Styrelseärende
Styrelsen 2014-03-13
Ärende 8

Handläggare: Lars Brogren
Telefon: 08-508 370 00 (vx)

Till styrelsen

Granskning av IT intern kontroll

VD:s förslag till beslut

Styrelsen för Svenska Bostäder beslutar följande.

Rapporten godkänns.

Vällingby den 28 februari 2014

Pelle Björklund
VD

Ärendet

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 ökad 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.

Bilagor

Granskningsrapport av IT intern kontroll

_____

Stockholms Stadshus AB

Granskning av IT intern kontroll

25 november 2013

EY
Building a better working world

Innehåll

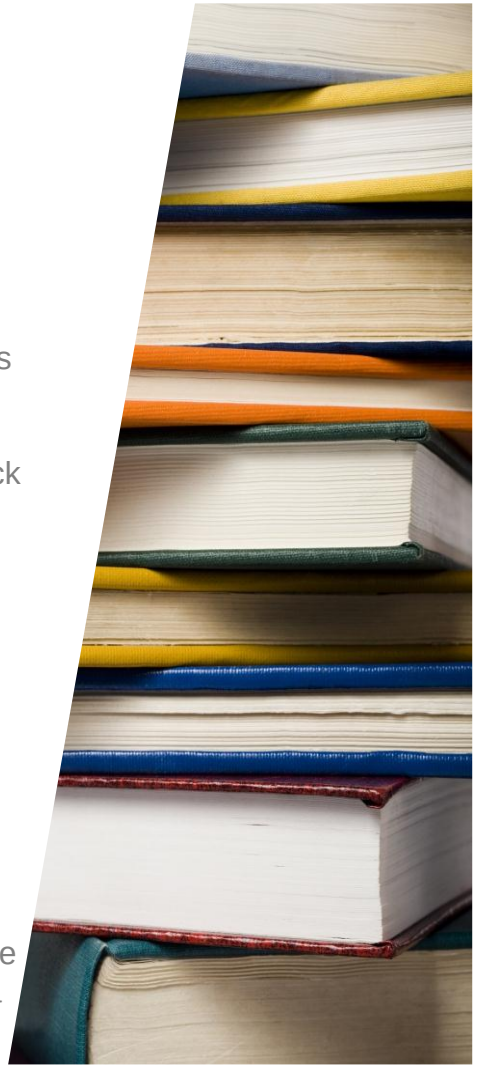
1	**Sammanfattning**	**3**
2	**Introduktion**	**5**
	Bakgrund och syfte	6
	Omfattning och avgränsning	7
	Utvärderingskriterier	8
3	**Granskningsresultat, iakttagelser samt rekommendationer**	**10**
	Resultat	11
	Generella iakttagelser	16
4	**Appendix**	**23**
	Iakttagelser för respektive bolag	24
	Granskningsdetaljer	70

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:**

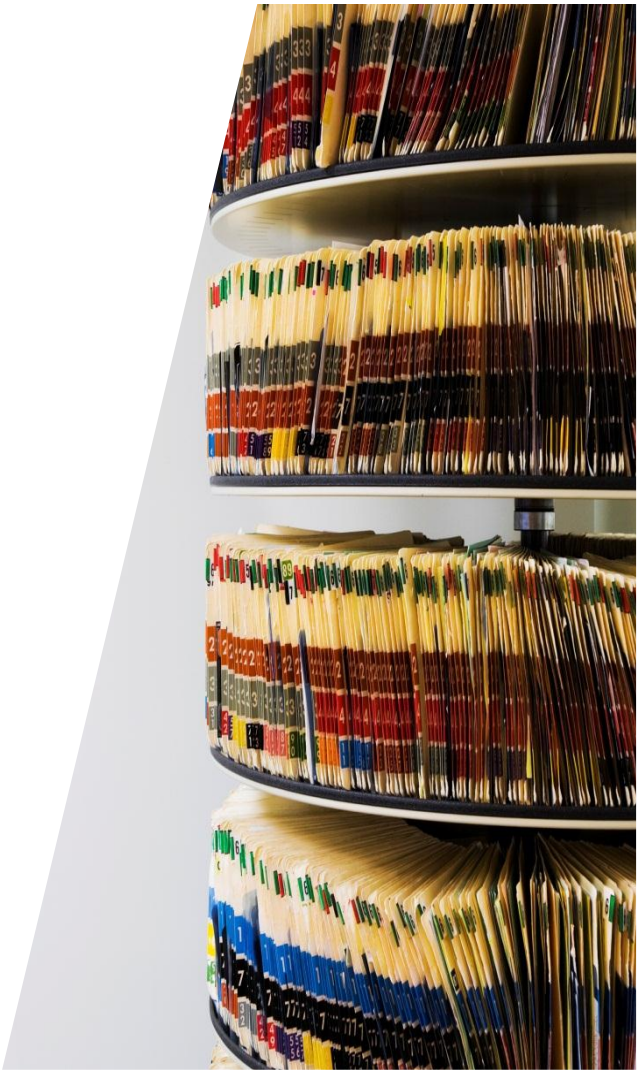
  Rutiner kring samt dokumentation av programförändringar och relaterade processer. Förväntade områden för kontroller inkluderar beställning, acceptans test av och godkännande för produktionssättning.

