BUN 2013-06-12
Ärende 1.3

Uppsala KOMMUN

KONTORET FÖR BARN, UNGDOM OCH ARBETSMARKNAD

Handläggare
Wicks Elaine

Datum
2014-04-11

Diarienummer
BUN-2014-0631

Barn och ungdomsnämnden

Kommunrevisionen: Granskning av generalla IT-kontroller 2013

Förslag till beslut
Barn- och ungdomsnämnden föreslås besluta

att som svar på rapport avseende Granskning av generalla IT-kontroller 2013 till Kommunrevisionen avge upprättat förslag till yttrande.

Sammanfattning
Kommunrevisionen vill ha nämndens svar på fyra brister som noterades i en granskning av Extens som gjordes av PwC under november och december 2013. Vissa åtgärder är redan implementerade och andra ska implementeras i förvaltningsplanen för Extens.

Bakgrund
Kommunrevisionen begär yttrande över vilka åtgärder som planerar vidtas för att komma till rätta med de problem som revisionen uppmärksammat genom en uppföljande granskning av generalla IT-kontroller inom ramen för kommunrevisionen granskning av nämndernas ansvar för den interna kontrollen **(bilaga 1)**. Granskningen har fokuserat på säkerheten i applikationer, operativsystem och databaser.
Förslag till yttrande har upprättats (**bilaga 2**).

Ärendet
Granskning har fokuserat på IT-styrning, programutveckling och förändring, åtkomstikontroll, datadrift och infrastruktur med utgångspunkt i applikationer, databas och operativsystem, vilka bedöms kunna ha en påverkan på den finansiella revisionen. Barn- och ungdomsnämnden (BUN) berörs applikationen Extens som är ett skoladministrativt system. Rapporten påpekar följande brister i Extens och förslår rekommendationer till åtgärdar:

1. Kontinuitet- och katastrofplan för Extens är inte formaliserade

Observation: Genom intervju noterades det att ingen formell kontinuitets- eller katastrofplan finns implementerade för applikationen Extens.

Svar: Det finns en katastrofplan för Agresso **(bilaga 3)** med en sekundär infrastruktur som skulle kunde vara förslag till en lösning. Implementering av detta ska inkluderas i

Postadress: Uppsala kommun, kontoret för barn, ungdom och arbetsmarknad, 753 75 Uppsala
Besöksadress: Stationsgatan 12 • Telefon: 018-727 87 00 (växel) • Fax: 018-727 86 50
E-post: barn-ungdom-arbetsmarknad@uppsala.se
www.uppsala.se

förvaltningsplan för Extens. Det vore bra om det fanns en kommungemensamt tekniskt lösning för tekniskt lösning för samtliga applikationer som fanns med i granskningen.

2. *Periodisk granskning av användare*

Observation: Genom intervju noterades att periodisk granskning av användare i applikationerna är baserat på utdrag av beställningar i IRIS (ett system som hanterar beställningar för bland annat systembehörigheter). Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt.

Svar: Påpekandet är åtgärdat och det finns en dokumenterad process **(bilaga 4)** för hur detta ska ske.

3. *Bristande säkerhetsinställningar*

Observation: Genom intervju och inspektion noterades det att rådande säkerhetsinställningar i applikationen inte är uppsatta enligt god praxis. Lösenord behöver endast bytas var 6:e månad och kräver endast ett fem tecken långt lösenord.

Svar: Ändrar följande inställningar för lösenord för att ökar säkerheten:

- Antal tecken ska ändras från fem till åtta
- Kravet ska vara minst en siffra samt stora och små tecken. Idag finns inga krav på blandat lösenord
- Hur ofta en tvingande lösenordsbyte ska göras tas med i kontorets förvaltningsplanen för Extens.

4. *Avsaknad av dokumentation gällande återläsningstest*

Observation: Genom intervju noterades att det saknas en rutin för periodisk återläsning av kritisk data i Extens. Vidare noterades det att det inte sker några formaliserade återläsningstester.

Svar: Återläsning (kopiering) av data görs inte till produktion men med jämna mellanrum så sker det en återläsning från produktion till test. Observationen i rapporten menar att data ska tars från säkerhetskopiorna och läser in det i systemet. En katastrof plan bör innehålla dokumentation och rutiner om hur återläsningsdelen ska gå till och hur ofta detta ska göras. Detta ska inkluderas i förvaltningsplan för Extens.

