Stockholms Stadshus AB

Granskning av IT-intern kontroll
11 December 2014

EY
Building a better working world

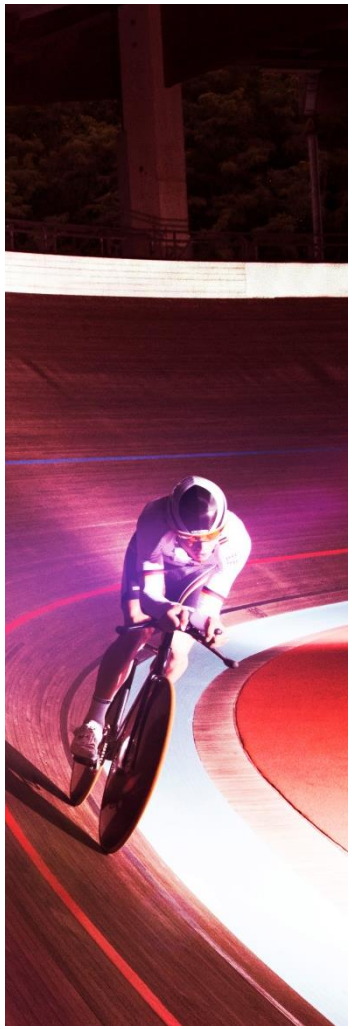
Innehåll

Inledning

Sektion 1

Sammanfattning

- Baserat på 2013-års granskning har Stockholm Stadshus AB uppdragit åt EY att göra en uppföljande genomgång av intern kontroll inom IT för utvalda bolag inom koncernen. Fokus ligger som tidigare på kontrollmiljö i relation till behörigheter och hantering av förändringar i applikationer som stödjer finansiell rapportering. Granskningens omfattning har för varje enskilt bolag prioriterats i relation till föregående års iakttagelser.
- Sammanfattningsvis kan konstateras en ökad medvetenhet om vikten av en god intern kontroll. Merparten av bolagen har utfört, respektive är i färd med att utföra åtskilliga förbättringsåtgärder i förhållande till de rekommendationer som tidigare förts fram av EY. I de fall åtgärder fortfarande håller på att implementeras är det nu viktigt att uppdaterade rutiner kommuniceras och införs. Stadens nya direktiv om ett gemensamt ekonomisystem innebär också att flera bolag hänvisar till att fortsatt utveckling av processer och kontroller kommer vid implementering av detta.
- I följande delar av rapporten beskrivs genomförd granskning och resultatet av denna, i översikt och på bolagsnivå. Som mera generella iakttagelser kan noteras:
  - Rutiner kopplat till processen för programförändringar följs inte fullt ut.
  - Brister i rutiner för periodisk genomgång av behörigheter.
  - Möjligheten till strukturerad rutin för återläsningstester.
- Även om flertalet av iakttagelserna bör hanteras inom rimlig tid, bedöms ingen av observationerna vara av karaktären att de innebär en omedelbar risk för verksamheten inom Stockholms stad.
- Stockholms Stadshus AB rekommenderas att kommunicera iakttagelser till respektive dotterbolag för utvärdering och åtgärd.



Introduktion

Sektion 2

Bakgrund och syfte

- Stockholms Stadshus AB har beslutat att genomföra en uppföljning av den granskning av IT intern kontroll och informationssäkerhet som utfördes 2013.
- 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.
- Granskningen har genomförts genom intervjuer med områdesansvariga inom de olika bolagen samt genomgång av tillhandahållen dokumentation.

Omfattning av granskning

- Storleken på årets granskning bygger på de iakttagelser som gjordes 2013 och prioriteras i relation till hur pass kritiska de ansetts vara för organisationen. Dotterbolagen är uppdelade och prioriterade i tre olika nivåer:
  - **Bolag med högre prioritering**
    - Uppföljning av rekommendationer.
    - Genomgång av processer programförändringar, behörighetshantering, lösenordsinställningar och/eller backuphantering.
    - Test av ett stickprov.
  - **Bolag med lägre prioritering**
    - Uppföljning av rekommendationer.
  - **Bolag utan behov av uppföljning**
    - De bolag som är exkluderade har inte haft några iakttagelser av högre dignitet.

