2014-12-18 147753
Dnr: REV 33:2-2014

Landstingsstyrelsen
Hälso- och sjukvårdsnämnden

Styrning och kontroll av IT-avbrottsplaner

Granskningen av landstingets IT-avbrottsplaner är en uppföljning av en granskning från år 2010. Uppföljningen visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit tillräckliga åtgärder för att komma till rätta med de brister som identifierades i granskningen år 2010. Varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har följt upp och kontrollerat att deras verksamheter har fungerande avbrottsplaner. Vårt stickprov visar att två av tio verksamhetskritiska system saknar övergripande avbrottsplaner. Granskningen visar även att det finns brister lokalt ute i verksamheterna vad gäller avbrottsplaner. Övriga iakttagelser i granskningen är att det saknas:

- En översikt över landstingets IT-system och avbrottsplaner
- Riktlinjer för vad en avbrottsplan ska innehålla.
- Beslutad prioriteringsordning för vilka IT-system som är verksamhetskritiska i händelse av avbrott.
- Regler och anvisningar för hur prioriteringen ska göras.
- Överenskommelser mellan verksamheterna och informatikenheten vad gäller kritiska tidpunkter för exempelvis IT-teknikernas inställelsetid i händelse av avbrott.
- Fastställda kriterier för vad en serverhall bör uppfylla för att vara lämplig för ändamålet.

Rekommendationer

Utifrån iakttagelserna rekommenderar vi landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att:

- Det i landstingets ledningssystem finns riktlinjer för hur avbrottsplaner ska vara utformade, hur ofta de ska testas och revideras.
- Det av ledningssystemets riktlinjer framgår hur avbrottsplaner ska förvaras lokalt ute i verksamheterna samt hur dessa digitalt ska förvaras för att underlätta uppföljning och kontroll på övergripande nivå.
- Det finns kontroller som säkerställer att riktlinjerna följs.

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 görs 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.
- Det 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.
- Det finns ett beslut om vilken nivå av IT-resurser som behövs för att bibehålla kontinuiteten i landstingets verksamheter i händelse av avbrott.
- Det finns beslutade kriterier för vad en serverhall i landstinget ska uppfylla för att vara lämplig för ändamålet.

Vid revisorernas överläggning den 18 december 2014 beslöt revisorerna enhälligt att ställa sig bakom slutsatser och rekommendationer i detta missiv. Missiv och underliggande rapport (nr 17/2014) lämnar revisorerna för yttrande till landstingsstyrelsen och hälso- och sjukvårdsnämnden. Yttrande med uppgifter om verkställda och planerade åtgärder ska lämnas till revisionskontoret senast den 17 april 2015.

För landstingets revisorer

Christer Fessé
Ordförande

Sven-Olov Södermark
Vice Ordförande

LANDSTINGSREVISIONEN

Landstingets styrning och kontroll av IT-avbrottsplaner - uppföljande granskning

Rapport nr 17/2014

VÄSTERBOTTENS LÄNS LANDSTING

December 2014

Eva Röste Moe, Certifierad kommunal revisor, revisionskontoret

Diarienummer: REV 33:2-2014

Innehåll

1. Sammanfattande analys

1.1. Bakgrund

År 2010 genomförde revisorerna en granskning om landstinget hade dokumenterade IT-avbrottsplaner. Granskningen visade att reglerna var otydliga och att landstingsstyrelsen inte hade kontroll över om det fanns avbrottsplaner bland verksamheterna. I granskningsplanen för år 2014 beslutade revisorerna att göra en uppföljande granskning med utgångspunkt i iakttagelser och rekommendationer från 2010 års granskning.

1.2. Resultat

Uppföljningen visar att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit tillräckliga åtgärder för att komma till rätta med de brister som identifierades i granskningen år 2010. Varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har följt upp och kontrollerat att deras verksamheter har fungerande avbrottsplaner. Det råder dessutom fortfarande oklarhet i hur många IT-system som finns i landstinget och om det finns avbrottsplaner för dessa system. Vår kontroll av avbrottsplaner visar att två av tio verksamhetskritiska system saknar övergripande avbrottsplaner.

