Missiv beslutsunderlag
Diarienr: 14LTK1283
Handläggare: Jan Cserpes, Kansliavdelningen
Datum: 2015-03-02

REGION KRONOBERG

Regionstyrelsen

Svar på revisionsrapport – Behörighetsgranskning Cosmic och Aplus, samt Granskning avseende IT- och informationssäkerhet

Förslag till beslut
Föreslås att regionstyrelsen beslutar

att ställa sig bakom svar till revisorerna.

att informera regionfullmäktige om rapport och svar.

Sammanfattning
EY har på revisorernas uppdrag genomfört en granskning av hanteringen av behörigheter samt uppföljningen av användandet av patientinformationen i Cosmic. Detta uppdrag har även innefattat kraftiga behörigheter i Region Kronobergs redovisningssystem Aplus. Därutöver har en granskning av IT- och informationssäkerhet för policys, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå genomförts.

Revisorerna konstaterar att strukturen för informationssäkerhetsarbetet inom organisationen fungerar tillfredsställande, även om områden finns som bör förbättras. Revisorerna uppfattar att det finns en god vilja att förbättra det interna kontrollarbetet i organisationen.

Revisorerna lyfter fram förbättringsområden i de båda rapporterna.

Behörighetsgranskning Cosmic och Aplus

Kommentar/förslag till revisorernas identifierade förbättringsområden

1. *En tydligare och mer sammanhållen process rörande behörigheter till SITHS-kort och behörigheter till Cosmic. Införa en slutlig kontroll som säkerställer att kontrollmomenten uppfyllts.*

REGION KRONOBERG

SITHS-koret är en tjänstelegitimation för både fysisk och elektronisk identifiering. Det ger i sig ingen behörighet till något system. Kortet är en säker identifiering av en person och det krävs en behörighet till själva systemet, exempelvis Cosmic. SITHS-kortet ger även en identifiering för användande av nationella eHälso-tjänster, som till exempel Pascal och Mina vårdkontakter.

Cosmic kräver ett SITHS-kort för identifiering. Utöver kortet behövs en behörighetstilldelning i Cosmic. Idag finns det en separat beställningen med ett eget webbformulär där behörig beställare fyller i ett antal parametrar. Dialoger pågår för att samordna Cosmics behörighetsbeställning och *anställningspaketet*. Det finns en del kvarstående frågor som t ex att behörighet i Cosmic ändras under en anställningsperiod och att det ”bakom” anställningspaketet finns en manuell hantering av alla parametrar.

Nationella eHälsotjänster kräver ett SITHS-kort för identifiering. Utöver kortet behövs en behörighetstilldelning i den nationella HSA-katalogen. Detta administrerar vårdenheterna själva direkt i Region Kronobergs verksamhetskatalog.

Avslut av SITHS-kortet, leder till att möjlighet att identifiera sig (inloggning) i Cosmic och i de nationella tjänsterna upphör. Förbättringsåtgärd kommer att vidtas för att säkerställa att behörigheten till Cosmic upphör. Det genom att ett automatgenererat ärende till VIS-support skapas, när en person avslutas via anställningspaketet. Region Kronoberg kommer att återgår till rutinen att ta bort behörigheter för användare som inte har varit aktiva på tre månader. Detta innebär en dubblerad säkerhet för att ta bort åtkomst till Cosmic. Är SITHS-kortet ogiltigt eller behörigheten i Cosmic avslutad får användaren inte någon åtkomst till Cosmic.

I samband med beställning av avslut av tjänst i anställningspaketet eller via ärende-hanteringssystemet (Easit) avslutas behörigheter i systemen. Kortet ska i samband med att avslut görs, skickas in till intern kundservice för makulering. Det är varje chefs ansvar att återta den anställdes e-tjänstekort vid avslut av tjänst. Det saknas idag en automatisk kontroll av att kort inkommer då anställningspaketet inte har någon påminnelsefunktion för de moment som ska genomföras. En rutin för manuell hantering ska upprättas och träda i kraft 2015-03-01. Det innebär en kontroll av samtliga avslutade ärenden för att säkerställa att kortet har inkommit för makulering. Ansvarig för upprättande av rutinen är avdelningschef för intern kundservice.

2. *Alla enheter bör använda Anställningspaketet (ett antal kontroller och dokument som används vid till exempel nyanställning) för att få en enhetlig kontrollstruktur.*

Samtliga anställda som har ett anställningsförhållande med Region Kronoberg hanteras via anställningspaketet, det gäller både vid nyanställning, byte av tjänst samt avslut av tjänst. Det är närmast ansvarig chef som tar initiativ till beställning av anställningspaketet. För övriga som har behov av ett e-tjänstekort hanteras beställningar via ärendehanteringssystemet Easit. Det kan gälla personer som är anställda vid kommuner, samt hyrpersonal.

3. *Uppföljning av att loggkontroller utförts bör utökas.*
4. *Införa tydligare instruktioner om hur de lokala loggkontrollerna ska utföras.*

Svar till punkterna 3 och 4.

Verksamhetschefen är ansvarig för att loggkontroller genomförs på sin vårdenhet. Detta har förtydligats i riktlinjen ”Behörighet och åtkomst till Cosmic” som gäller från 2014-11-10, denna omfattar även loggkontrollen.

I Region Kronobergs internkontrollsplan finns en central uppföljningspunkt för kontroll av loggar. Den centrala kontrollen är genomförd årligen med en uppföljning.

Processen för uppföljning förbättras genom att utöka antalet uppföljningar på de verksamheter som inte har en tillfredsställande dokumentation av loggkontrollen. Detta sker månadsvis tills de har en tillfredsställande dokumentation. Rutinen för loggkontroll har uppdaterats med denna förbättrade uppföljning.

Användare och verksamhetschefer har en hög förståelse för att loggkontroller ska genomföras. Dock finns det en stor önskan om ett bättre IT-stöd där ett avvikande beteende kan identifieras och följas upp. En förstudie om hur detta ska lösas för samtliga loggar av patientinformation (loggar från olika system) i Region Kronoberg ska genomföras. Syfte är finna en lösning där verksamhetscheferna (eller den de har delegerat uppdraget till) får ett bra IT-stöd, med beslutsstöd för loggkontroller. Region Kronoberg kommer, enligt de nationella riktlinjerna, även publicera loggen till invånarna själva när denna nationella tjänst finns tillgänglig i ”journal via nätet”.

5. *Finns många användare med kraftiga behörigheter till ekonomisystemet Aplus.*

Inför 2015 har samtliga behörigheter till ekonomisystemet Aplus gåtts igenom och gjorts om. De nya behörigheterna börjar användas 1 januari 2015 och de gamla stängs löpnade under de första månaderna 2015. I den nya behörighets-strukturen kommer endast sex personer ha kvar kraftiga behörigheter. Av dessa sex personer är det tre konsulter hos Aditro som fortsätter ha kraftiga behörigheter. Det för att Aditro ska kunna utöva den supportfunktion Region Kronoberg har behov för. Resterande kraftiga behörigheter innehas av två personer på IT systemstöd ekonomi och av en person på redovisningsstöd.

Granskning avseende IT- och informationssäkerhet

Kommentar/förslag till revisorernas identifierade förbättringsområden

1. *Det är naturligt att inta alla system och avdelningar har samma höga säkerhetsnivå som t ex Patientsystemet, men där det bör finnas en tydlighet vilka regler som gäller för vad.*

Region Kronoberg ska införa en modell informationsklassning.

REGION KRONOBERG

Modellen för klassificering ska baseras på säkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Nivåbestämningen ska utgå från bedömd skada vid obehörig åtkomst, bristande riktighet, bristande tillgänglighet och bristande spårbarhet. Klassificeringen av informationstillgångar ska ligga till grund för vilka skyddsåtgärder som ska utformas och vilka rutiner som ska gälla, dvs. hur informationen får hanteras, lagras, distribueras och avvecklas. Strävan är att åstadkomma en konsistent bedömning av en och samma informations värde oavsett var eller av vilken verksamhet informationen hanteras.

2. *Det finns omfattande policys och riktlinjer inom organisationen, men den generella uppfattning är att dessa inte riktigt när ut till användarna i den omfattning som behövs i den verksamhet som Lanstinget bedriver.*

Inom landstinget finns det en Policy, den är övergripande för hela verksamheten. I och med regionbildningen (1/1 2015) kommer denna policy ses över för att mer harmoniera med Region Kronobergs uppdrag. Avseende riktlinjerna inom organisationen ska även dessa ses över med hänsyn till Region Kronobergs uppdrag. Både policy och riktlinjer ska därefter kommuniceras till användarna i den omfattning som behövs för att bedriva den verksamhet som Region Kronoberg gör.

3. *Det bör även finnas tydligare instruktioner och struktur i hur det övergripande kontrollarbetet ska utföras, för att säkerställa att de kontroller Landstinget vill ha på plats, verkligen utförs som tänkt och i den omfattning som tänkt.*

Årligen ska det upprättas en granskningsplan för de interna kontrollerna, i syfte att följa upp att det interna kontrollsystemet fungerar tillfredsställande. Resultatet av den antagna planens uppföljning ska rapporteras i den omfattning som anges i planen.

Regiondirektören ska senast i samband med årsredovisningen ge en samlad återrapportering av resultatet från granskningen av den interna kontrollen till regionstyrelsen.

Martin Myrskog
Regiondirektör

Jan Cserpes
ITdirektör

Bilagor: Missiv IT-granskningar
Behörighetsgranskning Cosmic och Aplus
Granskning avseende IT- och informationssäkerhet

Revisionsrapport 2014
Genomförd på uppdrag av de förtroendevalda revisorerna i Landstinget Kronoberg

Behörighetsgranskning Cosmic och Aplus

Landstinget Kronoberg

18 augusti 2014

Revisionsrapport 2014
Genomförd på uppdrag av de förtroendevalda revisorerna i Landstinget Kronoberg

Innehåll

1 Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Landstinget Kronoberg har EY genomfört en granskning kopplad till patientsystem Cosmic. Detta för att få en uppfattning om hur behörigheter hanteras samt om uppföljning görs på användandet av patientinformationen. Uppdraget har även innefattat att titta på kraftiga behörigheter i Landstinget Kronobergs redovisningssystem Aplus.