Högre prioritering	Lägre prioritering	Ingen uppföljning
Stockholms Hamn AB	Stockholm Business Region AB	AB Stokab
MICASA AB	St. Eriks Livförsäkring AB	AB Familjebostäder
SISAB	St. Eriks Försäkring AB	Svenska bostäder
Stockholms Stadshus AB	Stockholm Parkering AB	Stockholm Globe Arena Fastigheter AB
Stockholm Vatten AB	Stockholms Stads Bostads-förmedling AB	St. Eriks Markutveckling AB
Kulturhuset / Stadsteatern AB	AB Stockholms-hem	

Utvärderingskriterier (1/2)

Följande områden har varit fokus i granskningen:

- **Programförändringar:**

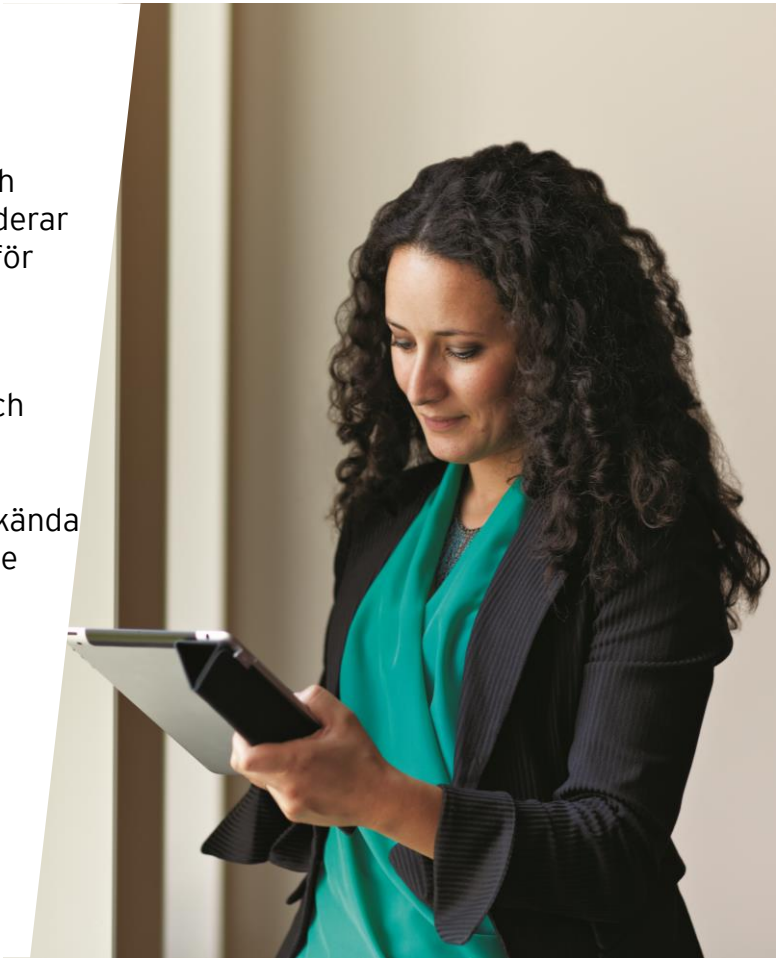
  Rutiner kring samt dokumentation av programförändringar och relaterade processer. Förväntade områden för kontroller inkluderar beställning, acceptanstest av förändringen och godkännande för produktionssättning.

- **Åtkomst:**

  Säkerställa lämplig antal användare med höga behörigheter och systemkonfiguration med passande lösenordsinställningar. Dessutom har granskningen innefattat behörighetsprocessens övervakning och dokumentation samt att behörigheter är godkända vid både tilldelning och vid regelbunden verifiering av tilldelade behörighetsnivåer.

- **Stockholms stads riktlinjer för informationssäkerhet:**

  Efterlevnad av stadens riktlinjer för informationssäkerhet i respektive bolags arbete med informationssäkerhet, införande 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.
	Godtagbar nivå, men där utrymme för åtgärd/förbättringar kan finnas.

