Uppsala kommun

Socialförvaltningen
Tjänsteskrivelse

Handläggare:
Thomas Fäldt

Datum:
2019-08-07

Diarienummer:
SCN-2019-0228

Socialnämnden

Yttrande till kommunrevisionen över granskning av IT-relaterade kontroller

Förslag till beslut

Socialnämnden föreslås besluta

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

Ärendet

Kommunrevisionen har genomfört en granskning av IT-relaterade kontroller i ett antal av kommunens system med betydelse för den finansiella rapporteringen. Fokus har legat på behörigheter och tilldelning av behörigheter. Revisionen har efter granskningen gjort bedömningen att kommunens behörighetshantering i stort är ändamålsenlig och att rimliga kontroller finns för de system som granskats. Inom vissa områden anser revisionen att kontrollerna bör förstärkas. Rekommendationerna rör bland annat frekvensen i behörighetskontroller, attester och loggfunktioner i några av kommunens IT-system. Kommunrevisionen har överlämnat en rapport över en genomförd granskning av IT-relaterade kontroller till kommunstyrelsen för yttrande senast den 30 augusti, bilaga 2. Socialnämnden och arbetsmarknadsnämnden har utöver kommunstyrelsen ombetts att yttra sig över granskningen.

Föredragning

Socialnämnden ser positivt på kommunrevisionens granskning av IT-relaterade kontroller. Trygga och säkra IT-lösningar är en förutsättning i en allt mer digital värld. Nämnden överlåter till kommunstyrelsen att besvara de enskilda förbättringsåtgärderna som kommunrevisionen föreslår då kommunstyrelsen är huvudansvarig för de olika systemen. Nämnden anser dock att de grundkontroller som genomförs minst en gång om året är tillräckliga ställt mot de omfattande resurser som kan krävas vid kontroll av systemen. Systemansvariga och förvaltningen har möjlighet att initiera ytterligare kontroller vid behov.

Postadress: Uppsala kommun, socialförvaltningen, 753 75 Uppsala
Telefon: 018-727 00 00 (växel)
E-post: socialforvaltningen@uppsala.se
www.uppsala.se

Nämnden är en av huvudanvändarna av verksamhetssystemet Pro Capita. För att säkerställa korrekt användning av systemet har nämndens förvaltning sedan flera år tillbaka en intern Pro Capita – organisation som leds av en samordnare. Syftet är dels att underlätta för förvaltningens handläggare att arbeta i systemet men även underlätta samverkan med kommunledningskontorets systemförvaltare avseende anpassning och utveckling av systemet. Socialnämnden har därutöver inget att tillägga.

Konsekvenser för barn, jämställdhet eller ekonomi

Ärendet har inte några konsekvenser ur barn-, jämställdhets- eller ekonomiskt perspektivet med föreliggande förslag till beslut.

Bilagor

Bilaga 1 – Yttrande till kommunrevisionen över granskning av IT-relaterade kontroller
Bilaga 2 – Granskning av IT-relaterade kontroller

Socialförvaltningen

Kaisa Björnström
Direktör

Uppsala kommun

Datum:
2019-08-07

Diarienummer:
SCN-2019-0228

Socialnämnden

Förslag

Handläggare:
Fäldt Thomas

Kommunrevisionen

Yttrande till kommunrevisionen över granskning av IT-relaterade kontroller

Socialnämnden ser positivt på kommunrevisionens granskning av IT-relaterade kontroller. Trygga och säkra IT-lösningar är en förutsättning i en allt mer digital värld. Nämnden överlåter till kommunstyrelsen att besvara de enskilda förbättrings-åtgärderna som kommunrevisionen föreslår då kommunstyrelsen är huvudansvarig för de olika systemen. Nämnden anser dock att de grundkontroller som genomförs minst en gång om året är tillräckliga ställt mot de omfattande resurser som kan krävas vid kontroll av systemen. Systemansvariga och förvaltningen har möjlighet att initiera ytterligare kontroller vid behov.

Nämnden är en av huvudanvändarna av verksamhetssystemet Pro Capita. För att säkerställa korrekt användning av systemet har nämndens förvaltning sedan flera år tillbaka en intern Pro Capita – organisation som leds av en samordnare. Syftet är dels att underlätta för förvaltningens handläggare att arbeta i systemet men även underlätta samverkan med kommunledningskontorets systemförvaltare avseende anpassning och utveckling av systemet. Socialnämnden har därutöver inget att tillägga.

Socialnämnden

Eva Christiernin
Ordförande

Lotta von Wowern
Sekreterare

KOMMUNREVISIONEN
Missivskrivelse

Datum:
2019-04-12

Diarienummer:
KRN-2019/21

Mottagare

Kommunstyrelsen	Svar senast 2019-08-31
Arbetsmarknadsnämnden	Svar senast 2019-08-31
Socialnämnden	Svar senast 2019-08-31
Övriga nämnder	För kännedom
Kommunfullmäktige	För kännedom

Granskning av IT-relaterade kontroller

KPMG har på uppdrag av de förtroendevalda revisorerna i Uppsala kommun granskat IT-relaterade kontroller i ett antal system med betydelse för den finansiella rapporteringen. Fokus har legat på behörigheter och tilldelning av behörigheter. Efter genomförd granskning gör vi be-dömningen att kommunens behörighetshantering i stort är ändamålsenlig och att rimliga kontroller finns för de system som granskats. Inom vissa områden anser vi att kontrollerna kan och bör förstärkas. Våra rekommendationer:

- För flera av de granskade systemen sker kontroll en gång om året att behörigheter överensstämmer mot vad som är beslutat enligt Iris. Vår rekommendation är att den kon-trollen görs mer frekvent.
- Heroma: Löner kan ändras av systemförvaltarna och IT-objektledarna själva. Det är upp till cheferna och medarbetarna att hitta eventuella felaktiga löner. Vi bedömer att det kan finnas en risk med att en felaktig lön inte uppmärksammas. Vår rekommendation är att införa en spärr som inte låter en enskild person ändra en lön.
- Agresso, I: Loggen som förs i systemet över ändringar i behörighetsregister kan kopp-las bort av systemförvaltarna och IT-objektledarna. Vår rekommendation är att logg-funktionen inte ska kunna slås av.
- Agresso, II: Manuella bokföringsordrar kräver inte attest i systemet. Vi rekommenderar att attestkrav införs för manuella bokföringsordrar över lämplig beloppsgräns.
- För Kommers är det viktigt att rätt behörigheter är inlagda då upphandlingarna är sekretessbelagda och det kan både få både negativ påverkan på upphandlingen och innebära skadestånd om obehöriga har åtkomst till systemet. Vår rekommendation är tydligare struktur på den kontrollen och att göra den mer frekvent.

