REGION KRONOBERG

Regionstyrelsen

Svar på revisionsrapport – Uppföljande granskning av IT-säkerhetsarbetet

Ordförandes förslag till beslut
Föreslås att regionstyrelsen beslutar

att godkänna svar på revisionsrapport Uppföljande granskning av IT-säkerhetsarbetet samt

att överlämna svaret till regionfullmäktige

Sammanfattning
Region Kronobergs revisorer har genomfört en uppföljande granskning av IT-säkerhetsarbetet i Region Kronoberg. Granskningen har utförts av konsulter från EY och har utgått från syfte och revisionsfrågor som revisorerna fastställt.

Revisionens sammanfattande bedömning av den uppföljande granskningen är att det har gjorts en del förbättringar sedan ursprungsgranskningarna genomfördes, men att merparten av rekommendationerna ännu inte genomförts.

Regionstyrelsen delar till stora delar revisorernas sammanfattande bedömning, men åtgärder har vidtagits på flertal punkter som revisionsrapporter pekar på. En handlingsplan har tagits fram för genomförande av kvarvarande åtgärder inför beslut i regionstyrelsen. Dessa redogörs för i svar på revisionsrapporten nedan.

Regionstyrelsen vill understryka att revisionen återigen har lyft brister inom systemet A-plus där regionstyrelsen i sitt tidigare svar har påtalat att detta kommer att hanteras i och med införandet av nytt ekonomisystem 2018-01-01.

Namn på revisionsrapport
Uppföljande granskning av IT-säkerhetsarbetet

Behörigheter i Cosmic

Revisionens synpunkt
I denna uppföljning har revisionens stickprov visat på att processen att stänga konton och SITHS-kort for inloggning i Cosmic är långsam. Revisionen rekommenderar att det dels beslutas hur lång tid inom vilket konton ska låsas, med möjlighet för beslutade undantag, efter att anställnings upphörande. Vidare bör det tydligt informeras hur processen ska gå till och vilka tidsramar som gäller.

En uppföljande instans bör finnas för att säkerställa att kort och konton fortare blir låsta. Revisionen tycker annars att det är en bra kompenserande kontroll att oanvända konton låses efter tre månader.

Regionstyrelsens kommentar

Genomförda åtgärder

Under EY´s revision hösten 2016 framkom ett antal synpunkter på processen för avslut av personkonto. Processen/arbetsrutinen används för att avsluta konto och behörigheter för medarbetare som slutar sin anställning i Region Kronoberg.

Till följd av synpunkterna från revisionen har flera åtgärder vidtagits för att förbättra rutinen. Den nya processen är fastställd 161130.

Följande förändringar har gjorts i beställningsformuläret:

1. Alla ärenden rörande avslut av personkonton som inkommer till IT hänvisas direkt vidare till formuläret *Avslut* i anställningspaket.

2. En möjlighet att avsluta Cosmicbehörighet har lagts till direkt i Avslutsformuläret. Ärendet skickas direkt till VIS-supporten i Easit för kontroll och åtgärd. Då behörigheten i Cosmic är borttagen meddelas kunden och Intern kundservice.

Handläggaren som arbetar med avslutsärendet säkerställer att både presentationskort med passager, e-tjänstekort och komplett avslutsbeställning inkommit till intern kundservice i möjligaste mån innan handläggningen av avslutsärendet påbörjas. E-legitimationen avregistreras i SITHS-administrationssystemet så snart kortet inkommit.

I de fall ett avslutsärende finns, men e-tjänstekortet inte har skickats in till intern kundservice (eller tvärt om), ringer handläggaren upp berörd chef. Handläggaren påminner 2 gånger om kort eller ärende saknas. Intern kundservice mål är att avslutsärendet skall vara expedierat inom 10 dagar från ärendets ankomstdatum.

Kommande åtgärder

- Se punkt 1.1 samt ny arbetsrutin, bilaga 1
- Tidsplan för när rutinen är införd skall tas fram senast Q2 2017.

