Region Gävleborg

Granskning av den generella IT-säkerheten i regionens redovisningssystem

Detaljerade observationer och rekommendationer

November 2019

Johan Jelbring
Emma Axelsson
Cecilia Axelsson

Innehållsförteckning

Sammanfattning av granskningen

I samband med revisionsplaneringen för Region Gävleborg 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 applikationen Agresso (ekonomisystem) genomförts. Granskningen har genomförts under oktober och november 2019. Syftet med granskningen är att bedöma förvaltning och intern kontroll för ekonomisystemet, vilken innehåller data som är kritiska för den finansiella informationen genom att besvara revisionsfrågan; Har Regionstyrelsen säkerställt att förvaltningen av kritiska applikationer stödjer kraven enligt ISA 315?

Revisorerna gör sin bedömning utifrån skalan ”ej uppfyllt”, ”i begränsad utsträckning”, ”till övervägande del” eller ”helt uppfyllt.

Baserat på genomförd granskning bedöms Regionstyrelsen **till övervägande del** ha grundläggande processer och rutiner på plats gällande förvaltning av Agresso för att stötta kraven i ISA315. Exempelvis finns det rutiner på plats för förändringar av applikationen samt en CMDB[1] på plats vilket gör det möjligt för användare att identifiera beroenden mellan processer, människor, applikationer och IT-infrastruktur för att hitta möjligheter till förändring och lösning till incidenter. Vidare finns det tydliga direktiv och riktlinjer för hanteringen av IT samt en klar och utarbetat rollstruktur på plats inom IT-organisationen.

I samband med granskningen noterades dock ett antal områden där Regionstyrelsen har möjlighet att förbättra och förstärka den interna kontrollen. I huvudsak berör våra observationer processer, rutiner och kontroller kopplade till hanteringen användare och behörigheter i Agresso. Baserat på granskningen noterades totalt fem observationer. Vi rekommenderar att Regionstyrelsen i första hand bör fokusera på följande områden:

- Avsaknad av rutin för periodisk granskning av användare,
- Avsaknad av granskning av priviligierade användares aktivitet.

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

[1] CMDB står för Configuration Management DataBase vilket är ett verktyg som hjälper en organisation att förstå förhållandet mellan komponenterna i ett system och att spåra deras konfigurationer

Bakgrund och omfattning

I samband med revisionsplaneringen för Region Gävleborg har en risk- och väsentlighetsanalys genomförts där system samt applikationer kopplat till den finansiella rapporteringen bedömts som kritiska.

Regionen har i sin verksamhet ett stort beroende av sina IT-system, vilket i sig kan medföra risker. Redovisningssystemet (Agresso) är komplext med många systembaserade försystem. Det sker en mängd olika filöverföringar från försystem till redovisningssystemet som sker automatiskt utifrån tidsschema. Flera av försystemen har en väsentlig inverkan på redovisningen. Om en filöverföring inte fungerar som tänkt kan det skapa stora fel i redovisningen. Eller om användare med felaktiga behörigheter vidtar felaktiga åtgärder kan det också skapa stora fel i redovisningen. Vidare kan det få förödande konsekvenser om systemet kraschar och rutinerna för säkerhetskopiering är bristfälliga.

Syftet med granskningen är att bedöma förvaltning och intern kontroll för ekonomisystemet, vilken innehåller data som är kritiska för den finansiella informationen. Granskningen syftar även till att säkerställa att data hanteras fullständigt och riktigt.

Granskningen tar sin utgångspunkt i SKYREVS´s utkast till vägledning för redovisningsrevision i kommuner och landsting[2].

Revisionsfråga

Har Regionstyrelsen säkerställt att förvaltningen av kritiska applikationer stödjer kraven enligt ISA 315?

Omfattning

Revisionskriterier utgörs av lagar, föreskrifter, regelverk, fullmäktigebeslut etc. och utgör underlag till de bedömningsgrunder som uttrycks i kontrollområdena.