Kontoret för barn, ungdom och arbetsmarknad

Jan Holmlund
Tf direktör

Uppsala KOMMUN

Kommunrevisionen

2014-03-13

Kommunstyrelsen
Nämnder och styrelser, f k

Granskning av generella IT-kontroller 2013

PwC har på vårt uppdrag gjort en uppföljande granskning av generella IT-kontroller inom ramen för vår granskning av nämndernas ansvar för den interna kontrollen. Granskningen som avrapporteras i denna rapport har fokuserat på säkerheten i applikationer, operativsystem och databaser.

Under 2012 års granskning noterades totalt 24 brister, jämfört med 20 brister under 2013 års granskning.

Vi kan konstatera att vissa åtgärder vidtagits/planeras för att skapa grundläggande IT-säkerhet och förvaltningsstruktur för kritiska applikationer. Fortfarande finns tidigare påpekade brister i systemen men även nya brister har tillkommit som behöver åtgärdas.

Vi ser särskilt allvarligt på att tidigare påpekade säkerhetsbrister kvarstår i kommunens datasystem.

Vi översänder rapporten för yttrade över vilka åtgärder som planerar vidtas för att komma tillrätta med probelmen. Vi önskar svar senast den 30/5 2014.

FÖR KOMMUNENS REVISORER

Lars-Olof Lindell
Ordförande

pwc

Revisionsrapport

Granskning av generella IT-kontroller 2013

Uppsala kommun

Hans Larsen
Gustaf Gambe
December 2013

pwc

Innehållsförteckning

pwc

Inledning

Kommunstyrelsen har uppsiktsplikt över att den interna kontrollen inom kommunen byggs upp och organiseras på ett tillfredsställande sätt. Nämnderna har det fulla ansvaret för den interna kontrollen inom sina verksamhetsområden och applikationer. Intern kontroll är en process som påverkas av nämnderna, kommunstyrelsen och tjänstemannaorganisationen, vilken utformas för att ge en rimlig försäkran om att kommunens mål uppnås inom följande områden:

- Ändamålsenlig och effektiv verksamhet
- Tillförlitlig ekonomisk och verksamhetsmässig rapportering
- Efterlevnad av tillämpliga lagar och förordningar

I samband med granskningen av Uppsala kommuns räkenskaper och förvaltning har en granskning genomförts av generella IT-kontroller (ITGC) för ett urval av de applikationer som kan påverka redovisningen. Vår granskning omfattar inte den interna kontrollen *inom* applikationerna, utan endast de generella IT kontrollerna.

Granskningen som avrapporteras i denna rapport har fokuserat på applikationer, operativsystem och databaser. Rapporten syftar till att presentera det aggregerade resultatet av respektive applikation där observationer noteras, vilka kommunledningen bör beakta i sitt arbete med att utveckla och förbättra förvaltningen och den interna kontrollen för Uppsala kommuns IT-miljö.

Vi vill tacka den personal på Uppsala kommun som hjälp oss att genomföra granskningen, för deras bemötande och goda samarbetsvilja.

Granskningens omfattning

Granskningen har utförts av Gustaf Gambe (PwC) under november och december 2013. Granskningen har genomförts genom intervju med systemförvaltare och nyckelpersoner inom Teknik & Service samt tester av stödjande dokumentation. Granskningen har fokuserat på nedanstående områden med utgångspunkt i applikationer, databas och operativsystem, vilka bedöms kunna ha en påverkan på den finansiella revisionen.

Område	Kontrollmål
IT-styrning	- Styrande dokument för IT-verksamheten finns definierade - Grundläggande säkerhetsnivå för IT-miljön finns definierad - Katastrof och avbrottsplan finns definierad
Programutveckling och förändring	- Systemförändringar till kritiska applikationer initieras genom formell begäran - Systemförändringar till kritiska applikationer godkänns fullständigt och riktigt - Begränsad åtkomst till produktionsmiljön för utvecklare - Systemförändringar som implementeras i produktionsmiljön godkänns fullständigt och riktigt före driftsättning
Åtkomstkontroll	- Formella rutiner vid upplägg av nya användare eller ändringar i befintliga behörigheter - Periodisk genomgång av användare och deras respektive behörigheter - Lösenordspolicy finns definierad och uppfyller god praxis - Kontroll och övervakning av åtgärder utförda av privilegierade användare
Datordrift	- Kontroll att vitala batchjobb genomförs fullständigt och riktigt - Backup-rutiner finns på plats.
Infrastruktur	- Direkt åtkomst till databasen är begränsad - Privilegierad åtkomst till kritiska servrar är begränsad

Nedan listas de applikationer, databaser och operativsystem som omfattats av granskningen.