Att behörigheter i system är korrekt satta är väsentligt, då de styr vad en användare kan göra och se. Om för kraftiga behörigheter delas ut finns risk för att den interna kontrollen försvagas. Borttag av behörigheter på användare som inte längre skall ha tillgång till information och system reducerar t ex risken att en gammal behöriget används av någon annan.

I vissa fall är det svårt att ha kontroller i systemet som förbjuder visst handlande, men där spårbarhet och granskning av vad användaren gjort blir kontrollen. Cosmic är ett öppet system där användarna t ex ska kunna titta på de flestas patientinformation, men där det då också är möjligt att titta i logglistor vem som tittat på vilken patients information.

Vid vår granskning kan vi konstatera att kontrollen att granska om en användare tittat enbart på ”sina” patienter inte fungerat tillfredsställande under året. Efter händelser som hamnade i media för några år sedan var kontrollen fungerande men har successivt försämrats sedan dess. Denna sekretesskontroll är viktig för att patienter ska känna en trygghet i att enbart inblandade parter har tillgång till känslig information, och det bör säkerställas omgående att granskningskontrollen utförs.

För inloggning i Cosmic krävs ett Smartcard och lösenord, där kortet ska låsas eller förstöras när en användare slutar anställningen. Vi har noterat att denna hantering bör förbättras, där sju av 25 stickprov inte hade låsts efter 15 dagar. Fyra av dessa var vid vår granskning olåsta, och tre av dem hade fortfarande aktiva konton öppna i Cosmic. Vår uppfattning är att en slutlig kontroll bör införas som summerar upp alla delmoment som ska utföras vid en anställds avslut. Vidare bör det finnas färre undantag som använder Anställnings-paketet på Intranätet, för att säkerställa spårbarhet och kontroller i systemet.

Vid samtal och erhållna listor från systemadministratörer, rörande de kraftigaste behörigheterna i ekonomisystemet, såg de ut att vara rimliga. När vi sedan fick ett direktutdrag från systemet fanns det ytterligare fem kraftfulla användare där, totalt 13 stycken. Detta antal bör minskas anser vi. Vidare föreslår vi att behörigheterna bör gås igenom då 30 % av alla användare har en kraftig behörighet till minst en av modulerna Redovisning, Leverantörsreskontra och Kundreskontra, och därmed har möjlighet att ändra i t ex fasta register.

2 Bakgrund

2.1 Uppdrag

Landstingsrevisorerna har gett EY i uppdrag att biträda dem för att genomföra en översiktlig genomgång av rutiner och kontroller rörande behörigheter till patient-systemet Cosmic och redovisningssystemet Aplus.

För patientsystemet Cosmic har vi granskat av hur uppföljning av logglistor sker, som påverkar tryggheten av hanteringen av patientinformationen. Granskning har omfattats av förändringar av behörigheter i Cosmics, då både vid nyanställning, flytt av anställning inom Landstinget Kronoberg och avslut av anställning. I redovisningssystemet Aplus har vi fokuserat på kraftiga behörigheter, som påverkar trovärdigheten i redovisningens material och interna kontroller.

2.2 Metod

Vår genomgång har bland annat genomförts i form av intervjuer med personal från Landstinget Kronoberg avseende Cosmic och Aplus. Se bilaga 1 för en översikt över vilka personer som intervjuats.

Uppdraget har även omfattats av genomgång av rutiner och dokumentation kring behörigheter av patientinformationen i Cosmic. Genomgång har utförts genom stickprov på behörigheter till Cosmic. Vi har även utfört stickprov på Landstinget Kronobergs logglistor i Cosmic och uppföljning av dessa. Vidare har vi inhämtat behörighetslistor ur Cosmic och Aplus.

Rapporten har delats upp i detta inledande kapitel, granskningen utförd på Landstinget och slutligen en sammanställning av våra iakttagelser samt tillhörande risker och rekommendationer.

2.3 Omfattning och avgränsning

I vår genomgång av rutiner, kontroller och förändringar rörande behörigheter i Cosmic har vi tittat på upplägg av behörigheter vid nyanställning, flytt av anställning inom Landstinget, och avslut av anställning. Vi har bildat oss en generell uppfattning om hur behörigheter till patientinformationen hanteras.

Granskning har gjorts av Cosmics loggkontroll, att uppföljning sker av hur användare använt patientinformation i systemet. Viss uppföljning har även gjorts att de lagar och föreskrifter som finns inom Landstinget efterlevs. Vi har inte granskat huruvida verksamhetscheferna har informerat sina anställda om att loggar kontrolleras regelbundet. Vi har inte heller granskat hur Landstinget har hanterat och gått tillväga vid vård av offentlig person eller misstanke om brott.

För att verifiera Landstinget Kronobergs antal och grad i behörigheter i Cosmic och Aplus har vi inhämtat behörighetslistor ur dessa system. Vi har inte granskat vad respektive behörighetsgrupp omfattar i de olika behörigheterna i Aplus utan enbart behörighet 99, som är den kraftigaste behörigheten. De något lägre behörigheterna men fortfarande kraftiga, 81-98, har vi inte tittat på. För att granska dessa krävs en större genomgång, för att förstå vad de innebär och hur det är kopplat till intern kontroll. Vi har inte haft möjlighet till denna genomgång inom detta uppdrag.

2.4 Behörighet

En behörighet i ett system innebär att användaren har access till data och program och denna access bör vara begränsad till användarens ansvarsområde. Behörigheten hos användare påverkar då trovärdigheten på systemet och dess data, då denna styr vilken data som kan ändras och även i viss mån hur ett system beter sig, t ex rörande kontroller och rapporter i systemet. Ju viktigare systemet och dess data är för verksamheten och dess beroenden, desto viktigare är det att förändringarna av behörigheter görs med rimlig nivå på kontrollmoment, men även dokumenteras för att ge historik i förändringarna.

Behörigheter i Cosmic och hantering av patientdata styrs av Patientdatalagen. Loggar används för att kontrollera att de anställda använder sina behörigheter på ett korrekt sätt och i Cosmic för att kontroller att patientens integritet skyddas. Enligt Landstingets – Rutin för kontroll av loggar: ”Behandlingshistorik (logg) ska finnas för att kontrollera åtkomsten till personregister enligt patientdatalagen (SFS 2008:355) samt föreskriften SOSF 2008:14”. Loggningskontroller är till för att spåra åtkomsten av patientdata. Loggar sätts upp efter vad man vill ska loggas.

I vår granskning har vi utgått från vad man kan komma åt i systemet, och bortser då från t ex manuella blanketter och kontroller som ska genomföras för att t ex få tillåtelse att titta på en patient på en annan avdelning.

2.4.1 Behörighet till patientinformationen

I Cosmics är behörigheter viktiga för att undvika att oegentligheter skulle kunna ske då medarbetare hanterar patientinformation felaktigt, t ex receptförskrivning. Systemet är ändå så öppet att det inte krävs en kopplad vårdrelation (t ex att chef kopplar ihop sköterska med patient inne i systemet) i Cosmic för att ha möjlighet att se en patients journal. Däremot finns det möjlighet att spärra viss patient-information från denna öppenhet. Spårbarheten gör däremot att det i efterhand går att se vem somt ex varit inne och tittat på en specifik patients information.

Enligt uppgift av Landstinget krävs i första hand ett aktiverat konto i Cosmics, men därefter även ett aktivt Siths-kort, som ska vara upplagt med aktiverat användar-id, för att få access till patientinformationen och Cosmics. Siths-kortet är kopplat till den anställda med fotografi på och sätts in i datorn tillsammans med den anställdes personliga användar-id och lösenord. Inom Landstinget Kronoberg används samma användar-id på samtliga IT-system, enligt uppgift.

2.4.2 Behörighet till redovisningen

I Aplus, redovisningssystem, är behörigheter viktiga för att undvika oegentligheter och försummelse av Landstingets redovisning, för att redovisningen ska bli trovärdig och tillförlitlig.

För att komma in i programmet till redovisningen och Aplus har vi informerats om att användaren måste läggas upp först som användare i Aplus, men även ha ett konto i nätverket och att detta nätverkskonto gets tillåtelse att öppna programmet Aplus.

3 Patientsäkerhet i Cosmic och loggkontroller

3.1 Bakgrund

Vid samtliga nyanställningar, byte av tjänst eller avslut inom Landstinget Kronoberg, används ett fördefinierat så kallat Anställningspaket på Intranätet, där registrering av behörig chef ska ske. Ändringen begärs i Anställningspaketet, vilket sedan utförs av avdelningen Kortservice, Service 2020, hos Landsting Kronoberg.

3.2 Granskning av behörigheter och förändringsprocessen rörande dem

3.2.1 Processen enligt teorin

För förändringar i behörigheter i Cosmic finns det en dokumenterad process om hur det ska gå till. Vid förändringar av behörigheterna rörande: Nyanställd, Ska byta tjänst eller Slutar inom Landsting, används formuläret ”Anställningspaket”, som finns tillgängligt på internwebben.

Vid nyanställning fylls formuläret Anställningspaketet i av verksamhetschefen, som även ansvarar för att formuläret fylls i korrekt. Verksamhetschefen ansvarar även för att personen får rätt behörighet och utbildning efter de behov som tjänsten kräver.

Om en anställd byter tjänst inom Landsting Kronoberg fyller aktuell chef i Anställningspaketet om att den anställda byter tjänst, och ansvarar för att gamla behörigheter tas bort. Den nya chefen ansvarar för att den anställda får nya korrekta behörigheter till den nya tjänsten.

Avslut av sin anställning sker också via Anställningspaketet, där den anställde ansöker om avgång och verksamhetschefen godkänner avgången, och därefter ansvarar för att avslut genomförs korrekt. Vid inhyrning av medarbetare och denna slutar klipps Siths-kortet sönder, men användaren ligger kvar i systemet.

Avdelningen Kortservice, ”2020”, genomför efter information från Anställnings-paketet registrering eller avregistrering av Siths-kortet efter aktuellt datum. Den anställdes Siths-kort avregistreras inte förrän Kortservice erhållit det sönderklippta kortet fysiskt. Det är respektive handläggare på Kortservice som ansvarar för att aktivt gå in och spärra Siths-kortet på rätt dag, när kortet erhållits av verksamhetschefen.

