

Handläggare
Ditz Catrin
Nilsson Maria

Datum
2015-02-03

Diarienummer
KSN-2014-1679

Kommunstyrelsen

Kommunrevisionen: granskning av generella IT-kontroller 2014

Förslag till beslut

Kommunstyrelsen föreslås besluta

att avge yttrande till kommunrevisionen enligt **bilaga 1**

Ärendet

Kommunrevisionen har överlämnat revisionsrapport Uppföljningsrapport IT-generella kontroller 2014 **bilaga 2**.

PwC har på kommunrevisionens uppdrag gjort en uppföljande granskning av generella IT-kontroller. Granskningen fokuserar på säkerheten i applikationer, operativsystem och databaser samt omfattar Agresso, Heroma, Procapita, Siebel, Extens och Teknik och Service.

Av totalt 20 brister som noterades under 2013 års granskning kvarstår 10 stycken som ej åtgärdade och för resterande 10 brister har aktiviteter påbörjats. För majoriteten av observationerna där aktiviteter påbörjats, utförs kontrollen i dagsläget, men de dokumenteras bristfälligt eller inte alls, varför PwC inte kan verifiera att kontrollen utförs ändamålsenligt.

Kommunrevisionen konstaterar att vissa åtgärder vidtagits/planeras för att skapa grundläggande IT-säkerhet och förvaltningsstruktur för kritiska applikationer, men ser särskilt allvarligt på att tidigare påpekade säkerhetsbrister kvarstår i kommunens datasystem.

Föredragning

I yttrandet framhålls att samtliga säkerhetsbrister är prioriterade och åtgärder är vidtagna eller planerade att genomföras under 2015. Kommunledningskontoret driver det arbetet.

IT i Uppsala kommun idag har förutsättningar som IT-styrning, gemensamma mål, en stark vilja att bygga tillsammans samt resurser till prioriterade åtgärder. Detta är förutsättningar som möjliggör att observerade brister kommer att hanteras under 2015 enligt framtagna åtgärdshantering.

Kommunledningskontoret

Joachim Danielsson
Stadsdirektör

Christoffer Nilsson
Chef för kommunledningskontoret

Handläggare
Catrin Ditz
Maria Nilsson

Datum
2015-01-20

Diarienummer
KSN-2014-1679

Kommunrevisionen

Svar på uppföljningsrapport IT-generella kontroller 2014, Uppsala kommun

PwC har på kommunrevisionens uppdrag gjort en uppföljande granskning av generella IT-kontroller 2013.

Av totalt 20 brister som noterades under 2013 års granskning kvarstår 10 stycken som ej åtgärdade och för resterande 10 brister har aktiviteter påbörjats. Kommunrevisionen har konstaterat att vissa åtgärder vidtagits/planerats för att skapa grundläggande IT-säkerhet och förvaltningsstruktur för kritiska applikationer, men ser särskilt allvarligt på att tidigare påpekade säkerhetsbrister kvarstår i kommunens datasystem.

Planerade åtgärder för att hantera identifierade säkerhetsbrister är prioriterade och kommer alla att hanteras under 2015. Planerade och vidtagna åtgärder presenteras nedan.

Planerade och vidtagna åtgärder

IT inom Uppsala har påbörjat en omfattande förändringsresa från en decentraliserad IT-styrning till en IT-styrning som drivs utifrån ett kommungemensamt helhetsperspektiv med medborgar- och verksamhetsnytta i fokus.

En IT-strategisk stab har etablerats på kommunledningskontoret. Kompetenser och bemanning omfattar både ledning och styrning, beställarkompetens och stöd till kommunens verksamheter. Staben har ett aktivt samarbete med kommunens förvaltningar, IT-produktion i egen regi samt externa leverantörer. Stabens uppdrag är att ta fram en ny långsiktig inriktning för kommunens IT samt, efter beslut, leda arbetet att verkställa denna.