Applikation	Databas	Operativsystem
Agresso	SQL	Windows 2003
Heroma	SQL	Windows 2003
Procapita IFO	Oracle	Windows 2003
Siebel	Oracle	Windows 2003
Extens	Oracle	Windows 2003

I samband med granskningen intervjuades ett antal personer i syfte att skapa förståelse för applikationer, rutiner och processer relaterade till IT. Följande personer intervjuades:

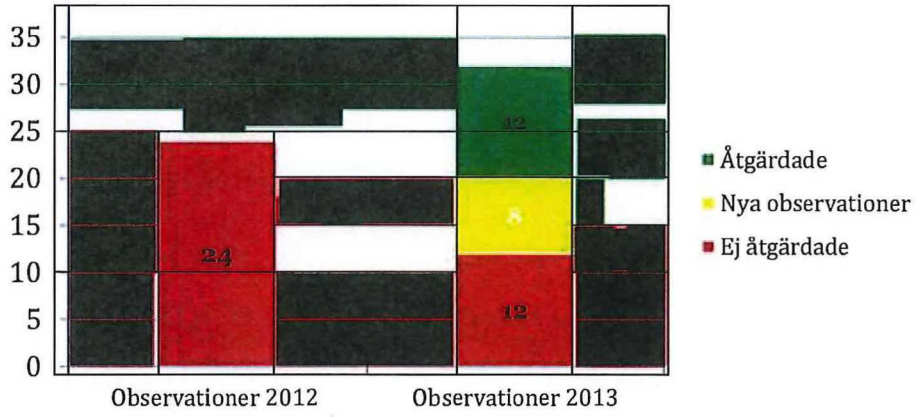
- Anders Dahlström (IT chef)
- Annika Eriksson (Teknik & Service)
- Elaine Wicks (Systemägare Extens)
- Eva Dahlén (Utvecklingsledare Teknik & Service)
- Gunilla Larsson (Systemförvaltare Agresso)
- Ingmari Andersson (Systemförvaltare Procapita IFO)
- Karim Zalila (Systemförvaltare Heroma)
- Leif Eriksson (Systemägare Siebel)
- Linus Jacobsson (Teknik & Service)
- Lotta Swahn Eriksson (Systemförvaltare Procapita IFO)
- Margit Lehman (Teknik & Service)
- Malin Eriksson (Systemförvaltare Siebel)
- Maria Huss-Landström (Systemägare Agresso och Heroma)
- Maria Kuisma (Systemägare Procapita IFO)
- Sara Johansson (Systemförvaltare Extens)

I kommande avsnitt sammanfattas årets granskning, följt av detaljerade observationer och rekommendationer per applikation. Systemägare är ansvarig för att säkerställa att observationerna åtgärdas i enlighet med rekommendation. Vidare bör systemägare säkerställa att ändamålsenliga avtal finns på plats mellan systemförvaltningen och Teknik & Service i syfte att tydliggöra roller samt ansvar gällande förvaltningen av kritiska applikationer.

Sammanfattning

Genom intervju och inspektion av underliggande dokumentation kan PwC konstatera att vissa åtgärder vidtagits/planeras för att skapa grundläggande IT-säkerhet och förvaltningsstruktur för kritiska applikationer.

Under 2012 års granskning noterades totalt 24 observationer, jämfört med 20 observationer under 2013 års granskning. Detta tyder på att kommunen har tagit till sig av tidigare års observationer och rekommendationer, och arbetar successivt med att stärka den interna kontrollen inom IT.



Dock noterades ett antal områden där PwC anser att Uppsala kommun bör fortsätta sitt arbete med att förstärka och förtydliga sina rutiner för att uppnå en god intern kontroll. Att likartade iakttagelser gjorts för ett antal system indikerar också att processer kan behöva ses över och eventuellt uppdateras, för att säkerställa att de kan tillämpas i praktiken.