1.2.1. Ansvar för avbrottsplaner

En positiv iakttagelse är att landstingsdirektören år 2012 beslutade om en reviderad systemförvaltningsmodell. I denna framgår att systemägaren har ansvaret för att det ska finnas en avbrottsplan innan ett nytt IT-system tas i drift. Det framgår även att verksamhetschefer i egenskap av informationsägare har ansvar för att det finns planer för hur verksamheterna ska bibehålla sin verksamhet i händelse av IT-avbrott. Det saknas däremot beslutade riktlinjer för vad en avbrottsplan ska innehålla.

1.2.2. Prioritetsordning

Det finns inte någon beslutad prioriteringsordning för vilka IT-system i landstinget som är verksamhetskritiska i händelse av större avbrott. Ett beslut om prioritetsordning vid återstarter av IT-system är ett viktigt beslut eftersom allvarliga IT-avbrott kan påverka såväl verksamheter som vården av enskilda patienter. Landstinget saknar regler och anvisningar för hur prioriteringen ska göras.

1.2.3. Servicenivåer

Det finns inga överenskommelser mellan verksamheterna och informatikenheten vad gäller kritiska tidpunkter för exempelvis beredskapsteknikers inställelse i händelse av ett avbrott utanför ordinarie arbetstid. Beredskapsteknikerna har enligt anställningsavtal en inställelsetid på två timmar om de behöver rycka ut efter ordinarie arbetstid. Det finns inga riskanalyser för om den tiden är tillräcklig.

1.2.4. Säkerhet kring serverhallar

När det gäller säkerheten kring landstingets serverhallar så har åtgärder enligt verksamhetschefen för informatikenheten genomförts genom att flytta servrar till en ny serverhall. Landstinget har nu tre hallar som är åtskilda och fungerar som back-up för varandra om ett avbrott skulle inträffa. En ny back-up utrustning finns i den nya hallen. Under hösten 2014 har verksamhetschefen vid informatikenheten också beslutat om riktlinjer för vilka som har behörighet att komma in i hallarna.

Av granskningen framgår att det inte finns några dokumenterade beslut i landstinget om vilka kriterier en serverhall bör uppfylla för att vara lämplig för ändamålet. Det är därför svårt för landstingsstyrelsen och hälso- och sjukvårdsnämnden att följa upp om säkerheten i den nya hallen är tillräcklig.

1.3. Rekommendationer

Landstingsstyrelsen och hälso- och sjukvårdsnämnden bör säkerställa att:

- Det i landstingets ledningssystem finns riktlinjer för hur avbrottsplaner ska vara utformade, hur ofta de ska testas och revideras.
- Det av ledningssystemets riktlinjer framgår hur avbrottsplaner ska förvaras lokalt ute i verksamheterna samt hur dessa digitalt ska förvaras för att underlätta uppföljning och kontroll på övergripande nivå.
- Det finns kontroller som säkerställer att riktlinjerna följs.
- Det görs 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.
- Det 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.
- Det finns ett beslut om vilken nivå av IT-resurser som behövs för att bibehålla kontinuiteten i landstingets verksamheter i händelse av avbrott.
- Det finns beslutade kriterier för vad en serverhall i landstinget ska uppfylla för att vara lämplig för ändamålet.

2. Bakgrund

År 2010 genomförde revisorerna en granskning av om landstinget hade dokumenterade och ändamålsenliga IT-avbrottsplaner. Med ändamålsenliga avsågs om avbrottsplanerna var reviderade och testade. Det ingick även att granska om det fanns dokumenterad prioriteringsordning för de olika IT-systemen i händelse av avbrott.

Resultatet av granskningen visade att landstingets regelverk var otydligt. Vem som ansvarade för olika system i landstinget var en tolkningsfråga och på landstingsövergripande nivå hade ingen kontrollerat om basenheterna tagit fram avbrottsplaner. Varken landstingsstyrelsen, tjänstemannaledningen eller någon annan i landstinget hade överblick över i vilken grad basenheterna hade fungerande avbrottsplaner.