Loggkontroll av patientinformation

Revisionens synpunkt

Loggkontrollerna utförs inte i den omfattning som finns noterat i rutinbeskrivningarna. Även om det tagits fram exempel så bör tydligare instruktioner utformas 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.

Revisionen 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.

Regionstyrelsens kommentar

Genomförda åtgärder

De rutiner som Region Kronoberg har gällande loggkontroll av patientinformation uppfattar regionstyrelsen är i linje med den checklista som Datainspektionen har tagit fram.

Regionstyrelsens uppfattning är att verksamheten många gånger har är svårt att prioritera arbetet med logguppföljning då det är tidsbrist. Ett effektivt systemstöd efterlyses av verksamheten, för att öka verkningsgraden av kontrollerna. Sommaren 2016 träffade Region Kronoberg en leverantör som håller på att utveckla ett logg-verktyg. Vid det tillfället var inte analysverktyget på den nivån att Region Kronoberg ville gå vidare med det. Att förbättra loggarna i Cosmic har funnits med i flera år och har först nu, under 2016 blivit högt prioriterat av kundgruppen.

Kommande åtgärder

1. Region Kronoberg har rutiner som följer Datainspektionens checklista. Rutinen ska säkerställa att den övergripande granskningen av loggkontroller dokumenteras.

2. Under våren 2017 planerar Region Kronoberg för att genomföra några utbildningstillfällen i Växjö och Ljungby kring loggkontroller. Målgruppen för utbildningarna är verksamhetschefer eller utsedda loggkontrollanter.

Kraftfulla behörigheter i A plus

Revisionens synpunkt

Som revisionen tidigare konstaterat finns det många kraftfulla konton i A plus även om de kraftfullaste har minskat. Revisionens rekommendation är att behörighetsprofiler har högprioritet vid framtida systembyte och att intern kontroll är en av de viktiga aspekterna.

Regionstyrelsens kommentar

Genomförda åtgärder

Efter den föregående revisionen gjordes en genomgång av personer med de högsta behörigheterna. Ett antal behörigheter plockades bort, men eftersom vissa funktioner som används av många personer kräver hög behörighet ligger det kvar för ganska många.

Kommande åtgärder

Eftersom ekonomisystemet kommer att bytas ut 2018-01-01 är det inte aktuellt att göra några större förändringar i nuvarande system för att försöka åtgärda detta, men vid uppsättningen av behörighetsstrukturen i det nya systemet skall stor vikt läggas vid att minimera antalet personer med höga behörigheter i systemet.

REGION KRONOBERG

Formella regler saknas för informationsklassning

Revisionens synpunkt

Det pågår en kartläggning av data och system inom regionen, där revisionens bedömning är att de skulle kunnat lägga till övriga aspekter på informationsklassning, vilket inte gjorts. Revisionen rekommenderar Region Kronoberg att upprätta en informationsklassnings-policy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.

Regionstyrelsens kommentar

Kommande åtgärder

Klassning av en organisations information utgör en av grunderna för att skapa effektiv informationshantering. Informationsklassning är ett sätt att värdera och prioritera information och dess tillgångar efter verksamhetens krav på sekretess, riktighet och tillgänglighet. Utifrån kraven kan informationen hanteras på ett effektivt sätt med rätt avvägda skyddsnivåer. Vilket även påverkar kostnaderna, då rätt skyddsnivå beroende på vilken information som hanteras. Detta minskar risken för att känslig information kommer på avvägar, förvanskas eller inte finns tillgänglig i den utsträckning som förväntas. Respektive verksamhet är ansvarig för sin information i systemen. Ett projekt för att införa informationsklassning inom Region Kronoberg ska prioriteras under 2017.

Granskning av efterlevnad

Revisionens synpunkt

Revisionen kan konstatera att flera av de iakttagelser man haft tidigare finns kvar, och där kontrollfunktion och ansvar inte finns tydligt fastställt. Revisionen rekommenderar att det tydligt fastställs vem eller vilken funktion som är ansvarig att beslutade kontroller och rutiner följs och verifierar detta. Detta för att säkerställa att riskerna inom regionen ligger på en rimlig nivå efter att kontroller utförts.