Bolagsspecifika resultat

Sektion 3

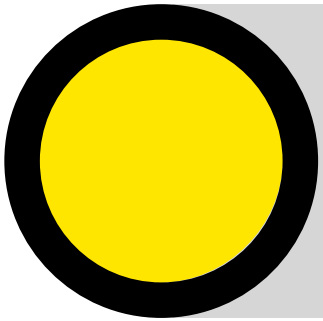
Översikt bolag

Bolag	Sida	Iakttagelser 2013	Iakttagelser 2014
Stockholms Hamn AB	12-13	🔴🔴🟡🟡🟡🟡🔴🟡	🟡🟢🟢🟢🟢🟢🟢🟢
MICASA AB	14-17	🔴🟡🟡🟡	🟡🟡🟢🟡
SISAB	18-19	🟡🟡🟡🟡🟡🟡	🟢🟢🟢🟢🟡🟡
Stockholms Stadshus AB	20-22	🟡🟡🟡	🟡🟢🟡
Stockholm Vatten AB	23-26	🔴🟡🟡🔴🟡	🟡🟡🟡🟢🟡
Kulturhuset / Stadsteatern AB	27-29	🔴🟡🟡🟡🟡	🟢🟢🟢🟢🟢🟡🟡
Stockholm Business Region AB	30	🟡🟡🟡	🟢🟢🟢
St. Eriks Livförsäkring AB	31	🔴	🟢
St. Eriks Försäkring AB	32-33	🔴	🟡
Stockholm Parkering AB	34	🟡	🟢
Stockholms Stads Bostads-förmedling AB	35-36	🔴🔴🔴🟡🟡	🟢🟢🟢🟢🟡
AB Stockholms-hem	37	🔴🟡🟡	🟢🟢🟢

Stockholms Hamn AB

2013	Iakttagelser	Status	2014
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Några återläsningstester har inte genomförts under året.	
	Gruppkonton förekommer i Agresso.	Stockholms Hamn AB använder sig av Start Stockholm för inloggning när externa leverantörer behöver åtkomst till Agresso. Det förs en manuell logg när leverantören efterfrågar access. Det går också att se i Windowsloggen när en inloggning har skett.	
	Bristande spårbarhet gällande leverantörers inloggning i produktionsmiljön.		
	Bristande dokumentation av godkännande för produktionssättning för mindre programförändringar.	Stockholm Hamn AB har tagit fram ett nytt testprotokoll med godkännande för införande i produktionsmiljön. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer.	Stockholm Hamn AB har utfört granskningar av aktiva användare i både Agresso och Port IT. Det är av vikt att denna process för periodisk granskning av tilldelade behörigheter formaliseras.	
	Samtliga användare i Agresso som arbetar på ekonomiavdelningen har behörighetsnivån super-user .	Stockholms Hamn AB har begränsat antalet användare med super-user access.	
	Lösenordsinställningar för användarkonton i Agresso följer inte Stockholms Stads riktlinjer för informationssäkerhet.	Stockholms hamn följer idag Stockholms Stads riktlinjer avseende lösenordskrav .	
	Bristande dokumentation av processen för tilldelning av behörigheter.	Stockholms Hamn har tagit fram en ny rutin för tilldelning av nya behörigheter, den finns beskriven i Ordning & Reda 3,0.	

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.

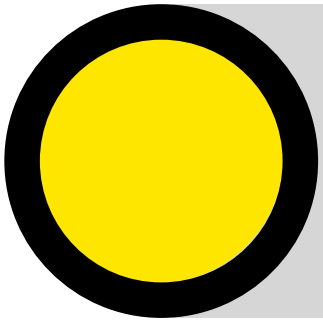
Rekommendation

I likhet med föregående år rekommenderar vi Stockholm Hamn AB att utifrån ett riskbaserat synsätt, överväga rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa.

MICASA

2013	Iakttagelser	Status	2014
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Några återläsningstester har inte genomförts under året.	
	Bristande spårbarhet i de periodiska genomgångarna av tilldelade behörigheter.	Micasa fastigheter AB har utfört den periodiska genomgången för Visma Control och Visma DCE under året och den finns dokumenterad med ansvarig kontrollägare. För fasad finns instruktion för hur sådana genomgångar ska genomföras och vem som ansvarar för dessa. Någon genomgång har ej utförts 2014.	
	Bristande tydlighet av roller och ansvarsfördelning i behörighetsprocessen.	Micasa fastigheter AB har tagit fram nya rutiner med ansvarsfördelning i behörighetsprocessen för Visma Control och Visma DCE samt Fasad. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Bristande dokumentation av rutiner för programförändringar.	Micasa Fastigheter AB har utvecklingsstopp i Visma och minimal utveckling av Fasad på grund av att systemen ska ersättas under 2015 respektive 2017. Detta innebär att inga resurser lagts på att utveckla nya rutiner för programförändringar till de befintliga systemen.	

