Stockholms Stadshus AB

Granskning av IT intern kontroll

25 november 2013

EY
Building a better working world

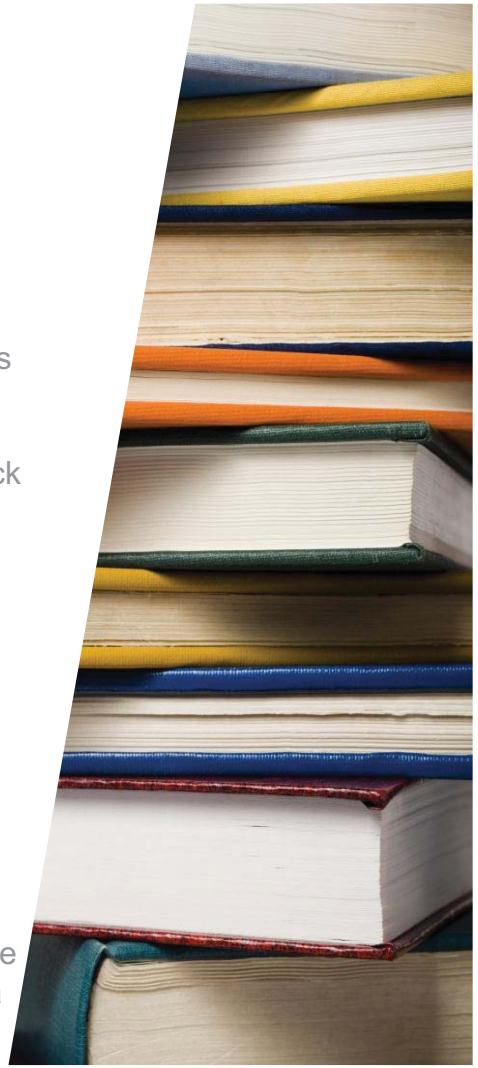
Innehåll

Sektion 1

Sammanfattning

Sammanfattning

- 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.
- Övergripande kan noteras en ökade medvetenhet om vikten av god intern kontroll inom IT samt att inga väsentliga skillnader i kvalitén på den interna kontrollen noterats mellan Stockholms Stads bolag och andra jämförbara organisationer. Vissa områden som kräver förbättringsåtgärder har dock noterats. Iakttagelser har gjorts för majoriteten av dotterbolagen. Vissa av observationerna bör åtgärdas skyndsamt. Dock bedöms ingen av observationerna ha karaktären av att de innebär en omedelbar risk för verksamheten inom Stockholms Stad. Följande generella områden för förbättring har identifierats:
  - Ansvarsfördelning gällande administration och godkännande av behörigheter
  - Dokumentation av rutiner och genomförda kontroller
  - Utbildning i informationssäkerhet
  - Tydlighet gällande vilka befattningar inom bolagen som är lämpliga för rollen som informationssäkerhetssamordnare
  - Genomförande av återläsningstester av backuper
- Stockholms Stadshus AB rekommenderas att kommunicera iakttagelser till respektive dotterbolag för utvärdering och åtgärd, samt att utvärdera de generella iakttagelserna för eventuella åtgärder.



Sektion 2

Introduktion

Bakgrund och syfte

- Stockholms Stadshus AB har beslutat att genomföra en granskning av IT intern kontroll och informationssäkerhet hos samtliga dotterbolag.
- Granskningen har fokuserat på applikationer inom bolagen som stödjer den finansiella rapporteringen med fokus på programförändringsrutiner, behörighetsrutiner samt utvalda aspekter av informationssäkerhet. Granskningen syftar till att ge en överblick av rådande status inom IT intern kontroll samt att i diskussion med bolagen adressera ansvarsfördelning inom området.
- Denna granskning syftar till att komplettera den föregående granskningen som tidigare under 2013 genomfördes utifrån motsvarande kontrollmål hos Volvo IT.
- Resultatet av granskningen baseras på intervjuer och genomgång av utvald relevant dokumentation.

