan sjukhus och övriga enheter. Uppdraget avsåg att bedöma hallarna ur perspektivet generell lämplighet

[1] Informatik Västerbotten tillhörde vid tidpunkten för beslutet verksamhetsområde Service

som fortsatta serverrum och dokumentera eventuella brister och risker. Uppdraget var avgränsat till att inte omfatta de IT-system som finns i hallarna. Den sammanfattande bedömningen som görs i konsultrapporten är att hallarnas funktion är klart undermåliga i jämförelse med den praxis som finns för säkra IT-rum. Landstingsstyrelsen beslutade att ge landstingsdirektören, med rätt att vidaredelegera, i uppdrag att:

- På kort sikt avhjälpa enklare brister samt löpande genomföra risk- och konsekvensanalys i befintliga hallar.
- På lång sikt bygga nya hallar som uppfyller de krav som idag ställs på IT-säkra rum (en investering på över 50 mkr). Strategin är att successivt flytta ut lokaldriften från Västerbottens läns landstings datorhallar till en extern leverantör där det redan finns färdiga funktioner som håller adekvat säkerhetsklass.

Access till serverhallarna regleras via passersystem med där behörig personal utrustas med personliga kort. Serverhallarna hålls låsta och loggar förs över inpassering. Det är ett begränsat antal anställda som har access till serverhallarna, och vilka personer som har access övervakas av leveransansvarig för infrastruktur och drift. Personliga kort låses vid avslutad anställning och loggar över vilka som har tillträtt hallarna gås igenom en gång per år eller vid behov.

2.5. Implementation av rekommendationer från tidigare granskningar

Revisionen har tidigare genomfört ett flertal granskningar vilka berört området informationssäkerhet. Nedan presenteras en uppföljning av de rekommendationer som getts genom dessa granskningar.

Färgkodning	Förklaring
	Rekommendation bedöms ej vara implementerad
	Rekommendation bedöms vara delvis implementerad
	Rekommendation bedöms vara implementerad

2.5.1. Behörigheter till journalsystemet (rapportnummer 18/2015)

I rapporten "Behörigheter till journalsystemet" påtalades att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte har säkerställt en tillräcklig kontroll av personalens behörigheter till journalsystemet NCS Cross (tidigare SYSteam Cross). Av fyra kontrollerade basenheter saknade samtliga dokumenterade rutiner för beställning, tilldelning, ändring och borttagning av behörigheter till såväl journalsystemet som till övriga IT-system.

Nedan presenteras en uppföljning av revisorernas rekommendationer:

Rekommendation	Uppföljning	
Verksamheterna har dokumenterade rutiner för administration av behörigheter till IT-system.	Rekommendation bedöms vara implementerad. Det finns övergripande dokumenterade rutiner i Riktlinje för informationssäkerhet – förvaltning och drift (168592).	

Verksamheterna genomför regelbundna kontroller av de anställdas IT-behörigheter.	Rekommendation bedöms ej vara implementerad. Det finns inte något övergripande systematiskt arbete för att säkerställa att verksamheterna genomför regelbundna kontroller av anställdas IT-behörigheter.
Personer som inte ska ha tillgång till journalsystemet inte har behörighet till systemet.	Rekommendation bedöms vara ej vara implementerad. I och med att det inte genomförs någon periodisk genomgång av anställdas behörigheter kan det inte garanteras att anställda har rätt behörigheter. Personer som avslutat sin anställning får sin access borttagen genom att deras accesskort blir ur funktion. Risken är således att anställda som byter tjänst behåller sin access från den tidigare anställningen om periodiska genomgångar inte genomförs.

2.5.2. Informationssäkerhet och hantering av personuppgifter (rapportnummer 22/2014)

I rapporten "Informationssäkerhet och hantering av personuppgifter" framkom att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte hade vidtagit åtgärder med anledning av de brister som framkommit i tidigare granskningar. Styrelsen och nämnden hade för år 2014 inte säkerställt styrning, uppföljning och kontroll av att personuppgifter hanteras i enlighet med gällande lagstiftning.