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

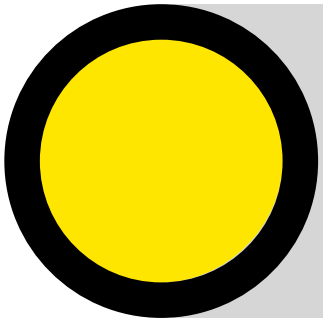
Risk

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

Rekommendation

I likhet med föregående år rekommenderar vi Micasa fastigheter AB att utifrån ett riskbaserat synsätt, överväga rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa.

Periodiska genomgångar av tilldelade behörigheter i Fasad



Iakttagelse

För Fasad finns en nyligen framtagen instruktion för hur periodiska genomgångar av tilldelade behörigheter ska genomföras och vem som ansvarar för dessa. Någon genomgång har ej utförts 2014.

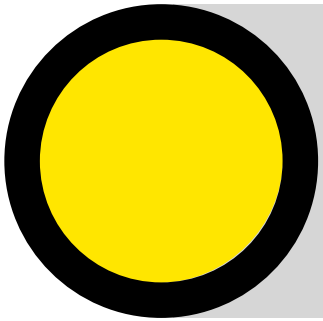
Risk

Avsaknaden av periodisk genomgång av användare ökar risken för att personer som inte längre arbetar kvar eller har fått ändrade arbetsuppgifter har kvar gamla eller felaktiga behörigheter i systemen.

Rekommendation

Micasa Fastigheter AB bör förankra den nya rutinen i verksamheten och säkerhetsställa att periodisk genomgång genomförs.

Bristande dokumentation av rutiner för programförändringar



Iakttagelse

Micasa Fastigheter AB har utvecklingsstopp i Visma och minimal utveckling av Fasad på grund av att systemen ska ersättas under 2015 respektive 2017. Detta innebär att inga resurser lagts på att utveckla nya rutiner för programförändringar till de befintliga systemen.

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.

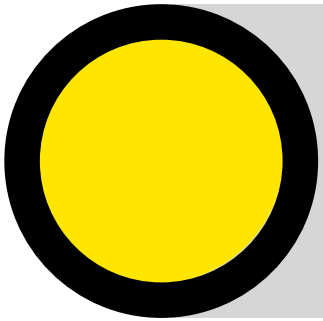
Rekommendation

Eftersom utvekling av Fasad fortfarande är aktuell bör Micasa fastigheter AB säkerställa en rutin för god internkontroll med god ansvarsfördelning och spårbarhet av kontroller inom processen. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

SISAB

2013	Iakttagelser	Status	2014
	Bristande spårbarhet av återläsningstester.	SISAB har utfört ett återläsningstest och dokumenterat resultatet.	
	Bristande dokumentation av rutiner för programförändringar.	SISAB har tagit fram och dokumenterat en ny rutin för förändringshanteringen som bygger på stadens F-guide och som gäller för samtliga programförändringar. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Bristande spårbarhet av godkännande för produktionssättning vid mindre programförändringar.		
	Systemleverantören Unit4 har konstant access till produktionsmiljön.	Efter förhandlingar med Volvo-IT angående tid på leverans av behörigheter har SISAB nu gått över till att begränsa Unit4´s access till produktionsmiljön.	
	Bristande spårbarhet i de periodiska genomgångarna av behörigheter.	SISAB har tagit fram en årsplan där de systemansvariga planerar in när de periodiska genomgångarna ska utföras. Dock fanns inga exempel på utförda behörighetsgenomgångar i samband med vår granskning. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Bristande dokumentation av rutiner för periodisk granskning av behörighetsnivåer.		

Periodiska genomgångar av tilldelade behörigheter



Iakttagelse

Inom SISAB finns en nyligen framtagen instruktion för hur periodiska genomgångar av tilldelade behörigheter ska genomföras och vem som ansvarar för dessa. Någon genomgång har ej utförts 2014.

Risk

Avsaknaden av periodisk genomgång av användare ökar risken för att personer som inte längre arbetar kvar eller har fått ändrade arbetsuppgifter har kvar gamla eller felaktiga behörigheter i systemen.

