UPPSALA KOMMUN
REVISORERNA 2017-01-13

Kommunstyrelsen
Kommunfullmäktige – för kännedom

Granskning av IT-processer och generella IT-kontroller

Kommunrevisionen i Uppsala har gett KPMG i uppdrag att granska IT-processer och generella IT-kontroller i kommunen.

Uppsala kommun har de senaste åren genomfört omfattande förändringar avseende kommunens IT-styrning där områden som centralisering, ägarskap och ansvarsfördelning varit centrala frågor. KPMGs sammanfattande bedömning är att Uppsala kommun till stor del lyckats nå önskvärda styrningseffekter. Ytterligare utvecklingsarbete är dock önskvärt. Revisionen rekommenderar 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

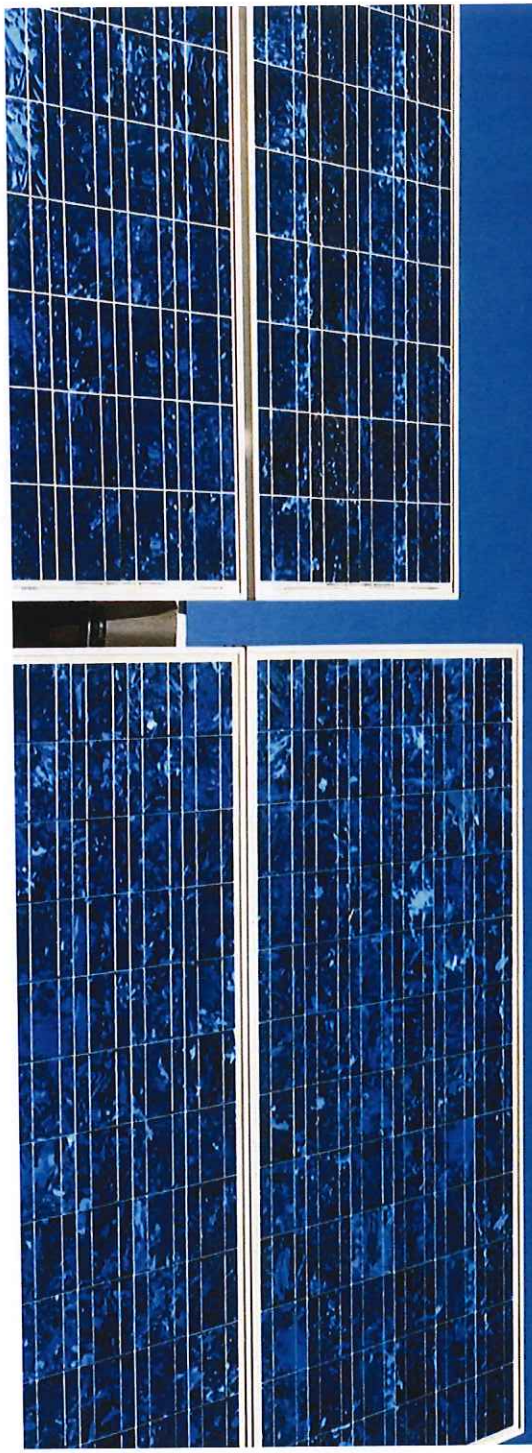
Revisionen rekommenderar vidare att kommunen tar till sig även övriga utvecklingsförslag som lämnas i KPMGs granskningsrapport.

Revisionen begär yttrande över bifogad granskning, senast 31 mars 2017.

För kommunrevisionen

Cecilia Hamenius

ordförande



KPMG

Uppsala kommun

IT-revisionsrapport 2016

2016-12-18

Innehållsförteckning

Kontaktpersoner KPMG:

