ÖSTERÅKERS KOMMUN
Revisorerna

Kommunstyrelsen
Kommunfullmäktige (för kännedom)

Vi har låtit genomföra en granskning av ekonomisystemet Agresso. Syftet med granskningen är att bedöma om förvaltningen och den interna kontrollen i IT-driften av ekonomisystemet är tillräcklig. Agresso innehåller data som är kritisk avseende tillförlitligheten i kommunens finansiella rapporter (ex. del- och årsbokslut). Granskningen har även syftat till att granska huruvida kommunens finansiella data hanteras på ett ändamålsenligt sätt.

Granskningen visar att även om den interna kontrollen avseende driften av Agresso i många avseenden fungerar väl, noteras två brister som vi avser att följa upp under 2016.

För det första noterades att den periodiska kontrollen av behörighet som genomförs årligen inte bedömer användarnas behörighetsnivå i Agresso. Kontrollen säkerställer att rätt användare är aktiva i applikationen. Vi rekommenderar att Kommunstyrelsen i sin periodiska kontroll, även inkluderar kontroll av att användare har rätt behörighetsnivå i Agresso, det vill säga att användarna har en roll i systemet som är motiverad utifrån dennes arbetsuppgifter. Exempelvis kan listan med användare med tillgång till Agresso skickas ut till berörda (enhets)chefer som får granska behörighetsnivån för sina anställda, i syfte att validera att behörigheter är fullständigt och riktigt tilldelade.

För det andra noterades att den process kommunen har avseende program-förändringar inte innehåller dokumenterade delar avseende; roller, ansvar, krav på test och godkännande. Vi rekommenderar att Kommunstyrelsen säkerställer att en relevant dokumentation kring rutiner för programförändringar (nya versioner) upprättas för Agresso.

Vi önskar återrapportering av planerade åtgärder för att hantera ovanstående brister samt när så avses ske senast den 31 mars 2016.

För Österåkers kommuns revisorer, 2016-01-19

Bengt Olin
Ordförande i kommunrevisionen

Revisionsrapport

IT-revision 2015

Agresso

Österåkers kommun

Utförd av: Johan Berggren och Joakim Hermansson

Kvalitetssäkrare: Fredrik Dreimanis

Januari 2016

Innehållsförteckning

Inledning

På uppdrag av Österåkers kommuns förtroendevalda revisorer har PwC genomfört en IT-granskning av ekonomisystemet Agresso.

Syftet med granskningen är att bedöma förvaltning och intern kontroll för ekonomisystemet. Agresso innehåller data som är kritisk avseende tillförlitligheten i kommunens finansiella rapporter (ex. del- och årsbokslut). Granskningen har även syftat till att granska huruvida kommunens finansiella data hanteras på ett ändamålsenligt sätt.

Granskningen besvarar följande revisionsfrågor:

- Stödjer kommunens hantering av kritiska applikationer kraven enligt ISA 315, avseende internkontroll kopplat till kritiska IT-system?
- Finns ändamålsenliga kontroller avseende programförändringar, behörighetshantering och IT-drift?

Avgränsning och metod

Granskningen avgränsas till att bedöma förvaltningens interna kontroll gällande användningen av Agresso för finansiell rapportering. Granskningsobjekt är Kommunstyrelsen.

Inom ramen för granskningen har intervjuer genomförts med systemförvaltare, redovisningschef, IT-tekniker och IT-chef.

En analys av stödjande dokument har genomförts.

Granskningens omfattning

Granskningen genomfördes under oktober 2015 och har omfattat nedanstående granskningsområden och kontrollmoment.

Granskningsområde	Kontrollmoment
ISA 315 – Förstå och utvärdera informationssystem och indirekta kontroller över IT	- En definierad IT-organisation finns på plats - Styrande dokument (ex. IT-policy etc.) finns på plats - Riskanalyser genomförs gällande driften av kritiska applikationer - Kritiska IT-projekt vilka påverkar applikationsförvaltningen finns tydligt definierade - Formell samlingsplan avseende applikationen finns upprättad - Rutiner och riktlinjer för tredjepartsförvaltning finns definierade - Väsentlig systemdokumentation finns på plats - Interna kontroller finns definierade - Interna kontroller testas regelbundet - Rutiner för backup och avbrottshantering finns definierade
Förändringshantering	- Formell förändringsprocess finns på plats - Förändringar är implementerade fullständigt och riktigt i produktionsmiljön
Åtkomst och behörigheter	- Formell behörighetsprocess finns på plats - Periodisk genomgång av användare och deras respektive behörigheter - Hantering av gruppkonton är begränsad och tydliggjord - Aktivitet av tredjepartsanvändare granskas regelbundet
Loggning och uppföljning	- Loggfunktionalitet finns aktiverad i kritiska applikationer - Regelbundna logguttag och analyser av utförda aktiviteter avseende tredjepartsanvändare genomförs