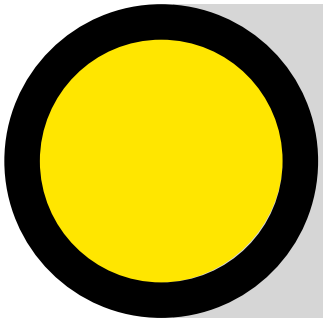
Rekommendation

SISAB bör förankra den nya rutinen i verksamheten och säkerhetsställa att periodisk genomgång genomförs.

Stockholms Stadshus AB

2013	Iakttagelser	Status	2014
	Bristande rutiner och spårbarhet för återläsningstester.	Tieto genomför med jämna mellanrum återläsningstester för Cognos. Dock finns det ej några dokumenterade resultat.	
	Svag beställningsprocess för nya behörigheter.	Stockholms Stadshus AB har en ny rutin för tilldelning av behörigheter i Cognos .	
	Gruppkonton förekommer i Cognos.	Stockholm stadshus har vidtagit åtgärder under året för att ersätta gruppkonton I Cognos med individuella konton. Det finns dock några konton med delad access.	

Bristande rutiner och spårbarhet för återläsningstester



Iakttagelse

Tieto genomför med jämna mellanrum återläsningstester för Cognos. Vid vår granskning noterade vi att det inte finns några dokumenterade resultat av dessa återläsningstester.

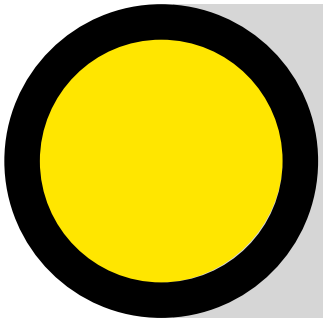
Risk

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

Rekommendation

Stockholm stadshus AB bör fortsätt arbetet med att regelbundet utföra återläsningstester utifrån ett riskbaserat synsätt för att säkerställa möjlighet att återläsa data och system, samt dokumentera resultatet av dessa.

Gruppkonton förekommer i Cognos



Iakttagelse

Stockholm stadshus har vidtagit åtgärder under året för att ersätta gruppkonton I Cognos med individuella konton. Det finns dock några konton med delad access. Exempel på detta är ett administratörskonto som används av Tieto

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. Ett administratörskonto ger vanligtvis obegränsad access till applikationen och medför därför en särskild risk.

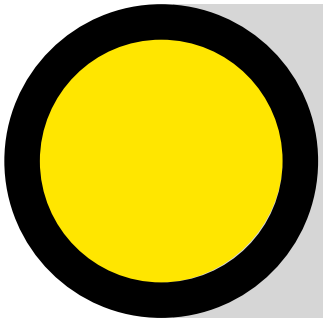
Rekommendation

Vi rekomederar Stockholms stadshus AB att utvärdera behovet av och möjligheten till att särskilt monitorera användandet av administratörskontot I Cognos.

Stockholm Vatten AB

2013	Iakttagelser	Status	2014
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Några återläsningstester har inte genomförts under året.	
	Bristande spårbarhet i genomgångar av höga behörigheter i Agresso.	Stockholm Vatten AB har tagit fram en ny kvartalsvis rutin för att granska de användare som slutat. Rutinen innebär att systemägaren tillika administrativ chef signerar dokumentet och står som yttersta ansvarig. Vi har dock noterat att priviligierade användare samt användare som bytt arbetsuppgifter inte omfattas av denna granskning.	
	Avsaknad av delaktighet från systemägare vid den periodiska genomgången av behörigheter i Agresso.		
	Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer i Lettera.	Stockholms Vatten AB har tagit fram en ny kvartalsvis rutin och den utförs av systemadministratören.	
	Gruppkonton förekommer i Agresso.	Iakttagelsen kvarstår.	

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 Stockholm Vatten AB. Vid vår granskning noterade vi att Stockholm Vatten AB inte beställer återläsningstester från Volvo IT och att återläsningstester därför inte genomförs regelbundet

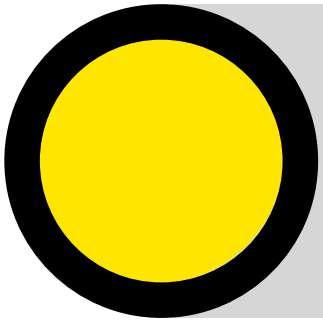
Risk

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

Rekommendation

I likhet med föregående år rekommenderar vi Stockholm Vatten AB att utifrån ett riskbaserat synsätt, överväga rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa.