Våra observationer sammanfattas i tabellen på nästa sida och en mer utförlig beskrivning av observationen, risker och våra rekommendationer återfinns i avsnittet "Observationer och rekommendationer".

pwc

Område	Observation/brist	Berörd applikation/enhet	Risk och prioritet
IT-styrning	• Katastrofplan är inte implementerad för samtliga applikationer	Heroma, Procapita IFO, Siebel och Extens	Avvikelse som ökar risken för eventuell dataförlust vid driftstopp och orimligt långa nedtider. Bör prioriteras för att minimera risken för dataförlust.
Förändrings-hantering	• Bristande dokumentation avseende förändringar i applikationer	Agresso och Procapita IFO	Avvikelse som ökar risken för att felaktiga eller ofullständiga förändringar appliceras i produktionsmiljön. Prioritet bör läggas på att skapa en tydligare spårbarhet i utförda förändringar.
Åtkomst till program och data	• Periodisk genomgång av användare har vid granskningstillfället inte utförts • Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis	Agresso, Heroma, Procapita IFO, Siebel, Extens och Teknik & Service Heroma, Extens och Teknik & Service	Avvikelser som ökar risken för obehörig åtkomst till applikationer, vilket ökar risken för obehörig åtkomst till kritisk information. Prioritet bör läggas på att genomföra periodiska granskningar av användare och stärka rådande säkerhetsinställningar.
Datordrift	• Inga formella återläsningstester av backup har genomförts	Agresso, Heroma, Procapita IFO, Siebel och Extens	Avvikelse som ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Prioritet bör läggas på att formalisera återläsningstester för att säkerställa att återläsning av backuper fungerar.

pwc

Observationer och rekommendationer - Agresso

Granskningsområde	Gradering	Observationer
1. Programutveckling och förändring (PU/PF)		**Bristfällig spårbarhet avseende förändringar i Agresso** **Observation:** Genom intervju och inspektion av stödjande dokumentation noterades att den dokumentation som finns avseende förändringsbegäran, utförda tester och godkännande före produktionssättning är bristfällig med avseende på spårbarhet. En av tre testade förändringar saknar ett formellt godkännande före produktionssättning. Dock avsåg denna förändring ingen förändrad funktionalitet, varför risken för felaktigheter bedöms som låg. **Risk:** Bristande efterlevnad av förändringsprocessen ökar risken för att felaktiga eller ofullständiga förändringar appliceras i produktionsmiljön vilket kan påverka transaktioner och data som är kritiska för den finansiella rapporteringen. **Rekommendation:** PwC rekommenderar att Uppsala kommun ser över processen för hantering av förändringar i Agresso. Processen bör säkerställa att alla förändringar är: - Formellt initierade - Testade och utförda tester dokumenteras - Formellt godkända före produktionssättning Om undantag från ovanstående process skall kunna göras vid exempelvis "små förändringar", så bör processen definiera vilka slags förändringar som ryms därinom och därmed inte kräver föreslagna formella kontrollpunkter. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
2. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
3. Infrastruktur (IF)		**Avsaknad av dokumentation gällande återläsningstest.** **Observation:** Genom intervju noterades att en rutin för periodisk återläsning av kritisk data i Agresso är under framtagande. Dock är inte denna rutin implementerad ännu och det sker inga formaliserade återläsningstester. **Risk**: Avsaknad av återläsning och testning gällande backup ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun färdigställer rutinen för periodisk testning och återläsning av kritisk data. Vidare bör formell dokumentation gällande återläsning upprättas i syfte att skapa spårbarhet i genomförda tester. **Systemägarens kommentar:**