På uppdrag, eller en gång om året (vanligtvis sommaren) granskas de anställdas behörigheter att de är korrekta av verksamhetschefen. Det är dennes ansvar att anställda på sin avdelning är korrekt och har rätt behörigheter. Vanligtvis dokumenteras inte denna kontroll och det går då inte i efterhand att verifiera att kontroll skett.

3.2.2 Kontroll utanför Anställningspaketet

Huvuddelen av de anställda inom Landstinget Kronoberg använder Anställnings-paketet, förutom anställda inom Tandvårdcentrum. Det finns även ytterligare ett fåtal användare inom Landstinget Kronoberg som ligger utanför Anställnings-paketet. Dessa finns på en separat lista, som kontrolleras var tredje månad av Kortservice, för att verifiera att listan är aktuell.

3.2.3 Resultat

Vi har i vår granskning kontrollerat hur processen fungerar vid nyanställning, avslut av anställning och vid flytt till annan tjänst inom Landstinget Kronoberg.

Rörande avslut av anställning och flytt av anställning inom Landstinget Kronoberg har vi utfört 25 stickprov. Se sammanfattning i tabellen nedan.

Antal dagar	Förflyttad	0-3	3-8	8-15	>15	Ej Spärrade	Totalt
Antal stickprov	13	3	1	1	3	4	25
%	52%	12%	4%	4%	12%	16%	

Utförd granskning visade att fyra av 25 Siths-kort inte blivit spärrade efter avslutad anställning. Av dessa fyra var tre anställningar avslutade på lönavdelningen men Siths-kortet var fortfarande aktivt. Kortet avslutades vid vårt besök och kontroll utfördes. Ett kort var fortfarande aktivt trots att personen slutat i februari 2014. Detta Siths-kort ligger, enligt information från avdelningen, sönderklippt hos dem men är inte inskickat till Kortservice och inte heller korrekt avslutat av aktuell chef. Av de fyra korten som inte blivit spärrade hade tre fortfarand aktiva konton i Cosmic.

Vi har även utfört stickprov på nyanställda och då främst tittat på att det är rätt chef som beställt och gjort ansökan om Siths-kort. Se sammanfattning i nedan tabell.

Antal beställningar	Beställningsunderlag		Godkänd av	
	Korrekt	Saknas	Chef	Godkänd ställföretr.
Antal stickprov	13	2	6	9
%	87%	13%	40%	60%

Alla ansökningar var godkända av behörig person. Däremot kan vi konstatera att rutinerna säger att beställande chef ansvarar för att spara historiken av beställningar under lång tid. På IT-avdelningen sparas denna historik under tre månader och sedan raderas den. Vid personalbyte mm kommer denna historik då inte att vara tillgänglig och det finns då inte någon säkerhet att det går att se vem som godkänt en beställning om den är äldre än tre månader. Det är fallet med de två underlag som saknas i tabellen ovan.

3.3 Loggkontroller

3.3.1 Teori

Landstinget har en tydlig rutin upprättad för hur loggar ska kontrolleras. Rutinen beskriver att verksamhetschefen (eller delegerad person) slumpmässigt ska välja ut patienter och användare (personal) varje månad, för att se vilka användare som varit inne på vilken patients information. Vidare beskriver rutinen att all personal ska kontrolleras minst en gång per år, men även att kontroll ska utföras vid misstanke om brott. Det är verksamhetschefernas ansvar att informera medarbetarna om insatsen som görs. Enligt rutinen ansvarar IT-avdelningen för att kontrollera att kontrollen av loggar utförs. Rutinen beskriver även att förvaltaren av personregistret löpande ska kontrollera loggarna övergripande.

Från och med 2013 har Landstinget Kronoberg en central enhet för utlämnande av loggrapporter efter en patients förfrågan, enligt ”Årlig rapportering av informationssäkerhet i enlighet SOSFS 2008:14 för verksamhetsåret 2013”. Detta har noterats i Rutin för kontroll av loggar att ”Informationen ska vara så utformad att patienten kan göra en bedömning av om åtkomsten har varit befogad eller inte.”

Loggkontrollerna dokumenteras i ett Exceldokument per vårdenhet i mappar (ca 60 vårdenheter). Dokumentationen innefattar information om tidpunkt för utförd kontroll, granskad period, om vilken patient eller användare det avser, resultat av granskningen och signatur på vem som utfört granskningen.

3.3.2 Resultat

Vid vår granskning noterar vi att det inte finns bestämt urval på hur de slumpmässiga urvalen ska tas för att välja patient eller anställd. Vi har utfört stickprov på 25 stycken vårdenheter och deras loggkontroller gjorda 2014. Se sammanfattning i tabellen nedan.

Kontroll utförd	2014-05	2014-01 till 2014-03	Inte alls under 2014	Totalt
Antal stickprov	15	3	7	25
%	60%	12%	28%	

Vårt urval visade att 10 vårdenheter inte utfört sin loggkontroll enligt de rutiner som finns. Vår granskning visade även att vårdenheterna utför loggkontrollerna på olika tidsspann (vissa månadsvis, vissa över några få dagar). Enligt information från en vårdavdelning på Landstinget så utförs extra kontroll när offentlig person kommer in på avdelningen. I vårt urval fanns ingen loggkontroll som utförts på grund av misstanke eller att patienten var offentlig person, vilket inte utesluter att denna kontroll ändå utförs.

4 Behörigheter i redovisningssystemet Aplus

4.1 Bakgrund

Information vi fått från Landstinget är att användaren måste läggas upp som användare i Aplus, men även ha ett användar-id i nätverket, som ska vara kopplat till nätverksgruppen Aplus för att komma in i systemet. Inloggning i Aplus sker automatiskt genom ett så kallat Singel Sign on, där nätverkskontroller verifierar vilka som får logga in på ett specifikt system.

4.2 Granskning av kraftfulla behörigheter i redovisningssystemet Aplus

En kraftfull behörighet innebär vanligtvis att användaren har rätt att göra förändringar på hur systemet arbetar (t ex göra så en kontroll slutar fungera eller ändra i en rapport), initiera och genomföra transaktioner (lägga upp leverantör, lägga in faktura och få den betald), och ändra behörigheter i vad andra användare har rätt att göra och se (t ex ge medarbetare behörigheter med eller utan chefs godkännande). Risk finns att användare kan utföra dessa funktioner av misstag men även utifrån ett bedrägeriperspektiv.

Målsättningen för dessa kraftfulla behörighetskonton är att det ska vara så få användare som möjligt som har dem. Det bör även finnas kompenserande kontroller som fångar upp misstag och bedrägerier om det specifika området innebär extra stor risk för organisationen. Kontrollen för tilldelande av dessa behörigheter bör även vara förstärkt jämfört med vanlig tilldelning, liksom den löpande genomgången att användarna som har denna behörighet verkligen fortfarande är i behov av den.

4.2.1 Process enligt teorin

Behörighetssystemet är uppbyggt på att ju högre siffra du tilldelats, mellan 0 och 99, desto högre behörighet. En användare som har 99 räknas som administratör och kommer åt all information och alla funktioner i systemet. En användare tilldelas även ett ansvarsområde, t ex LK1 som står för koncernredovisning. En användare kan ha behörighet till flera ansvarsområden och däri olika behörighetsnivåer, t ex Redovisning 30-Kundreskontra 80-Levreskontra 50.

I Aplus har vi tittat på kraftfulla behörigheter, de med behörighet 99 inom någon av funktionerna Redovisning, Leverantörsreskontra och Kundreskontra. För att t ex göra ändringar på annan användares behöriget krävs 99. Vi har tittat på både listan som förvaltarna använder för sin administration, men främst listan som vi fått ut från systemet, på olika behörigheter.

Vi vill även notera att vi inte har tittat på t ex användare som har 81-98, vilket skulle kunna innebära kraftfull behörighet, och därmed möjlighet att gå förbi interna kontroller i systemet. T ex benämns en användare med behöriget över 80 som ” Administratör, Avancerad registrering” och har enligt information möjlighet till funktioner som ”Nyupplägg av kunder, leverantörer mm, filimport och export”. I

detta uppdrag har vi koncentrerat oss på de mest kraftfulla behörigheterna. För att granska övriga behörigheter krävs en större genomgång, för att förstå vad de innebär och hur det är kopplat till intern kontroll. Vi har inte haft möjlighet till denna genomgång inom detta uppdrag, men föreslår att detta görs i en kommande granskning, för att få en bättre uppfattning om intern kontroll i behörigheterna.

4.2.2 Resultat

Förvaltarna av systemet har en Excellista som de använder för att ha översikt på vilka personer som har vilken behörighet. I vår granskning har vi noterat att denna lista på anställda och behörigheter inte överensstämmer med den lista som systemet genererar i form av behörigheter.

Full access till	Redovisning	Leverantörs-reskontran	Kund-reskontran
Enligt System	13	12	12
Enligt intern översikt	8	7	7

Av ovanstående konton från systemrapporten, med användare som har full behörighet (99) i något område, ser sex konton ut att tillhöra normala användare, tre ser ut som testkonton och övriga tillhöra externa konsulter. Enligt information från systemförvaltare är det enbart två användare inom organisationen som ska ha full behörighet, men där vi då fann ytterligare fyra konton som ser ut att tillhöra anställda. Två administratörer med full behörighet ser rimligt ut, men om ytterligare fyra har denna behörighet bör analys utföras om detta antal är nödvändigt, med hänsyn tagen till den ökade risk som dessa konton medför.

Vid analys framgår det att det finns 50 användare av totalt 164 med behörighet över 80 (30 %) i minst ett av områdena Redovisning, Leverantörsreskontra eller Kundreskontra. Detta innebär att det är många som kan ändra i fasta register och initiera t ex nya leverantörer och fakturor. Vårt förslag är att en genomgång görs framöver av behörigheterna inom redovisningssystemet för att få en bild av hur den interna kontrollen är uppsatt i systemet.