Nedan presenteras en uppföljning av revisorernas rekommendationer:

Rekommendation	Uppföljning
Styrelsen och nämnden bör få rapporter om granskningar, riskanalyser, skyddsåtgärder m.m. av betydelse för informationssäkerhetsarbetet i landstinget.	Rekommendationen bedöms vara ej implementerad. I patientsäkerhetsberättelsen för verksamhetsåret 2016 inkluderades en informationssäkerhetsberättelse som innehöll en summering av uppföljningar, riskanalyser och åtgärder som vidtagits. Uppföljningen inkluderade dock inga övergripande riskanalyser, då några sådana enligt Patientsäkerhetsberättelsen inte förkommer inom Landstinget. I övrigt sker ingen ytterligare återrapportering om informationssäkerhetsarbetet.

Det bör finnas informationssäkerhetsansvarig och personuppgiftsombud och funktionerna bör har skriftliga uppdragsbeskrivningar.	Rekommendationen bedöms vara delvis implementerad. Personuppgiftsombud finns sedan tidigare och en informationssäkerhetsstrateg anställdes i augusti 2017. Funktionerna har dock inte några skriftliga uppdragsbeskrivningar.	
Riktlinjer för informationssäkerhet och hantering av personuppgifter bör vara kända bland verksamheterna och att verksamheterna följer riktlinjerna.	Rekommendationen bedöms ej vara implementerad. Riktlinjer för informationssäkerhet finns att tillgå för samtliga anställda via intranätet, dock sker ingen utbildning i dessa eller övergripande uppföljning av att riktlinjerna är kända och efterlevs.	

2.5.3. Styrning och kontroll av IT-avbrottsplaner (rapportnummer 17/2014)

I rapporten "Styrning och kontroll av IT-avbrottsplaner" uppmärksammades att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte hade vidtagit tillräckliga åtgärder för att komma till rätta med de brister som identifierades genom 2010 års granskning. Enligt revisorerna rådde det oklarhet i hur många IT-system som fanns i Landstinget och för vilka av dessa det fanns avbrottsplaner. Det saknades avbrottsplaner för vissa verksamhetskritiska system på såväl övergripande nivå som hos granskade basenheter i landstinget.

Dokumentation fanns i ledningssystemet där det framgick vem som var ansvarig för avbrottsplaner både på lokal och övergripande nivå. Däremot saknades landstingsövergripande riktlinjer för vad en avbrottsplan ska innehålla.

Vidare fanns inga överenskommelser mellan verksamheterna och informatik Västerbotten vad gällde kritiska tidpunkter för IT-teknikers inställelse i händelse av ett avbrott.

Nedan presenteras en uppföljning av revisorernas rekommendationer:

Rekommendation	Uppföljning	
Det bör i landstingets ledningssystem finnas riktlinjer för hur avbrottsplaner ska vara utformade, hur ofta de ska testas och revideras.	Rekommendationen bedöms vara ej implementerad. Det finns inga landstingsövergripande riktlinjer för utformning eller test av avbrottsplaner i landstinget. Enligt informatik Västerbottens systemförvaltningsmodell ska respektive systemägare ansvara för avbrottsplaner för respektive system.	
Det bör av ledningssystemets riktlinjer framgå hur avbrottsplaner ska förvaras lokalt ute i verksamheterna samt hur dessa	Rekommendationen bedöms ej vara implementerad.	