Granskningen har omfattat behörigheter och förändringshantering för följande applikationer:

Ref. nr.	Applikation
1	Agresso

Sammanfattning

Efter genomförd granskning bedömer vi att Österåkers kommun till stor del har en tydlig hantering gällande ekonomisystemet Agresso, där ändamålsenliga kontroller finns på plats för att säkerställa en god kontroll kopplat till behörighetshantering, programförändringar och IT-drift. Sedan PwC genomförde en granskning avseende behörigheter föregående år har åtgärder genomförts där kommunen under året strukturerat om och begränsat behörigheter samt genomfört en periodisk granskning av användare i ekonomisystemet.

Granskningen har visat på några områden där Österåkers kommun fortfarande har möjlighet att förstärka och förbättra rutiner samt processer för IT i syfte att ytterligare stärka den interna kontrollen.

Vi har noterat att det genomförs en formell årlig kontroll för att bedöma om en användare ska ha behörighet till Agresso eller inte. Kontrollen skulle kunna förstärkas ytterligare genom att kontroll sker av att befintliga användare även har rätt behörighetsnivå i systemet.

Vidare bör kommunen säkerställa att det finns en dokumenterad förändringshanteringsrutin samt att det i den dokumenterade rutinen tydligt framgår vilka roller och ansvar som verksamhetsansvariga respektive IT-enheten har för genomförande av programförändringar.

Resultat av granskning

Baserat på genomförd granskning gjordes två observationer avseende internkontroll kopplat till Agresso. Observationerna har bedömts efter dess väsentlighet. Graderingen definieras nedan:

- **Hög** – En brist med stor påverkan på system, processer eller intern kontroll vilken kan medföra att verksamheten exponeras för betydande förluster eller väsentliga fel i den finansiella rapporteringen.

- **Medium** – En brist med påverkan på system, processer eller intern kontroll som kan medföra att verksamheten exponeras för förluster eller betydande fel i den finansiella rapporteringen.

- **Låg** – En mindre brist eller fel där risken för otillbörlig användning och/eller felaktigheter i bokföringen är lägre, men där det ändå bedöms finnas utrymme för förbättringar.

Ref.	Observation	Prioritet
1.	**Behörighetsnivå granskas inte i samband med genomgång av användare och behörigheter i Agresso.**	Låg
2.	**Avsaknad av dokumenterad process gällande programförändringar.**	Låg

För mer information och detaljer avseende respektive observation se avsnittet ”Observationer och rekommendationer” nedan.

Observationer och rekommendationer

Nedan specificeras respektive observation i detalj med relaterad risk samt vår rekommendation.

Ref.	Observation	Rekommendation
1.	**Behörighetsnivå granskas inte i samband med genomgång av användare och behörigheter i Agresso.** Det noterades att den periodiska granskningen av behörighet som genomförs årligen inte bedömer behörighetsnivå för användare i Agresso. Kontrollen genomförs årligen och säkerställer att rätt användare är aktiva i systemet. **Risk:** Avsaknad av granskning gällande behörighetsnivåer ökar risken för felaktig eller bedräglig åtkomst till kritisk data. Felaktig eller bedräglig åtkomst till kritisk data kan påverka transaktioner eller information vilken är kritisk för den finansiella rapporteringen. **Prioritet:** Låg	Kommunen bör i sin periodiska kontroll, även inkludera kontroll av om användare har rätt behörighetsnivå i Agresso, det vill säga att användarna har rätt roll i systemet utifrån deras arbetsuppgifter. Exempelvis kan listan med användare med tillgång till Agresso skickas ut till berörda (enhets)chefer som får granska behörighet för sina anställda, i syfte att validera att behörigheter är fullständigt och riktigt tilldelade.
2.	**Avsaknad av dokumenterad process för programförändringar.** Det noterades att den process kommunen har avseende programförändringar inte innehåller dokumenterade delar avseende; roller, ansvar, krav på test och godkännande. **Risk:** Avsaknad av tydlig dokumentation avseende programförändringsprocessen ökar risken för minskad spårbarhet gällande implementerade förändringar. Minskad spårbarhet för implementerade förändringar ökar risken för felaktiga förändringar i produktionsmiljön, vilket kan påverka funktionaliteter och data som är kritiska för den finansiella rapporteringen. **Prioritet:** Låg	Kommunen bör säkerställa att dokumentation kring programförändringsrutiner upprättas, samt att den är tydlig och ändamålsenlig i förhållande till hanteringen av Agresso.