Observationer och rekommendationer - Heroma

Granskningsområde	Gradering	Observationer
1. IT-styrning (IS)		**Kontinuitet- och katastrofplan för Heroma är inte formaliserade.** **Observation:** Genom intervju noterades det att ingen formell kontinuitets- eller katastrofplan finns implementerad för applikationen Heroma. **Risk**: Avsaknad av katastrof- och avbrottsplan ökar risken för brister och dataförlust vid driftstopp, som även kan leda till orimligt lång nedtid. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun dokumenterar de åtgärder som behöver vidtas, och ansvariga personer, för att effektivt återställa system, applikationer och processer vid en eventuell katastrof eller incident. Detta görs med fördel med hjälp av Teknik & Service som ansvarar för den tekniska delen av kontinuitetsplanen. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
2. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
3. Åtkomstkontroll (ÅK)		**Bristande säkerhetsinställningar i applikationen Heroma.** **Observation:** Genom intervju och inspektion noterades det att rådande säkerhetsinställningar i applikationen inte är uppsatta enligt god praxis. Lösenord behöver endast bytas var 180:e dag och kräver endast 6 tecken långt lösenord. **Risk**: Bristfälliga lösenordsparametrar ökar risken för otillåten åtkomst till applikationen, vilket ökar risken för obehörig åtkomst till kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en lösenordspolicy för Heroma som uppfyller god praxis. Exempel på vad policyn kan innehålla: • Forcerat lösenordsbyte efter 90 dagar • Lösenordet måste innehålla minst 8 tecken • Samma lösenord kan inte användas inom loppet av 18 månader • Krav på minst en siffra samt stora och små tecken • Kontot låses efter 3 misslyckade inloggningsförsök Vidare rekommenderar vi att det utförs en periodisk genomgång av rådande inställningar för att säkerställa att inställningarna inte har förändrats eller nollställts. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
4. Infrastruktur (IF)		**Avsaknad av dokumentation gällande återläsningstest.** **Observation:** Genom intervju noterades att det saknas en rutin för periodisk återläsning av kritisk data i Heroma. Vidare noterades det att det inte sker några formaliserade återläsningstester. **Risk**: Avsaknad av återläsning och testning gällande backup ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun färdigställer rutinen för periodisk testning och återläsning av kritisk data. Vidare bör formell dokumentation gällande återläsning upprättas i syfte att skapa spårbarhet i genomförda tester. **Systemägarens kommentar:**

Observationer och rekommendationer – Procapita IFO

Granskningsområde	Gradering	Observationer
1. IT-styrning (IS)		**Kontinuitet- och katastrofplan för Procapita IFO är inte formaliserade.** **Observation:** Genom intervju noterades det att ingen formell kontinuitets- eller katastrofplan finns implementerad för applikationen Procapita IFO. **Risk**: Avsaknad av katastrof- och avbrottsplan ökar risken för brister och dataförlust vid driftstopp, som även kan leda till orimligt lång nertid. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun dokumenterar de åtgärder som behöver vidtas, och ansvariga personer, för att effektivt återställa system, applikationer och processer vid en eventuell katastrof eller incident. Detta görs med fördel med hjälp av Teknik & Service som ansvarar för den tekniska delen av kontinuitetsplanen. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
2. Programutveckling och förändring (PU/PF)		**Bristfällig spårbarhet avseende förändringar i Procapita IFO** **Observation:** Genom intervju och inspektion av stödjande dokumentation noterades att den dokumentation som finns avseende förändringsbegäran, utförda tester och godkännande före produktionssättning är bristfällig med avseende på spårbarhet. Två av två testade förändringar saknar ett formellt godkännande före produktionssättning. **Risk:** Avsaknad av en formell förändringshanteringsprocess ökar risken för att felaktiga eller ofullständiga förändringar appliceras i produktionsmiljön, vilket kan påverka transaktioner och data som är kritiska för verksamheten. **Rekommendation:** PwC rekommenderar att Uppsala kommun ser över processen för hantering av förändringar i Procapita IFO. Processen bör säkerställa att alla förändringar är: - Formellt initierade - Testade och utförda tester dokumenteras - Formellt godkända före produktionssättning Om undantag från ovanstående process skall kunna göras vid exempelvis "små förändringar", så bör processen definiera vilka slags förändringar som ryms därinom och därmed inte kräver föreslagna formella kontrollpunkter. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
3. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
4. Infrastruktur (IF)		**Avsaknad av dokumentation gällande återläsningstest.** **Observation:** Genom intervju noterades att det saknas en rutin för periodisk återläsning av kritisk data i Procapita IFO. Vidare noterades det att det inte sker några formaliserade återläsningstester. **Risk**: Avsaknad av återläsning och testning gällande backup ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en rutin för periodisk testning och återläsning av kritisk data. Vidare bör formell dokumentation gällande återläsning upprättas i syfte att skapa spårbarhet i genomförda tester. **Systemägarens kommentar:**