Postadress: Uppsala kommun, Kommunrevisionen, 753 75 Uppsala
Kommunrevisionens kansli, telefon: 018-727 11 32
E-post: Kommunrevisionen@uppsala.se
www.uppsala.se

Revisionen begär yttrande över revisionens iakttagelser, utifrån frågeställningarna nedan, senast 2019-08-31 till kommunrevisionen@uppsala.se och till det sakkunniga biträdet bo.adel@kpmg.se.

- Med avseende på den genomförda granskningen, vilka åtgärder avser ni att genom-föra i syfte att komma tillrätta med de påtalade bristerna?
- Under vilken tidsperiod avser ni att genomföra dessa åtgärder?
- Hur kommer ni att avläsa effekten av dessa åtgärder?
- Hur kommer dessa åtgärder att påverka innehållet i nästa revision av intern-kontrollplanen?
- Om ni inte anser att revisionens granskning behöver besvaras eller att den har aktuell bäring på ert nuvarande arbete vänligen utveckla skälen till er bedömning.

För kommunrevisionen

Karolina Larfors

Karolina Larfors, ordförande

Granskning av generella IT-kontroller

Rapport

Uppsala kommun

KPMG AB

2019-04-11

Antal sidor 15

Uppsala kommun
Granskning av generella IT-kontroller
Rapport
2019-04-11

Innehållsförteckning

Uppsala kommun
Granskning av generella IT-kontroller
Rapport
2019-04-11

1 Sammanfattning

Uppsala kommun är landets fjärde största kommun. Inom alla områden där kommunen bedriver verksamhet sker en omfattande digitalisering och med digitala beslutsflöden. Det gäller inköp, löner, redovisning, beställningar etc. På de förtroendevalda revisorernas uppdrag har KPMG genomfört en granskning med huvudsaklig inriktning mot behörighetshantering.

Vår bedömning är att kommunens behörighetshantering i stort är ändamålsenlig och att rimliga kontroller finns för de system vi tittat på. Inom vissa områden anser vi att kontrollerna kan och bör förstärkas. Våra rekommendationer:

- För flera av de granskade systemen sker kontroll en gång om året att behörigheter överensstämmer mot vad som är beslutat enligt Iris. Vår rekommendation är att den kontrollen görs mer frekvent.
- Heroma: Löner kan ändras av lönekonsulter och systemförvaltare. Det är upp till cheferna och medarbetarna att hitta eventuella felaktiga löner. Vi bedömer att det kan finnas en risk med att en felaktig lön inte uppmärksammas. Vår rekommendation är att införa en spärr som inte låter en enskild person ändra en lön.
- Agresso, I: Loggen som förs i systemet över ändringar i behörighetsregister kan kopplas bort av systemförvaltarna och IT-objektledarna. Vår rekommendation är att loggfunktionen inte ska kunna slås av.
- Agresso, II: Manuella bokföringsordrar kräver inte attest i systemet. Vi rekommenderar att attestkrav införs för manuella bokföringsordrar, över lämplig beloppsgräns.
- För Kommers är det viktigt att rätt behörigheter är inlagda då upphandlingarna är sekretessbelagda och det kan både få både negativ påverkan på upphandlingen och innebära skadestånd om obehöriga har åtkomst till systemet. Vår rekommendation är tydligare struktur på den kontrollen och att göra den mer frekvent.

2 Bakgrund

Uppsala kommun hanterar årligen ca 450.000 leverantörsfakturor och ca 230.000 lönespecifikationer. Ekonomisystemet Agresso hanterar årligen miljontals transaktioner. IT-relaterade kontroller utgör en kritiskt viktig del av den interna kontrollmiljön. Eventuella brister kan få effekt på hela revisionens omfattning och inriktning. Systemen innehåller i sig automatiserade kontroller och omgärdas av generella IT-kontroller såsom olika nivåer av behörigheter.

Revisorerna har i olika granskningar av IT-miljön de senaste åren identifierat brister i de generella IT-kontrollerna som delvis kvarstått i uppföljande granskningar.

KPMG genomförde 2016 en granskning av IT-processer och generella IT-kontroller i kommunen, med inriktning mot system med stor betydelse för den finansiella rapporteringen. Efter genomförd granskning konstaterade vi att kommunen de senaste åren genomfört omfattande förändringar avseende kommunens IT-styrning där områden som

centralisering, ägarskap och ansvarsfördelning varit centrala frågor. Vår sammanfattande bedömning var att kommunen till stor del lyckats nå avsedda styrningseffekter. Ytterligare utvecklingsarbete bedömdes dock behövas och vi rekommenderade att:

- Styrande IT-dokument vidareutvecklas
- Övergripande organisatorisk IT-riskanalys upprättas
- Klassning av kritiska informationstillgångar och kommunens applikationsportfölj vidareutvecklas
- Periodisk genomgång av samtliga användare i kritiska system vidareutvecklas

Kommunen har ca 14.000 anställda och en kontinuerlig rörlighet på personal.

Granskningen av delårsrapport och årsredovisning utgår till stor del ifrån en bedömning att identifierade automatiserade kontroller fungerar.

Revisorerna har i sin risk- och väsentlighetsanalys för 2018 bedömt att en medelhög risk finns för brister i bland annat behörighetshanteringar i en så stor organisation och att en uppföljning ska göras av den granskning av IT-relaterade kontroller som genomfördes 2016. Uppdraget ingår i revisionsplanen för år 2018.