5 Iakttagelser och rekommendationer

5.1 Behörigheter och förändringsprocess Cosmics

Landstinget Kronoberg har utvecklat ett system och rutinbeskrivning som stöder anställning, byte av tjänst och avslut av tjänst. Vår granskning har visat på att det fungerar i de flesta fall men att kontrollen och processen kan förbättras. Främst är det möjlighet till mer sammanhängande process och ett mer strukturerat arbetssätt, som bör minska risken för de fel vi påträffat. Vår bedömning är att rutinen bör se över och lägga till kontrollen att få en summering av avslutet av en anställning. Vidare bör Landstinget även utbilda respektive avdelning i Anställningspaketet. Landstinget bör höja kravet så att alla använder Anställnings-paketet och att undantag inte är tillåtna, annat än om högre chef godkänner detta vid respektive tillfälle.

5.2 Loggkontroll av patientinformation

Loggkontrollerna utförs inte i den omfattning som finns noterat i rutinbeskrivningarna. Det bör utformas tydligare instruktioner om hur loggkontrollen ska utföras och dokumenteras, för att säkerställa att de kontrollmoment som önskas verkligen genomförs, och på ett sätt som fångar upp riskerna som identifierats.

Det finns även en övergripande rutin som ska verifiera att dessa loggkontroller genomförs. Då denna inte dokumenteras går det inte att verifiera om den genomförts eller hur den gjorts. Vi föreslår att dessa rutinbeskrivningar blir tydligare om vilka kontrollmoment som ska ingå och även hur det ska dokumenteras för att ge en spårbarhet att kontrollen utförts.

5.3 Kraftfulla behörigheter i Aplus

Det fanns fler kraftfulla användare än systemförvaltarna noterat, i systemet, vilket ökar risken. Det finns även många vanliga användare med kraftfulla behörigheter, vilket gör att vi rekommenderar en genomgång av behörigheterna, för att säkerställa att behovet finns, och att profiler är uppsatta för att möta en god intern kontroll.

Bilaga 1 – Respondenter

Roll
Vårdinformationssystemansvarig: Helena Sjögren
Informationssäkerhetsstrateg: Ann-Katrin Axelsson
CTO: Karl Langen
Avdelningschef Service 2020: Annika Elmgren
Anställd Service 2020: LiseLotte W
Förvaltare och ansvariga för ekonomisystemet Aplus: Ingrid Hakamäki, Linda Friman, Claes Andersson,
Avdelningschef Ekonomi: Åsa Lupton

Revisionsrapport 2014 v2
Genomförd på uppdrag av de förtroendevalda revisorerna i Landstinget Kronoberg

Granskning avseende IT- och informations-säkerhet

Landstinget Kronoberg

18 augusti 2014

Innehåll

1. Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Landstinget Kronoberg har EY genomfört en granskning av IT- och informationssäkerhet, vad gäller policys, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå. IT-revisionens syfte har varit att granska och bedöma informationssäkerheten på en övergripande nivå i Landstinget. Som grund har granskningen gjorts utifrån Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS, och dess säkerhetsnivåer. BITS står för *Basnivå för informationssäkerhet* och har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000. En jämförelse har även gjorts med resultatet från liknande granskningar i andra offentliga organisationer.

Övergripande slutsatser

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Aktuellt område i BITS är hanterat och kontroll bedöms rimligen implementerad:	**66%**
Kontrollen identifierad och bedöms delvis implementerad:	**26%**
Kontroll har ej identifierats/Har inte kunna identifierats som implementerad:	**6%**
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2%**

Som siffrorna ovan visar finns det en struktur för informationsarbetet inom Landstinget som fungerar tillfredsställande, även om det finns områden som bör förbättras. Vi har också uppfattat det som att det finns en god vilja att förbättra det interna kontrollarbetet, i diskussioner vid våra besök och kontakter med Landstinget.

Det är naturligt att inte alla system och avdelningar vi kommit i kontakt med har samma höga säkerhetsnivå som t ex Patientsystemet, men där vi skulle vilja se en tydlighet vilka regler som gäller för vad. Det finns omfattande policys och riktlinjer inom Landstinget, men vår uppfattning är att dessa inte riktigt når ut till användarna i den omfattning som behövs i en verksamhet som Landstinget bedriver.

Vi skulle även vilja se tydligare instruktioner och struktur i hur kontrollarbetet ska utföras, för att säkerställa att de kontroller Landstinget vill ha på plats, verkligen utförs som tänkt och i den omfattning som tänkt.

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Bedömningen har gjorts utifrån om det anses vara en nyckelkontroll och hur stor risk det innebär för organisationen och dess interna kontroll, på kort och lång sikt. För HÖG prioritet rekommenderar vi att bristen snarast åtgärdas. Fullständiga iakttagelser med riskbedömningar och rekommendationer finns i kapitel 4.

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Formella regler saknas för informationsklassning, Information klassas formellt främst utifrån Tillgänglighet. Enligt BITS rekommenderas att alla system och information ska klassas utifrån Sekretess, Riktighet och Tillgänglighet. **Rekommendation:** Vi rekommenderar Landstinget att upprätta en informationsklassningspolicy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.	**Hög**
Iakttagelse: Borttag av behörigheter Rörande processen för Låsning och borttag av konton på personer som slutat finns det brister, där konton och kort ligger öppna för lång tid efter att personen lämnat organisationen. **Rekommendation:** Tydligare riktlinjer kan tas fram för hur information ska hanteras när anställd slutar och att denna kommuniceras till berörd personal regelbundet.	**Hög**
Iakttagelse: Granskning av efterlevnad I vår granskning kan vi konstatera att varken överordnade kontrollmoment eller kontrollen att granska de anställda fungerar i den utsträckning som är tänkt. **Rekommendation:** Vi rekommenderar att kontroller och rutiner verifieras regelbundet för att säkerställa en följsamhet och efterlevnad.	**Hög**

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Process för programändringar bör förstärkas Vissa delar av förändringsprocesserna är formella inom Landstinget. Det finns däremot ingen generell plan i Landstingets IT-säkerhetsanvisningar gällande förändringar i system och driftgodkännande. **Rekommendation:** Vi rekommenderar Landstinget Kronoberg att utveckla den existerade processen för programförändringar och väsentliga konfigureringar.	**Medel**
Iakttagelse: Olika nivå på tillgänglighetsbedömningar och rutiner Det finns centrala katastrofplaner med t ex vem som beslutar om katastrof-läge. Vår uppfattning är att det saknas en samstämmighet i Landstinget om tillgänglighetstider i olika system. Av annan information vi fått ser det ut som att det är olika nivå på reservrutiner, och kunskapen om hur de ska handla om systemen inte finns tillgängliga. **Rekommendation:** I första hand bör verifiering ske av de bedömningar som idag finns satta per system, med verksamheten. Därefter bör det säkerställas att verksamheterna tagit fram reservrutiner.	**Medel**
Iakttagelse: Utbildning Vår uppfattning är att det finns mycket policys och riktlinjer dokumenterat. Däremot behöver denna information kommuniceras ut till berörd personal mer regelbundet än vad som görs idag. **Rekommendation:** Vi rekommenderar att Landstinget löpande utför utbildning och att utförandet av denna dokumenteras på något sätt.	**Medel**
Iakttagelse: Uppföljning av tilldelade behörigheter Det finns ingen formell rutin i Landstinget för att följa upp att rätt användare ligger i respektive system och att användaren har rätt behörigheter utifrån ansvarsuppgifter och intern kontroll. I vissa fall utförs kontroller men de dokumenteras inte och det går då inte se att de har utförts. **Rekommendation:** Vi rekommenderar Landstinget Kronoberg att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen.	**Medel**

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Extern kommunikation Administration av brandväggar görs av Landstinget. Det finns inte någon beslutad lista på regler och tjänster som skall vara tillgängliga i brandväggen, som det är möjligt att verifiera mot. De tester som sker av säkerheten i brandväggen sker enbart internt och inte av några externa experter. **Rekommendation:** Uppsättningen av brandväggen bör beslutas och dokumenteras. Vi rekommenderar att det finns policy som tydliggör hur och när tester ska ske av brandväggen och där överväga om extern expertis ska involveras.	**Medel**

2 Bakgrund

2.1 Syfte

Idag bedrivs en stor del av all verksamhet i ett landsting med hjälp av någon form av datoriserat stöd. Stödet har med tiden utvecklats till att bli en förutsättning för att kunna bedriva verksamheten. För att uppnå Landstingets verksamhetsmål krävs att informationen i verksamhetsstödet är tillgängligt, riktigt, har korrekt sekretess samt är spårbart.

På uppdrag av landstingsrevisorerna i Landstinget Kronoberg har EY genomfört en granskning av IT- och informationssäkerhet. Granskningen har varit inriktad på policys, riktlinjer och hantering av säkerhetsfrågor på en övergripande nivå i Landstiget.

Syftet med granskningen har varit att få en översiktlig bild av hur arbetet med IT- och informationssäkerhet inom Landstinget hanteras. I granskningen har gällande säkerhetsnivåer bedömts mot BITS, Myndigheten för samhällsskydd och beredskaps (tidigare Krisberedskapsmyndigheten) ramverk för informationssäkerhet. BITS står för *Basnivå för informationssäkerhet* och har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000. En jämförelse har även gjorts med resultatet från liknande granskningar i andra offentliga organisationer.

2.2 Metod

Baserat på erfarenheter från tidigare granskningar inom offentlig verksamhet har EY valt ut ett antal relevanta kontroller som presenteras i BITS, fördelat på elva huvudområden:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

Rapporten redovisar i vilken grad Landstinget uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom granskning av erhållen dokumentation.

Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

Ja	Aktuellt område i BITS är hanterat och kontroll bedöms vara rimligen implementerad. I förekommande fall ges rekommendationer och kommentarer även till denna bedömning.
Delvis	Kontrollen är identifierad men bedöms delvis vara implementerad.
Nej	Kontroll har ej identifierats/Har inte kunnat identifieras som implementerad.
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl.