Åtgärdshantering för identifierade brister

Åtgärder beskrivs nedan utifrån rapportens fem områden:

1. IT-styrning
2. Programutveckling och förändring
3. Åtkomstkontroll
4. Infrastruktur

Roller och ansvar vid åtgärdande av identifierade brister:

- Objektägaren är ansvarig för att brist åtgärdas
- Objektledare/Funktionsansvarig drift genomför åtgärd eller är sammanhållande
- IT-koordinator ansvarar för att status rapporteras till IT-stab. IT-koordinator stöttar/leder objektledare enligt behov
- IT strateg följer upp och sammanställer åtgärdsstatus för samtliga brister

Status för arbetet rapporteras löpande i samarbetsforum för ändamålet. Aktiviteter skrivs in och resurssätts i förvaltningsplan för respektive system.

Observation, nuläge och åtgärder för området IT-styrning

Observation samt nuläge är att katastrofplan inte är implementerad för följande system:

- Procapita IFO, aktiviteten är påbörjad
- Heroma, Siebel och Extens, aktiviteten är ej påbörjad

Hantering av åtgärder

Objektledaren tar med stöd av IT-koordinator fram katastrofplan eller slutför katastrofplan. IT-koordinator/objektledare får stöd av Funktionsansvarig drift.

Funktionsansvarig drift säkrar att katastrofplaner tas fram på likartat sätt och att insatser för ett system kan återanvändas.

När rutinen är framtagen för respektive system ur ett verksamhetsperspektiv tar Funktionsansvarig drift frågan vidare med enheten för drift av servrar. Driften kompletterar de tekniska delarna.

Objektledaren kompletterar respektive förvaltningsplan med test av katastrofplan.

Observation, nuläge och åtgärder för området Programutveckling och förändring

Observation samt nuläge är bristande dokumentation avseende förändringar i applikationer för följande system:

- Agresso, aktivitet är påbörjad genom att förvaltningsmodell pm3 har implementerats. Enligt erhållen information finns rutinerna på plats med det är inte fastställt att de efterslevs fullt ut i verksamheten
- Procapita IFO, aktivitet är påbörjad genom att en process för ändringshantering är införd. Dock dokumenteras inte förändringarna på det sätt så att det går att följa ärendet från ändringsbegäran till driftsättning.

Hantering av åtgärder

Objektledare för Agresso och Procapita IFO säkrar med stöd av IT-koordinator att befintliga rutiner för ändringshantering efterlevs.

Observation, nuläge och åtgärder för området Åtkomstkontroll

Observation samt nuläge är att:

- Periodisk genomgång av användare hade vid granskningstillfället inte utförts för
 - Agresso, Heroma, Procapita IFO, Uppsala kommun har under året genomfört periodisk genomgång av användare. Dock har PwC inte kunnat verifiera att kontrollen utförts, därför kvarstår observationen.
 - Siebel, Uppsala kommun har under året genomfört periodisk genomgång, dock är inte genomgången formaliserad.
 - Extens, Uppsala kommun har inlett arbetet med att registrera alla externa användare och ny rutin för periodisk genomgång är under etablering.
 - Teknik och Service, rutinen är implementerad sedan tidigare, uppföljning av genomförd granskning i maj genomfördes ej fullt ut på grund av omprioritering av resurser
- Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis för:
 - Heroma, Extens och Teknik och Service, Lösenordsinställningar för dessa system följde Uppsala kommuns riktlinjer, dock uppfyller inte riktlinjerna vid tidpunkt för granskning god praxis. Under december 2014 ändrades riktlinjerna så att de nu överensstämmer med god praxis.

Hantering av åtgärder

Objektledare för Agresso, Heroma och Procapita IFO med stöd av IT-koordinator dokumenterar tillvägagångssätt för periodisk granskning på sådant sätt att det kan verifieras av oberoende part att kontrollen utförs.

Objektledare för Siebel, Extens och Teknik och Service med stöd av IT-koordinator etablerar befintlig kommungemensam process för periodisk genomgång av användare.

Tillämpning av den nya lösenordspolicyn vilken uppfyller god praxis pågår. Arbetet leds av objektledare vad gäller Siebel och Extens och funktionsansvarig drift för Teknik och Service.