Isabella Jonsson

IT Advisory, Risk Consulting

Manager

Tel: + 46 70 882 22 03

isabella.jonsson@kpmg.se

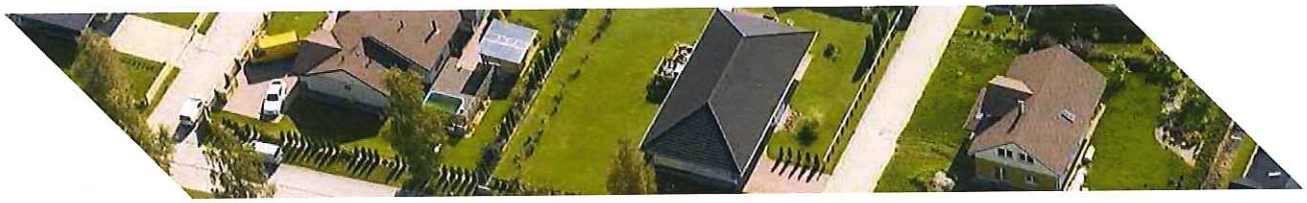
Bo Ädel

Auktoriserad revisor

Tel + 46 70 627 30 99

Bo.adel@kpmg.se

Innehållsförteckning: **Sida:**



Introduktion

Bakgrund

KPMG har inom ramen för årets redovisningsrevision utvärderat Uppsala Kommuns styrande IT-processer samt generella IT-kontroller och IT-relaterade interna kontrollrutiner omfattande processerna för inköp och lön.

Denna rapport syftar till att sammanfatta vår övergripande uppfattning inklusive iakttagelser. Rapporten är vidare utformad för att inkludera rekommendationer som kan bidra till en förbättrad kontrollmiljö och därmed reducera risken för förluster eller fel. Brister inom granskade processer riskerar ha en negativ inverkan på såväl fullständighet som riktighet i den finansiella rapporteringen. Kvaliteten på kontrollmiljön är kommunens ansvar.

Omfattning

Vår granskning har innefattat en översiktlig kartläggning och bedömning inom följande tre områden:

- ❑ **Övergripande organisatorisk IT-mognad:**
  - Utvärdering av organisationens centrala IT-processer, enligt:
    Organisation & ledning, system & tekniskt stöd, lokalisering, styrning & uppföljning, medarbetare & kompetens samt tjänster, funktioner & processer
- ❑ **Intern kontroll inom inköp & lön:**
  - Genomgång av aktuell systemarkitektur för berörda processer
  - Processkartläggning samt utvärdering av kontrollmiljö
- ❑ **Granskning av generella IT-kontroller:**
  - Behörighetsadministration
  - Ändringshantering
  - IT-operationer

Följande funktioner har intervjuats:

- ❑ Enhetschef Skol IT
- ❑ Enhetschef Arbetsplats & telefoni
- ❑ IT-arkitekt
- ❑ IT-koordinator
- ❑ GIS-strateg
- ❑ IT-strateger
- ❑ Ansvariga för upphandling
- ❑ Enhetschef systemförv. Ekonomi, HR & ärenden
- ❑ Enhetschef Redovisning stab ekonomi
- ❑ Strateg, Stab HR
- ❑ Inköpschef stab kvalitet & utveckling

Avgränsningar

I denna granskning omfattas endast de processer, rutiner och kontroller som hanteras av Uppsala kommun. Processer, rutiner och kontroller som utförs av extern leverantör har ej utvärderats.

Sammanfattning

Inledning

Uppsala kommun har sedan 2014/2015 genomgått en omfattande förändringsresa avseende kommunal IT-styrning där områden som centralisering, ägarskap och ansvarsfördelning varit centrala frågor. Vår sammanfattande bedömning är att Uppsala kommun till stor del lyckats nå de önskvärda styrningseffekter och fördelar man eftersökte med detta förändringsarbete, även om organisationen i vissa hänseenden drabbats av växtvärk och inte till fullo hängt med i kontrollmiljön.

Sammanfattning av våra huvudsakliga observationer

- ❑ **Övergripande organisatorisk IT-mognad & intern kontroll:**
  - Styrande IT-dokument bör vidareutvecklas
  - Övergripande organisatorisk IT-riskanalys bör upprättas
  - Verksamhetsstyrning med hjälp av KPI & nyckeltal kan med fördel vidareutvecklas
  - Kompenserande kontroller för löneutbetalningar saknas
  - Klassning av kritiska informationstillgångar samt kommunens applikationsportfölj bör vidareutvecklas
  - Kommunens IT-plan kan med fördel vidareutvecklas
  - Avsaknad av möjlighet till matchning av faktura & avtal

- ❑ **Granskning av generella IT-kontroller:**
  - Periodisk genomgång av samtliga användare i kritiska system bör vidareutvecklas
  - Kommunal processbeskrivning gällande ändringshantering kan med fördel vidareutvecklas
  - Informationssäkerhetspolicy bör uppdateras

Gradering av risk

Utförligare observationer återfinns på följande sidor i denna rapport. Iakttagelserna har graderats i tre nivåer, enligt nedan.