digitalt ska förvaras för att underlätta uppföljning och kontroll på övergripande nivå.	Det finns inga riktlinjer i ledningssystemet för hur avbrottsplaner skall förvaras.	
Det bör finnas kontroller som säkerställer att riktlinjerna följs.	Rekommendationen bedöms ej vara implementerad. Kontroller som säkerställer att riktlinjerna följs ligger på respektive verksamhets ansvar, men det finns ingen övergripande uppföljning som säkerställer att riktlinjerna efterlevs.	
Det bör göras en inventering av landstingets IT-system där en förteckning skapas som underlag för bedömningen av vilka system som är strategiskt viktiga och verksamhetskritiska för landstinget.	Rekommendationen bedöms vara delvis implementerad. En förteckning har skapats vilken inkluderar cirka 50 verksamhetskritiska system som driftas av informatik Västerbotten. Dock finns ingen heltäckande förteckning av samtliga IT-system som används inom landstinget. Enligt informatik Västerbotten finns betydligt fler system än de 50 som anses som verksamhetskritiska.	
Det bör utifrån bedömningen fattas beslut om vilken prioritetsordning som ska gälla vid återstart i händelse av avbrott. En utredning bör göras om på vilken nivå i landstinget som beslut bör fattas.	Rekommendationen bedöms ej vara implementerad. Dock har utredning om prioritetsordning gjorts av beredskapssamordnare i samråd med chefsläkargruppen. Denna resulterade inte i någon detaljerad ordning då detta bedömdes vara svårt att fastställa, eftersom olika system kan vara olika kritiska för olika verksamheter, under olika tidpunkter på dygnet och beroende på vilka anställda som finns på plats. Det har inte gjorts någon formell utredning gällande på vilken nivå beslutet för prioritetsordning bör tas.	
Det bör finnas ett beslut om vilken nivå av IT-resurser som behövs för att bibehålla kontinuiteten i landstingets verksamheter i händelse av avbrott.	Rekommendationen bedöms vara implementerad. Informatik Västerbotten har beredskap dygnet runt. Tf verksamhetschef informatik Västerbotten uppger att beslutet måste ha tagits 10-20 år sedan av dåvarande verksamhetsområdeschef.	
Det bör finnas beslutade kriterier för vad en serverhall i landstinget ska uppfylla för att vara lämplig för ändamålet.	Rekommendationen bedöms ej vara implementerad. Det finns inga formellt beslutade kriterier för vad en serverhall ska uppfylla.	

2.5.4. Granskning av virusskydd (rapportnummer 23/2010)

I rapporten "Granskning av virusskydd" uppdagades följande brister:

Styrning:

- Avsaknad av formell, skriftlig och kommunicerad IT-strategi som adresserar infrastruktur och teknisk plattform
- Avsaknad av formellt informationssäkerhetsramverk, inklusive informationssäkerhetspolicy och anvisningar för användare, förvaltning och drift
- Brister i kommunikationen av gällande policys till verksamheten
- Verksamheten saknar rutiner för uppföljning av efterlevnaden av informationssäkerhetspolicys
- Reaktivt istället för proaktivt arbete med efterlevnad
- Verksamhetschefer upplever bristande egen kompetens i förhållande till det ansvar de har för informationssäkerhet
- Verksamhetschefer upplever bristande stöd från informatik Västerbotten beträffande informationssäkerhet
- Det saknas ett utpekat centralt ansvar för utbildning och centralt utbildningsmaterial finns ej att tillgå
- Utbildningsnivån på respektive enhet kan inte säkerställas och kan skilja stort
- Inga specifika samarbeten mellan landsting beträffande IT- och informationssäkerhet

Förvaltning:

- Centrala riktlinjer för riskhantering av system saknas
- Avsaknad av avtalade servicenivåer, som exempelvis tillgänglighet, mellan beställare och informatik Västerbotten
- Behörighetsadministration till medicinteknisk utrustning faller utanför informatik Västerbottens och kundservice kontroll utan görs av externa leverantörer
- Riktlinjer för regelbundna kontroller av behörigheter saknas
- Identifierat nyckelpersonberoende av landstingets enda virusexpert

Infrastruktur:

- Det finns 37 servrar och 21 klienter som använder operativsystem som underhålls av leverantör, vilket ökar risken för att sårbarheter utnyttjas
- Med nuvarande utbytestakt kommer det att finnas klientdatorer som använder nuvarande operativsystem då dess support går ut 2014
- Attack- och penetrationstester har inte gjorts under de senaste tio åren
- Ett verktyg, kallat HIAB, har till viss del använts för generella, interna tester, men tester som inriktar sig på specifika riskområden, exempelvis patientsäkerhet, har ej genomförts
- Landstinget använder en antivirusprogramvara. Programvara från flera leverantörer kan öka effektiviteten hos skyddet mot skadlig kod. Detta bör dock ställas mot de prestandakrav verksamheten har
- Båda datorhallarna ligger i samma byggnad (dock i olika brandceller), samt nära varandra i nätverket vilket kan öka risken för snabbare spridning av skadlig kod mellan servrarna

