Region Gotland

Generella IT kontroller – Visma och HR Plus

Detaljerade observationer och rekommendationer

Februari 2017

Fredrik Dreimanis
Jonas Leander

Innehållsförteckning

Sammanfattning av granskningen

I samband med revisionsplaneringen för Region Gotland 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 ekonomi- (Visma) och lönesystemet (HR Plus) genomförts. Granskningen har genomförts under februari månad 2017 av Fredrik Dreimanis (PwC) och Jonas Leander (PwC). Granskningen har genomförts i syfte att bedöma förvaltning och intern kontroll för dessa system.

Baserat på genomförd granskning bedöms det finnas grundläggande processer och rutiner inom Region Gotland gällande förvaltning av kritiska applikationer. Exempelvis finns det inarbetade rutiner gällande hantering av behörigheter, drift och förändringar till de systemen om omfattas av granskningen.

Region Gotlands system för ekonomi och lön är standardsystem där inga specifika anpassningar har genomförts av systemen. Uppdatering och utveckling sker endast genom leverantörsanspassade förändringar. Vidare finns det processer för behörighetstilldelning vilka kräver attest och dokumentation innan användare får åtkomst till kritiska funktioner. Region Gotland har flertalet kontroller på plats i processer kopplade till ekonomi och lön vilka säkerställer att förändringar genomförs fullständigt och riktigt, vidare är loggningsfunktionalitet aktiverad i systemen vilka stödjer spårbarhet och uppföljning av kritiska aktiviteter. I syfte att ytterligare förstärka den interna kontrollen kan Region Gotland analysera om det finns möjlighet att proaktiv arbeta med loggning och spårbarhet i transaktioner.

Vår granskning har inte resulterat i några områden där vi noterat kritiska brister i processer och rutiner. Dock noterades områden där Region Gotland har möjlighet att förstärka och förbättra den interna kontrollen. Totalt noterades sju observationer, vår observationer berör i huvudsak behovet av att formalisera och dokumentera processer och rutiner. Vi rekommenderar att Region Gotland i första hand bör fokusera på följande områden:

- Dokumentation av väsentliga processer och rutiner gällande förvaltning av ekonomi- och lönesystem,
- Implementering och dokumentering av rutiner för periodisk granskning av behörigheter i ekonomi- och lönesystem,
- Dokumenterade återläsningstest av kritisk data.

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

Bakgrund och omfattning

I samband med revisionsplaneringen för Region Gotland 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 Visma (ekonomi system) och HR Plus (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 december 2016 för ITGC domänerna i tabellen nedan och följande applikationer:

- Visma (ekonomisystem),
- HR Plus (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 Region Gotland och granskning av underliggande dokumentation.

Följande personer har varit involverade i granskningen:

- Mats Nyberg (Systemförvaltare, Visma),
- Pernilla Ridal (Inköp/Fakturering, Visma),
- Siv Niklasson (Systemförvaltare, HR Plus/Medvind),
- Mikael Söderberg (IT-drift),
- Mikael Wollbo (Redovisningschef),
- Anders Granvald (Chef Verksamhetsutveckling).

Vårt arbete har utförts in enlighet med PwC's revisionsmetodik och under februari månad i Region Gotlands lokaler, Visby.

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 Region Gotland 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	Visma	Avsaknad av uppdaterade förvaltningsplan.	Medium
2.	Åtkomst till program och data	Visma	Avsaknad av rutin för periodisk granskning av användare.	Medium
3.	Datordrift	Visma	Avsaknad av rutin för återläsningstest.	Låg
4.	IT-styrning	HR Plus	Avsaknad av uppdaterade förvaltningsplan.	Medium
5.	Åtkomst till program och data	HR Plus	Avsaknad granskning gällande priviligerade användares aktivitet.	Medium
6.	Åtkomst till program och data	HR Plus	Avsaknad av rutin för periodisk granskning av användare.	Medium
7.	Datordrift	HR Plus	Avsaknad av rutin för återläsningstest.	Låg

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

	Observation	Risk	Rekommendation
1.	**Avsaknad av uppdaterade förvaltningsplan. (M)** *(Visma)* Under granskningen noterades att förvaltningsplan inklusive instruktioner och riktlinjer för applikationen Visma inte var uppdaterad. Exempelvis saknades uppdaterad dokumentation gällande: ▪ Riskanalys, ▪ Roller och ansvar, ▪ Rutiner gällande förändringshantering, ▪ Rutiner gällande behörighetshantering. Dock noterades att Region Gotland arbetar med att uppdatera dokumentation kopplat till förvaltningen av applikationen Visma. Vidare noterades att det finns rutiner och processer för hur förändringar- och behörigheter hanteras till applikationen Visma.	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 Region Gotland fortsätter med de arbete som initierats kopplat till att uppdatera förvaltningsplanen för applikationen Visma. Förvaltningsplanen 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 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.