Observationer och rekommendationer - Siebel

Granskningsområde	Gradering	Observationer
1. IT-styrning (IS)		**Kontinuitet- och katastrofplan för Siebel är inte formaliserade.** **Observation:** Genom intervju noterades det att ingen formell kontinuitets- eller katastrofplan finns implementerad för applikationen Siebel. **Risk:** Avsaknad av katastrof- och avbrottsplan ökar risken för brister och dataförlust vid driftstopp, som även kan leda till orimligt lång nertid. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun dokumenterar de åtgärder som behöver vidtas, och ansvariga personer, för att effektivt återställa system, applikationer och processer vid en eventuell katastrof eller incident. Detta görs med fördel med hjälp av Teknik & Service som ansvarar för den tekniska delen av kontinuitetsplanen. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
2. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
3. Infrastruktur (IF)		**Avsaknad av dokumentation gällande återläsningstest.** **Observation:** Genom intervju noterades att det saknas en rutin för periodisk återläsning av kritisk data i Siebel. Vidare noterades det att det inte sker några formaliserade återläsningstester. **Risk**: Avsaknad av återläsning och testning gällande backup ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en rutin för periodisk testning och återläsning av kritisk data. Vidare bör formell dokumentation gällande återläsning upprättas i syfte att skapa spårbarhet i genomförda tester. **Systemägarens kommentar:**

Observationer och rekommendationer – Extens

Granskningsområde	Gradering	Observationer
1. IT-styrning (IS)		**Kontinuitet- och katastrofplan för Extens är inte formaliserade.** **Observation:** Genom intervju noterades det att ingen formell kontinuitets- eller katastrofplan finns implementerad för applikationen Extens. **Risk**: Avsaknad av katastrof- och avbrottsplan ökar risken för brister och dataförlust vid driftstopp, som även kan leda till orimligt lång nertid. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun dokumenterar de åtgärder som behöver vidtas, och ansvariga personer, för att effektivt återställa system, applikationer och processer vid en eventuell katastrof eller incident. Detta görs med fördel med hjälp av Teknik & Service som ansvarar för den tekniska delen av kontinuitetsplanen. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
2. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
3. Åtkomstkontroll (ÅK)		**Bristande säkerhetsinställningar i applikationen Extens.** **Observation:** Genom intervju och inspektion noterades det att rådande säkerhetsinställningar i applikationen inte är uppsatta enligt god praxis. Lösenord behöver endast bytas var 6:e månad och kräver endast 5 tecken långt lösenord. **Risk**: Bristfälliga lösenordsparametrar ökar risken för otillåten åtkomst till applikationen, vilket ökar risken för obehörig åtkomst till kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en lösenordspolicy för Extens som uppfyller god praxis. Exempel på vad policyn kan innehålla: • Forcerat lösenordsbyte efter 90 dagar • Lösenordet måste innehålla minst 8 tecken • Samma lösenord kan inte användas inom loppet av 18 månader • Krav på minst en siffra samt stora och små tecken • Kontot låses efter 3 misslyckade inloggningsförsök Vidare rekommenderar vi att det utförs en periodisk genomgång av rådande inställningar för att säkerställa att inställningarna inte har förändrats eller nollställts. **Systemägarens kommentar:**

Granskningsområde	Gradering	Observationer
4. Infrastruktur (IF)		**Avsaknad av dokumentation gällande återläsningstest.** **Observation:** Genom intervju noterades att det saknas en rutin för periodisk återläsning av kritisk data i Extens. Vidare noterades det att det inte sker några formaliserade återläsningstester. **Risk**: Avsaknad av återläsning och testning gällande backup ökar risken för förlust av data vid incidenter och driftsstopp och kan även förlänga återställningstiden. Förlust och ofullständighet i data kan påverka kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en rutin för periodisk testning och återläsning av kritisk data. Vidare bör formell dokumentation gällande återläsning upprättas i syfte att skapa spårbarhet i genomförda tester. **Systemägarens kommentar:**