Drift:

- Viss medicinteknisk utrustning patchas (uppdateras) ej förrän leverantören testat och godkänt uppdateringen
- Viss fördröjning av patching av Java Runtime Environment, Acrobat Reader, Acrobat och Flash Player

Nedan presenteras en uppföljning av revisorernas rekommendationer:

Rekommendation	Uppföljning	
Landstinget bör ta fram ett heltäckande informationssäkerhetsramverk med informationssäkerhetspolicy och anvisningar riktade mot användare, förvaltning och drift.	Rekommendationen bedöms delvis vara implementerad. Landstinget har utvecklat en riktlinje för användare och en för förvaltning och drift, vilka finns tillgängliga på intranätet. Det finns dock ingen informationssäkerhetspolicy.	
Utbildning och uppföljning av efterlevnad rörande informationssäkerhet bör samordnas av informatik Västerbotten.	Rekommendationen bedöms vara delvis implementerad. Det finns en e-utbildning för anställda framtagen av informatik Västerbotten. Utbildningen är dock inte obligatorisk och det ingen uppföljning av hur många eller vilka anställda som gått den. Vidare har informatik Västerbotten inget formellt ansvar för de delar av informationssäkerhetsarbetet som faller utanför ramen för IT-säkerhet, detta ansvar ligger fortfarande hos respektive verksamhet.	
Riktlinjer för riskhantering av landstingets gemensamma system bör tas fram.	Rekommendationen bedöms ej vara implementerad. Det finns inga övergripande riktlinjer för riskhantering av landstingets gemensamma system.	
Landstinget bör införa rutin för periodisk genomgång av behörigheter.	Rekommendationen bedöms ej vara implementerad. I dagsläget ligger ansvaret för att utföra periodisk genomgång på systemägaren och de lokalt systemansvariga. Det finns ingen gemensam dokumenterad rutin för periodisk genomgång.	
Det bör undersökas om det går att minska tidsfördröjningen mellan det datum säkerhetsuppdateringar för tredjepartsmjukvara släpps och då de installeras.	Rekommendationen bedöms vara implementerad. Landstinget har regelbundna fönster för säkerhetsuppdateringar och alla förändringar föregås av en riskanalys	
Det bör göras en utredning om installation av säkerhetsuppdateringar kan göras på medicinteknisk utrustning där leverantörer i dagsläget ej tillåter detta.	Rekommendationen bedöms vara delvis implementerad. Enligt informatik Västerbotten är det inte möjligt att göra säkerhetsuppdateringar på medicinteknisk utrustning. Dock har det inte gjorts någon formell utredning.	

Landstinget bör minska sitt nyckelpersonberoende av nuvarande virusexpert.	Rekommendationen bedöms vara implementerad. Informatik Västerbotten har idag tre anställda som arbetar med virusskydd. Arbetet leds under förvaltningen Nät och IT-säkerhet.	

3. Slutsatser

Syftet med granskningen är att bedöma om landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer en tillräcklig styrning, uppföljning och kontroll av IT-systemen så att en säker hälso- och sjukvård kan bedrivas.

Nedan besvaras revisionsfrågorna.

Färgkodning	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
1. Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en ändamålsenlig organisation med tydlig ansvarsfördelning avseende IT- och informationssäkerhetsarbetet?	Nej. Roller och ansvar finns förvisso fördelade i organisationen men landstings- och nämndsövergripande styrning, uppföljning och utbildning saknas, vilket leder till att det finns en risk för att nivån på informationssäkerheten varierar beroende på verksamhet.	
2. Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att det finns riskanalyser gällande informationssäkerhet dokumenterade och uppdateras denna dokumentation löpande?	Nej. Det finns inga övergripande riskanalyser gällande informationssäkerhet eller informationsklassning.	
3. Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig styrning av drift- och kontinuitetsfrågor?	Nej. Det saknas överenskommelser för ca 30 av 50 system om längsta tid system kan ligga nere utan att produktionen i verksamheten äventyras. Informatik Västerbotten har dock processer för att hantera incidenter och eventuella avbrott.	
4. Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt att drift- och kontinuitetsplanering genomförs på ett ändamålsenligt sätt utifrån de behov av informationssäkerhet som verksamheterna har?	Nej. Eftersom verksamhetens behov inte är uttryckta i leveransöverenskommelser för samtliga system är det svårt att bedöma om drift- och kontinuitetsplanering genomförs utifrån de behov som verksamheten har för samtliga system.	