Rekommendationerna i revisorernas missiv som skickades för kännedom till landstingsstyrelsen och hälso- och sjukvårdsnämnden sammanfattas nedan:

- Landstingets regelverk borde tydliggöra vem eller vilka i landstinget som hade ansvar för att det fanns fungerande avbrottsplaner. I detta låg även att det i regelverket skulle finnas regler och rutiner för hur och när avbrottsplaner skulle upprättas och revideras.
- Landstingets IT-system och avbrottsplaner borde inventeras och en förteckning borde skapas över dessa. Av förteckningen borde framgå vilka system som var strategiskt viktiga för landstinget. Ett beslut borde därefter fattas av vilken prioritetsordning systemen skulle ha vid återstart i händelse av avbrott.
- Landstingsstyrelsen och hälso- och sjukvårdsnämnde borde säkerställa att det fanns fungerande avbrottsplaner för aktuella IT-system.
- Landstingsstyrelsen och hälso- och sjukvårdsnämnde borde säkerställa rutiner för lagring av digitala avbrottsplaner. Detta för att underlätta uppföljning och kontroll. Vid granskningstillfället år 2010 hade basenheterna olika rutiner för var de förvarade sina avbrottsplaner.

Av revisorernas missiv från februari år 2011 framgick även att revisorerna planerade att genomföra uppföljande granskningar inom området avbrottsplaner. Detta för att undersöka vilka åtgärder styrelsen eller nämnden vidtagit med anledning av iakttagelserna i granskningen.

Revisorerna beslutade i sin granskningsplan för år 2014 att genomföra en uppföljande granskning av landstingets arbete med IT-avbrottsplaner.

3. Revisionsfrågor

Granskningens syfte är att följa upp rekommendationerna från 2010 års granskning. Den övergripande revisionsfrågan är om landstingsstyrelsen och hälso- och sjukvårdsnämnden har vidtagit åtgärder med anledning av de brister som identifierades i granskningen av IT-avbrottsplaner år 2010 (nr 28/2010).

Uppföljning omfattar att granska om landstingsstyrelsen och hälso- och sjukvårdsnämnden har säkerställt att det:

- Finns det regler i landstingets ledningssystem där det framgår vilka i landstinget som har ansvar för att det finns fungerande avbrottsplaner?
- Finns regler eller rutiner för hur och när avbrottsplaner ska upprättas och revideras?
- Finns en uppdaterad förteckning över landstingets samtliga IT-system och avbrottsplaner?
- Finns avbrottsplaner på en övergripande nivå för de tio systemen som av verksamhetsområdeschefer och informatikenhet värderats som mest verksamhetskritiska för landstinget?
- Finns avbrottsplaner på verksamhetsnivå för de enligt verksamheterna mest verksamhetskritiska systemen?
- Finns någon formellt beslutad prioritetsordning för återstart av olika IT-system i händelse avbrott?
- Finns en central uppföljning av att aktuella IT-system har fungerande avbrottsplaner?
- Finns regler eller rutiner för hur avbrottsplaner ska förvaras?

3.1. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. Vi har utgått från nedanstående revisionskriterier:

- Kommunallagen 6 kap 7 §
- Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14
- Socialstyrelsens föreskrifter om ledningssystem för systematiskt kvalitetsarbete SOSFS 2011:9
- Landstingets interna regler

3.2. Metod och avgränsning

Granskningen har genomförts genom dokumentationsstudier och samtal med verksamhetsområdeschef service, verksamhetschef för informatikenheten samt landstingets beredskapssamordnare. Vidare har vi haft kontakter med utvalda verksamhetschefer och avdelningschefer inom verksamhetsområdena medicin, kirurgi och regionvård. Vi har intervjuat medarbetare inom informatikenheten som arbetar med kvalitet, incidenter och drift. Vi har även haft kontakter med systemägare eller systemförvaltare för de system som ingår i granskningen.

Vi har i granskningen valt att kontrollera avbrottsplaner för tio av landstingets IT-system. Urvalet av dessa tio system har utgått dels från informatikenhetens uppskattningar av vilka system som är verksamhetskritiska i landstinget och dels från verksamhetsområdeschefernas uppfattning om vilka IT-system som är mest kritiska för deras verksamheter.

Kontrollen av avbrottsplanerna för de tio utvalda IT-systemen har genomförts vid nio basenheter inom verksamhetsområdena medicin, kirurgi och regionvård.