- Kommunallag
- Lagen om kommunal bokföring och redovisning
- Redovisningsrekommendationer
- Interna styrande och stödjande dokument

Granskningen kommer att bedömas utifrån följande uppställda kontrollområden:

- Indirekta kontroller
- Förändringshantering
- Åtkomst och behörigheter
- Loggning och uppföljning

[2] 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.

Avgränsning

Granskningen omfattar ekonomisystemet. Granskningsobjekt är regionstyrelsen. Granskningen avser perioden 1 januari till 31 oktober 2019 och avgränsas till att omfatta kontrollmålen enligt ISA 315[3] för domänerna i tabellen nedan:

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.
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 batchjobb, ▪ Katastrof- och kontinuitetshantering,

Metod

Granskningen genomförs genom:

- Inledande kartläggning och genomgång av interna och externa regelverk, dvs de styrande och stödjande dokument som finns för förvaltningen av applikationerna.
- Intervjuer med ansvariga nyckelpersoner inom IT (chefer för IT-förvaltning, IT-system, IT-infrastruktur, serverdrift mm), objektsförvaltare av Agresso samt chef på Ekonomiservice.
- Begränsade tester av dokumentation och underlag.

Vårt arbete har utförts i enlighet med PwC's revisionsmetodik och under oktober månad i Region Gävleborgs lokaler, *Gävle*.

---

[3]ISA 315 behandlar revisorns ansvar för att identifiera och bedöma riskerna för väsentliga felaktigheter genom att förstå företaget och dess miljö. Här ingår företagets interna kontroll.

Detaljerade observationer och rekommendationer

Observationerna i denna rapport har graderats efter bedömd väsentlighet, graderingen illustreras med hjälp av definitionerna i tabellen nedan. 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 Region Gävleborg 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 granskningen med relaterad riskgradering baserad på dess väsentlighet.

Ref #	Område	Observation	Risknivå
1.	IT-styrning/Förvaltning	Avsaknad av uppdaterade och antagna förvaltningsdokument.	Låg
2.	Åtkomsthantering	Avsaknad av rutin för periodisk granskning av användare.	Medium
3.	Åtkomsthantering	Avsaknad av granskning av priviligierade användares aktivitet.	Medium
4.	Datordrift	Avsaknad av rutin för återläsningstest.	Låg
5.	Datordrift	Avsaknad av larmfunktion för automatiska batchjobb.	Låg

För mer information och detaljer gällande respektive observation se tabell på nästkommande sida.

	Observation	Risk	Rekommendation
1.	**Avsaknad av uppdaterade och antagna förvaltningsdokument. (L)** Under granskningen noterades att dokumentation gällande förändringshantering samt kontinuitet och katastrofhantering ej finns uppdaterade och formellt antagna. Dock noterades det att Regionstyrelsen arbetar med att definiera och implementera formell dokumentation av ovan nämnda områden.	Avsaknad av en uppdaterad förvaltningsdokumentation ökar risken för att kritiska applikationer inte hanteras i enlighet med verksamhetens krav. Kritiska applikationer som inte hanteras i enlighet med verksamhetens krav kan påverka kritisk data och tillgänglighet för verksamheten.	PwC rekommenderar att Regionstyrelsen fortsätter arbetet med förvaltningsdokumentationen för applikationen Agresso. Förvaltningsdokumentationen bör som minimum, men inte begränsat till, innehålla följande: ▪ Riskanalys, ▪ Definition av roller och ansvar kopplat till förvaltningen av applikationen, ▪ Rutiner för uppdatering och förändring av applikationen, ▪ Rutiner för hantering av behörigheter i applikationen, ▪ Instruktion och beskrivning av de loggningar som genomförs i applikationen, ▪ Beskrivning av backuphantering, ▪ Kontinuitet och katastrofhantering. Vidare rekommenderas att en rutin upprättas där förvaltningsdokumentationen 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.