Observationer och rekommendationer – Teknik & Service

Granskningsområde	Gradering	Observationer
1. Åtkomstkontroll (ÅK)		**Periodisk granskning av användare.** **Observation:** Genom intervju noterades att periodisk granskning av användare i applikationerna initieras av Teknik & Service baserat på utdrag av beställningar i IRIS. Verksamheten ansvarar sedan för att säkerställa att behörigheterna enligt IRIS är korrekta och återkopplar sedan till Teknik & Service. Denna genomgång är under granskningstillfället pågående, varför PwC inte kan uttala sig om kontrollen fungerar ändamålsenligt. **Risk:** Felaktigheter i behörigheter ökar risken för otillåten åtkomst. Otillåten åtkomst ökar risken för avsiktlig förändring av kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun utvärderar processen för den periodiska granskningen av behörigheter för att säkerställa dess tillämpbarhet i verksamheten. PwC ser som angeläget att en ändamålsenlig process finns på plats och tillämpas. **Teknik & Service kommentar:**

Granskningsområde	Gradering	Observationer
2. Åtkomstkontroll (ÅK)		**Bristande säkerhetsinställningar i Active Directory.** **Observation:** Genom intervju och inspektion noterades det att rådande säkerhetsinställningar i Active Directory inte är uppsatta enligt god praxis. Lösenord behöver endast bytas var 180:e dag, kräver endast 6 tecken långt lösenord och har inga krav på komplext lösenord. **Risk**: Bristfälliga lösenordsparametrar ökar risken för otillåten åtkomst till operativsystemet, vilket ökar risken för obehörig åtkomst till kritisk information. **Rekommendation:** PwC rekommenderar att Uppsala kommun upprättar en lösenordspolicy för Active Directory som uppfyller god praxis. Exempel på vad policyn kan innehålla: • Forcerat lösenordsbyte efter 90 dagar • Lösenordet måste innehålla minst 8 tecken • Samma lösenord kan inte användas inom loppet av 18 månader • Krav på minst en siffra samt stora och små tecken (komplext lösenord) • Kontot låses efter 3 misslyckade inloggningsförsök Vidare rekommenderar vi att det utförs en periodisk genomgång av rådande inställningar för att säkerställa att inställningarna inte har förändrats eller nollställts. **Teknik & Service kommentar:**

Handläggare
Elaine Wicks

Datum
2013-04-22

Diarienummer
BUN-2012-0631
Bilaga 2

FÖRSLAG

Kommunrevision

Yttrande över Granskning av generalla IT-kontroller 2013

Kommunrevisionen har av barn- och ungdomsnämnden begärt svar på fyra brister. Nämnden svarar härmed:

1. Kontinuitet- och katastrofplan för Extens är inte formaliserade
Svar: Det finns en katastrofplan för Agresso med en sekundär infrastruktur som skulle kunde vara ett eventuellt förslag till en lösning. Implementering av detta ska inkluderas i förvaltningsplan för Extens. Nämnden anser att det vore bra om det fanns en kommun gemensamt tekniskt lösning för applikationer som fanns med i granskningsomfattningen.

2. Periodisk granskning av användare:
Svar: Påpekandet är åtgärdat och det finns en dokumenterad process för hur detta ska ske.

3. Bristande säkerhetsinställningar
Svar: För att ökar säkerheten kommer nämnden tillse att inställningar för lösenord ändras.
- Antal tecken ska ändras från fem till åtta
- Kravet ska vara minst en siffra samt stora och små tecken.
- Tar med aktiviteten om hur ofta ett tvingande lösenordsbyte ska göras i kontorets förvaltningsplan.

4. Avsaknad av dokumentation gällande återläsningstest
Svar: Återläsning (kopiering) av data görs inte till produktion men med jämna mellanrum så sker det en återläsning från produktion till test. Observationen i rapporten menar att data ska tars från säkerhetskopiorna och läser in det i systemet. En katastrof plan bör innehålla dokumentation och rutiner om hur återläsningsdelen ska gå till och hur ofta detta ska göras. Nämnden kommer att tillse att detta implementeras i förvaltningsplan för Extens.