5. Har landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställt en tillräcklig fysisk säkerhet till serverhallar?	Nej. Det har inte beslutats om vilka kriterier en serverhall ska uppnå för med avseende på fysisk säkerhet. Dock har beslutats om att lokaldriften skall läggas på extern leverantör för att på så sätt uppnå adekvat säkerhet.
6. Hur väl har landstingsstyrelsen och hälso- och sjukvårdsnämnden implementerat rekommendationerna för att minska de brister i informationssäkerheten som lyfts i tidigare granskningar?	Nej. Fyra av 20 rekommendationer har implementerats. Sju av 20 rekommendationer har delvis implementerats Nio av 20 rekommendationer har ej implementerats
7. Säkerställer landstingsstyrelsen och hälso- och sjukvårdsnämnden en tillräcklig uppföljning och kontroll av arbetet med informationssäkerhet?	Nej. Det saknas landstings- och nämndövergripande uppföljning och kontroll av arbetet med informationssäkerhet. En informationssäkerhetsstrateg har dock nyligen tillträtt.

4. Iakttagelser och rekommendationer

Nedan följer en beskrivning av de iakttagelser och risker som identifierats genom granskningen, tillsammans med rekommendationer och förslag på åtgärder riktat till landstingsstyrelsen och hälso-och sjukvårdsnämnden.

4.1. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt tillräcklig styrning, uppföljning och kontroll av informationssäkerhetsarbetet

Granskningen visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden har ålagt verksamhetschefer ett stort ansvar för informationssäkerhetsarbetet men har inte tillräcklig styrning av arbetet, vilket är nödvändigt för att säkerställa att det bedrivs på en ändamålsenlig nivå. Riktlinjer för informationssäkerhetsarbetet ämnade för förvaltning och drift samt för användare har upprättats och finns att tillgå på ledningssystemet, dock görs inga kontroller av efterlevnaden av dessa.

Risk:

Avsaknad av styrning, uppföljning och kontroll av verksamheternas informationssäkerhetsarbete kan medföra risk att olika verksamheter arbetar på olika sätt med informationssäkerheten och att arbetet därmed inte genomförs med tillräckligt hög nivå.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att se över styrning, uppföljning och kontroll för informationssäkerhet genom att införa en högre grad av landstings- och nämndövergripande styrning och fler kontrollrutiner. Detta för att säkerställa att informationssäkerhetsarbetet bedrivs på en harmoniserad och tillfredsställande nivå i landstingets olika verksamheter.

4.2. Landstingsstyrelsen och hälso-och sjukvårdsnämnden har inte säkerställt ändamålsenlig rapportering för arbetet med informationssäkerhet.

Landstingsstyrelsen och hälso- och sjukvårdsnämnden har bristfällig rapportering gällande arbetet med informationssäkerhet. I dagsläget sker detta endast genom internkontrollplanen och patientsäkerhetsberättelsen, vilka inte innehåller tillräcklig information om informationssäkerheten i landstinget. Dessutom har inte samtliga verksamhetschefer inte svarat på frågan om de har genomfört loggkontroller. Riskerna definierade i 4.5, 4.7, 4.8, 4.9, 4.10, 4.11 och 4.13 är exempel på risker som inte täcks in i internkontrollplanen.

Risk:

Det finns en risk att eventuella brister i informationssäkerhetsarbetet hos enskilda verksamheter inte upptäcks.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att aktivt följa upp arbetet med informationssäkerheten i landstinget alternativt besluta om

utökad intern kontroll inom området och öka kraven på återrapportering i patientsäkerhetsberättelsen.