Rutin för genomgångar av behörigheter i Agresso



Iakttagelse

Stockholms vatten AB har tagit fram en kvartalsvis rutin för att periodiskt granska att användare som slutat på bolaget inte har fortsatt behörighet i Agresso. Genomgången omfattar inte användare med hög behörighet. Genomgången omfattar inte heller användare som bytt roll och/eller erhållit ändrade behörigheter i Agresso.

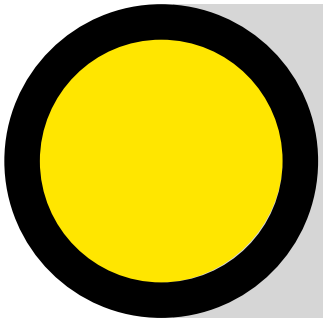
Risk

En process för periodisk granskning som inte omfattar även användare med privilegierade accesser och fall där förändringar har skett inom befintliga accesser täcker inte fullt risken för felaktigt tilldelade behörigheter.

Rekommendation

Stockholm Vatten AB bör införa en rutin för att periodiskt granska samtliga behörigheter i Agresso. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer. Utvärdring bör ske huruvida genomgång skall omfatta även individer med tittabehörighet (Self-Service).

Gruppkonton förekommer i Agresso



Iakttagelse

Utveckling och implementering av programförändringar i produktionsmiljön för Agresso genomförs av leverantören Agresso. När leverantören ska genomföra en produktionssättning skickas en SMS-kod ut för att ge access till stadens Citrix-inloggning. Vid mindre supportärenden används fortfarande gruppkontot.

Risk

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

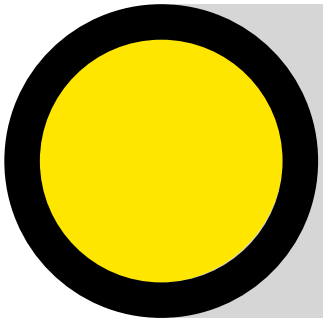
Rekommendation

Stockholm Vatten AB bör eftersträva att enbart personliga konton används för åtkomst till samtliga applikationer, databaser och servrar. I de undantagsfall detta inte är möjligt bör en rutin tas fram för att monitorera externa användares aktiviteter i systemet. För Agresso bör Stockholm Vatten AB överväga att använda sig av Start Stockholms rutin med SMS för alla ärenden som kräver programförändringar, även mindre ärenden.

Kulturhuset Stadsteatern AB

2013	Iakttagelser	Status	2014
	Programförändringar testas inte i testmiljö innan produktionssättning.	Kulturhuset Stadsteatern AB har tagit fram en process och checklista för hantering av programförändringar. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Bristande dokumentation av godkännande för mindre programförändringar i Klara.	Se ovan. Kulturhuset Stadsteatern AB har tagit beslut om att alla ändringar ska gå igenom samma process.	
	Bristande ansvarsfördelning och personberoende för programförändringar i Klara.	Kulturhuset Stadsteatern AB har initierat ett projekt Klara 2.0 för att bygga bort brister i ansvarsfördelningen och personberoendet. Det är av vikt att detta projekt fullföljs enligt angiven tidsplan för att avhjälpa problematiken med personberoende och lämplig ansvarsfördelning.	
	Lösenord för användarkonton i Visma, Agda och Klara följer inte Stockholms Stads riktlinjer för informationssäkerhet.	Kulturhuset Stadsteatern har uppdaterat lösenordsinställningarna för Visma, Agda och Klara med högre komplexitet och följer numera de riktlinjer som definierats inom Stockholm stad. Se dock nedan angående lösenord för biljettkassesystemet.	
	Rutiner för programförändringar och behörighetshantering är inaktuella och uppdateras inte regelbundet.	Kulturhuset Stadsteatern AB har tagit fram en ny instruktion för förändringshantering av driftsmiljö och applikationssystemen (se ovan) samt hantering av behörigheter.	
	Nya Iakttagelser 2014		
	Lösenord för användarkonton i biljettkasse systemet följer inte Stockholms Stads ritlinjer för informations säkerhet.		
	Avsaknad av rutin för periodisk genomgång av användare.		