	Observation	Risk	Rekommendation
2.	**Avsaknad av rutin för periodisk granskning av användare.** (M) *(Visma)* Under granskningen noterades att ingen formaliserad kontroll finns på plats gällande periodisk granskning för modulen Redovisning och Reskontra (RoR) i applikationen Visma. Dock noterades det att en rutin initierats för att periodisk granska användare i modulen Inköp- och fakturering (IoF) finns på plats. Vidare noterades att Region Gotland arbetar med att definiera och implementera en rutin för periodisk granskning av användare i RoR modulen.	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 Region Gotland fortsätter med de arbete som initierats gällande att upprätta rutiner och dokumentation för periodisk granskning av användare i modulen RoR. Granskningen bör som minimum, men ej begränsat till, omfatta följande; ▪ Arbetar användaren kvar inom Region Gotland, ▪ Har användaren åtkomst i enlighet med sin arbetsuppgifter. Region Gotland rekommenderas att genomföra granskningen, som minimum, årligen. Vidare bör dokumentationen signeras, dateras och arkiveras i syfte at skapa spårbarhet och stärka den interna kontrollen.

	Observation	Risk	Rekommendation
3.	**Avsaknad av rutin för återläsningstest.** (L) *(Visma)* Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen Visma. Dock noterades att återläsning av backuper sker till testmiljön flertalet gånger per år, under 2016 har ingen återläsning av data från backup media misslyckats vilket medför att backuphantering för applikationen Visma fungerar enligt definierad rutin.	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 Region Gotland upprättar dokumentation vid återläsning av data för applikationen Visma. 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.

	Observation	Risk	Rekommendation
4.	**Avsaknad av uppdaterade förvaltningsplan. (M)** *(HR Plus)* Under granskningen noterades att förvaltningsplan inklusive instruktioner och riktlinjer för applikationen HR Plus inte var uppdaterad. Exempelvis saknades uppdaterad dokumentation gällande: ▪ Riskanalys, ▪ Roller och ansvar, ▪ Rutiner gällande förändringshantering, ▪ Rutiner gällande behörighetshantering. Dock noterades att Region Gotland arbetar med att uppdatera dokumentation kopplat till förvaltningen av applikationen HR Plus. Vidare noterades att det finns rutiner och processer för hur förändringar- och behörigheter hanteras till applikationen HR Plus.	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 Region Gotland fortsätter med de arbete som initierats kopplat till att uppdatera förvaltningsplanen för applikationen HR Plus. Förvaltningsplanen 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 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.

	Observation	Risk	Rekommendation
5.	**Avsaknad granskning gällande priviligerade användares aktivitet.** (M) *(HR Plus)* Under granskningen noterades att ingen formaliserad kontroll finns på plats för uppföljning av aktivitet utförd av priviligerade användare. Vidare noterades att samtliga priviligerade användare (sex stycken) i HR Plus har samma åtkomstnivå trots skilda roller, vilket medför att systemet inte stödjer den ansvarsfördelning som finns i löneorganisationen. Det noterades att loggning av kritiska transaktioner är aktiverade i applikationen HR Plus, dock granskas dessa endast i händelse av en incident.	Avsaknad av en processer och rutiner för uppföljning av priviligerade 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 Region Gotland analyserar möjligheten begränsa systemadministratörsrollen i HR Plus Webb så behörigheten reflekterar användares ansvar och arbetsuppgifter. Saknad möjligheten bör manuella kompenserande kontroll implementeras för att säkerställa att användare endast utför aktiviteter i enlighet med sina arbetsuppgifter. Vidare bör en formaliserad kontroll införas där uppföljning av förändringar till kritisk data genomförs i syfte att säkerställa fullständighet och riktighet i genomförda transaktioner. Granskningen bör genomföras av en användare utan åtkomst till att förändra och/eller påverka data. Känsliga transaktioner och data som skall övervakas bör definieras i riskanalysen för HR Plus (*klient*).

	Observation	Risk	Rekommendation
6.	**Avsaknad av rutin för periodisk granskning av användare.** (M) *(HR Plus)* Under granskningen noterades att ingen formaliserad kontroll finns på plats gällande periodisk granskning av användare i applikationen HR Plus.	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 Region Gotland implementerar rutiner och processer för att periodisk granska behörigheter i applikationen HR Plus. Granskningen bör som minimum, men ej begränsat till, omfatta följande; ▪ Arbetar användaren kvar inom Region Gotland, ▪ Har användaren åtkomst i enlighet med sin arbetsuppgifter. Region Gotland rekommenderas att genomföra granskningen, som minimum, årligen. Vidare bör dokumentationen signeras, dateras och arkiveras i syfte at skapa spårbarhet och stärka den interna kontrollen.

	Observation	Risk	Rekommendation
7.	**Avsaknad av rutin för återläsningstest.** **(L)** *(HR Plus)* Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen HR Plus. Dock noterades att återläsning av backuper sker till testmiljön flertalet gånger per år, under 2016 har ingen återläsning av data från backup media misslyckats vilket medför att backuphantering för applikationen HR Plus fungerar enligt definierad rutin.	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 Region Gotland upprättar dokumentation vid återläsning av data för applikationen HR Plus. 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.

2017-02-21

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