Analysen baseras på erhållen dokumentation samt på intervjuer med följande funktioner:

- Förvaltare informationssystem och eHälso-strateg
- Redovisningschef
- Redovisningsekonom
- Förvaltare för ekonomisystemetet Aplus
- Informationssäkerhetsstrateg, Personuppgiftsombud
- Avdelningschef Fastighetsdrift
- Verksamhetschef Medicinkliniken
- Driftschef Nätverk
- Administratör säkerhetskort inloggning Cosmic (Avd 2020)

Granskningen har genomförts av Per Magnusson, auktoriserad revisor, CISA och IT-revisor, Jessica Andersson och Josefine Olsson under maj-juni 2014.

Kvalitetssäkring har skett av auktoriserad och CISA-certifierad revisor inom EY samt Peter Bjureberg, auktoriserad revisor. Utöver EY:s interna kvalitetssäkring har intervjuade haft möjlighet att lämna saksynpunkter på rapportutkastet. Detta för att säkerställa att revisionsrapporten bygger på korrekta fakta och uttalanden.

2.3 Avgränsningar

Iakttagelser och analyser baseras enbart på information som har inhämtats vid intervjuer och aktuell dokumentation. Få tester har genomförts, t ex att en kontroll är implementerad. Det kan finnas brister i Landstingets hantering av IT som vi inte har identifierat inom ramen för denna granskning. Arbetet har inte omfattat test av generella IT-kontroller eller applikationskontroller.

Denna rapport tar endast hänsyn till nuläget i Landstinget Kronoberg. De områden som ingått i denna genomgång är följande:

- Cosmic
- Ekonomisystemet Aplus
- Fastighetsförvaltning
- Viss verksamhetsinformation, t ex från Medicinkliniken.

3 Iakttagelser

I detta avsnitt presenteras de iakttagelser som framkommit i granskningen. Systemen i tabellen nedan är de verksamhetskritiska system som identifierats av respektive deltagande intervjuperson och det är dessa system som ingått i granskningen:

System	Beskrivning	Leverantör
Cosmic	Socialt verksamhetssystem	Cambio
Aplus	Utförarsystem integrerat med ProCapita	Aditro
	Fastighetssystem	

3.1 Granskningsprotokoll

Granskningsområden		Kommentar	Utvärdering
1 Säkerhetspolicy			
1.1	Har Landstinget en informations-/IT-säkerhetspolicy?	Det finns informationspolicys. Dokumentet ”Regler för IT-användare” riktar sig övergripande till användare. Därutöver finns ett flertal riktlinjer för olika områden.	Ja
2 Organisation av säkerheten			
2.1	Finns det en informationssäkerhetssamordnare/-funktion för informationssäkerhet	Det finns en anställd inom Landstinget med funktionen som informationssäkerhetsansvarig. Enligt policy står det även att Landstingsdirektören har det övergripande ansvaret för informationssäkerheten.	Ja
2.2	Har ledningen utsett systemägare för samtliga informationssystem?	Centralt på IT-avdelningen finns det ett register med alla system och dess ägare och förvaltare. Under året håller man även på att förändra förvaltningsmodellen för att följa metodiken PM3, vilket till viss del även ändrar ansvarsområdena.	Ja
2.3	Har organisationen utsett systemansvariga?	Det finns en tydlig ansvarsroll som system-förvaltare och det finns dokumenterat.	Ja
2.4	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?	Det finns arbetsgrupper med representanter från olika verksamheter inom Landstinget.	Ja
2.5	Har ansvaret för informationssäkerheten reglerats i avtal för informationsbehandling som lagts ut på en utomstående organisation?	I stort sett all information hanteras inne i det egna kontrollerade nätverket. Den information som går utanför är antingen krypterad eller annars inte personidentifierbar, t ex rapportering från pacemakerpatienter automatiskt. Det finns avtal som ska signeras när externa parter ska få tillgång till Landstingets nät, t ex systemkonsulter.	Ja

Granskningsområden		Kommentar	Utvärdering
3 Hantering av tillgångar			
3.1	Är organisationens information klassad avseende sekretess/riktighet/tillgänglighet?	IT-avdelningen har gjort en intern bedömning på tillgänglighetskraven på olika system. Vårdsystemet Cosmic hanteras utifrån kraven på hög sekretess men det finns inte något dokumenterat. I de flesta fall skrivs det på tystnadsplikt vid anställning.	Nej
3.2	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning.	Certifiering av installation av programvara sker av IT, som då även förtecknar dessa. Egen installation ska inte vara tillåten eller möjlig.	Ja
3.3	Finns det en ansvarsfördelning för organisationens samtliga informationstillgångar.	Det finns ingen självklar och tydlig ansvarfördelning av informationen. Formell ägare finns men i verkligheten inte så tydligt. Förvaltare finns för samtliga system men inte säkert för alla informationstillgångar. Verksamhetschefer är ansvariga för sin information/data i systemet och de sätter upp riktlinjer för vem som har behörighet till vad.	Delvis
3.4	Finns det upprättat dokument för hur informations-behandlingsresurser får användas?	I dokumentet "riktlinjer för IT-användare" finns mycket av informationen. Finns även andra riktlinjer för specifika områden. Då det inte finns någon klassning på informationen finns det inte heller tydlighet hur man får behandla informationen i alla system. T ex finns det ett passagesystem som enbart Polisen eller säkerhetsavdelningen får beställa information från, men där denna rutin och begränsning är oskriven.	Delvis
4 Personalresurser och säkerhet			
4.1	Granskas nyanställdas bakgrund vid nyanställning i proportion till kommande arbetsuppgifter?	Finns oskrivna rutiner beroende på i vilken verksamhet man ska arbeta på och då görs olika undersökningar av bakgrund. I vissa fall tas information fram från belastningsregister, men det har även förekommit fall där det i efterhand framkommit från externa källor att person har olämplig bakgrund rörande brott.	Delvis
4.2	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller?	Inhyrd personal har samma krav som de ordinarie anställda. De anställdas individuella avtal styr vilken information de behöver och det framgår även av samarbetsavtalet med uthyraren att det i de flesta fall är uthyrningsföretaget som ansvarar för utbildningen av säkerhetskraven. För t ex vikarier finns det enligt Landstinget en egen resursenhet som behandlar detta.	Ja
4.3	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information?	Krav framgår både genom juridiskt stöd av lagar, att t ex allt skall dokumenteras i journal, men även internt att anställda ska får utbildning. Riktlinjer, arbetssätt och lagen går hand i hand för att arbetet ska kunna utföras. Riktlinjer finns för vissa arbetsgrupper och de är då mer specifika. I intervjuer framkommer det ändå synpunkter på att kraven i vissa fall borde vara högre, då främst kunskapen i systemen är för låg som då orsakar användarfel.	Ja

Granskningsområden		Kommentar	Utvärdering
4.4	Finns det framtagna dokumenterade säkerhetsinstruktioner för användare?	Det finns instruktioner i "Riktlinjer för IT-användare", som täcker området generellt men saknas specifika instruktioner för t ex ekonomisystemet.	Delvis
4.5	Genomförs utbildningsinsatser inom informationssäkerhet regelbundet?	Utbildningar genomförs men de är inte regelbundna.	Nej
4.6	Finns det användarhandledning för ett informationssystem att tillgå?	Ja, användarhandledningar finns att tillgå.	Ja
4.7	Dras åtkomsträtten till information och informationsbehandlingsresurser in vid avslutande av anställning eller vid förflyttning?	Standardiserat dokument finns för när någon slutar eller byter avdelning. Vid granskning av 25 stickprov rörande avslut på inloggningskortet, som är krav för inloggning i Cosmic, fanns det fyra användare som slutat mer än en vecka tidigare utan att kortet var låst. I något fall över två månader. Det finns även andra avdelningar, där andra program än Cosmic används, som upplever att kommunikationen till systemförvaltarna att ta bort användare inte fungerar som önskat.	Delvis
5 Fysisk och miljörelaterad säkerhet			
5.1	Finns funktioner för att förhindra obehörig fysisk tillträde till organisationens lokaler och information?	*Informationen rörande detta område, 5 Fysisk och miljörelaterad säkerhet, har vi enbart muntligen fått ta del av.* Lokalerna har gott fysiskt skydd med låsta dörrar och kodlås, men även rent fysiskt väl skyddade från omgivningen.	Ja
5.2	Har IT-utrustning som kräver avbrottsfri kraft identifierats?	Avbrottsfri kraft är kopplat till IT-rummen och alla IT-system har avbrottsfri kraft. Det finns även dokumentation som beskriver var avbrottsfri kraft finns.	Ja
5.3	Finns larm kopplat till larmmottagare för: - brand, temperatur, fukt - sker test till larmmottagare	Larm finns för olika områden och testning sker regelbundet.	Ja
5.4	Finns i direkt anslutning till viktig dator- kommunikationsutrustning kolsyresläckare?	Ja, det ska finnas släckningsutrustning i och i anslutning till främst serverrum.	Ja
5.5	Regleras tillträde till utrymmen med känslig information eller informationssystem utifrån informationens skyddsbehov? Tillträdesrättigheter, rutiner för upprättande?	All känslig information är samlad i IT-rummen och passerkort krävs för att komma in i dessa, som då ger en loggning på användare som gått in i dem.	Ja
5.6	Är korskopplingsskåp låsta?	Ja, alla skåp är låsta.	Ja
5.7	Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds?	När fysisk utrustning tas ur drift plockas all lagring bort från maskinen. All lagringsutrustning som tas ur drift skickas till extern leverantör, som dokumenterar serienummer och att all information på artikeln är helt rensad.	Ja
5.8	Finns särskilda säkerhetsåtgärder för utrustning utanför ordinarie arbetsplats?	För uppkoppling på Landstingets nät används Citrix. Uppkoppling sker med engångslösenord. För t ex mobiltelefoner används programvara för att kryptera information som är kopplad till Landstingets program.	Ja

