pwc

Vallentuna kommun

Generella IT kontroller – Visma Control

Detaljerade observationer och rekommendationer

Maj 2017

Fredrik Dreimanis
Johan Jelbring
Hanna Altsäter

Innehållsförteckning

Sammanfattning av granskningen 3
Bakgrund och omfattning 4
Detaljerade observationer och rekommendationer 6

Sammanfattning av granskningen

I samband med revisionsplaneringen för Vallentuna 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 Visma Control (ekonomisystem) genomförts. Granskningen har genomförts under mars/april 2017 av Johan Jelbring (PwC) och Hanna Altsäter(PwC) under ledning av Fredrik Dreimanis (PwC). Granskningen har genomförts i syfte att bedöma förvaltning och det interna kontrollsystemet i ekonomissytemet.

Baserat på genomförd granskning bedöms det finnas grundläggande processer och rutiner i kommunen gällande förvaltning av ekonomisystemet. Det finns exempelvis inarbetade rutiner för hur systemförändringar ska hanteras, hur hantering av behörigheter inklusive loggning av känslig data ska ske samt hur drift (backuprutin och automatiska överföringar mellan och i olika IT-system) säkerställs.

I granskningen har det dock noterats områden där kommun har möjlighet att förbättra och förstärka den interna kontrollen. Noterade observationer berör i huvudsak avsaknaden av rutinbeskrivningar och dokumentation vilket försvårarar spårbarheten i den interna kontrollen. Baserat på granskningen noterades fem observationer, som vi ser som prioriterade att åtgärda.

Dessa är:

- Avsaknad av uppdaterad förvaltningsplan,
- Avsaknad av policy gällande lösenordshantering,
- Utvecklare med tillgång till produktionsmiljö,
- Avsaknad av dokumenterad rutin för periodisk granskning av användare,
- Avsaknad av rutin för återläsningstest.

Bakgrund och omfattning

I samband med revisionsplaneringen för Vallentuna 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 applikationen Visma Control (ekonomisystem) 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:

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 automatiska körningar (överföringar mellan och i olika IT-system), ▪ Katastrof- och kontinuitetshantering, ▪ Hantering av tredjepartsleverantör.

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

Följande personer har varit involverade i granskningen:

- Anette Jonsson (Controller/Systemförvaltare Visma),
- Monika Smidestam (IT-chef).

Vårt arbete har utförts in enlighet med PwC's revisionsmetodik och under mars månad i Vallentuna kommuns lokaler, *Stockholm*.

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 Vallentuna 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/Förvaltning	Visma	Avsaknad av uppdaterad förvaltningsplan.	Medium
2.	Åtkomsthantering	Visma	Utvecklare med tillgång till produktionsmiljö.	Medium
3.	Åtkomsthantering	Visma	Avsaknad av policy gällande lösenordshantering.	Medium
4.	Åtkomsthantering	Visma	Avsaknad av dokumenterad rutin för periodisk granskning av användare.	Låg
5.	Datordrift	Visma	Avsaknad av rutin för återläsningstest.	Låg

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

	Observation	Risk	Rekommendation
1.	**Avsaknad av uppdaterad förvaltningsplan.** (M) Under granskningen noterades att ingen dokumenterad förvaltningsplan finns på plats vilken definierar hur hantering och förvaltning av applikationen Visma Control genomförs. Vidare noterades att rutiner gällande förändrings- och behörighetshantering inte finns dokumenterade eller formaliserade.	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 Vallentuna kommun att upprätta en förvaltningsplan för applikationen Visma Control. 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.

Kommunens kommentar:
Systemförvaltaren upprättar en förvaltningsplan enligt Vallentunas mall i samarbete med IT. Arbetet kommer att utföras efter PwC rekommendationer.