4. Resultat av granskningen

Socialstyrelsen har i sin handbok till föreskrifterna om informationshantering och journalföring (SOSFS 2008:14) förtydligat kraven som ställs på hälso- och sjukvården vad gäller patientuppgifternas tillgänglighet. Socialstyrelsen skriver i sin handbok att tillgängligheten bland annat säkerställs genom avbrotts- och kontinuitetsplaner. Dessa planer ska säkerställa att verksamheten kan fortsätta att fungera även om ett IT-system störs eller slutar att fungera.

I landstingsstyrelsens strategi för säkerhet och beredskap finns en definition av begreppet "allvarlig händelse". En allvarlig händelse är en händelse som är så omfattande eller allvarlig att landstingets resurser måste organiseras, ledas och användas på särskilt sätt. Bland exemplen på allvarliga händelser omnämns funktionsstörningar som omfattar IT.

4.1. Landstingets regler kring ansvaret för avbrottsplaner

Landstingsdirektören beslutade i juni år 2012 om en reviderad systemförvaltningsmodell. Av modellen framgår att ett viktigt moment som ingår i förvaltningen av ett IT-system är att genomföra riskanalys och upprätta avbrottsplan. Med detta avses att planera och vidta åtgärder för att säkerställa tillgänglighet, minimera risker och följder av ett driftstopp eller annan störning.

I förvaltningsmodellens checklista står att systemägaren har ansvar för att det innan ett IT-system tas i drift ska finnas en avbrottsplan. Avbrottsplanen ska klarlägga vilka åtgärder som ska vidtas om systemet drabbas av driftavbrott.

4.2. Landstingets kontroll av avbrottsplaner

Under granskningen har vi inte kunnat få svar på hur många IT-system eller IT-applikationer som finns i landstinget. Enligt en arbetslista från informatikenheten från år 2010 fanns över 200 system och applikationer. Enligt en uppskattning från tidigare biträdande verksamhetschef vid informatikenheten är antalet närmare 900 om man även inkluderar mindre lokala system. Ett 50-tal IT-system har systemförvaltningar som drivs inom informatikenheten. Övriga system har förvaltningsorganisationer som inte omfattar personal från informatikenheten.

I landstinget finns ingen sammanhållande funktion eller rutiner i ett ledningssystem som säkerställer kontroller av att IT-system har aktuella avbrottsplaner.

Systemägaren har enligt systemförvaltningsmodellen ansvar för att IT-systemet fungerar på avsett sätt. Ansvaret omfattar bland annat att avbrottsplaner är framtagna och följs.

Vi har kontrollerat systemägarnas avbrottsplaner för de tio IT-system som verksamhetsområdeschefer och informatikenheten bedömt som mest verksamhetskritiska i landstinget.

IT-system	Har en utsedd systemägare?	Har system-förvaltning inom informa-tikenheten?	Har dokumen-terad av-brottsplan på en övergri-pande nivå?	Kommentar
Systeam Cross	Ja	Ja	Ja	Använder informatikenhe-tens mall för avbrottsplan.
Master befolkning	Ja	Ja	Ja	Använder informatikenhe-tens mall för avbrottsplan.
Plexus	Ja	Ja	Ja	Använder informatikenhe-tens mall för avbrottsplan.
Flexlab	Ja	Ja	Ja	Använder informatikenhe-tens mall för avbrottsplan.
ROS	Ja	Ja	Ja	Använder informatikenhe-tens mall för avbrottsplan.
Orbit	Ja	Ja	Ja	Följer **inte** informatikenhe-tens mall för avbrottsplan
Sectra RIS-PACS	Ja	Nej	Ja	Följer **inte** informatikenhe-tens mall för avbrottsplan
Call me	Ja	Nej	Ja	Följer **inte** informatikenhe-tens mall för avbrottsplan
PICIS	Ja	Nej	Nej	**Saknas** en systemteknisk avbrottsplan på övergri-pande nivå.
Patientövervakning	Ja	Nej	Nej	Det **saknas** en systemtek-nisk avbrottsplan. Uppbygg-nad av förvaltningsorgani-sationen pågår. Systemet är i drift.