Lösenord för användarkonton i biljettkasse systemet följer inte Stockholms Stads riktlinjer för informations säkerhet



Iakttagelse

Under vår granskning 2014 noterades att Kulturhuset Stadteatern AB har knutit Agda, Visma och Klara till Volvo-IT och deras singel-sign-on-lösning. Dock har de inte genomfört denna förändring för samtliga användare vid kontrolltillfället och vi noterade att biljettkassemoduler i Klara endast har lägre inloggningskrav. Kulturhuset Stadsteatern AB har planerat för åtgärder i och med projektet Klara 2.0 för att kunna möta Stockholm Stads riktlinjer för informationssäkerhet.

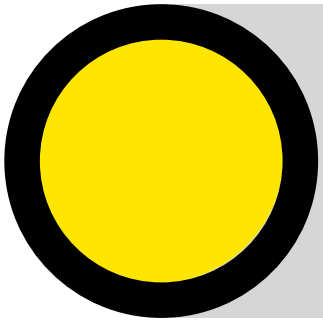
Risk

Svaga krav på lösenord ökar risken för obehörig åtkomst till biljettkasse systemet.

Rekommendation

I projektplanen Klara 2.0 har Kulturhuset Stadsteatern AB planer på förhöjda lösenordskrav. Denna projektplan bör fullföljas för att kunna säkerställa att användarkonton i samtliga applikationer följer Stockholms Stads riktlinjer för informationssäkerhet.

Avsaknad av rutin för periodisk genomgång av användare



Iakttagelse

Under vår granskning noterades att det inte finns en rutin för periodisk genomgång av användare. I dagsläget görs en genomgång av användare sporadiskt men det finns ingen formell ägare till denna kontroll. En kontroll genomförs också mot listor från Volvo-IT avseende användare som varit inaktiva under längre tid.

Risk

Avsaknad av en rutin kan leda till att det inte finns ett gemensamt arbetssätt för kontrollen och därmed kan viktiga steg utebli eller kringgås. Detta leder till ökad risk för att personer med felaktig behörighet förblir oupptäckta.

Rekommendation

Kulturhuset Stadsteatern AB bör säkerställa en rutin för periodisk genomgång av användare. Denna rutin bör dokumenteras samt regelbundet granskas och uppdateras vid behov. Denna rutin bör baseras på Stockholms Stads centrala riktlinjer.

Stockholm Business Region AB

2013	Iakttagelser	Status	2014
	Avsaknad av dokumenterade rutiner för tilldelning av nya behörigheter.	Stockholm Business region har utformat och dokumenterat nya rutiner för Visma Control 5,5, samt CRM systemen LIME och Aladdin. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	
	Avsaknad av formaliserad rutin för periodisk granskning av tilldelade behörighetsnivåer i Visma.	Stockholm Business region har utformat en ny periodisk rutin där kontrollen utförs av den administrativa chefen.	
	Avsaknad av dokumenterad rutin för programförändringsprocessen.	Stockholm Business Region AB har beslutat att implementera Stockholms stads process för programförändringar (F-guide). Stockholm Business Region bör fortsätta arbetet med att implementera rutiner enligt stadens F-guide vid programförändringar, men de bör också utforma rutinen så att den passar verksamheten samt regelbundet granska och uppdatera rutinen vid behov.	

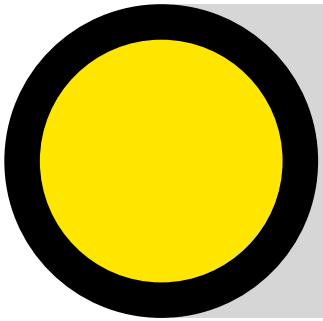
S:t Erik Livförsäkring AB

2013	Iakttagelser	Status	2014
	Avsaknad av regelbundna återläsningstester	S:t Erik Livförsäkring AB har utfört ett återläsningstest under 2014 utan anmärkning.	

S:t Erik Försäkring AB

2013	Iakttagelser	Status	2014
	Avsaknad av regelbundna återläsningstester	Iakttagelsen kvarstår.	

Avsaknad av regelbundna återläsningstester



Iakttagelse

S:t Erik Försäkring AB tar regelbundet backuper av sina system. Vid vår granskning noterade vi att inga 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

I likhet med föregående år rekommenderar vi S:t Erik Försäkring AB att utifrån ett riskbaserat synsätt, överväga rutiner för att regelbundet säkerställa möjlighet att återläsa data och system, till exempel genom att genomföra återläsningstester, samt dokumentera resultatet av dessa.