3 Syfte och granskningsfrågor

Syftet med granskningen har varit att bedöma den interna kontrollmiljön, med särskilt fokus på IT-relaterade kontroller. Eventuella brister i dessa kontroller riskerar att få en negativ inverkan på såväl fullständighet som riktighet i den finansiella rapporteringen.

Granskningen har även haft som syfte att följa upp de rekommendationer som lämnades i granskningen av IT-miljön 2016.

4 Avgränsning

Granskningen har inriktats mot IT-system med väsentlig betydelse för finansiell rapportering och uppföljning;

- Huvudbok, reskontror och anläggningsregister: Agresso
- Manuella bokföringsordrar: Agresso
- Digitala inköpsattester: Agresso
- Beställningar: e-Handel
- Upphandlingar: Kommers
- Avtalsregister: Kommers
- Försystem: Extens (IKE), stöd till enskilda, bidrag (Pro Capita)
- Löner: Heroma
- Behörighetshanteringssystem: Iris

5 Revisionskriterier

Granskningen har utgått ifrån kommunallagens 6 kap 6§ om nämndernas skyldighet att se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

6 Ansvariga nämnder

Granskningen har berört kommunstyrelsen och samtliga nämnder.

7 Metod

Granskningen har genomförs genom:

- Intervjuer med tjänstemän på IT-staben, redovisningschef, IT-objektledarna och systemförvaltare för de system som omfattas av granskningen.
- Inhämtande och analys av relevanta styrdokument
- Genomgång av aktuella digitala behörighetsförteckningar till de olika systemen
- Stickprovsvisa kontroller av registrerade behörigheter i olika system mot beslutade behörigheter
- Specifika stickprovsvisa kontroller att personer med behörighet fortfarande har anställning i kommunen respektive har en sådan befattning som motiverar behörigheten
- Avslutande sammanställning, analys och rapport

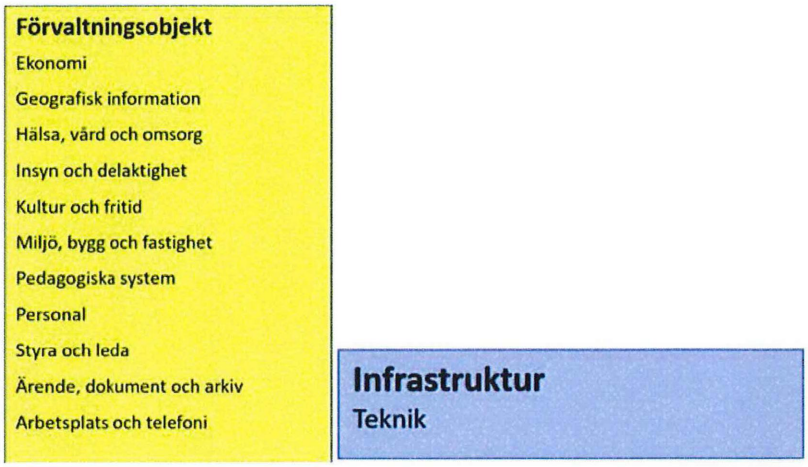
8 Projektorganisation

Granskningen har genomförts under ledning av Bo Ädel, auktoriserad revisor och certifierad kommunal yrkesrevisor.

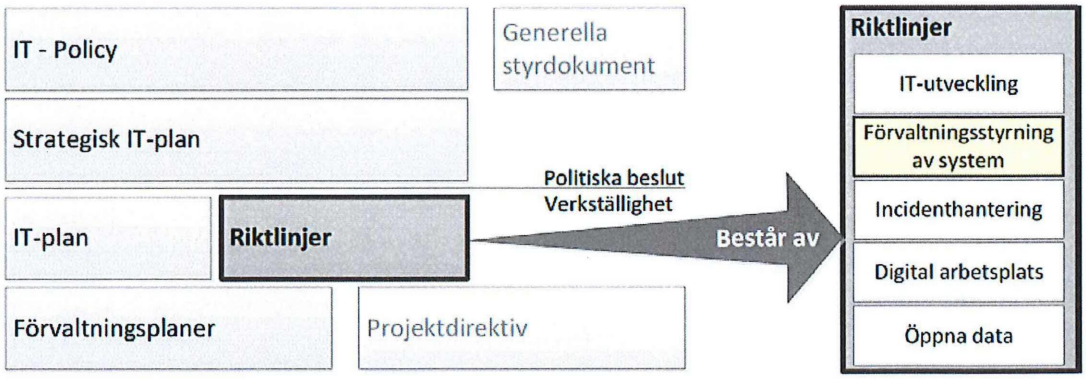
9 Resultatet av granskningen

9.1 IT-organisation och övergripande användarregler

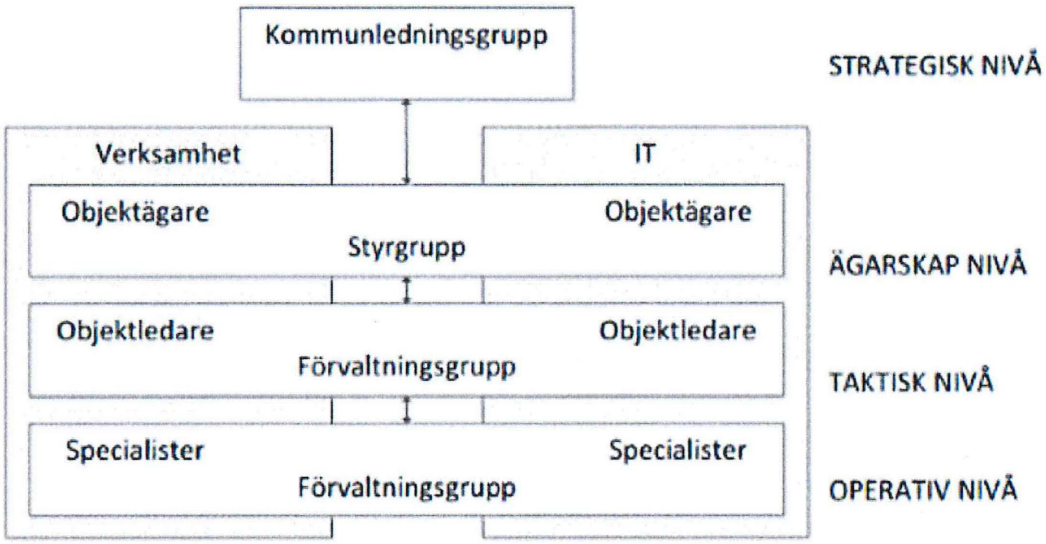
IT i Uppsala kommun är uppdelat i olika förvaltningsobjekt utifrån funktion. Ett förvaltningsobjekt har i detta sammanhang karaktären av ett projekt med organisation, mätbara mål, budget, aktiviteter och förvaltningsplaner.