Omfattning och avgränsning

- De bolag som har omfattats av granskningen är;
  - AB Familjebostäder
  - AB Stockholmshem
  - AB Stokab
  - Kulturhuset Stadsteatern AB
  - Micasa Fastigheter AB
  - SISAB
  - S:t Erik Försäkring AB
  - S:t Erik Livförsäkring AB
  - S:t Erik Markutveckling AB
  - Stockholm Business Region AB
  - Stockholm Globe Arena Fastigheter AB
  - Stockholms Hamn AB
  - Stockholm Parkering AB
  - Stockholms Stadshus AB
  - Stockholms Stads Bostadsförmedling AB
  - Stockholm Vatten AB
  - Svenska Bostäder
- Granskningen har inte innefattat detaljerade tester av enskilda förhållanden eller identifierade kontroller. Resultatet av granskningen har baserats på genomförda intervjuer samt på erhållet material från respektive bolag.

Utvärderingskriterier (1/2)

Följande områden har varit fokus i granskningen:

- **Programförändringar:**

  Rutiner kring samt dokumentation av programförändringar och relaterade processer. Förväntade områden för kontroller inkluderar beställning, acceptans test av och godkännande för produktionssättning.

- **Åtkomst:**

  Säkerställande av systemkonfigurations, lösenordinställningars och antalet användare med höga behörigheters lämplighet. Dessutom har granskningen innefattat behörighetsprocessens övervakning och dokumentation samt att behörigheter är godkända vid både upplägg och vid regelbunden granskning

- **Stockholms stads riktlinjer för informationssäkerhet:**

  Med avseende till stadens riktlinjer för informationssäkerhet respektive bolags arbete med informationssäkerhet, implementering av rutiner, informationsklassning, utbildning, säkerhetskopiering samt riskanalys av kritiska system

Utvärderingskriterier (2/2)

Iakttagelser har bedömts med färgkodning utifrån:

Iakttagelse	Åtgärd
	Iakttagelser där bolaget bör överväga skyndsam åtgärd.
	Iakttagelser där bolaget bör överväga åtgärd inom rimlig tid.
	Acceptabel nivå, men där utrymme för åtgärd/förbättringar kan förekomma.

Sektion 3

Granskningsresultat, iakttagelser samt rekommendationer

Granskningsresultat i jämförelse mellan bolag

Introduktion till granskningsresultat:

- I denna sektion presenteras resultatet av vår granskning i form av en jämförelse utifrån de bedömningskriterier som finns presenterade i sektion 2.
- Eftersom stadens bolag är av olika natur har vi delat upp jämförelsen på komplexa och mindre komplexa bolag. Bolag har i detta avseende bedömts som mindre komplexa om de har en mindre komplex IT miljö, lägre förändringstakt inom IT samt lägre antal anställda.
- Jämförelsen syftar till att ge en överblick och resultatet baseras på de intervjuer som har genomförts.
- Den operationella effektiviteten av nämnda kontroller i matrisen har inte testats.
- Utfallet för de komplexa bolagen är inte direkt jämförbart med de mindre komplexa bolagen eftersom större förändringstakt inom behörigheter och system ställer högre krav på intern kontroll inom IT.

Granskningsresultat i jämförelse – komplexa bolag (1/2)

Område	Stockholms Stadshus AB	Stockholms Hamn AB	AB Stokab	AB Stockholms Hem	AB Familje-bostäder	Micasa Fastigheter AB	Stockholm Vatten AB	Stockholms Stads Bostads-förmedling AB	SISAB	Svenska Bostäder
Programförändringar är godkända för utveckling										
Programförändringar är testade										
Programförändringar är godkända för införande i produktionsmiljö										
Det existerar ändamålsenlig ansvarsfördelning inom programförändrings-processen										
Lösenordsinställningar är lämpliga										
Höga behörigheter är begränsat till lämpligt antal användare										
Behörigheter är godkända vid upplägg samt vid regelbunden granskning										