4.3. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt en ändamålsenlig kommunikation och utbildning gällande riktlinjer för informationssäkerhet

Den riktlinje som riktas mot användare av informationssystem, Riktlinje för informationssäkerhet – användare, finns tillgänglig på intranätet men har inte formellt kommunicerats ut till den avsedda målgruppen varför det ej kan säkerställas att alla medarbetare har tagit del av informationen. Det finns en e-utbildning i informationssäkerhet avsedd för användare av IT-system inom landstinget, men den är inte obligatorisk och ingen uppföljning av deltagandet görs.

Risk:

Att inte kommunicera ut gällande riktlinjer och policys och/eller utbilda medarbetarna inom informationssäkerhet medför risk för att medarbetarna har bristande kunskap om informationssäkerhet. Således finns också en risk för att det dagliga arbetet med att hantera verksamhetens information inte sker på ett säkert sätt.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att utbildning inom informationssäkerhet för medarbetare inom respektive styrelse/nämnds ansvarsområden koordineras på landstingsövergripande nivå och görs obligatorisk, samt att deltagandet följs upp. Vi rekommenderar även att landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer att relevanta styrdokument kommuniceras ut till alla berörda anställda.

4.4. Landstingsstyrelsen har inte säkerställt att det finns informationssäkerhetspolicy i landstinget

Landstingsstyrelsen har inte berett en informationssäkerhetspolicy för landstingsfullmäktige att besluta om. I dagsläget är de högsta beslutade dokumenten i ledningssystemet för informationssäkerhet två riktlinjer; en riktad mot kontinuitet och drift samt en för användare.

Risk

Utan en informationssäkerhetspolicy finns en risk styrelse och nämnders ansvar, inriktning och övergripande mål, befogenheter, betydelsen av informationssäkerhet samt struktur för riskbedömning och riskhantering inte implementeras och kommuniceras till verksamheten.

Rekommendation

Vi rekommenderar landstingsstyrelsen att en informationssäkerhetspolicy arbetas fram för landstingsfullmäktiges beslut. Policyn bör inkludera minst styrelse och nämnders ansvar, inriktning och övergripande mål, befogenheter, betydelsen av informationssäkerhet samt struktur för riskbedömning och riskhantering.

4.5. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att informationsklassning genomförts för system som bedöms som verksamhetskritiska

Klassificering av information med hänsyn till krav på skyddsnivå har ej genomförts och dokumenterade regler för hur klassning ska genomföras finns ej att tillgå. Det bedrivs inte heller något strukturerat arbete med att upprätta systemsäkerhetsanalyser för system som bedöms som verksamhetskritiska.

Risk:

Att inte klassa verksamhetens information och upprätta säkerhetsanalyser för verksamhetskritiska system medför risk för att arbetet med att bedriva ett ändamålsenligt säkerhets- och kontinuitetsarbete försvåras.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att informationsklassning genomförs.

4.6. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att landstinget implementerat de rekommendationer som getts i tidigare granskningar

Under granskningen har det noterats att 16 av 20 av de rekommendationer som lyfts i tidigare granskningar helt eller delvis inte implementerats. Dessa granskningar har tillhandahållit analyser av områden av vikt för det löpande informationssäkerhetsarbetet, såsom personuppgiftshantering, virusskydd och avbrottsplaner.

Risk:

Att inte följa upp rekommendationer givna i tidigare granskningar medför risk att viktiga identifierade brister i informationssäkerheten kvarstår och således också att de risker som föreligger i relation till dessa inte hanteras.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa uppföljning och kontroll av att rekommendationer från tidigare granskningar utreds och om möjligt implementeras.

4.7. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att det bedrivs ett systematiskt övergripande arbete med riskanalyser

Under granskningen har noterats att det inte bedrivs något landstingsövergripande arbete med att identifiera och adressera samtliga risker relaterade till informationssäkerhet. Lokala initiativ till riskanalyser såsom vid systemförändringar har tagits inom informatik Västerbotten, dock saknas gemensamma riktlinjer för riskhantering inom organisationen.