Fem riktlinjer syftar till en enhetlig och effektiv styrning av IT och digital utveckling.



Ägarskapet för IT är uppbyggt enligt bilden nedan, som visar beslutsnivåer för förvaltningsorganisationerna. Varje system ingår i ett av elva förvaltningsobjekt som har en objektledare IT och en eller flera objektledare från verksamhetssidan. Objektägarna är ansvariga för de system som ingår i förvaltningsobjektet. I förvaltningsobjekten bedrivs utveckling och underhåll av systemen. IT-objektägare och systemförvaltare ansvarar för att lägga upp behörigheter i olika system när de beslutats i systemet Iris som används för ansökan och godkännande av behörigheter. Det är i allmänhet IT-objektledarna och systemförvaltarna som har fulla behörigheter för systemen vilket krävs för bland annat utveckling och underhåll. Kommunen har både egenutvecklade system och system för vilka licens upphandlats.



Det finns strikta regler för hur internet, social medier, e-post och tjänstetelefoner får användas inom kommunen som medarbetarna kan se via dokument på insidan. Inloggning på insidan sker med det användarnamn och lösenord som finns i kommunens *Active Directory*. Ibland används tvåfaktorsautentisering genom engångs-sms. Lösenordet behöver ändras var 90:e dag. När man ansöker om ett konto för en nyanställd följer behörighet till Insidan och nätverket med.

Den totala IT-budgeten; systemkostnad, kostnad för förvaltning, drift m m, fördelas till alla förvaltningar. En mindre del är anslagsfinansierad. Införandet av ett nytt IT-system ska alltid hanteras via ett förvaltningsobjekt. En verksamhet kan i princip aldrig köpa in och införa ett eget system.

9.2 IT-system i kommunen

Uppsala kommun använder cirka 380 olika system och applikationer. I den interna portalen Insidan kan man via en systemöversikt se de olika systemen och läsa om dem. Det finns ett flertal parametrar exempelvis ”antal användare” och ”syfte” där man kan se hur många som använder systemen och vad de används till (se bild nedan). I denna fördjupningsgranskning har sju stora system valts ut som kan påverka ekonomiska transaktioner eller av annat skäl bedömts att större vikt att granska och är utskrivna nedan i rapporten.

Systemöversikt Uppsala kommun

Sök system

System | Funktion --Samtliga--
Används av --Samtliga--
Förvaltningsobjekt --Samtliga-- | Systemtyp --Samtliga--
Visa | Rensa fält | Excelvy

Antal träffar 381

ID	Systemnam
1158	2c8
1560	AARO
1555	Actiway
1234	AD Active Directory Skolnet
1303	AD Active Directory UPPSALA
1274	ADDIS Ung-net
1121	Adobe Connect Pro
176	Agresso (UBW)
1161	AGS
1185	Aktivitetsstöd

1 2 3 4 5 6 7

Gemensamt för systemen är att de behörigheter som krävs ansöks och attesteras via systemet Iris. I Iris är ansöker medarbetare om behörigheter och chef som är ansvarig för det området attesterar och antingen godkänner eller avvisar, se utförligare beskrivning längre ner i rapporten. Årsvisa kontroller görs mellan Iris och de flesta system där jämförelser görs mellan vilka behörigheter som godkänts i Iris och de behörigheter som registrerats i systemen. Ansvaret ligger på cheferna att rätt behörigheter för medarbetarna är upplagda i systemen. Se dokumentation av årsvis kontroll på bilden nedan. Genomgångarna av systemen görs nödvändigtvis inte samtidigt men åtminstone en gång per år. Samtliga personer inlagda i systemen granskas. Systemförvaltarna kan exempelvis få ut en excelfil från Iris och en från systemet där de sedan jämförs.

Uppsala kommun

Granskning av användare

7.5 Periodisk granskning användare

Genomgång av periodisk granskning användare enligt rutin (att detta är utfört för IT-system).
Periodisk granskning av användare för Procapita skedde tidigare 1 ggr/år enligt rutin: **Granskning av behörigheter i kommungemensamma system inom systemförv.docx.**

Ansvaret ligger numera på verksamhetschefer att se till och avsluta behörigheter när personal slutar.

Datum/referens	Utförd för System	Status
	Chefer i verksamheten ansvarar för att avbeställa behörighet i Iris om behörigheten inte ska vara kvar. Användare som inte varit inloggade på 6 månader avslutats (endast KIR och biståndshandläggare som använder Procapita). Verksamheten brukar själva avbeställa behörigheter i Iris där användare avslutat sin anställning i förtid.	

9.3 Stickprov och uppföljning

Vid genomförda intervjuer har stickprov gjorts utifrån behörigheter inlagda i respektive system i jämförelse med vad som godkänts enligt Iris. Vi har även kontrollerat behörigheter för personer som blivit borttagna ur systemet och Iris (personer som t ex slutat sin anställning i kommunen) och jämfört att det skett och inom rimlig tid.

Totalt har tio stickprov tagits där jämförelse gjorts mellan i Iris beslutade behörigheter och de behörigheter som lagts upp i ett system (varav minst ett stickprov per system). Samtliga stickprov visade överensstämmelse mellan Iris och system.

Vi har även tagit tio stickprov över personer som fått behörigheter borttagna från Iris där vi granskat att borttagande av behörigheter från systemen skett inom rimlig tid. Samtliga behörigheter hade blivit borttagna från systemen inom rimlig tid.

För Agresso har stickprov genomförts på större inköpsfakturor att de attesterats enligt fastställt attestreglemente och att de personer som attesterat varit behöriga att göra det. Fem fakturor granskades och samtliga hade attesterats av behöriga personer.