Granskningsresultat i jämförelse – komplexa bolag (2/2)

Område	Stockholms Stadshus AB	Stockholms Hamn AB	AB Stokab	AB Stockholms Hem	AB Familje-bostäder	Micasa Fastigheter AB	Stockholm Vatten AB	Stockholms Stads Bostads-förmedling AB	SISAB	Svenska Bostäder
Det existerar ändamålsenlig ansvarsfördelning inom behörighetsprocessen										
Ägare av informationstillgångar har fastställts och dokumenterats										
Medarbetare har fått utbildning i informationssäkerhet	*	*		*	*	*		*	*	*
Regelbunden säkerhetskopiering och återläsning										
Konsekvent rapportering av incidenter och säkerhetsmässiga svagheter										
Riskanalys av klassificerade system är genomförd										

*Endast beskriven som en generell iakttagelse med rekommendation, se sida 21 för ytterligare detaljer.

Granskningsresultat i jämförelse
– mindre komplexa bolag (1/2)

Område	Stockholm Globe Arena Fastigheter AB	Stockholm Business Region AB	S:t Erik Mark-utveckling AB	S:t Erik Livförsäkring AB	S:t Erik Försäkrings AB	Kulturhuset Stadsteatern AB	Stockholm Parkering AB
Programförändringar är godkända för utveckling							
Programförändringar är testade							
Programförändringar är godkända för införande i produktionsmiljö							
Det existerar ändamålsenlig ansvarsfördelning inom programförändrings-processen							
Lösenordsinställningar är lämpliga							
Höga behörigheter är begränsat till lämpligt antal användare							
Behörigheter är godkända vid upplägg samt vid regelbunden granskning							

Granskningsresultat i jämförelse – mindre komplexa bolag (2/2)

Område	Stockholm Globe Arena Fastigheter AB	Stockholm Business Region AB	S:t Erik Mark-utveckling AB	S:t Erik Livförsäkring AB	S:t Erik Försäkrings AB	Kulturhuset Stadsteatern AB	Stockholm Parkering AB
Det existerar ändamålsenlig ansvarsfördelning inom behörighetsprocessen							
Ägare av informationstillgångar har fastställts och dokumenterats							
Medarbetare har fått utbildning i informationssäkerhet		*	*	*	*	*	*
Regelbunden säkerhetskopiering och återläsning							
Konsekvent rapportering av incidenter och säkerhetsmässiga svagheter							
Riskanalys av klassificerade system är genomförd							

*Endast beskriven som en generell iakttagelse med rekommendation, se sida 21 för ytterligare detaljer.

Generella iakttagelser

- I granskningen har vi identifierat liknande iakttagelser hos ett flertal bolag, dessa iakttagelser presenteras som generella iakttagelser.
- Har iakttagelser identifierats för ett specifikt bolag finns den även med under respektive bolag i appendix.

Brister i den ändamålsenliga ansvarsfördelningen gällande administration och godkännande av behörigheter

Iakttagelse	För ett flertal bolag finns brister i den ändamålsenliga ansvarsfördelningen gällande utförande av upplägg och godkännande av nya behörigheter i applikationer kritiska för den finansiella rapporteringen.
Risk	Brister i den ändamålsenliga ansvarsfördelningen ökar risken för brister i spårbarhet gällande godkännanden vilket i sin tur kan leda till att fel behörigheter tilldelas. Vidare kan personberoende innebära att problem och uppdateringar inte kan hanteras i de fall personen inte är tillgänglig.
Rekommendation	För de bolag där iakttagelse har gjorts gällande brister i ansvarsfördelning följ upp att åtgärder med hänsyn till bolagens natur genomförs för att stärka den ändamålsenliga ansvarsfördelningen mellan den som godkänner och som administrativt utför själva upplägget av en ny behörighet.