Granskningsområden		Kommentar	Utvärdering
5.9	Finns information och regler som förklarar att informationsbehandlingsresurser inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?		Ej Tillämpligt
6 Styrning och kommunikation av drift			
6.1	Finns det driftdokumentation för verksamhetskritiska informationssystem?	Systemdriftsdokumentation och serverdrifts-dokumentation, beroende på vad ärendet avser. I något fall ser dokumentationen inte att vara fullständigt ifylld men de väsentligaste områdena finns på plats.	Ja
6.2	Är klockorna i informationssystemen synkroniserade med godkänd exakt tidsangivelse?	Ja, de är synkade enligt information från Landstinget.	Ja
6.3	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftmiljön?	All utveckling, som sker av externa konsulter, görs först i utvecklingsmiljö, vanligtvis i konsulternas miljöer. Testning sker sedan i testmiljö på Landstinget, för att därefter flyttas in i produktion när Landstinget godkänner detta.	Ja
6.4	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	Tjänster från utomstående är externa beställningar. I vissa fall kommer externa leverantörer och gör arbete och då finns det informella rutiner för att dessa inte får lämnas ensamma t ex.	Delvis
6.5	Godkänner lämplig personal (systemägaren) driftsättningar av förändrade informationssystem?	Förvaltningsledningsgruppen eller Förvaltarna för systemet tar beslutet.	Ja
6.6	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	Finns skydd både på servrar och klienter, enligt Landstinget.	Ja
6.7	Regleras och dokumenteras rätten att installera nya program, programversioner?	Finns i policyn "Regler för IT-användare" och att användare inte är administratörer på sina maskiner.	Ja
6.8	Har organisations nätverk delats upp i mindre enheter (segmentering), så att en (virus) attack enbart drabbar en del av nätverket?	Segmentering har gjorts i den utsträckning som Landstinget anser behövligt.	Ja
6.9	Genomförs säkerhetskopiering regelbundet?	Kontinuerlig backup körs. Både differentiella backuper var 10 minut på väsentliga system, och full backup varje natt. Data lyfts också ut till annat rum, med samma säkerhet, men då annan risk än vad som är för ursprungsdata.	Ja
6.10	Genomförs regelbundna tester för att säkerställa att informationssystem kan återstartas från säkerhetskopior?	Testning för främst Cosmic att återstart från säkerhetskopior är möjlig, sker regelbundet. Viss återläsning sker även för andra system, då de ligger i samma backuphantering som Cosmic.	Ja
6.11	Finns det en aktuell förteckning över samtliga externa anslutningar?	Ja, det finns dokumenterat.	Ja
6.12	Saknas alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket?	Finns inga alternativa vägar in i nätverket, enligt information från Landstinget.	Ja

Granskningsområden		Kommentar	Utvärdering
6.13	Är det möjligt att logga säkerhetsrelevanta händelser?	I patientsystemet Cosmic finns det loggningar på alla väsentliga händelser, inklusive vem som tittat på vilken patient. I t ex ekonomisystemet finns det inte mycket loggfunktioner, men där det är ett pågående uppgraderingsprojekt för att få denna funktion. Planeras vara klart till hösten.	Delvis
6.14	Finns särskilda skyddsåtgärder för att skydda sekretess och riktighet när data passerar allmänna nät liksom skydd av anslutna system och utrustning?	Inte mycket information passerar över allmänna nät men det som gör det är antingen krypterade eller helt anonymiserade.	Ja
6.15	Finns det riktlinjer avseende förvaringstid för datamedia?	Det finns riktlinjer för hur data ska arkiveras för väsentliga system, men i vissa fall är dessa äldre och ny översyn behöver göras.	Delvis
6.16	Finns det dokumenterade regler avseende vilken information som får skickas utanför organisationen?	Ja, i dokumentet "Regler för IT-användare" finns viss information, men även hänvisningar till ytterligare policys och Personuppgiftslagen.	Ja
6.17	Gäller det för e-postsystem och andra viktiga system att de är isolerade från externa nät? (DMZ) t.ex. genom någon form av brandväggsfunktion.	Ja, det finns.	Ja
6.18	Finns olika typer av autentiserings-metoder med olika grad av skydd?	Ja det finns enligt Landstinget. I känsliga system används kort och lösenord och i mindre känsliga system används lösenord. Inloggning på nätet använder engångslösenord.	Ja
6.19	Sparas revisionsloggar för säkerhetsrelevanta händelser?	Ja, i de fall de finns tillgängliga.	Delvis
7 Styrning av åtkomst			
7.1	Har organisationen satt upp dokumenterade regler för åtkomst/tillträde för tredjeparts åtkomst till information eller informationssystem?	Finns regelverk för hur externa parter ska hanteras.	Ja
7.2	Tilldelas användare en behörighetsprofil som endast medger åtkomst informationssystem som krävs för att lösa arbetsuppgifterna?	Enligt information från Landstinget tilldelas enbart behörigheter i den utsträckning de behövs. Rörande behörighet på ekonomiavdelningen sätts behörigheter så lågt det är möjligt för att utföra arbetsuppgifterna, enligt systemförvaltare på ekonomisystemet.	Ja
7.3	Begränsas rätten att installera nya program i nätverket samt den egna arbetsstationen till endast utsedd behörig personal?	Användare är inte Admin på sina maskiner och kan inte installera normala program.	Ja
7.4	Har samtliga administratörer fullständiga systembehörigheter, eller endast i den utsträckning som krävs för arbetsuppgifterna?	Behörigheterna är satta i den utsträckning de behöver det för sitt arbete, enligt Landstinget.	Ja
7.5	Har organisationen en dokumenterad rutin för tilldelning, borttag eller förändring av behörighet? Är de kommunicerade till ansvarig för behörigheter?	Det finns dokumenterad rutin hur det ska gå till och ska vara kommunicerad. Vissa verksamheter sköter inte återrapportering av personer som slutat på ett helt korrekt sätt. Se separat rapport om behörigheter.	Delvis
7.6	Får nya användare ett initialt lösenord som de måste byta, till ett eget valt lösenord vid första användning?	Enligt policy och instruktion får ny användare ett tillfälligt lösenord som ska bytas omgående, enligt de riktlinjer som satts upp av Landstinget.	Ja

Granskningsområden		Kommentar	Utvärdering
7.7	Genomförs kontinuerlig (minst en gång per år) kontroll av organisationens behörigheter?	Olika rutiner finns på olika avdelningar. Minst en gång per år görs genomgång av användare att de är aktuella i t ex Cosmic och ca varje kvartal i ekonomisystemet, enligt Landstinget. Vanligtvis dokumenteras inte detta och det är då inte möjligt att se när och om kontrollen har utförts.	Delvis
7.8	Har systemadministratörer/-tekniker/-användare individuella unika användaridentiteter?	Ja, och vanligtvis har administratör både Admin-konto och vanligt konto, om de är del i verksamheten på något sätt.	Ja
7.9	Öppnas låsta användarkonton först efter säker identifiering av användaren?	Ja lösenordsfråga används.	Ja
7.10	Finns en gemensam lösenordspolicy?	Det finns en tvingande policy för Windows-inloggning, som används för de mest väsentliga systemen. Det finns även en skriven policy för Landstinget, även om den främst är riktad till Windowsinloggningen. För övriga system finns inte kraven, annat än om nyupphandling sker, och risk finns att alla system inte följer policyn. Finns inte förteckning över vilka dessa system skulle kunna vara.	Delvis
7.11	Sker automatisk aktivering av skärmsläckare och automatisk låsning av obevakade arbetsstationer efter visst givet tidsintervall? Upplåsning kan endast ske med lösenord.	Enligt skärmbild från Cosmic är skärmsläckaren inställd på en timma om säkerhetskortet sitter i. Detta verkar även gälla även om datorn står oanvänd. Om Cosmic inte är aktivt har vi fått information från Landstinget att det ska vara 15 minuter, men inte fått detta verifierat. En timma är lång tid för påloggade datorer av användare med kraftig behörighet.	Delvis
7.12	Är brandväggsfunktionen den enda kanalen för IP-baserad datakommunikation till och från organisationen?	Ja, enligt Landstinget.	Ja
7.13	Finns en dokumenterad brandväggspolicy där det beskrivs vilka tjänster brandväggen skall tillhandahålla?	Uppsättning sker internt men det finns inte någon dokumentation på hur det ska vara uppsatt, med möjlighet att verifiera periodiskt verklig uppsättning mot önskad uppsättning.	Nej
7.14	Används trådlösa lokala nät? I så fall, finns det åtgärder mot obehörig avlyssning och obehörigt utnyttjande av resurser?	För påloggning av trådlösa nätverk används lösen och certifikat. Finns inga gästnät inom Landstinget.	Ja
7.15	Finns det en karta över nuvarande säkerhetsarkitektur (tekniska anvisningar) för interna och externa nät och kommunikationssystem?	Enligt Landstinget finns det dokumenterat.	Ja
7.16	Har organisationen upprättat dokumenterade riktlinjer avseende lagring?	Lokal lagring på sin egen dator kan göras men det ska det inte göras enligt "Regler för IT användare".	Ja
7.17	Har verksamheten ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Vid användande av mobil dataenhet så får säkerhetspolicy skrivas under. I t ex mobiltelefoner används även programvara som krypterar den data som tillhör Landstinget. Det är även enbart t ex tillåtet att ha landstingsmail kopplade till mobiltelefoner som tillhandahålls av Landstinget.	Ja