9.4 Delegationsbestämmelser och utseende av attestanter

Styrelse och nämnder beslutar om delegationsordningar inom sina verksamheter. Bestämmelser kring delegation finns i kommunallagens 6 kap 33-38 §§. Vissa slag av ärenden får inte delegeras, t ex ärenden som avser verksamhetens mål, inriktning, omfattning eller kvalitet, yttranden och vissa ärenden i myndighetsutövningen.

För de ärenden där delegation är möjlig ges delegation i första hand till förvaltningschefen och enligt 37 § får nämnden även besluta att förvaltningschefen har rätt att ge beslutsrätt åt andra anställda.

Förvaltningschefens beslut att ge andra anställda beslutsrätt dokumenteras i en attestförteckning. Denna upprättas upp till tre gånger per år och undertecknas av förvaltningsdirektör och ekonomichef. Av dokumentet framgår att förvaltningsdirektören delegerar rätt att agera för berörda ansvarskoder, dvs organisatoriska delar inom förvaltningen och vad som förväntas av attestanten.

9.5 Attestreglemente

Gällande attestreglemente fastställdes av kommunfullmäktige 2016-10-03. Reglementet gäller för samtliga ekonomiska transaktioner, inklusive transaktioner för medel som kommunen ålagts eller åtagit sig att förvalta.

Av reglementet framgår vilka roller som finns i attestflödet och den uppgift som följer med respektive roll, t ex att kontrollera leverans och pris. En person sakattesterar och en annan slutattesterar. Den som utför en kontroll ska ha tillräcklig kompetens för uppgiften och en självständig ställning gentemot den kontrollerade. En attestant får aldrig slutattestera en ekonomisk händelse som avser slutattestantens egen användning. Samma regel gäller rörande närstående, person i beroendeställning eller om jäv föreligger. Attesten ska då eskaleras till närmaste chef vilket även gäller så snart osäkerhet föreligger kring vem som ska attestera.

9.6 Systemgenomgång KPMG

9.6.1 Asta

Asta är ett system som används som registreringsunderlag för anställning. Det är användarvänligt och det är tänkt att vara svårare att göra fel än om man fyllt i uppgifterna via papper. Det är som ett förarbete inför inläggningen av uppgifterna i Heroma (se nedan).

Alla anställda kan använda systemet, ingen särskild behörighet krävs. När uppgifterna är ifyllda ska ansvarig chef väljas för attest innan den skickas vidare. Det skickas till chefen för attest innan den är redo. Behörighet för cheferna att attestera ansöks och beslutas om via systemet Iris. Då en person inte blir inskriven som anställd i Asta utan i Heroma bedöms risken för Asta som system relativt lågt. Det fungerar som ett försystem för att underlätta i bland annat Heroma.

Vid KPMGs genomgång valdes en fiktiv person för anställning genom Asta. Den attestbehörige chefen följdes i systemet upp till Stadsdirektörsnivå för att se att behörigheter följt längs organisationsträdet. Kontrollen skedde utan anmärkning.

9.6.2 Heroma

Heroma är det IT-system som används för löne- och personaladministration. I systemet registreras personliga uppgifter, befattning, lön och pensionsavtal m m. Vid nyanställning görs förarbetet i Asta varefter uppgifterna registreras i Heroma. Det varierar men ett snitt är ungefär 19 000 lönespecifikationer per månad.

Alla ändringar som görs i systemet sparas i en logg som inte kan raderas.

Lönekonsulter och systemförvaltare kan registrera och ändra löner direkt i systemet. Ingen extra attest krävs vilket innebär att chefer och medarbetare själva har ansvar för att se till att korrekt lön registreras i systemet.

Ur kontrollsynpunkt innebär det alltid en risk när en registrering av uppgift som underlag för utbetalningar kan ske utan godkännande av annan person, utöver den person som berörs. I en annan kommun upptäcktes under 2018 att en person uppburit lön i 14 år utan att utföra arbete, anställd och löneskatt av en närstående person, anställd i kommunen. I Uppsala kommun ska underlag för utbetalning godkännas av behörig person. Alla löner ska kontrolleras av ansvariga och felaktigheter som upptäcks ska rapporteras och rättas. Utbetalning av lön sker dock oavsett slutligt underlag attesterats eller inte, vår kommentar.

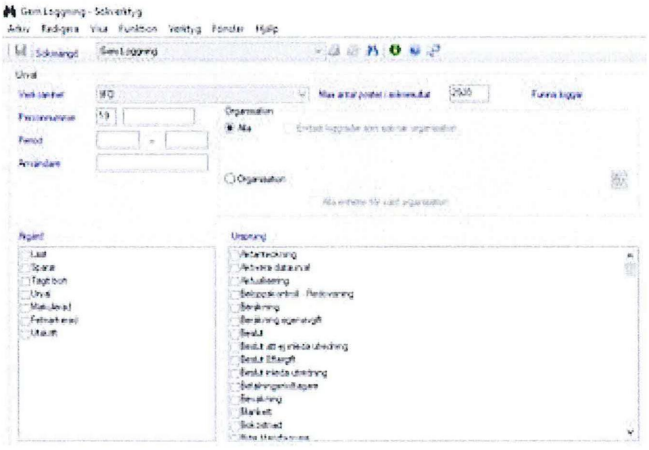
9.6.3 Procapita IFO

Procapita är det verksamhetssystem som används för barn, unga och vuxen inom Individ och familjeomsorg samt försörjningsstöd. Där registreras bland annat beslut angående stöd och utbetalningar. Systemet används av Arbetsmarknadsförvaltningen och Socialförvaltningen. Själva överföringen av utbetalningar sker inte via Procapita och det görs av annan person än den som beslutar om utbetalningen. En och samma person kan inte registrera en utbetalning via Procapita och sedan göra överföringen. Det finns ca 900 aktiva användare (907 vid intervjun).