Hög risk – Iakttagelsen kan på kort tid resultera i finansiell eller operationell förlust inom området om den inte åtgärdas.

Medel risk – Iakttagelsen är av återkommande karaktär eller bedöms kunna resultera i finansiella eller operationella förluster om inga åtgärder vidtas.

Låg risk – Iakttagelsen bedöms troligen inte kunna resultera i finansiella eller operationella förluster men kan inrymma möjligheter att förbättra effektivitet och ändamålsenlighet.

KPMG

Detaljerade iakttagelser och rekommendationer

1. Övergripande organisatorisk IT-mognad & intern kontroll (1/3)

Bakgrund

Uppsala Kommun präglas av en centraliserad IT-organisation som kännetecknas av gemensamma IT-processer och ett enhetligt arbetssätt, såväl mot som inom kommunens förvaltningar. Dagens situation är till stor del en konsekvens av det upprensande IT-styrningsarbete som skedde under 2015, då även förvaltningsmodellen PM3 implementerades. Organisationen har med stor framgång nått de effekter man eftersträvade, men kombinationen av ett sedan tidigare vildvuxet IT-landskap samt den snabba styrningsförändringen har även resulterat i framtida förbättringsområden. Inom ramen för årets IT-revision har vi identifierat nedan iakttagelser som mest centrala kopplat till utvärdering av kommunorganisationens IT-mognad samt interna kontrollnivå:

Iakttagelser och identifierade risker	Gradering
1.1 Styrande IT-dokument bör vidareutvecklas ❑ I dagsläget använder kommunen flertalet generella styrdokument (Policy för IT-utveckling och digitalisering, strategisk plan, IT-plan, förvaltningsplaner och riktlinjer) gällande hur IT skall styras och hanteras inom organisationen. Inom ramen för dessa dokument redogörs dock inte för riktlinjer avseende informationsklassificering, lösenordskrav, krypteringsbestämmelser, nedladdningspolicy för internet, hantering av USB-minnen och mobila enheter, virusskydd och skydd mot övrig skadlig mjukvara samt livecykelpolicy för system- och applikationsmjukvara. Ofullständiga styrdokument kan utgöra risk i att kommunens IT-säkerhet inte är tillräcklig för att möta förväntade behov.	◆
1.2 Övergripande organisatorisk IT-riskanalys bör upprättas ❑ Uppsala kommun saknar i dagsläget en övergripande IT-riskanalys som redogör för vilka IT-relaterade risker organisationen är exponerad mot. En sådan riskanalys bör upprättas och omfatta områden såsom leverantörsberoenden, risker kopplat till upphandlingsmål, operativa IT-risker, hantering av tillstånd och övriga regulatoriska regelverk samt informationssäkerhetsrisker. Avsaknad av genomförd IT-riskanalys kan utgöra risk i att verksamheten bedrivs utan rättvisa risk-beaktanden.	◆
1.3 Verksamhetsstyrning med hjälp av KPI & nyckeltal kan med fördel vidareutvecklas ❑ Enligt uppgift tillämpar berörda verksamheter och tillhörande processer inte KPI- och nyckeltalsstyrning i någon större utsträckning. Ett effektivt styrningsarbete med hjälp av KPI och nyckeltal kan reducera risk i att felaktiga beslut fattas samt att kritiska aktiviteter lättare och snabbare synliggörs.	◆
1.4 Kompenserande kontroller för löneutbetalningar saknas ❑ I dagsläget betalas lön ut till månadsanställda oavsett om chef har attesterat löneutbetalningen eller ej. När en anställd vidare avslutar sin anställning är det chefens ansvar att se till att HR samt löneadministrationen nås av denna information. I det fall denna aktivitet blir fördröjd riskerar lön att felaktigt bli utbetald, då uppfångande kompenserande kontroller idag saknas i processflödet.	◆

1. Övergripande organisatorisk IT-mognad & intern kontroll (2/3)