- **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							

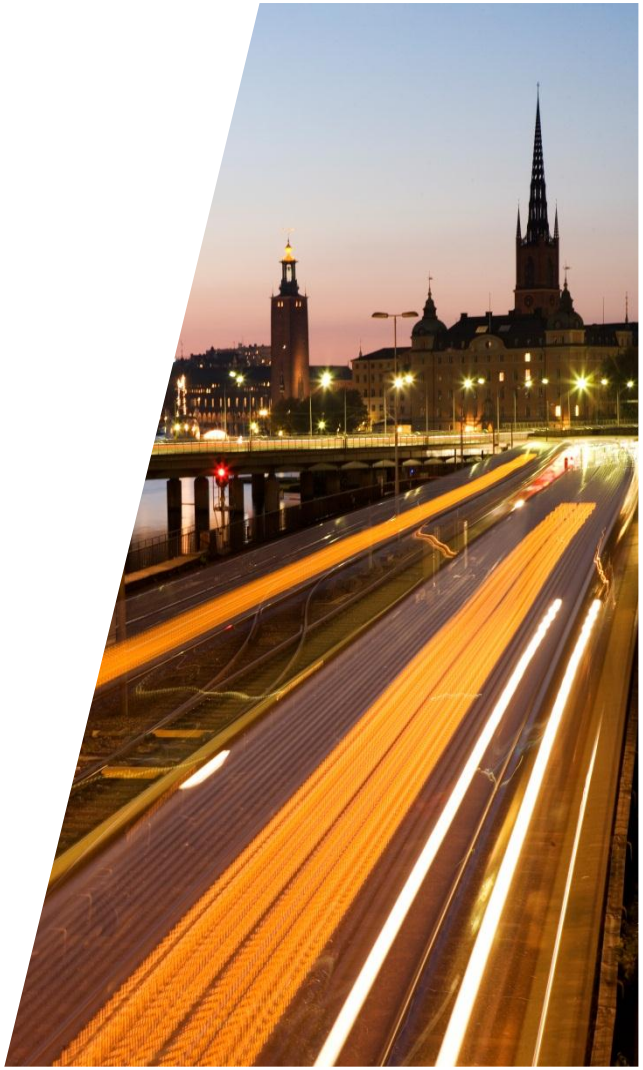
Granskningsresultat i jämförelse – mindre komplexa bolag (2/2)

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.

Sektion 4

Appendix

Företagsspecifika iakttagelser

Appendix

Bolag	Sida	Iakttagelser
AB Familjebostäder		
AB Stockholmshem	25-27	
AB Stokab		
Kulturhuset Stadsteatern AB	28-32	
Micasa Fastigheter AB	33-36	
SISAB	37-42	
S:t Erik Försäkring AB	43	
S:t Erik Livförsäkring AB	44	
S:t Erik Markutveckling AB		
Stockholm Business Region AB	45-47	
Stockholm Globe Arena Fastigheter AB		
Stockholms Hamn AB	48-56	
Stockholm Parkering AB	57	
Stockholms Stadshus AB	58-60	
Stockholms Stads Bostadsförmedling AB	61-65	
Stockholm Vatten AB	66-70	
Svenska Bostäder		

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 där med 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.

Avsaknad av rutin för regelbunden granskning av programförändringsprocessen

Iakttagelse	IT-avdelningen på AB Stockholmshem har upprättat en wiki där beställningsprocessen, ändringsprocessen och driftsförvaltningsprocessen 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.

Återläsningstester genomförs inte för servrar hos Volvo IT

Iakttagelse

Volvo IT tar regelbundet backuper 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.

Programförändringar testas inte i testmiljö innan produktionssättning

Iakttagelse

Utveckling av programförändringar för Visma och Agda genomförs av respektive leverantör då nya uppdateringar finns tillgängliga. När programförändringar är implementerade kontrollerar verksamheten att viktiga funktioner i systemen fungerar på tillfredsställande sätt. Vid vår granskning noterade vi däremot att ingen dokumentation av dessa tester sker och att verksamheten inte testar programförändringarna i testmiljö för ändringar i Agda innan förändringen implementeras i produktionsmiljön.

Risk

Att inte testa och dokumentera tester vid programförändringar ökar risken för att förändringar som inte är tillräckligt testade förs in i produktionsmiljön, vilket kan leda till ökade kostnader på grund av störningar och avbrott i kritiska system samt affärsprocesser.

Rekommendation

Kulturhuset Stadsteatern AB bör upprätta en process för att dokumentera utförande och resultat av testade programförändringar. Särskild uppmärksamhet bör iakttas vid förändringar i Agda efter uppdatering av produktionsmiljön.

Bristande dokumentation av godkännande för mindre programförändringar i Klara

Iakttagelse

Utveckling av programförändringar för Klara genomförs av IT-chefen på begäran av systemägaren. Vid stora förändringar ska önskad funktionalitet samt beslut för produktionssättning dokumenteras. Vid vår granskning noterade vi att ingen dokumentation av godkännande för utveckling samt godkännande för produktionssättning sker vid mindre programförändringar.

Risk

Brister i spårbarhet gällande godkännanden innebär ökad risk för att ändamålsenlig ansvarsfördelning inte följs. Brister i ändamålsenlig ansvarsfördelning kan i sin tur leda till att felaktiga ändringar implementeras i produktionsmiljön. Detta gäller vanligtvis samtliga förändringar oavsett storlek.

Rekommendation

Innan produktionssättning av förändringar bör godkännande inhämtas av systemägare för samtliga förändringar. Vid akuta ändringar kan godkännande dokumenteras i efterhand.

