Tyresö kommun

Generella IT kontroller – Economa och Heroma

Detaljerade observationer och rekommendationer

Juni 2017

Fredrik Dreimanis
Johan Jelbring
Tina Emami

Innehållsförteckning

Sammanfattning av granskningen

I samband med revisionsplaneringen för Tyresö kommun har en risk- och väsentlighetsanalys genomförts där system samt applikationer kopplat till den finansiella rapporteringen bedömts som kritiska. Baserat på detta har en granskning av applikationerna Economa (bokföringssystem) och Heroma (lönesystem) genomförts. Granskningen har genomförts under april 2017 av Johan Jellbring (PwC) och Tina Emami (PwC) under ledning av Fredrik Dreimanis (PwC). Granskningen har genomförts i syfte att bedöma förvaltning och intern kontroll för dessa applikationer.

Baserat på genomförd granskning bedöms det finnas grundläggande processer och rutiner inom Tyresö kommun gällande förvaltning av kritiska applikationer. Det noterades att det finns rutiner på plats gällande behörigheter och åtkomst till data. Vidare noterades att loggning av kritisk data genomförs, dock finns det ingen formaliserad kontroll och/eller aktiv uppföljning av loggar gällande förändringar.

I samband med granskningen noterades dock att ett antal av de rutiner och processer som finns på plats gällande förvaltningen av dessa system är informella där dokumentationen inte är uppdaterad eller saknas. Totalt noterades sex detaljerade observationer vilka i huvudsak berör roller, ansvar, formalisering och dokumentation. I syfte att förbättra och förstärka den interna kontrollen rekommenderar vi kommunstyrelsen att fokusera på följande områden:

- Dokumentation av väsentliga processer och rutiner för applikationer,
- Rutiner och processer för periodisk uppföljning av användares behörigheter i applikationerna,
- Rutiner och processer för loggning och uppföljning av användare i kritiska system,
- Definiera rutiner för återläsningstest av backup för kritiska system.

För mer information avseende observationer se sektionen ”Detaljerade observationer och rekommendationer”.

Bakgrund och omfattning

I samband med revisionsplaneringen för Tyresö kommun har en risk- och väsentlighetsanalys genomförts där system samt applikationer kopplat till den finansiella rapporteringen bedömts som kritiska. Granskningen tar sin utgångspunkt i SKYREVS´s utkast till vägledning för redovisningsrevision i kommuner och landsting[1]. Baserat på denna analys har applikationerna Economa (bokföringssystem) och Heroma (lönesystem) granskats i syfte att bedöma rutiner avseende förvaltning och intern kontroll. Granskningen har baserats på generella IT-kontroller (ITGC) inom domäner som specificeras i nedanstående tabell.

Granskningen avser perioden 1 januari till 31 mars 2017 för ITGC domänerna i tabellen nedan och följande applikationer:

- Economa (bokföringssystem),
- Heroma (lönesystem).

ITGC Domän	Kontrollområde
IT-styrning/Förvaltning	▪ Policy och styrande dokument, ▪ Roller och ansvar, ▪ Gränssnitt mellan IT och verksamhet, ▪ IT organisation och kontroll över IT, ▪ Förståelse för applikationerna och IT-miljön.
Förändringshantering	▪ Rutin och process gällande förändringar till kritiska applikationer, ▪ Testning av nya förändringar, ▪ Godkännande av förändringar innan produktionssättning.

[1] Vägledningen baseras på ISA, International Standards on Auditing och behandlar ett antal förhållanden som kräver särskilda tillämpningsanvisningar. Syftet är att utveckla god revisionssed för redovisningsrevision i kommunal sektor.

ITGC Domän	Kontrollområde
Åtkomsthantering	▪ Process för uppläggning, ändring och borttagning av behörigheter, ▪ Periodisk granskning av behörigheter, ▪ Hantering av säkerhetsinställningar, ▪ Loggning och översyn av loggar, ▪ Hantering av priviligierade användare.
Datordrift	▪ Backup hantering och återläsning, ▪ Hantering av batch jobb, ▪ Katastrof- och kontinuitetshantering, ▪ Hantering av tredjepartsleverantör.