För att minimera påverkan för kommunens användare sker detta under en längre tid, med slutdatum juli 2015.

Objektledare/funktionsansvarig drift ansvarar för att lösenordspolicyn dokumenteras i systemdokumentation för berört system.

Observation, nuläge och åtgärder för området Infrastruktur

Observation samt nuläge är att inga formella återläsningstester av backup har genomförts för:

- Agresso, Uppsala kommun har påbörjat arbete med att upprätta formella återläsningstester av backup. I dagsläget utförs dock inga formella återläsningstester.
- Heroma, Rutiner finns på plats, men det har inte skett några formella återläsningstester under verksamhetsåret.
- Procapita IFS, Siebel och Extens, aktivitet ej påbörjad

Hantering av åtgärder

Funktionsansvarig drift tar med stöd av medarbetare på enheten för drift av servrar fram en rutin. Rutinen förankras med IT-koordinator och objektledare för berört system. Rutin etableras.

Objektledaren kompletterar respektive förvaltningsplan gällande formella återläsningstester av backup.

Verifiering av kontroller

Samtliga åtgärder dokumenteras på sådant sätt att oberoende part kan verifiera att kontrollen utförs ändamålsenligt.

Kommunstyrelsen

Marlene Burwick
Ordförande

Astrid Anker
Sekreterare



KRN 2014/74
Exp 2014-12-18 *146*

Kommunrevisionen

UPPSALA KOMMUNSTYRELSE	
Ink.	2014 -12- 22
Diar.nr.	KSN-2014-1679
	04 Akbil. 1

2014-12-18

Kommunstyrelsen
Styrelsen för teknik och service
Kommunledningskontoret
Nämnder och styrelser, f k

Granskning av generella IT-kontroller 2014

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. Granskningen omfattar Agresso, Heroma, Procapita, Siebel, Extens och Teknik & Service.

Av totalt 20 brister som noterades under 2013 års granskning kvarstår 10 stycken som ej åtgärdade och för resterande 10 brister har aktiviteter påbörjats. Brister som inte har åtgärdats är följande:

- Katastrofplan är inte implementerad för Heroma, Siebel eller Extens
- Inga formella återläsningstester av backuper har genomförts för Heroma, Procapita, Siebel eller Extens
- Lösenordsinställningar uppfyller inte god praxis – Heroma eller Teknik & Service
- Periodisk genomgång av användare har inte utförts för Siebel

Vi kan konstatera att vissa åtgärder vidtagits/planeras för att skapa grundläggande IT-säkerhet och förvaltningsstruktur för kritiska applikationer, men vi ser särskilt allvarligt på att tidigare påpekade säkerhetsbrister kvarstår i kommunens datasystem.

Vi översänder rapporten för yttrade över vilka åtgärder som planeras vidtas för att komma tillrätta med problemen. Vi önskar svar senast den 27 februari 2015.

FÖR KOMMUNENS REVISORER

Lars-Olof Lindell
Ordförande



Revisionsrapport

Uppföljningsrapport

IT-generella kontroller 2014

Uppsala kommun

Anders Gustafson
Gustaf Gambe

Oktober 2014

Innehållsförteckning

Inledning	3
Granskningens omfattning.....	3
Sammanfattning	5
Resultat och status på observationer	6

Appendix 1 – Intervjuade personer

Inledning

I samband med den finansiella revisionen 2014 har PwC genomfört en uppföljning av de observationer som identifierades i samband med 2013 års granskning avseende IT-generella kontroller för verksamhetskritiska applikationer inom Uppsala kommun.

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

Syftet med uppföljningen är att identifiera vilka förändringar som Uppsala kommun har genomfört gällande den interna kontrollen under 2014 och hur detta har påverkat föregående års observationer. Rapporten presenterar det aggregerade resultatet av respektive applikation med en status för varje observation, 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 hjälpt oss att genomföra granskningen, för deras bemötande och goda samarbetsvilja.