Bristande ansvarsfördelning och personberoende för programförändringar i Klara

Iakttagelse

IT-chefen har utvecklat applikationen Klara och är för närvarande den enda person som har tillräcklig kunskap för att kunna utveckla programförändringar och genomföra produktionssättningar. Utredning pågår för närvarande som ska ge riktlinjer för hur Klara och besläktade system ska hanteras.

Risk

Brister i spårbarhet gällande godkännanden tillsammans med personberoende innebär ökad risk för att ändamålsenlig ansvarsfördelning ej följs. Det kan i sin tur leda till att felaktiga ändringar implementeras i produktionsmiljön. Vidare kan personberoende innebära att problem och uppdateringar inte kan hanteras i de fall personen inte är tillgänglig.

Rekommendation

Kulturhuset Stadsteatern AB bör fortsatt se över möjliga lösningar för att minska personberoendet och säkerställa ändamålsenlig ansvarsfördelning.

Lösenord för användarkonton i Visma, Agda och Klara följer inte Stockholms Stads riktlinjer för informationssäkerhet

Iakttagelse

För att logga in på applikationerna Visma, Agda och Klara behöver användaren först logga in i Active Directory. Vid vår granskning noterade vi att det, i de tre applikationerna, inte finns några lösenordsinställningar så som krav på komplexitet, byte efter ett begränsat antal dagar eller antal tecken, vilket är i konflikt med Stockholms Stad riktlinjer för informationssäkerhet.

Risk

Svaga krav på lösenord ökar risken för obehörig åtkomst till de nämnda applikationerna.

Rekommendation

Kulturhuset Stadsteatern AB bör säkerställa att användarkonton i samtliga applikationer följer Stockholms Stads riktlinjer för informationssäkerhet.

Rutiner för programförändringar och behörighetshantering är inaktuella och uppdateras inte regelbundet

Iakttagelse	Kulturhuset Stadsteaterns rutiner gällande programförändringar och behörighetshantering är inaktuella och uppdateras inte regelbundet.
Risk	Bristande dokumentation av rutiner kan leda till att det inte finns ett gemensamt arbetssätt för exempelvis testförfarande, behörighetshantering eller produktionssättning och därmed kan viktiga kontroller utebli eller kringgås.
Rekommendation	Kulturhuset Stadsteatern AB bör uppdatera rutiner för programförändringsprocessen samt behörighetsprocessen där periodisk genomgång och regelbundna uppdateringar bör ingå. Dessa rutiner bör baseras på Stockholms Stads centrala riktlinjer.

Bristande spårbarhet i de periodiska genomgångarna av tilldelade behörigheter

Iakttagelse

För Visma finns en rutin för periodisk genomgång av användare i systemet och denna utförs årligen av systemförvaltaren. Vid vår granskning noterade vi att systemägaren inte godkänner och därmed inte heller ansvarar för resultatet av den periodiska genomgången. Vi noterade även att utförandet och resultatet inte dokumenteras.

Risk

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

Rekommendation

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

Återläsningstester genomförs inte för servrar hos Volvo IT

Iakttagelse

Volvo IT tar regelbundet backuper enligt avtalet mellan Volvo IT och Stockholms Stad. Volvo IT genomför dock inte återläsningstester. Återläsningstester måste beställas av Micasa Fastigheter AB. Vid vår granskning noterade vi att Micasa Fastigheter AB inte beställer återläsningstester från Volvo IT och att återläsningstester därför inte genomförs regelbundet.

Risk

Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.

Rekommendation

Micasa Fastigheter AB bör, utifrån ett riskbaserat synsätt, regelbundet säkerställa möjligheten att återläsa data och system, till exempel genom att genomföra återläsningstester. Micasa Fastigheter AB bör även säkerställa att FFG gör likvärdig kvalitetssäkring för FASAD, samt att de dokumentera och kommunicera resultaten.

Bristande tydlighet av roller och ansvarsfördelning i behörighetsprocessen

Iakttagelse

Micasa Fastigheter AB har en dokumenterad processbeskrivning för tilldelning av nya behörigheter. Vid vår granskning noterade vi att roller och ansvarsfördelning saknas i denna rutin, till exempel vem som är behörig att beställa, godkänna och effektuera beställningen.

Risk

Bristande dokumentation av roller och ansvarsfördelning i behörighetshanteringen innebär ökad risk att viktiga kontroller kringgås vilket i sin tur kan leda till att olämpliga behörigheter tilldelas.

Rekommendation

Micasa Fastigheter AB bör säkerställa en god arbetsfördelning samt dokumentera roller och ansvar i den befintliga processbeskrivningen av tilldelning av nya behörigheter. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Bristande dokumentation av rutiner för programförändringar

Iakttagelse	Micasa Fastigheter AB har utvecklingsstopp i Visma och därför har inga förändringar genomförts under 2013. Vid vår granskning noterade vi att det inte finns en dokumenterad rutin för programförändringar.
Risk	Bristande dokumentation 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.
Rekommendation	När nyutveckling i ekonomisystemet åter blir aktuellt bör Micasa Fastigheter AB säkerställa en rutin för god arbetsfördelning och dokumentation för programförändringar. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Bristande dokumentation av rutiner för programförändringar

Iakttagelse

Programförändringar hos SISAB följer olika rutiner beroende på omfattning av ändringen. Vid vår granskning noterade vi att dessa rutiner inte finns dokumenterade.

Risk

Bristande dokumentation 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.

