

AB STOCKHOLMSHEM

Appendix 6

AB STOCKHOLMSHEM REKOMMENDATIONER FRÅN REVISIONEN

GRANSK- NINGSÅR	REKOMMENDATION	Rekomen- dationen följs upp (datum)	ÅTGÄRDAT			KOMMENTAR FRÅN FÖRETAGSLEDNINGEN
			Ja	Nej	Delvis	
2012	Avstämningsmöte avseende respektive distrikts driftskostnader sker tertialvis inom förvaltningsavdelningen map på utfall jämfört med budget och input till kommande prognos. Dokumentation från dessa möten sker genom enklare minnesanteckningar. Vi bedömer detta som en god övergripande kontroll och ser att värdet av den skulle kunna höjas ytterligare genom att även inkludera distriktets intäkter och genom en ökad standardisering och dokumentation. Förslagsvis genom upprättande av standardrapporter som underlag med fastställda nivåer för avvikelser att kommentera på. Vidare att även dokumentera iakttagelser, ställningstaganden och beslut avseende ekonomiskt utfall. Uppdatering 2013: Resultatuppföljning görs på övergripande nivå av ekonomichef. Ett arbete pågår med att implementera prognos-/ resultatuppföljningsverktyget Insikt för att kunna utföra resultatuppföljningar på områdesnivå. Det behöver utarbetas	Boksluts- granskning 2013				Kommentar 2013 Bolaget kommer arbeta vidare med strukturer och rutiner för uppföljning och analyser med stöd av Insikt. Kommentar 2012 Bolaget genomför en organisationsförändring som ska träda i kraft 1/1 2013. I samband med denna kommer nya lägre "ansvarsnivåer" att införas. Vidare kommer uppföljnings- och återrapporteringsmallar att uppdateras i syfte att större enhetlighet ska erhållas. Bolaget genomför även en implementering av ett nytt budget och prognosverktyg som ska hjälpa områdescheferna att gör budget och resultatuppföljningar. Bolaget anställer under 2013 två controllers som ska assistera områdescheferna i budget och utfallsfrågor.

AB STOCKHOLMSHEM

Appendix 6

	klara rutiner och ansvarsområden för resultatuppföljning kopplade till verktyget gällande vem som är ansvarig, när uppföljning skall ske och med definierade avvikelsetintervall.					
2013	Bolaget har implementerat ett nytt IT-verktyg under 2013 Insikt som skall användas för resultat- och budgetuppföljning vilket även kommer att omfatta investeringsprojekt, men denna rutin finns ännu inte på plats. Idag finns ett flertal projekt som överskrider budget utan tillägsbeställningar. Tanken är att uppföljning av dessa projekt skall göras i Insikt och kommenteras. I samband med implementeringen är det viktigt att klargöra vem som är ansvarig, när uppföljning skall ske och med definierade avvikelsetintervall	Bokslutsgranskning 2013				Se ovan <u>Underhållsprojekt:</u> <u>Rutin för avvikelserapportering avseende projekt finns. Fokus under 2014 är att all kommunikation om ev avvikelser ska dokumenteras i Insikt.</u> <u>Controller kommer att ha månatliga avstämningar med projektledarna, vilket innebär att varje projektledare kommer att ha en avstämning ca 6 ggr/år.</u> <u>Tertialvisa projektgenomgångar/prognoser kommer att ske med projektledare och beställare.</u> <u>Nyproduktion:</u> <u>Rutin för avvikelserapportering finns. Under 2014 fokus på dokumentation i Insikt.</u>
2013	Redovisningschef bör genom attestgodkänna månadsavstämningar i moderbolaget.	Bokslutsgranskning 2013				Genomgångar med avstämningsansvariga kommer att ske månadsvis. Redovisningsansvarig kommer även att attestera sammanställning över avstämningarna. <u>Genomgångar sker månadsvis med respektive avstämningsansvariga. Attest av</u>

AB STOCKHOLMSHEM

Appendix 6

						avstämningarna sker av Redovisningschef för moder- och dotterbolag.
2013	Bolaget har utfört rimlighetsanalys av den årliga hyreshöjningen. Denna är inte attesterad vilken är en avvikelse från bolagets rutiner. Vi har följt upp att analysen är korrekt utförd och bedömer att avvikelsen inte har någon effekt på årets revision.	Intern kontroll-granskning 2014				Bolaget ser över sina rutiner inför nästa år.
2013	Det finns ett flertal anställda på ekonomiavdelningen som har höga behörigheter i M3, vilket ger möjlighet att nyregistrera/ändra fast data i leverantörsregistret såsom bankgirouppgifter. Redovisningschefen har denna höga behörighet och kan samtidigt slutatstestera fakturor. Bolaget rekommenderas att reducera antalet användare med dessa behörigheter och se över ansvarsfördelning för att begränsa risken för oriktiga uppgifter i leverantörsregistret vilka kan påverka betalningar. Bolaget bör även införa rutin att kontrollera nyupplägg och ändringar i leverantörsregistret. Alt 1: införa en spärr i systemet att nyupplägg och ändringar måste godkännas (förebyggande kontroll) Alt 2: ta ut logglistor på upplägg och	Boksluts-granskning 2013				Bolaget ser över möjligheten att separera behörigheter i M3 och skapa fler rollstyrda behörigheter. Arbetet är påbörjats att förfina behörighetsrollerna, klart februari 2014. Bolaget kommer att införa en kontroll över nyupplägg och ändringar i leverantörsregistret. Ändrad rutin vid upplägg av ny leverantör, två i förening, sedan september 2013.