Risk:

Brist på medvetenhet om de risker som föreligger i relation till organisationens information, IT-system och hårdvara medför ökad sannolikhet att

informationssäkerhetsincidenter inträffar, samt att eventuella konsekvenser av incidenter riskerar att förvärras.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att utarbeta landstingsövergripande riktlinjer för riskidentifiering och riskhantering. Vi rekommenderar att kritisk information, IT-system och hårdvara kartläggs och att det utförs riskanalyser för dessa. Vidare bör landstingsstyrelsen tillse att arbetet med riskanalyser utförs regelbundet och vid större verksamhetsförändringar.

4.8. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att kontroll av programförändringar genomförs

Det genomförs ingen kontroll av programförändringar i syfte att säkerställa att programförändringar föregås av godkännande och testning.

Risk:

Det finns en risk att otillåtna och/eller felaktiga programförändringar genomförs om de inte kontrolleras.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att kontroll av programförändringar i verksamhetskritiska system genomförs.

4.9. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att förteckning över landstingets samtliga informationssystem upprättats

Vi har noterat att det totala antalet informationssystem som används inom landstinget inte kontrollerats, varvid ingen exakt siffra har kunnat erhållas. Ett 50-tal system har bedömts som verksamhetskritiska och har systemförvaltare vilka organisatoriskt tillhör informatik Västerbotten. Dock framgår av intervjuer att det sammantaget rör sig om ett väsentligt större antal IT-system och IT-applikationer vilka är i bruk inom landstinget, inkluderat mindre lokala system.

Risk:

Utan en komplett förteckning över de informationssystem som används föreligger risk att organisationen inte har adekvat kontroll över att dess information behandlas enligt de riktlinjer som ställts.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att en inventering av landstingets informationssystem genomförs. En förteckning över samtliga system bör sammanställas, där det framgår vilka av dessa som är att betrakta som kritiska för verksamheten.

4.10. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att det genomförs en periodisk kontroll av användare med fysisk access till servrar och databaser

Det genomförs ingen periodisk kontroll av användare med fysisk access till servrar och databaser i syfte att identifiera obehörig personal.

Risk

Det finns en risk att obehörig personal har tillgång till servrar och databaser.

Rekommendation

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att periodisk kontroll av fysisk access till servrar och databaser genomförs.

4.11. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att det genomförs någon kontroll av inloggning till och aktivitet i servrar och databaser

Under granskningen noterades att det inte sker någon kontroll av inloggning till och aktivitet i servrar och databaser.

Risk:

Det finns en risk för att olämplig inloggning och aktivitet i servrar och databaser inte upptäcks.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att inloggning till servrar och databaser kontrolleras. Vi rekommenderar även att en utredning görs för att implementera revisionsloggar för aktivitet i kritiska databaser och servrar.

4.12. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt tillräcklig fysisk säkerhet till serverhallar

Vid granskningen har det noterats att landstingets serverhallar ej uppfyller kraven på tillräcklig säkerhet, trots att säkerhetsnivån har höjts i och med att en ny serverhall tagits i bruk. Det uppges även av Informatik Västerbotten att en tillfredsställande nivå av säkerhet är svår att uppnå givet de investeringar som krävs. De sammantagna krav som bör ställas på en serverhall för att denna ska vara lämplig för sitt ändamål har inte fastställts. Dåvarande direktör för Service har beslutat om att hyra andra lokaler och på så sätt öka säkerhetsnivån, dock råder fortfarande oklarhet i fråga om när detta beslut kommer att verkställas. Det finns även beslut om åtgärder på kort och lång sikt.

Risk:

Otillräcklig fysisk säkerhet i serverhallar ökar risken för avbrott vilka kan ha allvarlig påverkan på landstingets informationssystem. Utkontrakteras driften av serverhallar på extern leverantör utan att man internt beslutat om kriterier för vad dessa bör uppfylla föreligger risk att en adekvat säkerhetsnivå fortfarande inte upprätthålls.

Rekommendation:

Vi rekommenderar att landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer att beslut tas om kriterier för vad en serverhall inom landstinget ska uppnå med avseende på fysisk säkerhet. Dessa kriterier bör ligga till grund för de krav som ställs på framtida leverantör av lokaler. Vi rekommenderar även att säkerheten i de befintliga hallarna höjs till dess att andra lokaler hyrs samt att en tidsplan för att flytta servrarna fastställs.