Granskningen baseras på intervjuer med nyckelpersoner hos Tyresö kommun och granskning av underliggande dokumentation.

Följande personer har varit involverade i granskningen:

- Urban Petrén, IT-chef,
- Magnus Larsson, Driftchef IT,
- Hillevi Hedberg, Ekonomichef för ekonomiservice (Economa),
- Jenny Hesslin, Systemförvaltare ekonomisystem (Economa),
- Marie Friberg, Systemansvarig lönesystem (Heroma),
- Åsa Alvarsjö, Systemförvaltare lönesystem (Heroma).

Vårt arbete har utförts i enlighet med PwC's revisionsmetodik och under april/maj månad i Tyresö kommuns lokaler, Tyresö.

Detaljerade observationer och rekommendationer

Observationerna i denna rapport har graderats efter bedömd väsentlighet, graderingen illustreras med hjälp av definitionerna i nedan tabell. Även om graderingen ofrånkomligen är subjektiv och innehåller inslag av bedömningar och ställningstaganden kan definitionerna vara vägledande.

Hög (H)	*Kritisk, omedelbar åtgärd.* Visar på en brist med stor påverkan på system, processer och eller intern kontroll att det kan medföra att Tyresö kommun exponeras för betydande förluster eller väsentliga fel i den finansiella rapporteringen.
Medium (M)	*Otillräcklig, bör diskuteras av ledningen.* Visar på en brist, som ensam eller i kombination med andra brister kan påverka funktionaliteten/integriteten i system, processer och kontroller samt den finansiella rapporteringen.
Låg (L)	*Mindre avvikelse.* visar en brist som inte har någon väsentlig påverkan på system, processer och kontroller men som indikerar en möjlighet till förbättrad effektivitet och/eller verkningsgrad av processer och kontroller

Tabellen nedan visar en sammanfattning av de observationer som identifierats under årets granskning med relaterad riskgradering baserad på dess väsentlighet.

Ref #	Område	Applikation	Observation	Risknivå
1.	IT-styrning	Economa	Uppdatering av förvaltningsplanen har ej genomförts.	Låg
2.	Åtkomst till program och data	Economa	Avsaknad av rutin för periodisk granskning av användare.	Medium
3.	Datordrift	Economa	Avsaknad av rutin för periodisk granskning av databas användares aktivitet	Hög
4.	Datordrift	Economa	Avsaknad av rutin för återläsningstest	Låg
5.	IT-styrning	Heroma	Uppdatering av förvaltningsplanen har ej genomförts.	Låg
6.	Datordrift	Heroma	Avsaknad av rutin för återläsningstest	Låg

För mer information och detaljer gällande respektive observation se nedan tabell.

	Observation	Risk	Rekommendation
1.	**Uppdatering av förvaltningsplan har ej genomförts.** (L) *(Economa)* Under granskningen noterades att förvaltningsplan, inklusive instruktioner och riktlinjer, för applikationen Economa inte har uppdaterats med information gällande följande områden: ▪ Riskanalys, ▪ Rutiner gällande behörighetshantering, ▪ Loggning och övervakning av transaktioner, ▪ Beskrivning av backuphantering och återläsningstest ▪ Kontinuitet och katastrofhantering Dock noterades att processer avseende förändringshantering finns dokumenterad i förvaltningsplanen.	Avsaknad en uppdaterad förvaltningsdokumentation ökar risken för felaktig hantering av kritiska applikationer. Felaktig hantering av kritiska applikationer kan påverka data som är kritisk för den finansiella rapporteringen.	PwC rekommenderar att Tyresö kommun uppdatera förvaltningsplanen för applikationen Economa. Förvaltningsplanen bör som minimum, men inte begränsat till, innehålla följande: ▪ Riskanalys, ▪ Rutiner för hantering av behörigheter i applikationen, ▪ Instruktion och beskrivning av de loggningar som genomförs i applikationen, ▪ Beskrivning av backuphantering och återläsningstest ▪ Kontinuitet och katastrofhantering. Vidare rekommenderas att en rutin upprättas där förvaltningsplanen revideras årligen inklusive genomgång av riskanalysen. Dokumentationen bör dateras och signeras av ansvarig förvaltningsledare i syfte att skapa spårbarhet i genomförda aktiviteter och stärka den interna kontrollen.
Kommunens kommentar: Tyresö uppdaterar förvaltningsplanen årligen, viss komplettering till förvaltningsplanen finns i systemdokumentationen för Economa RoR.			