Behörigheter går genom Iris där de ansöks om och beslutas. Systemförvaltarna går dagligen igenom Iris efter åtgärder att utföra som att lägga till eller ta bort behörigheter. Systemförvaltarna kan lägga till alla behörigheter i programmet till alla personer förutom sig själva. Enligt nedskriven rutin granskar man användare i systemet 1ggr/år. Genomgången görs genom Iris där man kontrollerar godkända behörigheter och sedan stämmer av mot vad som ligger registrerat i Procapita. I anslutning till det görs de korrigeringar och uppdateringar som föranleds av kontrollen.

Kontrollerna sker med utgångspunkt från vad som registrerats i Iris och jämförs med samtliga användare i Procapita. Skulle det finnas användare som är registrerade (tex annan roll) i Procapita men ej i IRIS avslutas/ändras dessa.

I Procapita kan man ta fram loggar på läst, sparat, tagit bort, urval, makulerad, felmarkerad samt utskrift. Man kan även göra urval och titta på specifik användare eller klient samt välja tidsperiod. Bockar man inte i något fält får man alla loggar för de enheter man har behörighet att titta på. Verksamheten gör idag sina egna loggkontroller, behörigheten för dessa beställs via IRIS och man får endast behörighet till beställda enheter (organisation). Se bifogat skärmklipp nedan.



9.6.4 Iris

Iris är ett egenutvecklat system av kommunen som ersatte PDB (Persondatabasen) för fyra år sedan. Iris har uppgifter om all personal och alla bolag inom kommunen. I uppgifterna ingår förutom de personliga uppgifterna även vilka olika behörigheter och roller respektive person har inom kommunen. Det är även i Iris behörigheter och roller ansöks och beslutas om. Alla behörigheter i samtliga system i kommunen ansöks och godkänns via Iris. Därifrån sker för vissa system digital överföring medan för de flesta system systemförvaltarna för respektive system lägger upp behörigheterna manuellt.

Kontroller som görs är en årlig genomgång att de behörigheter och roller som finns i Iris stämmer med respektive system. Grundkravet är årligen, systemansvariga kan införa strängare krav. Varje chef kontrollerar registrerade uppgifter för sina medarbetare. För att underlätta kontrollen kan utskrift göras av lista från Iris eller som excel-format. Kontrollen utförs med andra ord inte av Iris-administratörer utan av respektive chef, som har ansvaret för att alla medarbetarna har rätt behörighet till rätt system. Efter genomförd

kontroll ska chefen bekräfta i Iris att den utförts. HR-avdelningen kontrollerar även årligen att cheferna har sett över behörigheterna. Det är även HR-avdelningen som skickar ut mail och påminner om att det är dags för den årliga kontrollen. HR-avdelningens kontroller i sig dokumenteras inte i Iris.

Även behörigheterna för Iris kontrolleras, och på likande sätt. Alla anställda och externa användare med åtkomst till Insidan har även access till Iris.

Kontroller som utförs i Iris sker på samma sätt. Kontroll sker då av behörigheterna för systemet Iris, t ex de personer som är upplagda att ha extra behörigheter (alla anställda och externa användare som kommer åt insidan kommer även åt Iris). Den kontrollen sker minst en gång om året. Utöver det görs extra kontroller på vissa system för behörigheter som bedöms extra viktiga exempelvis ersättare för attestanter, granskare och HR-behörigheter. Det är systemförvaltarna för Iris som utför de kontrollerna.

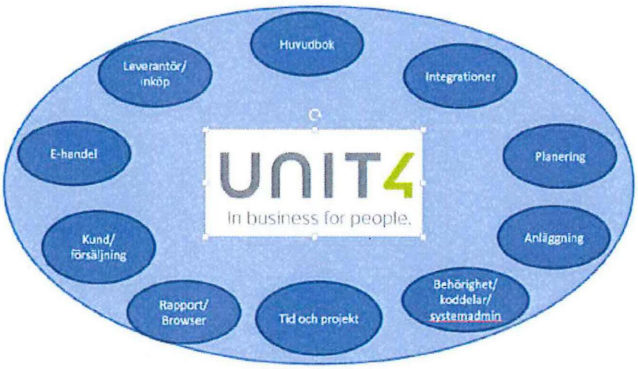
När en anställning upphör försvinner personens AD-konto (tillgång till Insidan). Varje natt skickas en fil från Heroma till Iris angående avslut och nyanställningar m m. Utan åtkomst till Insidan finns inte heller åtkomst till kommunens system. Den risk som kan finnas är det öppna fönster som skulle kunna bli om det är några dagars fördröjning mellan anställningens avslut och behörigheternas borttagande ur systemen.

Ansökan om behörighet i Iris kan göras av personen själv eller av annan person. Alla ansökningar och ändringar loggas och av loggen framgår vem som ansökt om vad och vem som attesterat m m. Loggningen kan inte raderas. Ingen kan attestera om sin egen behörighet, inte ens systemförvaltarna eller utvecklarna som i övrigt har full behörighet.

När en person ansökt om en behörighet går den vidare till chef för det ansvarsområdet för attest. Det går att välja ”fel attestant” och då kan man välja mellan andra attestanter (andra chefer). I de flesta fall är det närmaste chef som väljs i Iris. Om annan attestant väljs går ansökan initialt till systemförvaltarna för Iris som gör en rimlighetsbedömning angående den valda attestanten för den attesten.

9.6.5 Agresso

Agresso är kommunens stora ekonomisystem. Det är uppbyggt av moduler såsom huvudbok, redovisning, kundreskontra, försäljning, fakturering och anläggningsmodul. För användaren blir Agresso ett nav. Agresso finns både via webb och klient. I Agresso har 2 351 personer behörighet (uttag 20190314). Det finns 15 stycken som har systembehörighet och kan tilldela behörigheter. De kan även registrera bokföringsordrar. Det är 107 personer som har behörighet att registrera manuella bokföringsordrar. Det är inga begränsningar på belopp. Det är datakontroll på nämnd. Användarna kan endast registrera en order på sin egen nämnd. Vissa konton är även enbart knutna till vissa ansvar.