	Observation	Risk	Rekommendation
2.	**Avsaknad av policy gällande lösenordshantering.** (M) I samband med granskningen noterades att ingen policy eller styrande dokument finns på plats gällande hur lösenord ska vara konfigurerade i kritiska applikationer och nätverk. Vidare noterades att säkerhetskonfigurationen till nätverket idag inte omfattar: ▪ Tvingande komplexa lösenord, ▪ Lösenordslängd, ▪ Tvingande byten av lösenord.	Avsaknad av definition gällande lösenord ökar risken för svaga lösenord vilket kan medföra otillbörlig åtkomst till kritisk data. Otillbörlig åtkomst till kritisk data kan påverka information som är kritisk för den finansiella rapporteringen.	PwC rekommenderar att Vallentuna kommun definierar och dokumenterar en riktlinje för hur lösenord till kritiska applikationer och nätverk ska vara konfigurerade. Exempelvis bör riktlinjen definiera, men inte begränsas till; ▪ Lösenordslängd, ▪ Tvingande byte, ▪ Komplexitet, ▪ Låsning av användarkonto. Beslutad konfiguration bör implementeras i kritiska system och nätverk samt granskas, som minimum, årligen.

Kommunens kommentar:
Vi delar uppfattning och har redan påbörjat arbetet med att med hjälp av verktyget ARS skapa rekommenderade åtgärder. Just nu ligger testversionen ute för test på några skolor för att sedan kunna utvärderas.
Konfigurationen avser lösenordslängd, tvingande byte och komplexitet ska gälla generellt och för kritiska applikationer.

	Observation	Risk	Rekommendation
3.	**Utvecklare med tillgång till produktionsmiljö.** (M) Det noterades under granskningen att utvecklare har direkt till gång till produktionsmiljön för applikationen Visma Control. Dock noterades att kompenserade kontroller finns på plats där exempelvis användare måste kvittera ut behörighet till servermiljön. Vidare genomförs loggning och uppföljning av förändringar till kritiska data.	Utvecklare med åtkomst till produktionsmiljön ökar risken för felaktiga eller bedrägliga förändringar till kritiska funktioner. Felaktiga eller bedrägliga förändringar till kritiska funktioner kan påverka data som är kritisk för den finansiella informationen.	PwC rekommenderar att Vallentuna kommun undersöker möjligheten att begränsa och/eller ta bort åtkomst för utvecklare till produktionsmiljön. Finns inte möjligheten att ta bort utvecklare i produktionsmiljön rekommenderar vi att kompenserande kontroller implementeras för att säkerställa att aktiviteter utförda av utvecklare är fullständiga och riktiga samt inte påverkar kritisk information.

Kommunens kommentar:
Utvecklare kommer i framtiden att få tidsbegränsad inloggning. Uppföljning av inloggning på server kommer att ske löpande av IT-avdelningen.

	Observation	Risk	Rekommendation
4.	**Avsaknad av dokumenterad rutin för periodisk granskning av användare.** (M) Under granskningen noterades att ingen formaliserad kontroll finns på plats gällande periodisk granskning av användare i applikationen Visma Control. Dock noterades det att en periodisk kontroll av användare genomförs en gång per år av systemförvaltaren. Dock är detta ej en formaliserad rutin där underlag arkiveras för spårbarhet.	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 Vallentuna kommun formaliserar rutiner och dokumentation för periodisk granskning av användare. Granskningen bör dokumenteras av ansvarig manager vilken arkiverar underliggande underlag till granskningen, signerar och daterar i syfte att skapa spårbarhet samt stärka den interna kontrollen.

Kommunens kommentar:
Vi avser att dokumentera den kontroll som redan genomförs. Dokumentationen kommer att ske i vårt verksamhetssystem Stratsys.

	Observation	Risk	Rekommendation
5.	**Avsaknad av rutin för återläsningstest. (L)** Under granskningen noterades att ingen dokumenterad rutin finns på plats gällande återläsning av data för applikationen Visma Control. Dock noterades att återläsning av backuper sker till testmiljön flertalet gånger per år.	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 Vallentuna kommun upprättar dokumentation vid återläsning av data för applikationen Visma Control. 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:
Iakttagelserna är riktiga. Idag genomför vi återläsning av backup minst 4 ggr om året. Återläsningen bör vid aktuella tillfällen dokumenteras utifrån PwC:s rekommendationer.