	Observation	Risk	Rekommendation
2.	**Avsaknad av rutin för periodisk granskning av användare.** (M) *(Economa)* Under granskningen noterades att ingen formaliserad kontroll finns på plats gällande periodisk granskning av användare i applikationen Economa vilken säkerställer att rätt användare har åtkomst i enlighet med sina arbetsuppgifter. Det noterades att en ad-hoc granskning av behörigheter genomförs årligen, dock utan att dokumenteras.	Avsaknad av periodisk granskning av behörigheter ökar risken för felaktig åtkomst till kritiska applikationer och system. Felaktig åtkomst till applikationer och system ökar risken för felaktig och/eller bedräglig åtkomst till kritisk data vilket kan påverka den finansiella rapporteringen.	PwC rekommenderar att Tyresö kommun implementerar rutiner och processer för att periodisk granska behörigheter i applikationen Economa. Granskningen bör som minimum, men ej begränsat till, omfatta följande; ▪ Arbetar användaren kvar inom Tyresö kommun, ▪ Har användaren åtkomst i enlighet med sin arbetsuppgifter. Tyresö kommun rekommenderas att genomföra granskningen, som minimum, årligen. Vidare bör dokumentationen signeras, dateras och arkiveras i syfte at skapa spårbarhet och stärka den interna kontrollen.
Kommunens kommentar: Den noterade bristen av periodisk granskning av behörigheter har ringa betydelse utifrån en risk- och konsekvensanalys. Den noterade bristen skyddas i sin helhet genom den övergripande behörighetshanteringen för kommunens IT-resurser. När en person avslutar anställningen vid kommunen upphör per automatik samtliga behörigheter till nätverket och dess resurser, behörigheter i Economa/Visma Proceedo är till 100 % integrerade med kommunens övergripande behörighetsstruktur. En till synes kvarvarande behörighet i något av de specifika systemen upphör per automatik att fungera och ge tillgång till system i samband med den automatiska avvecklingen av användarens tillgång till kommunens nätverk och dess resurser. Med en risk och konsekvensanalys är bristen att notera som ringa/mycket låg.			

	Observation	Risk	Rekommendation
3.	**Avsaknad av formaliserad behörighetsprocess gällande användare med direkt åtkomst till databasen. (H)** *(Economa)* Under granskningen noterades att ingen formaliserad process finns på plats gällande hantering av användare med direkt åtkomst till databasen för applikationen Economa. Dock noterades att en genomgång av användare på kommunen IT-driftsavdelning nyligen genomförts ”ad-hoc”, dock utan att dokumenteras.	Avsaknad av kontroller kopplade till använder med direkt åtkomst till databasen ökar risken för felaktig och eller bedräglig åtkomst. Felaktig och/eller bedräglig åtkomst kan påverka data och funktioner som är kritiska för den finansiella rapporteringen.	PwC rekommenderar att Tyresö kommun formaliserar och dokumentera en behörighetshanteringsprocess för användare i kommunens driftsmiljö. Exempelvis kan detta omfatta, men inte begränsas till; ▪ Dokumentation av användare med direkt åtkomst till databaser. ▪ Periodisk granskning av användare, ▪ Rutiner för tilldelning, förändring och borttag Vidare rekommenderas Tyresö kommun att dokumentation upprättas, signeras, dateras och arkiveras i syfte at skapa spårbarhet och stärka den interna kontrollen. .
Kommunens kommentar: Vi håller med i observationen och ska analysera möjligheter för att åtgärda bristen samt hantera risken.			