Granskningens omfattning

Under föregående år granskning noterades avvikelser inom följande områden:

Område	Observation
IT-styrning	Katastrofplan är inte implementerad för samtliga applikationer
Programutveckling och förändring	Bristande dokumentation avseende förändringar i applikationer
Åtkomstkontroll	Periodisk genomgång av användare har vid granskningstillfället inte utförts
	Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis
Infrastruktur	Inga formella återläsningstester av backup har genomförts

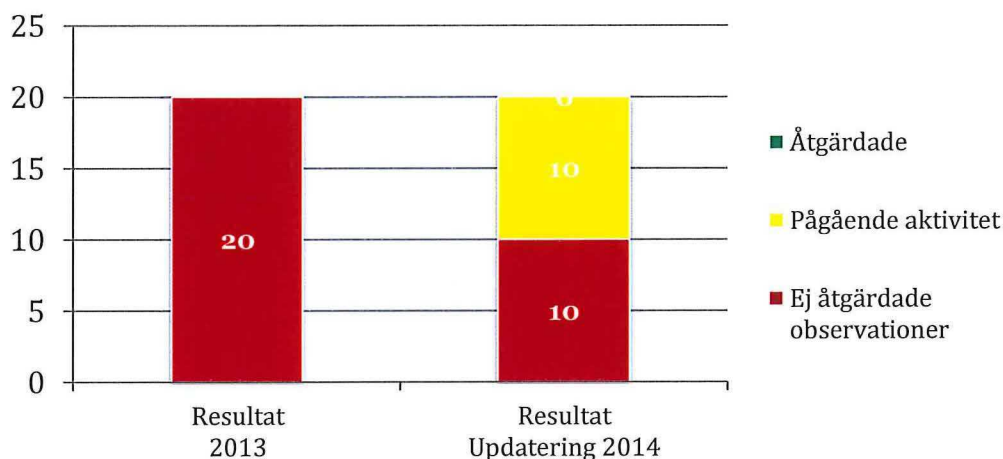
Vid applikationsgranskningar och granskning av processer för Teknik & Service noterades totalt 20 observationer enligt nedan fördelning vid föregående års granskning:

Applikation	Antal Observationer
Agresso	3
Heroma	4
Procapita Individ- och Familjeomsorg (IFO)	4
Siebel	3
Extens	4
Teknik & Service	2
Totalt antal observationer	20

PwC har under oktober 2014 följt upp ovan observationer med relevant personal på Uppsala kommun (se Appendix 1- Intervjuade personer).

Sammanfattning

Genom intervju och genomgång av dokumentation kan PwC konstatera att Uppsala kommun har påbörjat aktiviteter under verksamhetsåret för att åtgärda observationerna. Av totalt 20 observationer från föregående år kvarstår 10 (50%) stycken som ej åtgärdade och för resterande 10 (50%) har aktiviteter påbörjats. För majoriteten av observationerna där aktiviteter påbörjats, utförs kontrollen i dagsläget, men de dokumenteras bristfälligt eller inte alls, varför PwC inte kan verifiera att kontrollerna utförs ändamålsenligt. Se tabell nedan för illustration av resultatet.



Utifrån den uppföljning som är gjord har det framkommit att Uppsala kommun har genomfört samt håller på att genomföra förbättringar inom ett antal områden men att det fortfarande finns utrymme för förbättring gällande den interna kontrollen kopplat till IT. Förbättringar har skett under året trots att mycket resurser har lagts på det upphandlingsprojekt av telefon och IT som pågår, samt att det skett personalförändringar inom organisationen under verksamhetsåret. Till exempel har ny CIO och IT-säkerhetschef anställts, och det pågår arbete med att ta fram en styrmodell för IT-policys med tydliga roller och ansvar. Det pågår även informationsklassning som förväntas vara klar till årsskiftet.

För mer detaljer gällande status på respektive observation från föregående år, se avsnitt "Resultat och status på observationer" nedan.

Resultat och status på observationer

Observationer från föregående år har granskats genom intervju samt i förekommande fall via genomgång av dokumentation. Baserat på detta resultat har respektive observation graderats med en status. Observera att denna gradering inte är jämförbar med föregående års rapport.