Granskningen visar att det saknas avbrottsplaner för två av de tio systemen som verksamhetsområdeschefer och medarbetare inom informatikenheten bedömt vara mest verksamhetskritiska. Sex av de åtta systemen som har avbrottsplaner förvaltas av informatikenheten. Fem av dessa sex avbrotts-planer är skrivna utifrån informatikenhetens mall för avbrottsplanering och är även kvalitetssäkrad av en särskild funktion inom informatikenheten.

För de system som inte omfattas av informatikenhetens systemförvaltning har avbrottsplanerna varierande utformningar och innehåll.

Det finns inga beslutade riktlinjer för vad en avbrottsplan ska innehålla. In-formatikenheten har tagit fram egna mallar och riktlinjer för avbrottsplaner-nas innehåll. Dessa riktlinjer är endast tillgängliga för informatikenhetens medarbetare. Detta kan vara en förklaring till att avbrottsplaner till system som inte förvaltas av informatikenheten har varierande utformningar och innehåll.

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa att:

- avbrottsplaner finns på plats före IT-system tas i drift.

- det i ledningssystemet finns beslutade riktlinjer för avbrottsplanernas ut-formning och innehåll.

- det finns kontroller av att de beslutade riktlinjerna kring avbrottsplaner följs.

4.3. Avbrottsplaner för verksamhetens hantering av driftstopp

Enligt systemförvaltningsmodellen har verksamhetschefen där ett IT-system används en roll som informationsägare. Detta innebär att ett IT-system som används av flera verksamheter har flera olika informationsägare. Informationsägare (verksamhetschefer) har enligt modellen ansvar för att riskanalyser och avbrottsplaner tas fram inom sina verksamheter.

4.3.1. Lokala avbrottsplaner hos verksamheterna

Landstingsstyrelsen och hälso- och sjukvårdsnämnden har enligt kommunallagens 6 kap 7 § ansvaret för att den interna kontrollen är tillräcklig. Varken landstingsstyrelsen eller hälso- och sjukvårdsnämnden har följt upp och kontrollerat att deras verksamheter har fungerande avbrottsplaner.

Vår granskning visar att det hos samtliga granskade enheter saknades utskrivna avbrottsplaner till något eller några av de system som de själva bedömt som verksamhetskritiska.

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa:

- att samtliga verksamhetschefer inventerar vilka IT-system som är verksamhetskritiska för deras verksamhet och att det finns dokumenterade avbrottsplaner för dessa IT-system.

- att rutiner skapas för hur lokala avbrottsplaner ska förvaras ute i verksamheterna.

- att det finns kontroller av att kritiska system har lokala avbrottsplaner ute i verksamheterna och att avbrottsplanerna uppfyller ställda krav.

4.3.2. Digital förvaring av avbrottsplaner

Det finns ingen samlad förvaring av avbrottsplaner i landstinget. Några planer finns på intranätet under rubriken manualer och systemförvaltning medan andra finns lagrade i databaser hos enskilda basenheter.

Vi rekommenderar att det av riktlinjerna för avbrottsplaner framgår på vilket sätt digitala avbrottsplaner ska finnas tillgängliga. En viktig del i detta är att underlätta uppföljningen av befintliga avbrottsplaner på central nivå i landstinget.

4.4. Landstingets beredskap för systemavbrott

Enligt verksamhetschef för informatikenheten och ansvarig för driften av landstingets IT-system finns hos informatikenheten inga dokumenterade rutiner för återstarter av IT-system. Den prioriteringslista som omnämnts tidigare i rapporten baseras på drifttekniker kunskap och erfarenhet. Förutom tidigare nämnda IT-system omfattar prioriteringslistan även landstingets servrar. En större omstart kräver att servrar startas i en bestämd ordningsföljd för att allt ska fundera. Enligt driftansvarig vid informatikenheten är prioriteringslistan ännu inte testad i skarpt läge.

I händelse av ett större avbrott som inträffar utanför ordinarie arbetstid har beredskapstekniker enligt sina anställningsavtal en inkallelsetid på två timmar. Det finns inga dokumenterade krav på att inställelsetiden ska vara

kortare. Vi har fått information från verksamheter om att det för vissa viktiga system finns batteribackup i endast ca två timmar.