Barn- och ungdomsnämnden

Cecilia Forss
Ordförande

Kerstin Sundqvist
Sekreterare

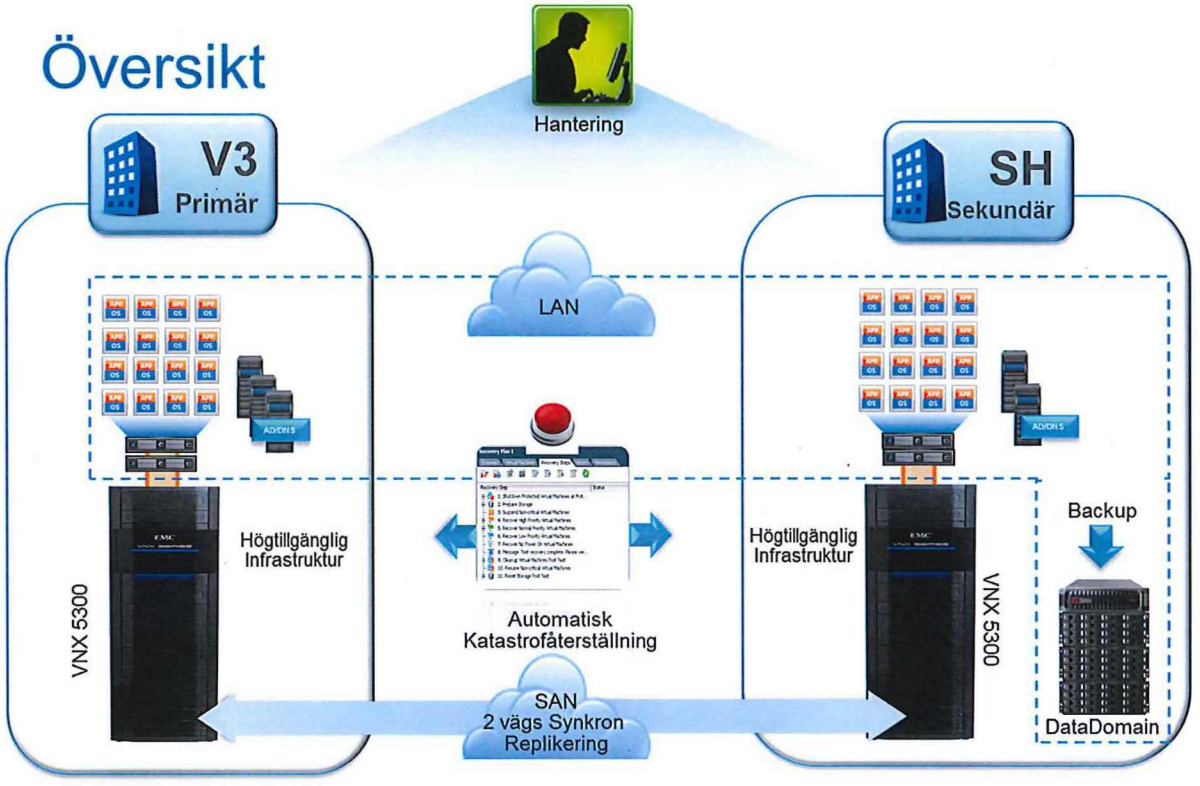
Katastrofplan Agresso

Bakgrund

Teknik och Service avdelning IT säljer IT-drift till Uppsala kommun. Driften körs i 2st separata datahallar. Den primära datahallen V3 uppfyller normen EN1047-2. Den sekundära hallen SH uppfyller inte den normen men har fullgott UPS-skydd.

Agresso

Uppsala kommuns ekonomisystem Agresso är helt virtualiserat. Systemet består av separata applikations-, webb- och databasservrar. Virtualiseringsplattformen är VMware Vsphere 5.0. Agressoservrarna existerar som VM (virtuella maskiner) i ett cluster med 5st Hostar som har 9st Datastores knutna till sig. Samtliga hostar i clustret använder funktionerna HA (High Availability), DRS (Distributed Resource Scheduler) och SRM (Site Recovery Manager)
HA innebär att om en host drabbas av hårdvarufel startas samtliga aktiva VM som fanns på den hosten om på någon annan host.
DRS flyttar aktiva VM mellan hostar i clustret baserat på lediga resurser.
SRM innebär enkelt uttryckt att de VM som utnyttjar tjänsten speglas till ett annat VMwarecluster i realtid. Det betyder att vid bortfall av en hel datahall kan hela miljön återstartas på ny plats inom 30-60 min. SRM-tjänsten kan köras i testläge där man genomför en hel katastrofåterställning utan att störa ordinarie drift.



Granskning av behörigheter i kommungemensamma system

2013-11-04/AE