Observationerna har graderats enligt följande modell:



- Observationen har inte åtgärdats sedan föregående års granskning vilket medför att relaterad risk och rekommendation kvarstår.



- Aktiviteter och åtgärder finns planerade eller är under genomförande, dock kvarstår risken då åtgärderna ännu inte är på plats.



- Åtgärder och aktiviteter för att begränsa risken har implementerats och underlag har granskats vilket säkerställer operativ effektivitet i kontrollen.

Nedan återfinnas resultatet av den uppföljningsgranskning som genomförts per observation.

Applikation	Ref	Observation	Status
Agresso	1.	Bristande dokumentation avseende förändringar i applikationer. Status 2014 Uppsala kommun har implementerat förvaltningsmodellen PM3 där rutiner för förändringshantering ingår. Enligt erhållen information finns rutinerna på plats men det är inte fastställt att de efterlevs fullt ut i verksamheten. Slutsats: Observationen kvarstår då rutinerna i dagsläget inte efterlevs fullt ut i verksamheten.	
	2.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Uppsala kommun har under året genomfört periodisk genomgång av användare i Agresso. Dock har PwC inte kunnat verifiera att kontrollen utförts, då underliggande dokumentation ej erhållits. Slutsats: Observationen kvarstår då PwC inte kunnat granska underliggande dokumentation.	

Applikation	Ref	Observation	Status
	3.	Inga formella återläsningstester av backup har genomförts. Status 2014 Uppsala kommun har påbörjat arbete med att upprätta formella återläsningstester av backup. Dock är arbetet pågående och i dagsläget utförs inga formella återläsningstester. Slutsats: Observationen kvarstår då formellt återläsningstest ännu ej har genomförts under verksamhetsåret.	
Heroma	1.	Katastrofplan är inte implementerad för samtliga applikationer. Status 2014 Uppsala kommun har inte påbörjat något arbete med att ta fram en katastrofplan för applikationen Heroma under verksamhetsåret. Slutsats: Observationen kvarstår då katastrofplan ännu ej är formellt implementerad.	
	2.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Uppsala kommun har under året genomfört periodisk genomgång av användare i Heroma. Dock har PwC inte kunnat verifiera att kontrollen utförts, då underliggande dokumentation ej erhållits. Slutsats: Observationen kvarstår då PwC inte kunnat granska underliggande dokumentation.	

Applikation	Ref	Observation	Status
	3.	Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis. Status 2014 Lösenordsinställningarna i Heroma följer Uppsala kommuns riktlinjer för lösenord. Dock uppfyller inte dessa god praxis, då endast ett 6 tecken långt lösenord kan användas. Slutsats: Observationen kvarstår då Uppsala kommuns lösenordspolicy inte uppfyller god praxis.	
	4.	Inga formella återläsningstester av backup har genomförts. Status 2014 Rutiner finns på plats men det har inte skett några formella återläsningstester under verksamhetsåret. Slutsats: Observationen kvarstår då formellt återläsningstest ännu ej har genomförts under verksamhetsåret.	
Procapita IFO	1.	Katastrofplan är inte implementerad för samtliga applikationer. Status 2014 Uppsala kommun har påbörjat arbete med att ta fram en katastrofplan för applikationen Procapita IFO. Dock är arbetet pågående och i dagsläget finns ingen katastrofplan implementerad. Slutsats: Observationen kvarstår då katastrofplan ännu ej är formellt implementerad.	

Applikation	Ref	Observation	Status
	2.	Bristande dokumentation avseende förändringar i applikationer. Status 2014 Samtliga förändringar i Procapita IFO hanteras av en utvecklingsgrupp och styrgrupp, där varje ärende hanteras. Dock dokumenteras inte förändringarna på det sätt så att det går att följa ärendet från ändringsbegäran till driftsättning. Dock är planen att ta fram en gemensam process för förändringshantering och hur de ska dokumenteras för samtliga system. Slutsats: Observationen kvarstår, då förändringarna inte dokumenteras så att spårbarhet i hela förändringsprocessen är möjlig.	
	3.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Uppsala kommun har under året genomfört periodisk genomgång av användare i Procapita IFO. Dock har PwC inte kunnat verifiera att kontrollen utförts, då underliggande dokumentation ej erhållits. Slutsats: Observationen kvarstår då PwC inte kunnat granska underliggande dokumentation.	
	4.	Inga formella återläsningstester av backup har genomförts. Status 2014 Uppsala kommun har inte påbörjat något arbete med att implementera rutiner för formella återläsningstester under verksamhetsåret. Slutsats: Observationen kvarstår då rutinen för formellt återläsningstest ännu ej är formellt implementerad.	