Rekommendation

SISAB bör säkerställa en rutin för god arbetsfördelning och dokumentation för programförändringar samt regelbundet granska och uppdatera rutinerna vid behov. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Bristande spårbarhet av godkännande för produktionssättning vid mindre programförändringar

Iakttagelse	Beslut för produktionssättning av mindre programförändringar fattas av förvaltningsansvarig i samråd med IT-avdelningen. Vid vår granskning noterade vi att ingen dokumentation av godkännande för produktionssättning sker vid mindre programförändringar.
Risk	Bristande ansvarsfördelning i programförändringsprocessen ökar risken att felaktiga ändringar implementeras i produktionsmiljön.
Rekommendation	SISAB bör säkerställa god dokumentation av viktiga kontroller i programförändringsprocessen så som resultat av användartester samt godkännande för produktionssättning för samtliga ändringar. God dokumentation vid förändringar underlättar till exempel vid eventuellt behov av felsökning.

Systemleverantören Unit4 har konstant access till produktionsmiljön

Iakttagelse	SISAB har i avtal med Volvo IT krav på konstant access till sina servrar för att garantera högre produktionssäkerhet. Vid vår granskning noterades att SISAB medvetet tillåter att systemleverantören UNIT4 har administratörskonton med konstant access till SISABs produktionsmiljö. I kommentar från SISAB vill de poängtera att de är medvetna om de permanenta behörigheter och att de, för att garantera högre produktionssäkerhet, beslutat att fortsätta med dessa tills Volvo-IT kan leverera temporära behörigheter inom rimlig tid.
Risk	Obegränsad access till produktionsmiljön ökar risken för obehörig åtkomst till applikationerna samt risk för att ändringar som inte är godkända implementeras.
Rekommendation	SISAB bör slutföra arbetet med att begränsa leverantörens accesser till produktionsmiljön.

Bristande spårbarhet i de periodiska genomgångarna av behörigheter

Iakttagelse	Granskning av behörigheter görs regelbundet av systemägarna. Vid vår granskning noterades att endast kritiska avvikelser dokumenteras vid genomgångarna men det totala resultatet av genomgången dokumenteras inte.
Risk	Bristande spårbarhet i utförandet av kontroller i behörighetsprocessen ökar risken för att personer som inte längre arbetar kvar eller har fått ändrade arbetsuppgifter har kvar gamla eller felaktiga behörigheter i systemen.
Rekommendation	SISAB bör dokumentera resultatet av de periodiska genomgångna av samtliga behörigheter. (Se även vidare iakttagelse avseende bristande dokumentation av rutiner för periodisk granskning av behörighetsnivåer)

Bristande dokumentation av rutiner för periodisk granskning av behörighetsnivåer

Iakttagelse

Systemägaren för varje system ansvarar för att genomföra granskningar av samtliga behörigheter i systemen. Vid vår granskning noterade vi att det inte finns dokumenterade rutiner för hur dessa granskningar ska genomföras samt att processen inte är gemensam för samtliga systemägare.

Risk

Bristande dokumentation av rutiner ökar risken för att rutiner inte följs och att viktiga kontroller kringgås.

Rekommendation

SISAB bör dokumentera rutinen för periodisk granskning av tilldelade behörighetsnivåer och säkerställa att den är gemensam för samtliga applikationer samt att genomgången involverar systemägaren. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Bristande spårbarhet av återläsningstester

Iakttagelse

SISAB genomför återläsningstester regelbundet då de flyttar backuper till testmiljö och verifierar att de fungerar. Agresso flyttas till testmiljö varannan månad och Vitec en gång per halvår. Vid vår granskning noterade vi att dessa återläsningstester inte dokumenteras.

Risk

Bristande spårbarhet av återläsningstester ökar risken för att data går förlorad och inte kan läsas tillbaka trots att backuper har tagits.

Rekommendation

SISAB bör dokumentera rutiner, utförande och resultat av samtliga återläsningstester. Detta underlättar bland annat vid eventuellt behov av felsökning.

Avsaknad av regelbundna återläsningstester

Iakttagelse

S:t Erik Försäkring AB tar regelbundet backuper av sina system. Vid vår granskning noterade vi att inga formaliserade regelbundna återläsningstester genomförs på dessa, dessutom dokumenteras inte resultatet.

Risk

Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.

Rekommendation

S:t Erik Försäkring AB bör, utifrån ett riskbaserat synsätt, införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa åtgärder.

Avsaknad av regelbundna återläsningstester

Iakttagelse	S:t Erik Livförsäkring AB tar regelbundet backuper av sina system. Vid vår granskning noterade vi att inga formaliserade regelbundna återläsningstester genomförs på dessa, dessutom dokumenteras inte resultatet.
Risk	Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.
Rekommendation	S:t Erik Livförsäkring AB bör, utifrån ett riskbaserat synsätt, införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa åtgärder.

Avsaknad av dokumenterade rutiner för tilldelning av nya behörigheter

Iakttagelse

Tilldelning av nya behörigheter görs av den administrative chefen och controllern, dessa har översyn över personal som ska ha tillgång till systemet. Vid tiden för vår granskning noterades att det inte fanns någon dokumenterad rutin för tilldelning av nya behörigheter. Under granskningens gång har detta däremot åtgärdats och en dokumenterad rutin har nu upprättats.

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 samt att personer med ändrade arbetsuppgifter har kvar gamla behörigheter i systemen.