Iakttagelser och identifierade risker	Gradering
1.5 Klassning av kritiska informationstillgångar samt kommunal applikationsportfölj bör vidareutvecklas ❑ Uppsala kommun tillämpar i dagsläget SKLs *KLASSA* som verktyg för klassificering av IT-system med avseende på informationssäkerhet. Denna klassning sker enligt uppgift utifrån en graderingsskala från 1-4 där 1 är allvarlig kritikalitet och 4 är ingen eller försumbar. Denna klassning kan dock med fördel vidareutvecklas för att omfatta samtliga system och applikationer inom den kommunala organisationen, men även för att inkludera information om systemens beroenden och integrationer, vilka regelverk som processad informationen i de berörda systemen träffas av, vilka pågående eller planerade IT-projekt som finns, vem som är system och objektsägare etc. Detta arbete kan vidare med fördel integreras som den del av den kommungemensamma applikationsportfölj som idag är kartlagd igenom flertalet källor som behöver sammankopplas för att få en fullständig bild. Avsaknad av en heltäckande informationsklassningsmodell kan bidra till att det blir svårt att ändamålsenligt övervaka, kontrollera och skydda kritiskt eller känslig information ändamålsenligt.	◆
1.6 Kommunens IT-plan kan med fördel vidareutvecklas ❑ Uppsala kommun använder sig av en kommungemensam IT-plan (roadmap) som omfattar pågående, planerade, nedprioriterade och genomförda projekt eller aktiviteter med ett tydligt IT-beroende. Denna kan med fördel vidareutvecklas för att få en tydligare koppling mot ekonomi, men även vad gäller projektens omfattning, dess ägarskap och eventuella beroenden samt kritiska kopplingar. En icke fullständig IT-aktivitetsplan kan utgöra risk i att samtliga kritiska projektaktiviteter inte beaktas och felaktigt planeras samt estimeras.	◆
1.7 Avsaknad av möjlighet till matchning av faktura & avtal ❑ I dagsläget saknas möjlighet att koppla ihop inköpsfakturor mot underliggande avtal. Detta innebär t ex att man inte kan beräkna avtalstrohet och fullständigt säkert kontrollera att verksamheterna köper korrekt mot avtal. Detta kan utgöra en risk i att kopplingen mot underliggande avtal frångås samt att inköp sker utanför ändamålsenlig rutin.	◆

1. Övergripande organisatorisk IT-mognad & intern kontroll (3/3)

Rekommendationer
Baserat på föregående sidas iakttagelser rekommenderar vi Uppsala kommun att överväga följande åtgärder:

- ❑ Att vidareutveckla de organisatoriskt styrande IT-dokumenten på ett sätt som fortsättningsvis inkluderar de områden som redogörs för under punkt 1.1.
- ❑ Att genomföra en övergripande kommunal IT-riskanalys, där bl a de områden som nämns under punkt 1.2 noggrant beaktas.
- ❑ Att utforma en strategi för hur verksamheterna med fördel kan arbeta effektivare med hjälp av olika KPI och nyckeltal. Inom ramen för detta arbete blir det centralt att inledningsvis börja med att kartlägga kritiska flöden och processer, för att därifrån bestämma vad man skall mäta och utvärdera.
- ❑ Att utforma effektiva kompenserande lönekontroller som täcker upp för chefer i de fall att de blivit släpande i information till HR och lön, avseende avslutade anställningar. Exempel på en sådan kompenserande kontroll skulle kunna vara att frysa löneutbetalning till månadsanställda som inte varit inloggade på sitt AD-konto under de senaste 20 dagarna och som saknar chefs löneattest i samband med månadslöneutbetalning (med eventuella undantag för semestertider).
- ❑ Att vidareutveckla det informationsklassningsarbete som påbörjats för de kommunala systemen. I samband med detta klassningsarbete bör kommunen även inkludera övrig relevant information, i enlighet med punkt 1.5.
- ❑ Att vidareutveckla den kommunala IT-planen (roadmapen) man idag arbetar efter, så att ekonomi får en tydligare koppling samt att övriga relevanta delar enligt punkt 1.6 även inkluderas fortsättningsvis.
- ❑ Att undersökta möjlighet till att systemmässigt skapa en logisk koppling och/eller automatisk kontroll avseende faktura kontra avtal.