Regionstyrelsens kommentar

Genomförda åtgärder

Region Kronoberg har en tydlig rutin för internkontroll ”Intern styrning och kontroll – Reglemente och tillämpningsanvisningar” som följs. Det innebär att man börjar med att genomföra en riskanalys, de risker som får högst riskvärde skall föras in i internkontrollen där det anges kontrollmoment, vem som är ansvarig samt frekvensen på uppföljningen.

Redovisning sker i oktober varje år och redovisas i respektive nämn/styrelse. Därefter redovisar förvaltningsdirektörerna/motsvarande resultat i regiondirektörens ledningsgrupp för förankring och förslag på förbättringsarbete till kommande internkontroll plan (som beslutas i december).

Kommande åtgärder

Förvaltningsdirektörerna/motsvarande får i uppdrag att i internkontrollplanen, säkerställa att kontrollmoment för beslutade kontroller och rutiner finns med och

att det fastställs vem eller vilken funktion som är ansvarig enligt mall i internkontrollplanen.

Process för programförändringar bör förstärkas

Revisionens synpunkt

Revisionen rekommenderar regionen att säkerställa att den fastlagda rutinen med kontroller införs på alla system och väsentliga infrastrukturområden, och att kontroller formaliseras där det finns risk. Revisionen rekommenderar även att alla förändringar på något sätt ska dokumenteras i Easit med spårbarhet till och från annan dokumentation, om inte allt dokumenteras i Easit.

Regionstyrelsens kommentarer

Genomförda åtgärder

Regionens IT-verksamhet har infört ett ”verksamhetssystem” under hösten 2014 som hanterar verksamhetens dagliga produktion, kallat Easit. Easit innehåller bl.a. processtöd för incidenter, larm, ändring, problem, beställning och inventarie, Grundstruktur i processer och kontroller, som IT-verksamheten steg för steg implementerar, är baserade på ITIL, som är ett internationellt erkänt ramverk av principer för att hantera IT.

Kommande åtgärder

Den gemensamma processen för att göra förändringar inklusive kontroller är fastställd och den implementeras stegvis för system och infrastrukturella områden. Implementationen är långsiktig och sker steg för steg utifrån prioritet, men även kopplat till att olika funktionella stöd utvecklas i Easit. IT-verksamhetens arbete med processer kopplade till ITIL är ett kontinuerligt förbättringsarbete. Tidsplan för implementationstakten tas fram under Q2 2017.

Utbildning

Revisionens synpunkt

Revisionen rekommenderar att regionen 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 regionen, och där informera om riskerna för verksamheten och de kontroller som finns för att minska den risken.

Regionstyrelsens kommentarer

Genomförda åtgärder

I samband med introduktion av nyanställda, så ska chefen gå igenom en checklista och utifrån den informera den nyanställda. På den checklistan finns det med ”Regler för IT-användare”. Reglerna stödjer god informationssäkerhet. Generellt är det hög informationssäkerhet inom Region Kronoberg. Det finns administrativt skydd, i form av riktlinjer och rutiner, samt teknisk skydd.

Kommande åtgärder

Informationssäkerhetsstrategen tillsammans med ansvariga för IT-säkerheten ska ta fram små utbildningspaket eller information som kan publiceras på webben. Förslag på utbildningspaket och resursåtgång tas fram senast Q2 2017.

REGION KRONOBERG

Uppföljning av tilldelade behörigheter

Revisionens synpunkt

Revisionen rekommenderar regionen att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med:

- Tydliga instruktioner att behörigheter ska granskas två gånger per år med de verktyg som nu finns framtagna, i väsentliga system.

- Godkännande och justeringar ska meddelas IT (eller service desk), via t ex intranätssida, för att det även ska gå att följa upp tydligt och enkelt att kontrollen utförts.

- IT (eller service desk) tar bort eller förändrar rättigheter enligt underlag.