	Observation	Risk	Rekommendation
2.	**Avsaknad av rutin för periodisk granskning av användare. (M)** Under granskningen noterades att ingen formaliserad kontroll finns på plats gällande periodisk granskning av användare i applikationen Agresso. Dock noterades det att det finns en tydlig rutin för tilldelning och borttag av användare.	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 Regionstyrelsen implementerar en rutin där användare i applikationen Agresso granskas regelbundet. Granskningen bör, som minimum, genomföras en gång per år och säkerställa att användare har behörighet till systemet i enlighet med sina arbetsuppgifter. Underlag och dokumentation av granskningen bör arkiveras och signeras i syfte att skapa spårbarhet av genomförd kontroll och stärka den interna kontrollen.
3.	**Avsaknad av granskning av priviligierade användares aktivitet. (M)** I samband med granskningen noterades att ingen formell process finns på plats för uppföljning och/eller övervakning av aktivitet som är utförd av användare med priviligierade åtkomst (dvs. hög behörighet) i applikationen Agresso. Dock noterades att loggning är aktiverad i systemet (dvs. spårbarhet i transaktioner finns på plats). Uppföljning sker vid incidenter, dock sker ingen aktiv uppföljning.	Avsaknad av processer och rutiner för uppföljning av priviligierade användares aktivitet ökar risken för felaktig och/eller bedrägliga transaktioner. Felaktiga och/eller bedrägliga transaktioner kan påverka data och funktioner som är kritiska för den finansiella rapporteringen.	PwC rekommenderar att Regionstyrelsen implementerar processer och rutiner för uppföljning av priviligierade användares aktivitet i syfte att validera fullständighet och riktighet i transaktioner och förändringar. Exempelvis kan en riskanalys genomföras av kritisk data i applikationen, loggfunktioner aktiveras för övervakning av data och en rutin implementeras där en användare periodiskt granskar dessa loggar. Användare bör inte ha åtkomst till applikationen och/eller högre behörighet i syfte att säkerställa oberoende granskning av förändringar till kritisk data. Underlag och dokumentation från genomförd uppföljning eller granskning bör arkiveras i syfte at skapa spårbarhet i genomförd kontroll och stärka den interna kontrollen.

	Observation	Risk	Rekommendation
4.	**Avsaknad av rutin för återläsningstest.** (L) Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen Agresso. Dock noterades det att återläsning görs ad hoc vid skapandet av en ny testmiljö för applikationen.	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 Regionstyrelsen upprättar en process för genomförande och dokumentation av återläsning av data för applikationen Agresso. 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.
5.	**Avsaknad av larmfunktion för automatiska batchjobb.** (L) Under granskningen noterades att ingen automatisk kontroll finns på plats vilken identifierar och larmar när ett batchjobb[3] har fallerat. Vidare noterades att ingen formell process finns på plats gällande uppföljning och åtgärd av fallerade batchjobb men att batchjobb följs upp av verksamheten i det dagliga arbetet.	Avsaknad av övervakning och larmfunktioner kopplade till batchjobb ökar risken för att kritiska transaktioner inte genomförs fullständigt och riktigt. Kritiska transaktioner som ej genomförts fullständigt och riktigt kan påverka data som är kritiskt för den finansiella rapporteringen.	PwC rekommenderar att Regionstyrelsen analyserar och utvärdera möjligheterna till att automatiskt övervaka kritiska batchjobb i applikationen Agresso Exempelvis kan en riskanalys utgöra grunden för vilka batchjobb som är kritiska i applikationen. Baserat på analysen bör övervakning och larmfunktioner upprättas där ansvarig användare noteras vid de tillfällen ett batchjobb inte genomförts fullständigt och riktigt. Vidare rekommenderar vi att Regionstyrelsen upprättar en formaliserad process vilken säkerställer att fallerade batchjobb åtgärdas fullständigt och riktigt. Fallerade batchjobb bör registreras som incidenter och dokumenteras i syfte att säkerställa spårbarhet i genomförda transaktioner samt stärka den interna kontrollen.

[3] Ett batchjobb är ett schemalagt program som körs utan användarintervention och används ofta för att automatisera uppgifter som måste utföras regelbundet