Granskningsområden		Kommentar	Utvärdering
7.18	Har systemägaren eller motsvarande beslutat om att ett informationssystems information ska få bearbetas på distans med stationär eller mobil utrustning?	Ja i den mån det görs, vilket är ytterst ovanligt och där vi klassat det som ej tillämpligt.	Ej Tillämpligt
7.19	Finns det aktuell dokumentation med regler för distansarbete?	Det finns rutiner och policys.	Ja
8 Anskaffning, utveckling och underhåll av informationssystem			
8.1	Har en systemsäkerhetsanalys upprättats och dokumenterats för varje informationssystem som bedöms som viktigt?	Finns en bilaga med krav vid upphandling av IT-system. Viss informell riskbedömning och även bedömning utifrån tillgänglighet i vissa fall, men inte en heltäckande riskanalys per system dokumenterad centralt. Ekonomi: Finns en riskbedömningen för systemen men den är inte väl kommunicerad inom verksamheten.	Delvis
8.2	Krypteras persondata som förmedlas över öppna nät?	Ja, allt krypteras.	Ja
8.3	Finns det angiven personal som ansvarar för systemunderhåll?	Ja, Förvaltaren är ansvarig.	Ja
8.4	Finns det regler för hur system- och programutveckling ska genomföras?	Ingen programutveckling görs av Landstinget själva utan sker av externa konsulter. Viss konfigurering sker (utveckling/ändra en redan gjord och godkänd leverans) internt. Förändringar testas via testmiljö innan förändringen flyttas över till produktions-miljön. Regler finns för vem som kan göra flytten men inte hur. Det finns inte skrivna regler att allt ska testas i testmiljön innan flytt till produktionsmiljö. All konfigurering loggas men det finns ingen samlad dokumentation för hur en konfiguration ska göras, vilka tester som ska göras eller vilken dokumentation som måste produceras. Utveckling och leverans finns dokumentation/regler för.	Nej
8.5	Finns det regler och riktlinjer avseende beslut om programändringar?	Om programförändringar ska ske i Cosmic beställs de antingen av förvaltningsledningsgruppen eller av de 8 landstingen tillsammans. Beslut om konfigurering tas av förvaltningsgrupperna (t.ex. läkemedelsgruppen). Det finns däremot inget tydligt rörande konfigurationer som ändrar hur systemet hanterar information (se punkt ovan).	Delvis
8.6	Finns det dokumenterade rutiner för hur utbildning ska genomföras för köpta system? Omfattar rutinen även kompletterande utbildning vid program- och funktionsändringar?	Finns inga fastslagna rutiner för utbildning även om det normalt ingår i upphandlingen av ett nytt system eller i förändringen av ett befintligt.	Nej
8.7	Finns det en uppdaterad och aktuell systemdokumentation för ett informationssystem?	För Cosmic anser personalen att system-dokumentationen följer de ändringar som gjorts. På vissa andra system finns det synpunkter att detta inte är uppdaterat.	Delvis
9 Hantering av informationssäkerhetsincidenter			
9.1	Finns det dokumenterade instruktioner avseende vart användare skall vända sig och hur de skall agera vid funktionsfel, misstanke om intrång eller vid andra störningar?	Finns instruktioner i till exempel dokumentet "Avvikelsehantering - rutin".	Ja

Granskningsområden		Kommentar	Utvärdering
10 Kontinuitetsplanering i verksamheten			
10.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Ja, två personer arbetar med detta heltid. IT och fastigheter har kompletterat, dokumenterat och testat rutinerna.	Ja
10.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	Enligt information vi fått finns ett pågående projekt att klassificera och prioritera alla system utifrån tillgänglighet. Ytterligare information ger att systemägare inte varit involverad i denna process. Generellt finns en stor kunskap och medvetenhet rörande tillgänglighetsfrågorna inom organisationen.	Delvis
10.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie driften?	Det finns instruktion om hur återläsning t ex ska utföras från säkerhetskopia.	Delvis
10.4	Kan verksamheten bedrivas med manuella eller maskinella reservrutiner under begränsad tid? Är befintliga reservrutiner dokumenterade?	Verksamheten står för reservrutiner. Finns information på Intranätet om detta. Vår uppfattning är att det är olika nivå på reservrutiner och planer. Fick information om att Cosmic inte var tillgängligt ca 30-60 minuter vid ett tillfälle och att vissa verksamheter då insåg att de behövde förstärka rutiner och utbildning rörande detta, medan andra låg väl framme.	Delvis
10.5	Har omständigheter som ska betecknas som kris/katastrof (extraordinära händelser) för verksamheten kartlagts?	Bedömning görs av respektive drifts-/beredskapsansvarig. Finns dokumenterat vad t ex ett avbrott är.	Ja
11 Efterlevnad			
11.1	Användas endast programvaror i enlighet med gällande avtal och licensregler?	Ja. Alla installerade program är kopplande till en AD-grupp. Man har därmed kontroll på hur mycket som är installerat så att antal licenser är rätt.	Ja
11.2	Finns det regler för godkännande och distribution av programvaror för att efterleva rådande upphovsrättsliga regler?	Ja, allt skall bli certifierat av IT-avdelningen innan installation får ske.	Ja
11.3	Har organisationen förtecknat och anmält personuppgifter till personuppgiftsombud?	Ja	Ja
11.4	Genomförs interna och externa penetrationstester kontinuerligt?	Extern penetrationstest har inte beställts under de senaste åren och de interna tester som gjorts har inte dokumenterats. Enligt information från Landstinget så utförs det ändå interna regelbundna tester.	Delvis
11.5	Granskar ledningspersoner regelbundet att säkerhetsrutiner, -policy och -normer efterlevs.	Årligen görs rapportering till Landstingsstyrelsen efter deras instruktioner (3 punkter). Loggkontroll per vårdenhet ska genomföras men vår separata granskning inom detta område visar att detta inte alltid fungerar som tänkt. Datainspektionen utför tillsyn att Landstinget hanterar personuppgifter på ett riktigt sätt, och då främst ur integritetsperspektivet.	Delvis

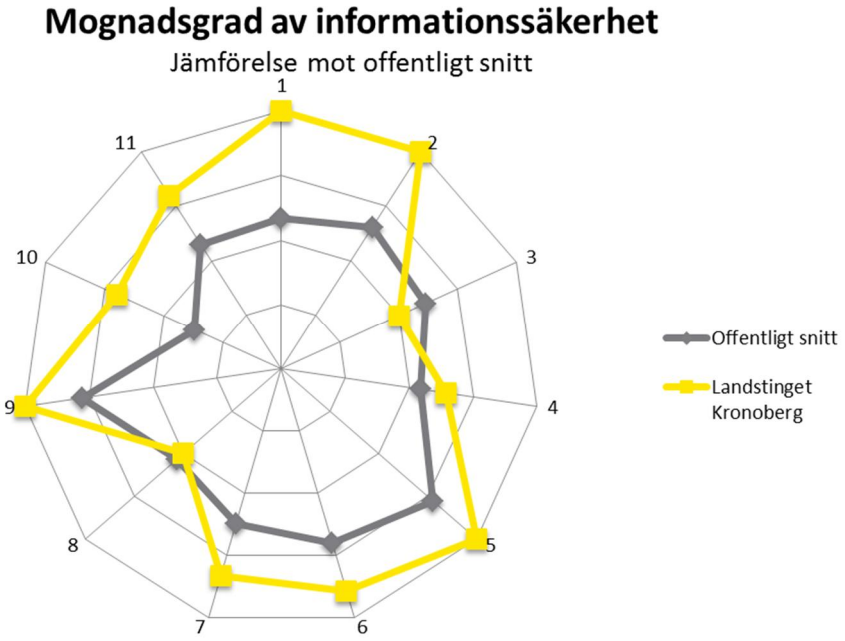
4 Jämförelse mot andra offentliga verksamheter

EY har gjort ett flertal analyser av offentliga verksamheter utifrån BITS som grund. Tack vare detta kan vi mäta Landstinget Kronobergs mognadsgrad rörande informationssäkerhet mot ett genomsnitt av de organisationer vi granskat.

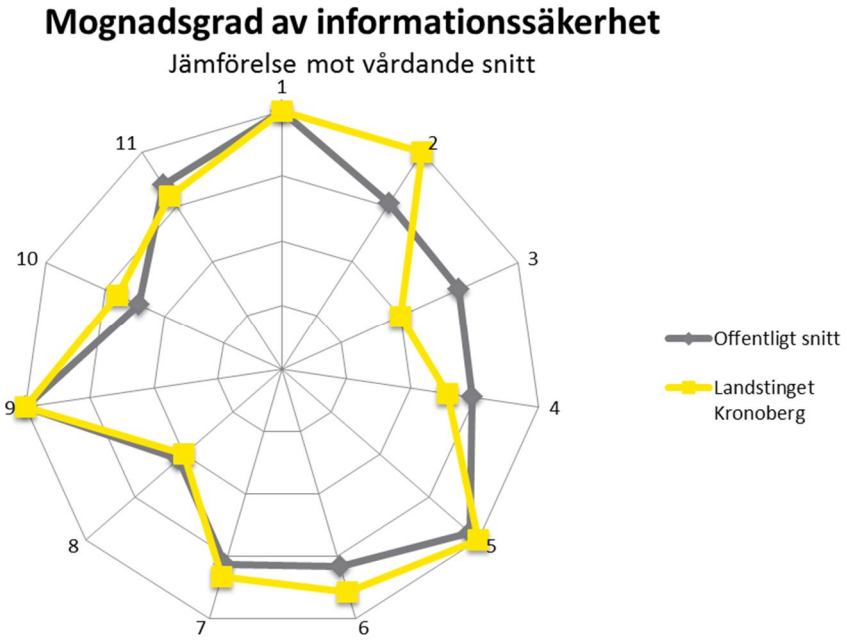
Siffrorna anger respektive område i BITS enligt:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

I diagrammet nedan representerar ytterkanten 100 % måluppfyllnad, medan mittpunkten anger 0 % måluppfyllnad.



Då stor del av jämförelsematerialet innehåller organisationer utan de krav som en patientstyrd verksamhet har, blir jämförelsen inte helt rättvisande, även om resultatet enbart skall användas som utgångspunkt för diskussioner om vilken kontrollmiljönivå organisationen önskar. I bilden nedan har vi jämfört Landstinget Kronobergs resultat med verksamheter som har patientinformation.



Här framgår det då tydligare att Landstinget ligger i nivå med övriga organisationer med vårdande funktioner och med de krav på verksamheten som det medför.

Det vi kan notera i materialet är att område ”Hantering av tillgångar” (3) och ”Personalresurser och säkerhet” (4) ligger något lägre än snittet. Rörande området för hantering av tillgångar är främsta orsaken att det finns en otydliget ute i verksamheten om ansvarsområden men även att system inte är klassade utifrån alla säkerhetsperspektiven utan främst efter tillgänglighetsnivå. I området personalresurser är det främst instruktioner och hantering av behörigheter som drar ner snittet. I båda dessa områden ser vi inte risken som större utan det handlar mer om att formalisera något mer i vissa fall, men även få ut informationen i verksamheten.