Rekommendation

Stockholm Business Region AB bör tillse att rutinen som nu upprättats implementeras samt regelbundet se över rutinerna för tilldelning av nya behörigheter för att säkerställa att de är uppdaterade och ändamålsenliga.

Avsaknad av formaliserad rutin för periodisk granskning av tilldelade behörighetsnivåer i Visma

Iakttagelse

När en anställd slutar på Stockholm Business Region (SBR) skickas ett mail automatiskt från löneavdelningen på SBR till Volvo IT och Volvo IT skickar sedan mailet vidare till den administrativa chefen på SBR som ser till att användarens konto avslutas. Den administrativa chefen går emellanåt igenom behörigheterna i Visma. Vid tiden för vår granskning noterades att det inte fanns någon rutin för hur den periodiska genomgången genomfördes och utförandet dokumenterades inte. Under granskningens gång har detta däremot åtgärdats och en dokumenterad rutin har nu upprättats.

Risk

Avsaknaden 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 applikationskontroller.

Rekommendation

Stockholm Business Region AB bör tillse att rutinen som nu har upprättats implementeras samt regelbundet se över rutinerna för att periodiskt granska samtliga behörigheter för att säkerställa att de är uppdaterade och ändamålsenliga.

Avsaknad av dokumenterad rutin för programförändringsprocessen

Iakttagelse	IT-samordnaren är kontaktperson mot leverantören och även den som beställer programförändringar av leverantören. Leverantören utvecklar och installerar sedan programförändringarna på plats hos Stockholm Business Region. Vid tiden för vår granskning noterade vi att det inte fanns någon dokumenterad rutin för programförändringsprocessen. Under granskningens gång har Stockholm Business Region däremot påbörjat ett arbete för att dokumentera rutiner för programförändringsprocessen.
Risk	Bristande dokumentation 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.
Rekommendation	Stockholm Business Region bör slutföra arbetet med att dokumentera rutiner för programförändringar samt regelbundet granska och uppdatera rutinerna vid behov.

Gruppkonton med opersonliga namn förekommer i Agresso

Iakttagelse

Vid vår granskning noterade vi att leverantören Agresso använder sig av gruppkonton med opersonliga namn. För att konsulter från systemleverantören ska få åtkomst till produktionsmiljön använder sig Stockholm Hamn av Start Stockholm vilket innebär att Stockholm Hamn får en sms-kod som de sedan meddelar leverantören när leverantören ska komma in i Stockholm Stads Active Directory och därmed även Agresso. Det ska ske en manuell logg över när leverantören har varit inne i produktionsmiljön, men det har visat sig att denna rutin inte fungerar. Däremot går det att se i windowsloggen när en inloggning har skett.

Risk

Användning av gruppkonton ökar risken för obehörig åtkomst till system och information. Gruppkonton innebär att spårbarheten minskar då det inte går att följa vem som har varit inne i systemet eller att koppla utförda aktiviteter till individer vid exempelvis felsökning.

Rekommendation

Stockholms Hamn AB bör säkerställa att enbart personliga konton används för åtkomst till samtliga applikationer, databaser och servrar. I de undantagsfall detta ej är möjligt ska detta noteras och beslut om undantag fattas och dokumenteras.

Bristande spårbarhet gällande leverantörers inloggning i produktionsmiljön

Iakttagelse

För produktionssättning på Stockholm Hamns egna servrar används Start Stockholm. När leverantören ska genomföra en produktionssättning får Stockholm Hamn en sms-kod som de sedan meddelar leverantören. När koden har använts försvinner den från telefonen. Det ska ske en manuell logg över när leverantören har varit inne i produktionsmiljön, men det har visat sig att denna rutin inte fungerar. Däremot går det att se i windowsloggen när en inloggning har skett.

Risk

Att inte logga kritiska aktiviteter relaterat till användarkonton innebär att spårbarheten begränsas då det inte går att följa vem som har varit inne i systemet eller att koppla utförda aktiviteter till varken leverantör eller individ.

Rekommendation

Stockholms Hamn AB bör säkerställa att kritiska aktiviteter i produktionsmiljön dokumenteras vilket bör inkludera leverantörers inloggning i produktionsmiljön dokumenteras.

Bristande dokumentation av godkännande för produktionssättning för mindre programförändringar

Iakttagelse

Vid större programförändringar ska beslut tas av IT-rådet och dessa möten ska protokollföras. Vid mindre förändringar tar systemförvaltaren beslut om produktionssättning. Vid vår granskning noterade vi att godkännande för produktionssättning vid mindre förändringar inte dokumenteras.

Risk

Bristande ansvarsfördelning och dokumentation i programförändringsprocessen ökar risken att felaktiga ändringar implementeras i produktionsmiljön.

Rekommendation

Stockholms Hamn AB bör dokumentera godkännande för produktionssättning för samtliga programförändringar. Vid akuta ändringar kan godkännande dokumenteras i efterhand. God dokumentation kan underlätta vid till exempel behov av felsökning.

Återläsningstester genomförs inte för servrar hos Volvo IT

Iakttagelse

Stockholms Hamn har servrar både på plats i Hamnen samt hos Volvo IT. För de servrar som finns hos Volvo IT tar Volvo regelbundet backuper. Återläsningstester måste dock beställas av Volvo IT. Under vår granskning noterades att Stockholms Hamn inte har 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 Hamn AB bör, utifrån ett riskbaserat synsätt, införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa åtgärder.

Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer

Iakttagelse

Stockholms Hamn AB använder sig av ett system som heter Ordning och Reda för hantering av bland annat behörigheter. Ordning och reda är kopplat till HR-systemet och om någon slutar på Stockholms Hamn avslutas automatiskt alla konton kopplade till personen. Vid vår granskning noterades att ingen genomgång av aktiva användares behörighetsnivåer görs.

Risk

Avsaknad av rutin för genomgång av behörighetsnivåer ökar risken för obehörig åtkomst till applikationerna. Det ökar även risken för att personer med ändrade arbetsuppgifter har kvar gamla behörigheter i systemen vilket kan användas för att kringgå applikationskontroller.

Rekommendation

Stockholms Hamn AB bör införa en rutin för att periodiskt granska samtliga behörigheter i applikationerna. Rutinen bör ta hänsyn till användarnas behörighetsnivåer och resultatet bör dokumenteras. Vidare bör systemägare godkänna resultatet. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Samtliga användare i Agresso som arbetar på ekonomiavdelningen har behörighetsnivån superuser

Iakttagelse

Samtliga användare i Agresso som arbetar på ekonomiavdelningen har behörighetsnivån superuser. Vi noterade även att ekonomichefen har behörighet att både godkänna och lägga upp en ny användare i Agresso.

Risk

Att användare har högre behörigheter än de som är nödvändiga för de specifika arbetsuppgifterna ökar risken för obehörig åtkomst till applikationer och information. Detta kan i sin tur innebära en risk för avsiktliga eller oavsiktliga fel.

Rekommendation

Stockholms Hamn AB bör säkerställa att alla användare har behörigheter som är relevanta för individens roll samt begränsa behörigheterna för användare som har högre behörigheter än nödvändigt.

Lösenordsinställningar för användarkonton i Agresso följer inte Stockholms Stads riktlinjer för informationssäkerhet

Iakttagelse	För att logga in i Agresso krävs först en inloggning i nätverket via Active Directory och sedan en separat inloggning i Agresso. Under granskningen noterades att de lösenordsinställningar som finns i Agresso inte möter de krav som ställs i Stockholms Stads riktlinjer för informationssäkerhet.
Risk	Svaga krav på lösenord ökar risken för obehörig åtkomst till applikationerna.
Rekommendation	Stockholms Hamn AB bör uppfylla lösenordskraven i Stockholms Stads riktlinjer.

Bristande dokumentation av processen för tilldelning av behörigheter

Iakttagelse

All behörighetshantering sker i systemet Ordning & Reda. Alla har rätt att beställa behörighet i systemet men det skall godkännas av systemägaren. Systemägarrepresentanten har sedan behörighet att lägga upp behörigheten i systemet. Vid vår granskning noterade vi att denna process inte finns dokumenterad.

Risk

Bristande dokumentation av rutiner ökar risken för att rutiner inte följs och att viktiga kontroller kringgås. Avsaknad av dokumentation försvårar även kommunikation och införande av rutiner.

Rekommendation

Stockholms Hamn AB bör dokumentera processen för tilldelning av behörigheter. Processen bör tydliggöra roller och ansvar gällande vem som får beställa en behörighet, godkänna samt effektuera beställningen.

Bristande dokumentation av rutiner för periodisk granskning av behörighetsnivåer

Iakttagelse	I samband med personalförändringar gör Stockholm Parkering en genomgång av behörighetsnivåer, men det finns ingen dokumenterad rutin för den periodiska genomgången. Nya rutiner kommer att tas fram i samband med att det nya verksamhetssystemet går i produktion.
Risk	Avsaknad av rutin för genomgång av behörighetsnivåer ökar risken för obehörig åtkomst till applikationerna. Det ökar även risken för att personer med ändrade arbetsuppgifter har kvar gamla behörigheter i systemen vilket kan användas för att kringgå applikationskontroller.
Rekommendation	Stockholm Parkering bör färdigställa arbetet med att införa en rutin för periodisk granskning av tilldelade behörighetsnivåer. Vidare bör systemägare godkänna resultatet. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Bristande rutiner och spårbarhet för återläsningstester

Iakttagelse

Stadsledningskontoret genomför med jämna mellanrum återläsningstester för Cognos. Vid vår granskning noterade vi att det inte finns någon dokumenterad rutin för genomförandet av regelbundna återläsningstester, det genomförs istället efter behov.

Risk

Avsaknad av rutin för regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.

Rekommendation

Stockholms Stadshus AB bör i dialog med Stadsledningskontoret och utifrån ett riskbaserat synsätt införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa åtgärder.

Svag beställningsprocess för nya behörigheter

Iakttagelse	Vid behörighetsbeställningar i Cognos mailas koncernredovisningsansvarig på Stadsledningskontoret angående beställningen. Volvo IT måste sedan beställa en behörighetsgrupp för Cognos till den aktuella användaren. När behörighetsgruppen är upplagd skapar koncernredovisningsansvarig en användare som han tilldelar aktuella behörigheter. Vid vår granskning noterade vi att beställningsprocessen för nya behörigheter är svag då den enbart går via mail.
Risk	Svaga beställningsprocesser för nya behörigheter ökar risken för att fel personer får åtkomst till systemen.
Rekommendation	Stockholms Stadshus AB bör i dialog med Stadsledningskontoret införa en formaliserad process för beställning av nya behörigheter i Cognos.