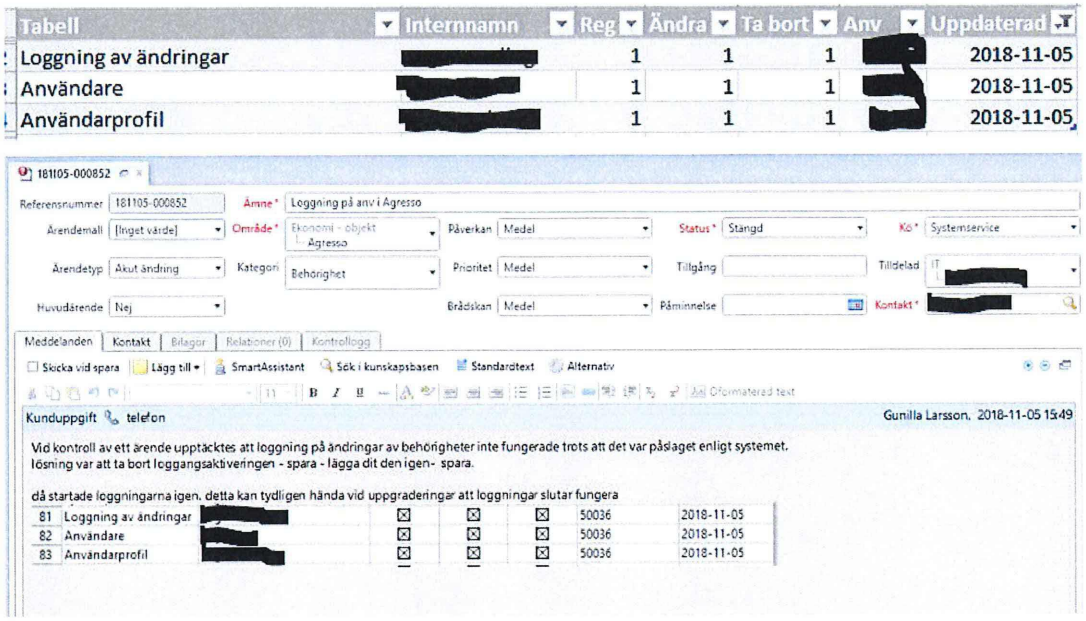
Översiktsbild på UWB – Agresso

Dessa moduler/processer använder Uppsala kommun i systemet.

Behörigheter till Agresso ansöks och godkänns via Iris. Ansvariga attesterar ansökan, därefter lägger systemförvaltarna upp behörigheterna i systemet. Vissa behörigheter har kurskrav. De flesta personerna i systemet är granskare och attestanter. Systemförvaltare och vissa högre ekonomer är s k superusers. Loggning sker av registerförändringar rörande behörigheter. Dessa loggningar kan inte raderas men funktionen loggning kan slås av. Av loggen framgår då vem som slagit av den men inte vad som gjorts under den tid den inte varit igång. Vid olika uppdateringar av systemet krävs en omstart vilket slår av loggen tillfälligt. Generellt ska den utvalda loggning som kommunen beslutat gälla och inte ändras. Under 2018 gjordes en ändring på loggning enligt ett ärende. I det fallet behövdes loggningen startas om. Se bilder nedan.

När systemet används, t ex vid registrering av bokföringsordrar, attest av faktura eller makulering av faktura sker en loggning som inte kan frånkopplas.

Manuella bokföringsordrar kräver inte attest i systemet. Vi rekommenderar att attestkrav införs för manuella bokföringsordrar, över lämplig beloppsgräns.



Tabell	Internnamn	Reg	Ändra	Ta bort	Anv	Uppdaterad
Loggning av ändringar	[redacted]	1	1	1	[redacted]	2018-11-05
Användare	[redacted]	1	1	1	[redacted]	2018-11-05
Användarprofil	[redacted]	1	1	1	[redacted]	2018-11-05

181105-000852

Referensnummer: 181105-000852 | Ämne*: Loggning på anv i Agresso
Ärendemall: [Inget värde] | Område*: Ekonomi - objekt, Agresso | Påverkan: Medel | Status*: Stängd | Kö*: Systemservice
Ärendetyp: Akut ändring | Kategori: Behörighet | Prioritet: Medel | Tillgång: | Tilldelad: IT [redacted]
Huvudärende: Nej | Brådskan: Medel | Påminnelse: | Kontakt*: [redacted]

Meddelanden | Kontakt | Bilagor | Relationer (0) | Kontrollogg

Skicka vid spara | Lägg till | SmartAssistant | Sök i kunskapsbasen | Standardtext | Alternativ

Kunduppgift telefon — Gunilla Larsson, 2018-11-05 15:49

Vid kontroll av ett ärende upptäcktes att loggning på ändringar av behörigheter inte fungerade trots att det var påslaget enligt systemet.
lösning var att ta bort loggangsaktiveringen - spara - lägga dit den igen- spara.

då startade loggningarna igen. detta kan tydligen hända vid uppgraderingar att loggningar slutar fungera

81	Loggning av ändringar	[redacted]	☒	☒	☒	50036	2018-11-05
82	Användare		☒	☒	☒	50036	2018-11-05
83	Användarprofil		☒	☒	☒	50036	2018-11-05

Årsvis görs kontroller av vilka roller som ligger i systemet och jämförs mot Iris. Rent praktiskt sker kontrollen genom att listor från de båda systemen jämförs mot varandra.

Det finns två roller i systemet som inte får kombineras: att vara attestant och kunna göra kontroll på fakturor med större belopp (fakturor överstigande 200 000 kronor går efter attesten vidare till ytterligare en kontroll). Kontroll görs årligen att det inte finns personer som har bägge behörigheterna.

Attester för fakturor kräver åtminstone två i förening, en person som sakgranskar och en som attesterar. För större fakturor överstigande 200 000 kronor är det minst tre då dessa går till en ytterligare kontroll. I attestflödet framgår vilken typ av attest olika personer gjort, exempelvis den extra kontrollen för fakturor med stora belopp.

Kommuninterna debiteringar har egna verifikationstypertyper. Attest krävs vid registrering av en kundorder på webben. Vid inläsning från ett försystem eller manuell registrering krävs attest på kostnaden, inte på intäkt.