Regionstyrelsens kommentarer

Genomförda åtgärder

Region Kronoberg har en ny rutin för ”Behörighet och BITS granskning” där punkt två och tre enligt ovan finns med. I rutinen saknas det dock hur ofta behörigheterna ska granskas enligt punkt ett. I rutinen saknas också hur kort tids anställningars uppföljning av behörigheter ska ske.

Kommande åtgärder

Regionservice får i uppdrag att komplettera befintlig rutin för ”Behörighet och BITS granskning” med hur korttidsanställningarnas behörigheter ska följas upp.

Extern kommunikation

Revisionens synpunkt

Revisionen rekommenderar att alla förändringar ska tydligt dokumenteras i Easit, men där dokumentation kan finnas på annat ställe, om det passar bättre, för att ge tydlig spårbarhet och kontroll över de förändringar som görs. Även om ett penetrationstest enbart visar en ögonblicksbild på säkerheten ger det ändå en indikation på parametersättningens säkerhetsnivå. Revisionen rekommenderar att brandväggarnas säkerhet verifieras regelbundet.

Regionstyrelsens kommentarer

Genomförda åtgärder

Regionens IT-verksamhet har infört ett ”verksamhetssystem” under hösten 2014 som hanterar verksamhetens dagliga produktion, kallat Easit. Easit innehåller bl.a. processtöd för incidenter, larm, ändring, problem, beställning och inventarie, Grundstruktur i processer och kontroller, som IT-verksamheten steg för steg implementerar, är baserade på ITIL, som är ett internationellt erkänt ramverk av principer för att hantera IT.

Kommande åtgärder

Den gemensamma processen för att göra förändringar inklusive kontroller är fastställd och den implementeras stegvis och för system och infrastrukturella områden. Dokumentation av beslut kopplat till ändringar avseende brandvägg

prioriteras nu upp och implementeras i Easit under våren 2017. Dokumentationen över brandväggens konfiguration hanteras utanför Easit med anledning av den rent tekniskt inte går att hantera i Easit samt utifrån ett åtkomst och säkerhetsperspektiv.

En extern analys gällande brandvägg kommer beställas, genomföras och utvärderas under 2017. I analysen kommer bl a penetration kontrolleras samt hantering av trafik kopplat av publicerade IT-tjänster gentemot internet och Sjunet.

Dataöverföring till A plus

Revisionens synpunkt

Övergripande finns det dokumentation om informationsöverföringar. Revisionen ser ändå en risk i om ett för-system inte skulle generera en fil och inga varningar finns för att filen inte genererats. Det finns då ingen fil att flytta och data blir då inte fullständig i A plus. Revisionen rekommenderar att ansvariga tydliggör de kontroller de utför nu och dokumenterar dem. I de fall där det saknas kontroller som säkerställer fullständighet och riktighet ska de införas. I ett framtida system bör automatiska överföringar ske där det även kommer tydliga varningar om filer inte flyttas i de scheman som förväntas.

Regionstyrelsens kommentarer

Genomförda åtgärder

En checklista har tagits fram för att checka av att alla filer blivit inlästa vid varje månadsbokslut. Där loggförs när alla filer blivit inlästa för att säkerhetsställa att importerna från alla försystem kommit in.

Kommande åtgärder

I designen av det nya systemet är grundtanken att all filöverföring skall ske med automatik och att även sätta upp varningar om systemet inte får de filer som ligger schemalagda. Tanken är att även i möjligaste mån sätta upp kontroller på att totalbeloppen i filen och antalet rader i filen ligger inom förväntat intervall, och att signaler går ut till berörda om så inte är fallet.

Anna Fransson
Regionstyrelsens ordförande

Martin Myrskog
Regiondirektör

Bilagor: Revisionsrapport Uppföljande granskning av IT-säkerhetsarbetet
Bilaga 1 behörighet och BITS-granskning

REGION KRONOBERG

Bilaga 1 - Behörighet och BITS granskning

Förslag på åtgärd till Behörigheter i Cosmic