5 Slutsatser och rekommendationer

5.1 Generella slutsatser

Förutsättningarna finns för ett effektivt informationshanteringsarbete och inom de flesta områden vi kommit i kontakt med är våra indikationer på att det fungerar tillfredsställande. Det finns även funktioner tillsatta på de flesta områden som borgar för ett effektivt arbete framöver. Sedan behövs det ytterligare kontroll-funktioner för att säkerställa att de kontroller som organisationen vill ska utföras verkligen finns på plats. Vi ser också att kommunikation till användare bör formaliseras för att säkerställa att den information som är viktig för Landstiget, t ex hur användare ska bete sig vid en viss situation, kommer fram till dem.

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Ja	Aktuellt område i BITS är hanterat och kontroll bedöms rimligen implementerad:	**66 %**
Delvis	Kontrollen identifierad och bedöms delvis implementerad:	**26 %**
Nej	Kontroll har ej identifierats/Har inte kunna identifierats som implementerad:	**6 %**
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2 %**

5.2 Rekommendationer

Nedan följer våra rekommendationer samt ett förslag på prioritering av dessa. Vi har valt att presentera de iakttagelser som vi anser är mest väsentliga, Hög och Medel. Rekommendationerna är prioriterade enligt följande:

Hög	Nyckelkontroll är inte på plats/är inte effektiv. Bristen bör åtgärdas snarast för att säkerställa god intern kontroll på kort sikt.
Medel	Nyckelkontroll delvis på plats/delvis effektiv. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Nyckelkontroll på plats men effektivitet kan förbättras. Bristen bör åtgärdas på lång sikt.

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Formella regler saknas för informationsklassning, BITS rekommenderar att klassning ska ske av data (och system) utifrån områdena Sekretess, Riktighet och Tillgänglighet. Dessa bör sedan delas upp i Bas-, Hög och Mycket hög nivå. Enligt information vi fått har systemen klassats enbart utifrån Tillgänglighet. Synpunkter från verksamheten har gällt att väsentlig personal inte varit med i processen och att slutlig bedömning som IT-personalen gjort inte stämmer överens med den bedömning lokal personal gjort. **Risk:** Att inte ha klara regler kring informationsklassning kan öka risken att konfidentiell och/eller känslig information kommer i orätta händer och att information behandlas på annat sätt än tänkt. **Rekommendation:** Vi rekommenderar Landstinget att upprätta en informationsklassnings-policy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.	**Hög**
	Iakttagelse: Borttag av behörigheter Ett gemensamt system används för att tilldela och ta bort behörigheter. Vår uppfattning är att tilldelning fungerar tillfredsställande i processen. Däremot finns det problem när användare främst slutar, och att dessa användares behörigheter ska plockas bort eller låses. **Risk:** Att inte ha en formell rutin för behörighetsadministration kan öka risken att icke-auktoriserade personer får åtkomst till system och information**.** **Rekommendation:** Tydligare riktlinjer kan tas fram för hur information ska hanteras när anställd slutar och att denna kommuniceras till berörd personal regelbundet.	**Hög**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Granskning av efterlevnad Inom många områden finns tydliga anvisningar om hur kontroller ska utföras men det finns inte mycket som styr hur det ska säkerställas att dessa kontroller utförs. I vissa fall ska det finnas en kontrollfunktion för kontrollerna, t ex att logglistor granskas över vilka patienter en anställd tittar på. I vår granskning kan vi konstatera att varken det överordnade kontrollmomentet fungerat, och inte heller kontrollen att granska de anställda mot logglistor. **Risk:** Om det tas fram ändamålsenliga kontroller som säkerställer att identifierade risker hamnar på en rimlig nivå, men kontrollerna inte utförs, kan riskerna hamna på en orimligt hög nivå. **Rekommendation:** Vi rekommenderar att kontroller och rutiner verifieras regelbundet för att säkerställa en följsamhet och efterlevnad. Detta för att säkerställa att riskerna inom Landstinget ligger på en rimlig nivå efter att kontroller utförts.	**Hög**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Process för programändringar bör förstärkas Vissa delar av förändringsprocesserna är formella i Landstinget. Det finns däremot ingen generell plan i Landstingets IT-säkerhetsanvisningar gällande förändringar i system och driftgodkännande. Det finns då inte en formell process för programförändringar, med tillhörande stödjande dokumentmallar för ändringsbegäran, testprotokoll och driftsgodkännande. Det finns heller ingen tydlighet om vad som skall räknas som förändring, t ex om enbart en konfigurering sker i befintligt system, men där systemet börjar arbeta annorlunda än tidigare. T ex om en konfigurering sker som gör att fler användare får access till nya funktioner. Information vi fått säger att det finns testmiljöer och att förändringar testas noggrant där innan de förs över till produktionsmiljön. Vissa kontrollmoment vi rekommenderar nedan finns dokumenterade i policys och riktlinjer. **Risk:** Att inte ha en dokumenterad och förankrad rutin för programförändringar ökar sannolikheten att förändringar ej testas fullständigt, vilket i sin tur ökar risken för att förändringar påverkar data och/eller funktionalitet i systemet på ett felaktigt sätt. **Rekommendation:** Vi rekommenderar Landstinget att utveckla den existerade processen för programförändringar. Följande kontroller och aktiviteter bör finnas med: • Om skillnad skall göras mellan processen för stora och små förändringar bör det tydligt definieras vad en stor och en liten förändring innebär. Även att detta gäller konfigureringar i befintligt system. • Det skall framgå vem som får beställa förändringar. • Alla beställningar av förändringar skall vara dokumenterade. • Riskanalys ska föregå projektet. • Informationssäkerhetsaspekten ska vara med som del i projektstyrning, för att säkerställa att t ex arkiveringsregler följs och att information hanteras korrekt i testmiljö och i framtida behörighetsregler. • Dokumentationen av beställningen bör innehålla numrerade krav. • Beställning skall godkännas av systemägare (eller liknande). • Utveckling av förändring skall göras i separat testmiljö. • Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning. • Testresultat skall godkännas av systemägare (eller liknande). • Migrering av förändring till produktionsmiljö skall ej göras av samma person som utvecklat förändringen. • Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras. • Utbildning och systemdokumentation är också delar i denna process för att säkerställa att systemet kan användas på rätt sätt framöver.	**Medel**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Olika nivå på tillgänglighetsbedömningar och rutiner Det finns centrala katastrofplaner med t ex vem som beslutar om katastrofläge. Det finns även återstartsrutiner av servrar. Varje verksamhetschef ansvarar sedan för att det finns lämpliga reservrutiner om systemen inte finns tillgängliga. Information vi fått är att det är olika nivå på dessa reservrutiner och kunskapen om hur de ska handla om systemen inte finns tillgängliga. Som nämnts i vår iakttagelse 1 ovan så finns inte en samstämmighet i Landstinget om tillgänglighetstider för olika system. **Risk:** Avsaknad av planerad kontinuitetsplanering ökar risken för att avbrott inte hanteras på ett för verksamheten optimalt sätt. Vidare är sannolikheten att verksamheten skall drabbas hårdare vid händelse av en incident, om reservplaner saknas. Om inte analys har gjorts av verksamheten för att bedöma hur länge den klarar sig utan stöd av IT-systemen, finns risk att bedömningar blir godtyckliga och inte återspeglar verkligheten, och därmed ökar risken. **Rekommendation:** I första hand bör verifiering ske av de bedömningar som idag finns satta per system, med verksamheten, och säkerställa att alla väsentliga system finns med. Därefter bör det säkerställas att verksamheterna tagit fram reservrutiner. För att säkerställa att de tidsramar som satts upp och kunskapen om reservrutiner finns bör dessa testas regelbundet.	**Medel**
	Iakttagelse: Utbildning Vår uppfattning är att det finns mycket policys och riktlinjer dokumenterat. Däremot behöver denna information kommuniceras ut till berörd personal mer regelbundet än vad som görs idag. **Risk:** Om verksamheten inte är medveten om de regler och riktlinjer som finns, eller inte utför de kontroller som planerats, ökar risken för Landstinget att t ex personal handlar fel utifrån okunskap. **Rekommendation:** Vi rekommenderar att Landstinget löpande utför utbildning och att utförandet av denna dokumenteras på något sätt. T ex kan det centralt tas fram utbildningspaket för t ex fyra tillfällen (separat träff eller del av avdelningsmöte) under året med de mest väsentliga riskerna för Landstinget, och där informera om riskerna för verksamheten och de kontroller som finns för att minska den risken.	**Medel**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Uppföljning av tilldelade behörigheter Det finns ingen formell rutin i Landstinget för att följa upp att rätt användare ligger i respektive system och att användare har rätt behörigheter utifrån ansvarsuppgifter och intern kontroll. Vi har fått information om att kontroller utförs men det finns inget dokumenterat som kan visa på när kontrollen utfördes eller i vilken omfattning. **Risk:** Att inte genomföra genomgång av behörigheter i systemen ökar risken för att personer som slutat eller bytt tjänst fortfarande har tillgång till system och information de inte ska ha tillgång till. **Rekommendation:** Vi rekommenderar Landstinget att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med: • IT (eller service desk) bör förse verksamhetsansvariga med listor över behörigheter två gånger per år. • Cheferna bör gå igenom listorna, markera felaktigheter, signera samt sända tillbaka listorna till IT (eller service desk). • IT (eller service desk) tar bort eller förändrar rättigheter enligt underlag.	**Medel**
	Iakttagelse: Extern kommunikation Administration av brandväggar, som styr vilken information som får komma in och ut ur Landstingets nätverk, görs av Landstinget själva. Det finns inte någon beslutad lista på regler och tjänster som skall vara tillgängliga i brandväggen, som det är möjligt att verifiera mot, utifrån hur den verkligen är satt. De tester som sker av säkerheten i brandväggen sker enbart internt och inte av några externa experter. **Risk:** Brandväggen är det väsentliga skyddet mot otillåten trafik och skyddet mot externa parter att komma in i Landstingets nätverk. Om detta inte fungerar tillfredsställande finns risk att obehöriga kommer åt känslig information eller på annat sätt kan störa Landstingets IT-stöd. **Rekommendation:** Uppsättningen av brandväggen bör beslutas och dokumenteras. Vi rekommenderar att det finns policy som tydliggör hur och när tester ska ske av brandväggen och annan utrustning som skyddar mot otillåten trafik, och där överväga om extern expertis ska involveras.	**Medel**