	Observation	Risk	Rekommendation
4.	**Avsaknad av rutin för återläsningstest.** **(L)** *(Economa)* Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen Economa.	Avsaknad av formaliserad process för återläsningstester av data ökar risken för att data inte kan återläsas i händelse av en incident. Data som ej kan återläsas kan påverka den operativa verksamheten och information som är kritisk för den finansiella rapporteringen.	PwC rekommenderar att Tyresö kommun upprättar dokumentation vid återläsning av data för applikationen Economa. Dokumentationen bör som minimum, men inte begränsat till, omfatta: ▪ När test genomfördes, ▪ Vad som testats, ▪ Resultatet av testet, ▪ Vem som genomfört testet. Återläsning av data bör som minimum genomföras en gång per år och dokumentationen bör arkiveras för att skapa spårbarhet samt stärka den interna kontrollen.
Kommunens kommentar: Vi håller med i observationen och ska analysera möjligheter för att åtgärda bristen samt hantera risken.			

	Observation	Risk	Rekommendation
5.	**Uppdatering av förvaltningsplan har ej genomförts.** (L) *(Heroma)* Under granskningen noterades att förvaltningsplan, inklusive instruktioner och riktlinjer, för applikationen Heroma inte har uppdaterats med information gällande följande områden: ▪ Riskanalys, ▪ Rutiner gällande behörighetshantering, ▪ Loggning och övervakning av transaktioner, ▪ Beskrivning av backuphantering och återläsningstest ▪ Kontinuitet och katastrofhantering Dock noterades att processer avseende förändringshantering finns dokumenterad i förvaltningsplanen.	Avsaknad en uppdaterad förvaltningsdokumentation ökar risken för felaktig hantering av kritiska applikationer. Felaktig hantering av kritiska applikationer kan påverka data som är kritisk för den finansiella rapporteringen.	PwC rekommenderar Tyresö kommun att uppdatera förvaltningsplanen för applikationen Heroma. Förvaltningsplanen bör som minimum, men inte begränsat till, innehålla följande: ▪ Riskanalys, ▪ Rutiner för hantering av behörigheter i applikationen, ▪ Instruktion och beskrivning av de loggningar som genomförs i applikationen, ▪ Beskrivning av backuphantering, återläsningstest ▪ Kontinuitet och katastrofhantering. Vidare rekommenderas att en rutin upprättas där förvaltningsplanen revideras årligen inklusive genomgång av riskanalysen. Dokumentationen bör dateras och signeras av ansvarig förvaltningsledare i syfte att skapa spårbarhet i genomförda aktiviteter och stärka den interna kontrollen.
Kommunens kommentar: Rutiner gällande behörighetshantering kommer att läggas in i den systemförvaltarplan som nu görs för 2018. Övriga punkter ses över tillsammans med leverantör och kommunens IT-avdelning**.**			

	Observation	Risk	Rekommendation
6.	**Avsaknad av rutin för återläsningstest.** **(L)** *(Heroma)* Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen Heroma. Dock noterades att återläsningstest sker vid återlagring av testmiljö samt är schemalagt för Tyresö kommun månadsvis av leverantören CGI.	Avsaknad av formaliserad process för återläsningstester av data ökar risken för att data inte kan återläsas i händelse av en incident. Data som ej kan återläsas kan påverka den operativa verksamheten och information som är kritisk för den finansiella rapporteringen.	PwC rekommenderar att Tyresö kommun upprättar dokumentation vid återläsning av data för applikationen Heroma. Dokumentationen bör som minimum, men inte begränsat till, omfatta: ▪ När test genomfördes, ▪ Vad som testats, ▪ Resultatet av testet, ▪ Vem som genomfört testet. Återläsning av data bör som minimum genomföras en gång per år och dokumentationen bör arkiveras för att skapa spårbarhet samt stärka den interna kontrollen.
Kommunens kommentar: Dokumenterad rutin kommer ses över tillsammans med leverantören.			

2017-06-28

Fredrik Dreimanis	***Carin Hultgren***
Projektledare	*Uppdragsledare*