4.13. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att längsta acceptabla tid som informationssystem bedöms kunna vara ur funktion har beslutats för alla verksamhetskritiska system

Under granskningen har det noterats att överenskommelser mellan systemägare och informatik Västerbotten gällande längsta acceptabla tid som informationssystems bedöms kunna vara ur funktion ej beslutats för 30 av 50 verksamhetskritiska system.

Risk:

Om överenskommelser gällande längsta acceptabla tid som systemen bedöms kunna vara ur funktion ej definieras finns det risk att informatik Västerbotten inte kan hantera incidenter och avbrott på ett ändamålsenligt sätt.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att längsta acceptabla tid verksamhetskritiska system kan vara ur funktion fastställs.

4.14. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att externa och interna penetrationstester genomförts

Interna eller externa penetrationstester genomförs inte. I en tidigare granskning från 2010 noterades att externa tester ej genomförts sedan 1998 och att interna tester ej genomförts sedan år 2000.

Risk:

Genomförs inte penetrationstester finns risk för oupptäckta sårbarheter i infrastruktur och drift, vilket kan öka risken för att obehöriga personer får tillgång till känslig data eller för att IT-system inte är tillgängliga för verksamheten.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att interna och externa penetrationstester i syfte att identifiera brister i Landstingets IT-miljö genomförs.

4.15. Landstingsstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att landstingets personuppgiftsombud och informationssäkerhetsstrateg har dokumenterade uppdragsbeskrivningar

Under granskningen noterades det att personuppgiftsombudet och informationssäkerhetsstrategen inte har dokumenterade uppdragsbeskrivningar.

Risk:

Utan dokumenterade uppdragsbeskrivningar finns risk att kritiska uppgifter inte genomförs.

Rekommendation:

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att personuppgiftsombudet och informationssäkerhetsstrategen har dokumenterade uppdragsbeskrivningar.

5. Bilaga 1: Förteckning över intervjuade funktioner

Landstingsdirektör
Hälso- och sjukvårdsdirektör
Stabsdirektör för ledningsstaben
Direktör Digitalisering och Medicinteknik
Landstingsjurist och Personuppgiftsombud
TF Verksamhetschef Basenhet informatik
Systemförvaltare NCS Cross
Systemägare NCS Cross
Systemförvaltare IAM
Leveransansvarig Infrastruktur och systemdrift
Leveransansvarig för Systemförvaltning
IT-strateg
IT-handledare
Informationssäkerhetsstrateg
Kvalitetsansvarig Basenenhet informatik
Leveransansvarig Service
Verksamhetschef Neurocentrum
Verksamhetschef Cancercentrum
Verksamhetschef Operationscentrum
Verksamhetschef Barn- och Ungdomscentrum

6. Bilaga 2: Dokumentförteckning

- Organisation Informatik Västerbotten
- Riktlinje för informationssäkerhet Användare
- Riktlinje för informationssäkerhet Förvaltning och drift
- Rutin för Säkerhetskopiering
- Servicenivåer Servicedesk Informatik Västerbotten
- Driftöverenskommelse NCS Cross 2015-03-03
- Drift- och supportöverenskommelse BAS för samtliga IT-tjänster
- Förvaltningsobjekt och systemförvaltare inom Informatik Västerbotten
- Mall Driftöverenskommelse
- Mall Supportöverenskommelse
- NCS Cross Supportöverenskommelse
- Prioritetsordning uppstart infrastruktur 2017
- Systemförvaltningsmodell VLL – Checklista (262981)
- Systemförvaltningsmodell VLL – Etableringsguide (263010)
- Systemförvaltningsmodell VLL – Rollbeskrivning
- Internkontrollplan-2017 HSN
- Internkontrollplan-2017 LTS
- Kvalitet och säkerhetspolicy (187886)
- 170620 Slutrapport driftstörning IT-system
- 170128 Slutrapport händelseanalys driftstörning NCS