Bristande dokumentation av rutiner för programförändringsprocesser

Iakttagelse	För flertalet bolag saknas dokumenterade rutiner för hur programförändringar ska hanteras. Inom Stockholms Stads riktlinjer för informationssäkerhet finns området systemutveckling beskrivet. Det kan även noteras att dessa riktlinjer är föremål för uppdatering.
Risk	Bristande dokumentation och kommunikation av rutiner kan leda till att det inte finns ett gemensamt arbetssätt för exempelvis testförfarande eller produktionssättning och därmed kan viktiga kontroller utebli eller kringgås med försämrad systemkvalitet som följd.
Rekommendation	Se rekommendation för respektive bolag i appendix. I övrigt bör Stockholms Stad centralt se över och utvärdera behov av att tydligare kommunicera de riktlinjer för programförändringsprocessen som nyligen har tagits fram samt följa upp hur dessa tas emot och införs på respektive bolag.

Bristande dokumentation av rutiner för periodisk genomgång av behörigheter

Iakttagelse	För flertalet bolag saknas dokumenterade rutiner för periodisk genomgång av applikationsbehörigheter samt dokumentation av resultatet av de genomgångar som genomförs. Området berörs övergripande i stadens riktlinjer för informationssäkerhet.
Risk	Bristande dokumentation av rutiner ökar risken för att rutiner inte följs och att viktiga kontroller kringgås. Det i sin tur ökar risken för obehörig åtkomst till applikationerna genom att personer som slutat och med ändrade arbetsuppgifter har kvar gamla behörigheter i systemen.
Rekommendation	Se rekommendation för respektive bolag i appendix. I övrigt bör Stockholms Stad centralt se över och utvärdera riktlinjer kring genomförande och dokumentation av rutiner för den periodiska genomgången av behörigheter.

Återläsningstester av backuper genomförs inte för applikationsmiljöer

Iakttagelse	För de applikationer som driftas hos Volvo IT tar Volvo IT regelbundet backup av innehåll på databaser. För återläsningstester måste bolaget dock göra en separat beställning hos Volvo IT. Flertalet av bolagen har inte beställt återläsningstester av Volvo IT sedan avtalet upprättades.
Risk	Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.
Rekommendation	Stockholms Stadshus AB bör tydligt kommunicera ansvarsfördelning för samtliga bolag gällande att, utifrån ett riskbaserat synsätt, säkerställa möjlighet att återläsa data och system. Samtliga bolag bör säkerställa att rutiner för detta finns, till exempel genom att genomföra återläsningstester samt dokumentera resultatet av dessa.

Ofullständig utbildning i informationssäkerhet

Iakttagelse	I flertalet av bolagen har inte samtliga anställda genomgått utbildning i informationssäkerhet.
Risk	Ofullständig utbildning i informationssäkerhet ökar risken för bristande förståelse av risker kopplat till användning av IT-stöd.
Rekommendation	Stockholms Stadshus AB/Stockholms Stad bör utvärdera hur behovet av gemensam utbildning i informationssäkerhet för samtliga anställda i bolagen ska säkerställas.

Otydlighet gällande vilka befattningar inom bolagen som är lämpliga för rollen som informationssäkerhetssamordnare

Iakttagelse	För en del bolag är IT-chefen även informationssäkerhetssamordnare. Flertalet IT-chefer har kommunicerat att de upplever att detta kan vara olämpligt men i stadens riktlinjer finner de däremot inget stöd i hur denna roll lämpligen ska fördelas.
Risk	Att IT-chefen även fungerar som informationssäkerhetssamordnare ökar risken för att person i ansvarsställning inte är helt oberoende i förhållande till uppgiften.
Rekommendation	Stockholms Stadshus AB bör utvärdera om rådande riktlinjer ska förtydligas gällande vilka roller som är lämpliga respektive mindre lämpliga som informationssäkerhetssamordnare.