AB STOCKHOLMSHEM

Appendix 6

	ändringar och följa upp mot underlag (upptäckande kontroll). Dessa alternativ kan med fördel kombineras. Bolaget rekommenderas att införa rutin att följa upp behörigheter i Basware regelbundet (t.ex. varje månad/ kvartal) då det inte är möjligt att lägga upp tidsbegränsning för tillfälliga behörigheter.					Logglistor kommer att tas ut månadsvis. Ekonomichef Svante kommer att godkänna ändringarna. Stockholmshem kommer att ta ut listor på behörigheter från Basware för genomgång och godkännande varje månad. Åsa Berglund och Svante Larsson godkänner behörigheterna.
--	--	--	--	--	--	---

Suante

Stockholms Stadshus AB

Granskning av IT intern kontroll

Bakgrund

Stockholms Stadshus AB har beslutat att genomföra en granskning av IT intern kontroll och informationssäkerhet inom utvalda områden hos samtliga dotterbolag, med fokus på applikationer inom bolagen som stödjer den finansiella rapporteringen.

Syftet med granskningen är att få en överblick över rådande status inom IT intern kontroll samt att i diskussion med bolagen adressera ansvarsfördelning inom området.

Stockholmshem har fått tre anmärkningar varav en kategoriseras för "skyndsam åtgärd".

- Bristande spårbarhet i de periodiska genomgångarna samt avsaknad av delaktighet från systemägare
- Avsaknad av rutin för regelbunden granskning av programförändringsprocessen
- Återläsningstester genomförs inte för servrar hos Volvo IT

Nedan redovisas, per punkt, revisionens iakttagelse, risk samt rekommendation ihop med Stockholmshems förslag på åtgärd.

Bristande spårbarhet i de periodiska genomgångarna samt avsaknad av delaktighet från systemägare

● Iakttagelse

Systemförvaltarna rapporterar till IT-avdelningen när den periodiska genomgången av behörigheter är genomförd, men resultatet av genomgången dokumenteras inte. Vi noterade även att systemägaren inte godkänner och därmed ansvarar för resultatet av den periodiska genomgången.

Risk

Avsaknad av spårbarhet och analys av ansvarig systemägare i utförandet av kontroller i behörighetsprocessen ökar risken för att personer som inte längre jobbar kvar eller har fått ändrade arbetsuppgifter har kvar gamla eller fel behörigheter i systemen. Detta kan användas för att kringgå befintliga kontroller i applikationen.

Rekommendation

AB Stockholmshem bör sammanställa och dokumentera resultatet av de periodiska genomgångarna. Systemägaren bör vara delaktig i att godkänna resultatet av genomgångarna.

Åtgärd

För att få spårbarhet och kontroll på aktiva och avaktiverade konton föreslås följande rutin;

Systemförvaltaren levererar till systemägaren en fullständig lista med användarkonton där det noterats med "OK" eller "Tas bort" på varje användare. Systemägaren godkänner sedan hela genomgången och att listan sparas hos Systemförvaltaren.

Tidpunkt föreslås till december månad varje år.

Avsaknad av rutin för regelbunden granskning av programförändringsprocessen

Iakttagelse	IT-avdelningen på AB Stockholmshem har upprättat en wiki där beställningsprocessen, ändringsprocessen och driftsvaltningsprocessen är tillgängliga och uppdateras vid behov. Varje process har en processägare som beslutar hur rutinerna ska vara utformade. Vid vår granskning noterade vi att det inte finns någon rutin för att regelbundet kvalitetssäkra programförändringsprocessen.
Risk	Då en wiki är ett levande dokument finns risk vid förändring att viktiga kontroller uteblir samt att förändringar inte kommuniceras.
Rekommendation	AB Stockholmshem bör införa rutiner för att regelbundet, exempelvis årligen, kvalitetssäkra programförändringsprocessen. Processägaren bör ta ansvar för att godkänna beskrivningen av programförändringsprocessen.

Åtgärd

För att säkerställa att dokumenterade rutiner är lämpliga och ändamålsenliga kommer IT-chef genomföra en genomgång med processägare en gång per år. Resultatet dokumenteras och godkänns av IT-chef.

Tidpunkt föreslås till december månad varje år.

Återläsningstester genomförs inte för servrar hos Volvo IT

Iakttagelse	Volvo IT tar regelbundet backupper enligt avtalet mellan Volvo IT och Stockholms Stad. Volvo IT genomför dock inte återläsningstester av den fullständiga applikationsmiljön. Återläsningstester måste beställas av AB Stockholmshem. Vid vår granskning noterade vi att AB Stockholmshem inte har beställt återläsningstester av Volvo IT.
Risk	Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.
Rekommendation	AB Stockholmshem bör, utifrån ett riskbaserat synsätt, regelbundet säkerställa möjligheten att återläsa data och system, till exempel genom att genomföra återläsningstester. AB Stockholmshem bör även säkerställa att FFG gör likvärdig kvalitetssäkring för FASAD, samt att de dokumentera och kommunicera resultaten.

Åtgärds

Stockholmshem genomför under 2014 återläsningstest för att verifiera rutiner hos driftleverantör samt systemleverantör.

Stockholmshem säkerställer att FFG gör likvärdig kvalitetssäkring för FASAD ihop med Micasa som fått motsvarande anmärkning.

Stockholmshem dokumenterar resultat och vidtar åtgärder för att rutinen ska vara tillfylles.

Tidpunkt föreslås till att planeras under januari och genomförande innan juni 2014.