Vi rekommenderar att landstingsstyrelsen utifrån en riskanalys säkerställer att landstinget har tillräckliga IT-resurser för att behålla kontinuiteten i landstingets verksamheter i händelse av IT-avbrott.

4.4.1. Prioritetsordning för återstart av system

Chefen för verksamhetsområde service har presenterat ett förslag på prioriteringsordning för omstart av system i händelse av större avbrott. Förslaget bygger på informatikenhetens sammanställning över IT-system. Prioriteringslistan bygger som tidigare nämnts på kunskap och erfarenheter hos informatikenhetens drifttekniker. Under hösten 2014 har förslaget presenterats för landstingets chefläkarråd. Chefläkarrådet har enligt sammanträdesanteckningarna gjort en första bedömning av prioriteringslistans innehåll.

4.4.2. Beslutsnivå för prioriteringsordning

Av granskningen framgår att det i Västerbottens läns landsting inte finns någon formellt beslutad prioriteringsordning för återstart av IT-system i händelse av avbrott.

När det gäller beslut om att prioritera strategiska IT-system så handlar det om beslut som kan ha stor påverkan på landstingets verksamheter. Vilken nivå som ska ta beslutet beror på beslutets karaktär. Enligt kommunallagen ska beslut av principiell karaktär fattas av fullmäktige.

Skulle det röra sig om ett beslut som inte faller inom ramen för principiell beskaffenhet så bör man fundera på om beslutet ska tas av ansvarig nämnd eller om det är möjligt att delegera beslutanderätten.

Vi rekommenderar landstingsstyrelsen och hälso- och sjukvårdsnämnden att säkerställa:

- att det görs en juridisk utredning om på vilken nivå beslut om prioriteringar av IT-system vid IT-avbrott ska fattas.

- att ett beslut om prioritetsordning för återstart av IT-system fattas på rätt nivå för deras respektive ansvarsområden.

- att beslut om prioritetsordning bygger på en inventering och värdering utifrån verksamheternas olika behov.

4.5. Fysiskt skydd av landstingets IT-infrastruktur

I augusti år 2012 drabbades landstingets serverhall av ett avbrott som i sin tur hade påverkan på de flesta av landstingets IT-system. Händelsen utreddes i en händelseanalys för att identifiera bakomliggande orsaker. Av analysen framkom en rad åtgärdsförslag. Ett av förslagen rörde behovet av en ny serverhall samt att serverhallarnas driftsäkerhet skulle ses över. Vidare fanns behov av en förnyad sårbarhetsanalys.

En ny serverhall togs i drift under våren 2014. De två gamla serverhallarna finns kvar som backup. Det finns back-up mellan de tre serverhallarna vilket ska säkerställa en kontinuerlig drift av landstingets IT-system. Enligt driftansvarig vid informatikenheten är planen att testa back-up systemet ett par

gånger varje år. Under år 2014 har en test genomförts i februari. Någon ytterligare test kommer inte att hinna genomföras under år 2014.

En byggbesiktning är gjord av landstingets fastighetsenhet. Serverhallen har dock inte genomgått någon kvalitetsbesiktning utifrån förutsättningarna att det är en serverhall. Det finns inga dokumenterade beslut i landstinget på vilka kriterier en serverhall bör uppfylla för att vara lämplig för ändamålet. Det går därför inte att bedöma om landstingets serverhall håller en säkerhets- och kvalitetsklass som är acceptabel för ändamålet.

När det gäller tillgången till datorhallarna har verksamhetschefen för informatikenheten under hösten 2014 beslutat om ett styrande dokument för behörigheter till datorhallarna. Dokumentet finns i informatikenhetens lokala ledningssystem. Styrdokumentet visar vilka rutiner som gäller för att lämna ut behörigheter till serverhallar och vilka personer som har denna access.

5. Sammanfattning av svar på revisionsfrågor

Vår bedömning utifrån granskningens resultat är att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte vidtagit tillräckliga åtgärder för att komma till rätta med de brister som identifierades i granskningen år 2010. Rekommendationerna från föregående granskning kvarstår.