Gruppkonton förekommer i Cognos

Iakttagelse	Vid vår granskning noterades att Tieto använder sig av gruppkonton för åtkomst till Cognos.
Risk	Användning av gruppkonton ökar risken för obehörig åtkomst till system och information. Gruppkonton innebär att spårbarheten minskar då det inte går att följa vem som har varit inne i systemet eller att koppla utförda aktiviteter till individer vid exempelvis felsökning.
Rekommendation	Stockholms Stadshus AB bör i dialog med Stadsledningskontoret säkerställa att enbart personliga konton används för åtkomst till Cognos. I de undantagsfall detta inte är möjligt ska detta noteras och beslut om undantag fattas och dokumenteras.

Viktiga kontroller i programförändringsprocessen sker informellt och dokumenteras inte

Iakttagelse

Processen för programförändringar hos Stockholms Stads Bostadsförmedling skiljer sig åt beroende på system, då de själva sköter utvecklingen för Bostoc medan en leverantör genomför utvecklingen för Raindance. Vid vår granskning noterades att en del av kontrollerna i programförändringsprocessen sker informellt och att det inte finns någon dokumenterad rutin.

Risk

Att inte dokumentera viktiga kontrollsteg som testning och godkännande för produktionssättning försämrar spårbarheten vid till exempel felsökning, beslut och test av funktionalitet.

Rekommendation

Stockholms Stads Bostadsförmedling AB bör dokumentera, kommunicera samt implementera programförändringsprocessen för respektive system där det framgår hur viktiga kontrollsteg i processen ska utföras samt hur resultatet av genomförda kontrollsteg (godkännanden med mera) ska dokumenteras. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer i Raindance

Iakttagelse	När en ny användare med attestantbehörighet läggs upp i Raindance ändras attestantförteckningen och då granskas samt godkänns den på nytt. Stockholms Stads Bostadsförmedling genomför även en granskning av leverantörsloggar kvartalsvis. Vid vår granskning noterades att det inte finns några dokumenterade rutiner för periodisk genomgång av samtliga användare och behörighetsnivåer i systemet samt att detta inte genomförs.
Risk	Avsaknaden 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.
Rekommendation	Stockholms Stads Bostadsförmedling AB bör införa en rutin för att periodiskt granska samtliga behörigheter i Raindance. Rutinen bör ta hänsyn till användarnas behörighetsnivåer och resultatet bör dokumenteras. Vidare bör systemägare godkänna resultatet. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Lösenordsinställningar för användarkonton i Raindance följer inte Stockholms Stads riktlinjer för informationssäkerhet

Iakttagelse	För att logga in i applikationen Raindance krävs en första inloggning i Active Directory. Vid vår granskning noterades att det inte finns några lösenordsinställningar som krav på komplexitet, byte efter ett begränsat antal dagar eller antal tecken i Raindance vilket inte följer Stockholms Stads riktlinjer för informationssäkerhet.
Risk	Svaga krav på lösenord ökar risken för obehörig åtkomst till applikationen.
Rekommendation	Stockholms Stads Bostadsförmedling AB bör säkerställa att användarkonton i samtliga applikationer följer Stockholms Stads riktlinjer för informationssäkerhet.

Återläsningstester genomförs inte för servrar hos Volvo IT

Iakttagelse

När programförändringar ska implementeras i testmiljö sätts den senaste huvudbackupen upp som testmiljö. Detta innebär att återläsningstest genomförs inför nya programförändringar. Vid vår granskning noterade vi dock att återläsningstester inte genomförs regelbundet efter rutin samt att utförandet och resultatet inte dokumenteras.

Risk

Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.

Rekommendation

Stockholms Stads Bostadsförmedling AB bör, utifrån ett riskbaserat synsätt, införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa

Avsaknad av dokumenterad rutin för tilldelning av nya behörigheter

Iakttagelse	Vid tilldelning av nya behörigheter krävs ett godkännande av ansvarig chef samt att en behörighetsadministratör effektuerar beställningen. Vid vår granskning noterades att rutinen för tilldelning av nya behörigheter inte finns dokumenterad.
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 samt att personer med ändrade arbetsuppgifter har kvar gamla behörigheter i systemen.
Rekommendation	Stockholms Stads Bostadsförmedling AB bör dokumentera, kommunicera och implementera rutiner för tilldelning av nya behörigheter. Dessa rutiner bör bygga på Stockholms Stads centrala riktlinjer.

Bristande spårbarhet i genomgångar av höga behörigheter i Agresso

Iakttagelse	Systemförvaltaren administrerar samtliga behörigheter i Agresso och granskar regelbundet användare med höga behörigheter. Vid vår granskning noterade vi att genomgången av höga behörigheter inte dokumenteras och sparas.
Risk	Avsaknaden 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.
Rekommendation	Stockholm Vatten AB bör dokumentera genomgångar av samtliga behörigheter. Vidare bör genomgången godkännas av systemägare eller chef.

Avsaknad av delaktighet från systemägare vid den periodiska genomgången av behörigheter i Agresso

Iakttagelse	Användare med höga behörigheter granskas regelbundet av systemförvaltaren. Vid vår granskning noterade vi att systemägaren inte godkänner och därmed ansvarar för resultatet av den periodiska genomgången.
Risk	Avsaknaden 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.
Rekommendation	Stockholm Vatten AB bör säkerställa att systemägaren är delaktig samt godkänner den periodiska genomgången. Dessutom bör godkännandet dokumenteras.

Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer i Lettera

Iakttagelse	Systemförvaltaren administrerar samtliga behörigheter i Lettera. Vid vår granskning noterades att det inte finns någon process på plats för att regelbundet granska samtliga behörigheter.
Risk	Avsaknad av rutin för genomgång av behörighetsnivåer ökar risken för obehörig åtkomst till applikationen. Det ökar även risken för att personer med ändrade arbetsuppgifter har kvar gamla behörigheter i system vilket kan användas för att kringgå applikationskontroller och ändamålsenlig ansvarsfördelning.
Rekommendation	Stockholm Vatten AB bör upprätta en rutin för att periodiskt gå igenom behörigheter samt ta hänsyn till behörighetsnivåer. Systemägare eller chef bör granska behörigheterna och säkerställa att resultatet av genomgången dokumenteras. Denna rutin bör baseras på Stockholms Stads riktlinjer.

Konton med generiska namn förekommer i Agresso

Iakttagelse

Utveckling och implementering av programförändringar i produktionsmiljön för Agresso genomförs av leverantören Agresso. Vid vår granskning noterade vi att leverantören har ett supportkonto i form av gruppkonto som används vid supportärenden. Syftet med detta konto är alltså inte att använda det för utveckling eller implementering av ändringar.

Risk

Användning av konton med generiska namn innebär att spårbarheten minskar då det inte går att följa vem som har varit inne i systemet eller att koppla utförda aktiviteter till individen.

Rekommendation

Stockholm Vatten AB bör säkerställa att enbart personliga konton används för åtkomst till samtliga applikationer, databaser och servrar. I de undantagsfall detta inte är möjligt ska avvikelsen noteras och beslut om undantag fattas och dokumenteras.

Återläsningstester beställs och genomförs inte regelbundet

Iakttagelse	Volvo IT tar regelbundet backuper enligt avtalet mellan Volvo IT och Stockholms Stad och återläsningstester måste beställas av Stockholm Vatten vilket genomförs regelbundet (1ggr/vecka) på en slumpmässigt utvald Windows Server och en katalog. Vid vår granskning noterades att Stockholm Vatten inte beställer återläsningstester för Agresso och Lettera av Volvo IT samt att utförande och resultat av återläsning inte dokumenteras.
Risk	Avsaknad av regelbundna återläsningstester ökar risken för att kritiska system inte går att återställa vid en incident.
Rekommendation	Stockholm Vatten AB bör, utifrån ett riskbaserat synsätt, införa rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa.

Sektion 4

Appendix

Granskningsdetaljer

Utvärderingskriterier i detalj

Följande kontrollmål och områden är fokus i granskningen:

- **Programförändringar:**

  1: Att programförändringar är godkända för utveckling
  2: Att programförändringar är testade
  3: Att programförändringar är godkända för införande i produktionsmiljön
  4: Att programförändringar övervakas
  5: Att det existerar ändamålsenlig ansvarsfördelning inom programförändringsprocessen

- **Åtkomst:**

  1: Att systemkonfiguration är lämplig
  2: Att lösenordsinställningar är lämpliga
  3: Att höga behörigheter är begränsat till lämpligt antal användare
  4: Att behörigheter till resurser som applikationen använder (databaser, operativsystem) är begränsat till lämpligt antal användare
  5: Att behörigheter är godkända vid både:
     a. Upplägg av nya behörigheter
     b. Regelbunden granskning av behörigheter
  6: Att fysisk säkerhet är begränsat till lämpligt antal individer
  7: Att behörighetsprocessen övervakas
  8: Att det existerar ändamålsenlig ansvarsfördelning inom behörighetsprocessen

- **Stockholms stads riktlinjer för informationssäkerhet**

  Under vårt möte kommer vi även diskutera roller och ansvar kopplade till kontrollmålen ovan. Vi vill vidare mera allmänt avseende stadens riktlinjer för informationssäkerhet, täcka frågor kopplade till organisation för arbetet med informationssäkerhet, implementering av rutiner, informationsklassning samt riskanalys av de kritiska systemen.

Omfattade bolag och kontaktpersoner

Bolag	Kontaktpersoner
AB Familjebostäder	Ulla Ritzén, EA & Susanne Kilgren, IT
AB Stockholmshem	Bengt Kylerud & Allan Hansson, IT
AB Stokab	Hans Fornestig, EA & Martin Adamsson, IT
Kulturhuset Stadsteatern AB	Åke Wetterblad, IT & Malin Dahlberg, EA
Micasa Fastigheter AB	Annika Rapp, EA & Kristian Arenander, IT
SISAB	Joachim Quiding, IT chef & Joakim Ekman, IT
S:t Erik Försäkring AB	Jan Willgård
S:t Erik Livförsäkring AB	Jan Willgård
S:t Erik Markutveckling AB	Peter Kvarnhem, IT
Stockholm Business Region AB	Lena Häggdahl, EA + IT
Stockholm Globe Arena Fastigheter AB	Conny Karlsson, IT & Susanne Tiderman, EA
Stockholms Hamn AB	Björn Hellerström, IT & Mats Lundin, EA
Stockholm Parkering AB	Ronny Hedman, IT & Boris Amsköld, EA
Stockholms Stadshus AB	Sara Feinberg
Stockholms Stads Bostadsförmedling AB	Mats Bothén & David Mancilla, IT
Stockholm Vatten AB	Lars Storm, IT & Torbjörn Lundgren, IT
Svenska Bostäder	Mikael Österberg, IT


Tack
EY
Building a better
working world