9.6.6 E-butiken

Det krävs inga behörigheter för att komma åt E-butiken; alla som har tillgång till insidan kommer åt den. Uppsala Kommun har ett centrallager för IT-artiklar. Beställningar från E-butiken går mot centrallagret. När en beställning är skickad går den till chef för attest. Om chefen nekar attesten avbryts beställningen, alternativt återsänds artiklarna. Namnet på den som gjort beställningen framgår och sparas. Därefter anges hur artiklarna ska levereras. Personen på ett ärende kan bli fel men av beställningsformuläret framgår vem som varit inloggad inom Uppsala domän och gjort beställningen.

9.6.7 Kommers

Kommers används som ett upphandlingsverktyg, samlar och håller avtalen. Det används både av upphandlingsstaben som verktyg vid upphandling och av övriga medarbetare som ett verktyg för att se aktuella avtal och vilka leverantörer som ska användas. De har 230 aktiva användare. Avtalen kan vara specifika för vissa nämnder/förvaltningar, företag eller för hela kommunen. När medarbetarna loggar in blir deras organisation kodad så att de kommer åt de avtal som just den medarbetaren och nämnden/förvaltningen ska komma åt. Kommers är ett externt system som Uppsala kommun köper licens för att använda. Kommunen kan inte göra större ändringar i systemet och när större ändringar ska göras utförs de av leverantören som kan lägga upp användare och lägga till nya kategorier m m.

En upphandling görs direkt i systemet och när hela processen är klar och avtalet tecknat (se stegen nedan) kommer det upp som ett av avtalen som går att söka bland i Kommers.

Upphandlingsstaben gör alla steg. Varannan vecka sker en genomgång av alla pågående och kommande upphandlingar för att fånga status, eventuella problem etc.

Det finns tre systemförvaltare som lägger in behörigheter och gör kontroller. Alla behörigheter som läggs upp går genom Iris där de först ansöks om och sedan godkänns. Ungefär en gång per kvartal kontrolleras alla konton genom att en lista tas ut och jämförs med vad som står i Iris. Detta kan enligt systemförvaltarna själva struktureras upp bättre då det är viktigt att inte fel behörigheter är upplagda. Upphandlingarna är sekretessbelagda och att fel personer kan se kan innebära skadestånd.

Eftersom det är ett externt system är det inte helt kopplat till AD-kontona (tillgång till insidan) och det går att komma åt inloggningen på Kommers även om AD-kontot är bortkopplat om det görs via deras egen hemsida. Systemförvaltarna går dagligen igenom Iris för att utföra ändringar gällande behörigheter. Fram tills det är gjort kan medarbetarna komma in på Kommers.

9.6.8 Extens

Extens är ett skoladministrativt system som används för grundskola, högskola, gymnasier och SFI. Det är ett externt system för vilket kommunen betalar licens. Systemet har funnits sen 1994 men kommunen byter till systemet IST administration till sommaren. IST administration har samma leverantör som Extens.

Systemet är till för och används främst av skoladministratörer. Elever läggs in i rätt klass, tilldelas aktiviteter och kopplas till lärare. Systemförvaltarna för Extens arbetar bland annat med att lägga upp behörigheter åt skoladministratörer och att skriva in att utbildningar har rätt antal timmar m m.

Inloggning sker via en klient, ett separat program, inte via insidan. Loggning sker till viss del men inte över alla ändringar m m. Med nya systemet IST administration kommer loggningen att bli mer omfattande.

Systemet används även till att beräkna och lämna underlag till Agresso för debitering av s k interkommunala ersättningar mellan kommuner och ersättningar mellan kommuner och friskolor.

Baserat på elevregistreringar i Extens betalade Uppsala kommun för 2018 till andra kommuner och friskolor i andra kommuner 265 mkr avseende 2 241 elever. Kommunen erhöll 179 mkr avseende 1 609 elever från andra kommuner.

9.7 Uppföljning av granskning 2016

Efter den granskning av IT i kommunen vi genomförde 2016 lämnade vi följande rekommendationer:

- Styrande IT-dokument bör vidareutvecklas
- Övergripande organisatorisk IT-riskanalys bör upprättas
- Klassning av kritiska informationstillgångar och kommunens applikationsportfölj bör vidareutvecklas
- Periodisk genomgång av samtliga användare i kritiska system bör vidareutvecklas

Den granskning som nu genomförts har som huvudsakligt syfte haft att bedöma kontrollmiljö, framför allt rörande hantering av behörigheter. Kommunen har sedan dess genomfört ett stort arbete inför införandet av GDPR i maj 2018. Det är vår bedömning att styrande dokument utvecklats och att en ändamålsenlig inventering av system och applikationer. Arbetet inom dessa områden måste dock fortgå löpande, inte minst utifrån den digitalisering som sker inom alla de områden där kommunen bedriver verksamheter.

9.8 Slutsatser och rekommendationer

Våra viktigaste slutsatser och rekommendationer:

- För flera av de granskade systemen sker kontroll en gång om året att behörigheter överensstämmer mot vad som är beslutat enligt Iris. Vår rekommendation är att den kontrollen görs mer frekvent.
- Heroma: Löner kan ändras av lönekonsulter och systemförvaltare. Det är upp till cheferna och medarbetarna att hitta eventuella felaktiga löner. Vi bedömer att det kan finnas en risk med att en felaktig lön inte uppmärksammas. Vår rekommendation är att införa en spärr som inte låter en enskild person ändra en lön.
- Agresso, I: Loggen som förs i systemet över ändringar i behörighetsregister kan kopplas bort av systemförvaltarna och IT-objektledarna. Vår rekommendation är att loggfunktionen inte ska kunna slås av.
- Agresso, II: Manuella bokföringsordrar kräver inte attest i systemet. Vi rekommenderar att attestkrav införs för manuella bokföringsordrar, över lämplig beloppsgräns.

- För Kommers är det viktigt att rätt behörigheter är inlagda då upphandlingarna är sekretessbelagda och det kan både få både negativ påverkan på upphandlingen och innebära skadestånd om obehöriga har åtkomst till systemet. Vår rekommendation är tydligare struktur på den kontrollen och att göra den mer frekvent.

KPMG, dag som ovan

Bo Ädel
Auktoriserad revisor
Certifierad kommunal yrkesrevisor

Detta dokument med bilagor har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.