Nedan följer en översiktlig sammanställning av revisionsfrågorna i tabellform.

Revisionsfråga	Bedömning	Kommentar
Finns det regler i landstingets ledningssystem där det framgår vilka i landstinget som har ansvar för att det finns fungerande avbrottsplaner?	Ja	Landstingsdirektören har beslutat om en systemförvaltningsmodell. Av modellen framgår att systemägaren har ansvar för att det finns en avbrottsplan innan ett IT-system tas i drift. Av förvaltningsmodellen framgår att verksamhetschefer i egenskap av informationsägare har ansvaret för att verksamheterna fungerande avbrottsplaner.
Finns regler eller rutiner för hur och när avbrottsplaner ska upprättas och revideras?	Delvis	Av systemförvaltningsmodellen framgår att avbrottsplaner ska finnas innan ett IT-system tas i drift. Hur avbrottsplanen ska se ut och vad den bör innehålla framgår inte av några dokumenterade riktlinjer. Vi har sett att avbrottsplaner som är upprättade inom informatikenhetens förvaltningar följer en gemensam mall. Avbrottsplaner där systemförvaltningen finns utanför informatikenheten följer inte någon gemensam struktur.
Finns en uppdaterad förteckning över landstingets samtliga IT-system och avbrottsplaner?	Nej	Det finns ingen samlad förteckning över landstingets IT-system och systemens avbrottsplaner.
Finns avbrottsplaner på en övergripande nivå för de tio systemen som av verksamhetsområdeschefer och informatikenhet värderats som mest verksamhetskritiska för landstinget?	Nej	Det finns dokumenterade avbrottsplaner för åtta av de tio mest verksamhetskritiska systemen. De IT-system som saknar avbrottsplan är i drift trots detta.
Finns avbrottsplaner på verksamhetsnivå för de enligt verksamheterna mest verksamhetskritiska systemen?	Nej	Granskningen visar att verksamheterna inte har avbrottsplaner för alla system som de själva har bedömt som kritiska för sina verksamheter.

Revisionsfråga	Bedömning	Kommentar
Finns någon formellt beslutad prioritetsordning för återstart av olika IT-system i händelse av-brott?	Nej	Det finns inte någon formellt beslutad prioritetsordning för återstart. Informa-tikenheten har upprättat en egen lista. Vid en förfrågan till landstingets verk-samhetsområdeschefer om vilka IT-system de anser mest prioriterade kunde vi se att dessa i stort överensstämde med informatikenhetens topp 10 lista.
Finns en central uppföljning av att aktuella IT-system har fungerande avbrottsplaner?	Nej	
Finns regler eller rutiner för hur avbrottsplaner ska förvaras?	Nej	Det finns inga rutiner vad gäller förva-ring vare sig för verksamheternas loka utskrivna avbrottsplaner eller för hur avbrottsplaner ska förvaras digitalt.

5.1. Rekommendationer

De flesta av våra rekommendationer från granskningen år 2010 kvarstår och sammanfattas nedan.
Vi rekommenderar att landstingsstyrelsen och hälso- och sjukvårdsnämnden säkerställer att:

- Det i landstingets ledningssystem finns riktlinjer för hur avbrottsplaner ska vara utformade, hur ofta de ska testas och revideras.
- Det av ledningssystemets riktlinjer framgår hur avbrottsplaner ska förva-ras lokalt ute i verksamheterna samt hur dessa digitalt ska förvaras för att underlätta uppföljning och kontroll på övergripande nivå.
- Det finns kontroller som säkerställer att riktlinjerna följs.
- Det görs en inventering av landstingets IT-system där en förteckning skapas som underlag för bedömningen av vilka system som är strate-giskt viktiga och verksamhetskritiska för landstinget.
- Det 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.
- Det finns ett beslut om vilken nivå av IT-resurser som behövs för att bibehålla kontinuiteten i landstingets verksamheter i händelse av avbrott.
- Det finns beslutade kriterier för vad en serverhall i landstinget ska upp-fylla för att vara lämplig för ändamålet.

Umeå den 4 december 2014

Eva Röste Moe
Certifierad kommunal revisor
Västerbottens läns landsting