Applikation	Ref	Observation	Status
Siebel	1.	Katastrofplan är inte implementerad för samtliga applikationer. Status 2014 Uppsala kommun har inte påbörjat något arbete med att ta fram en katastrofplan för applikationen Siebel under verksamhetsåret. Slutsats: Observationen kvarstår då katastrofplan ännu ej är formellt implementerad.	
	2.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Uppsala kommun har under året genomfört periodisk genomgång av användare i Siebel, dock är inte genomgången formaliserad. Slutsats: Observationen kvarstår då det inte genomförts någon formell periodisk genomgång under verksamhetsåret.	
	3.	Inga formella återläsningstester av backup har genomförts. Status 2014 Uppsala kommun har inte påbörjat något arbete med att implementera rutiner för formella återläsningstester under verksamhetsåret. Slutsats: Observationen kvarstår då rutinen för formellt återläsningstest ännu ej är formellt implementerad.	

Applikation	Ref	Observation	Status
Extens	1.	Katastrofplan är inte implementerad för samtliga applikationer. Status 2014 Uppsala kommun har inte påbörjat något arbete med att ta fram en katastrofplan för applikationen Extens under verksamhetsåret. Slutsats: Observationen kvarstår då katastrofplan ännu ej är formellt implementerad.	
	2.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Uppsala kommun har inlett arbete med att registrera alla externa användare och ny rutin för periodisk genomgång av användare kommer att implementeras inom två månader. Slutsats: Observationen kvarstår då periodisk genomgång av samtliga användare i applikationen ej genomförts under verksamhetsåret.	
	3.	Inga formella återläsningstester av backup har genomförts. Status 2014 Uppsala kommun har inte påbörjat något arbete med att implementera rutiner för formella återläsningstester under verksamhetsåret. Slutsats: Observationen kvarstår då rutinen för formellt återläsningstest ännu ej är formellt implementerad.	

Applikation	Ref	Observation	Status
	4.	Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis. Status 2014 Uppsala kommun har genomfört en riskanalys och arbete pågår för att övergå till e-legitimation vid inloggning i systemet. Arbetet är inplanerat till våren 2015. Slutsats: Observationen kvarstår då nuvarande lösenordsinställningar ej uppfyller god praxis.	
Teknik & Service	1.	Periodisk genomgång av användare har vid granskningstillfället inte utförts. Status 2014 Rutinen är implementerad sedan tidigare och uppföljning av genomförd granskning i maj genomfördes ej fullt ut på grund av omprioritering av resurser. Slutsats: Observationen kvarstår då uppföljning av genomförd granskning ej avslutats under verksamhetsåret.	
	2.	Lösenordsinställningar i applikationer och operativsystem uppfyller ej god praxis. Status 2014 Lösenordsinställningarna på operativsystemsnivå följer Uppsala kommuns riktlinjer för lösenord. Dock uppfyller inte dessa god praxis, då endast ett 6 tecken långt lösenord kan användas. Slutsats: Observationen kvarstår då Uppsala kommuns övergripande lösenordspolicy inte uppfyller god praxis.	



Appendix 1 – Intervjuade personer

I samband med revisionen har intervju genomförts med nyckelpersoner inom Uppsala kommun i syfte att skapa förståelse för vilka förändringar som genomförts sedan föregående års revision. Följande personer intervjuades:

- Catrin Ditz – CIO
- Anders Kylesten – Säkerhetschef
- Maria Nilsson – IT-strateg