2. Granskning av generella IT-kontroller (1/2)

Bakgrund

Vi har granskat generella IT-kontroller för områdena behörighetsadministration, ändringshantering (Change management) samt IT-operationer inom Uppsala kommun och gjort nedan iakttagelser:

Iakttagelser och identifierade risker	Gradering
2.1 Periodisk genomgång av samtliga användare i kritiska system bör vidareutvecklas ❑ Enligt den från 2016 nya styrande rutinen och kontrollbeskrivningen gällande behörighetshantering (*Rutin genomgång av systembehörigheter RU-2049*) skall samtliga användarbehörigheter i verksamheternas kritiska system säkerställas av verksamheterna två gånger årligen, en gång på våren (april-maj) och en på hösten (oktober-november). Under vår granskning har det dock framgått att denna kontroll inte genomförts och/eller återrapporterats för samtliga kritiska system under våren 2016. Detta kan utgöra risk i att felaktiga konton eller behörigheter förblir ohanterade och således möjliggör icke önskvärda aktiviteter i berörda system.	◆
2.2 Kommunal processbeskrivning gällande förändringshantering kan med fördel vidareutvecklas ❑ I dagsläget använder Uppsala kommun sig av ett gemensamt styrdokument för ändringshantering (*Förändringshantering processbeskrivning*). Inom ramen för detta dokument redogörs för hur förändringshanteringsprocessen skall genomföras, från början till slut. Det är dock emellertid vår uppfattning att detta dokument med fördel kan vidareutvecklas, för att tydligare följa den ITIL strategi man avser att arbete efter. Exempel på områden som kan inkluderas och/eller tydliggöras är: inkludering av hur patch management skall hanteras, hur tester och övriga kravställda kontrollaktiviteter i flödet mer konkret skall ske och dokumenteras (inklusive referens till tillämpbara mallar) samt att klassificera ändringar enligt minor och major, i syfte att skapa en tydligare överblick av ändringens omfattning och därtill rättvisande kontroll samt resurskrav. En icke fullständig ändringshanteringsprocess kan innebära risk i att förändringar sker icke ändamålsenligt, vilket i förlängningen riskerar att resultera i kritiska system- och funktionalitetsbrister.	◆
2.3 Informationssäkerhetspolicy bör uppdateras ❑ Aktuell informationssäkerhetspolicy (del av kommunal säkerhetspolicy) för Uppsala kommun är inte uppdaterad sedan 2012. Med bakgrund av den omfattande förändring som skett inom Uppsala kommuns sätt att arbeta med IT samt den påtagliga externa förändring som skett inom informationssäkerhetsområdet anses aktuell informationssäkerhetspolicy inom kommunen inte längre vara välanpassad mot verksamhetens behov och arbetssätt, vilket kan utgöra risk i att informationssäkerhet inte styrs och hanteras ändamålsenligt inom kommunens organisation.	◆

2. Granskning av generella IT-kontroller (2/2)

Rekommendationer
Baserat på föregående sidas iakttagelser rekommenderar vi Uppsala kommun att överväga följande åtgärder:

- ❑ Att snarast möjligt genomföra en periodisk genomgång av samtliga användare i kritiska system, i syfte att säkerställa aktualitet och korrekthet avseende dessa behörigheter.
- ❑ Att se över aktuell ändringshanteringsprocess (Change management) och utvärdera ifall delarna som framgår enligt punkt 2.2 med fördel bör inkluderas.
- ❑ Att snarast möjligt utarbeta och fastställa en ny informationssäkerhetspolicy.

Stockholm 2016-12-18

Isabella Jonsson
Risk consulting manager

Bo Ädel
Kundansvarig

KPMG

kpmg.com/socialmedia

kpmg.com/app

Bilaga till yttranden från kommunala nämnder och bolag till kommunrevisionen i Uppsala kommun

1) Med avseende på den genomförda granskningen vilka åtgärder föreslår ni att genomföra i syfte att komma tillrätta med de påtalade bristerna?
2) Under vilken tidsperiod avser ni att genomföra dessa åtgärder?
3) Hur kommer ni att avläsa effekten av dessa åtgärder?
4) Hur kommer dessa åtgärder att påverka innehållet på nästa revision av internkontrollplanen?
5) Om ni inte anser att revisionens granskning behöver besvaras eller att den har aktuell bäring på ert nuvarande arbete vänligen utveckla nedan skälen till er bedömning