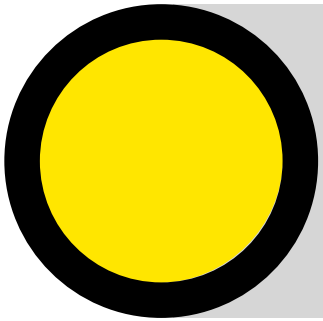
Stockholm Parkering

2013	Iakttagelser	Status	2014
	Bristande dokumentation av rutiner för periodisk granskning av behörighetsnivåer.	Stockholm parkering har utsett ansvarig för att utföra granskningen två gånger om året vilket är beskrivet i behörighetsdokumentet. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	

Stockholms Stads Bostadsförmedling AB

2013	Iakttagelser	Status	2014
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Stockholms Stads Bostadsförmedling AB har utfört ett återläsningstest av en server hos Volvo IT.	
	Viktiga kontroller i programförändringsprocessen sker informellt och dokumenteras inte.	Stockholms Stads Bostadsförmedling AB har dokumenterat samtliga kontroller i programförändringsprocessen. Vår genomgång visar att förändringsprocessen för både större releaser och enskilda mindre ändringar dokumenterats utförligt.	
	Avsaknad av rutin för periodisk granskning av tilldelade behörighetsnivåer i Raindance.	Stockholm Stads Bostadsförmedling AB har tagit fram en ny rutin där ekonomichefen ansvarar för att utföra och dokumentera den periodiska granskningen av behörighetsnivåer i Raindance.	
	Lösenordsinställningar för användarkonton i Raindance följer inte Stockholms Stads riktlinjer för informationssäkerhet.	Stockholms Stads Bostadsförmedling AB har granskat sina lösenordskrav och följer idag Stockholms Stads riktlinjer.	
	Avsaknad av dokumenterad rutin för tilldelning av nya behörigheter.	Stockholms Stads Bostadsförmedling har tagit fram en ny rutin för hantering av behörigheter i samband med nyanställning och avslut med en detaljerad beskrivning för respektive system. Rutinen infattar dock inte fall där befintlig person byter roll inom företaget.	

Avsaknad av spårbarhet när befintlig personal byter roll



Iakttagelse

Vid tilldelning av nya behörigheter krävs ett godkännande av ansvarig chef samt att en behörighetsadministratör effektuerar beställningen. I rutinen saknas dock riktlinjer för vad som gäller när personal byter roller inom bolaget som kräver förändrade behörigheter.

Risk

Bristande dokumentation av ändrade behörigheter ökar risken för obehörig åtkomst till applikationerna samt minskar spårbarheten.

Rekommendation

Stockholms Stads Bostadsförmedling AB bör komplettera sin befintliga process för tilldelning av borttag av behörigheter att även inkludera rutiner för förändring av behörigheter för befintliga anställda. Dessa rutiner bör bygga på Stockholms Stads centrala riktlinjer.

AB Stockholmshem

2013	Iakttagelser	Status	2014
	Återläsningstester genomförs inte för servrar hos Volvo IT.	AB Stockholmshem har utfört ett återläsningstest under 2014 utan anmärkning.	
	Bristande spårbarhet i de periodiska genomgångarna samt avsaknad av delaktighet från systemägare	AB Stockholmshem har en årlig process för genomgång av samtliga konton vilken utförs, dokumenteras och signeras av ekonomichefen.	
	Avsaknad av rutin för regelbunden granskning av programförändringsprocessen	AB Stockholmshem har tagit fram en ny rutin där IT-chefen och systemägaren årligen verifierar att processen för programförändringar är funktionell.	

Granskningsdetaljer

Sektion 4

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	Kontaktperson
Stockholms Hamn AB	Björn Hellerström, IT
MICASA AB	Anette Silfver Danielsson & Kristian Arenander, IT
SISAB	Joakim Ekman, IT
Stockholms Stadshus AB	Sara Feinberg
Stockholm Vatten AB	Lars Storm, IT
Kulturhuset / Stadsteatern AB	Åke Wetterblad, IT & Malin Dahlberg, EA
Stockholm Business Region AB	Lena Häggdahl, EA + IT
St. Eriks Livförsäkring AB	Jan Willgård
St. Eriks Försäkring AB	Jan Willgård
Stockholm Parkering AB	Ronny Hedman, IT & Boris Amsköld, EA
Stockholms Stads Bostads-förmedling AB	David Mancilla, IT
AB Stockholms-hem	Allan Hansson, IT

Tack!