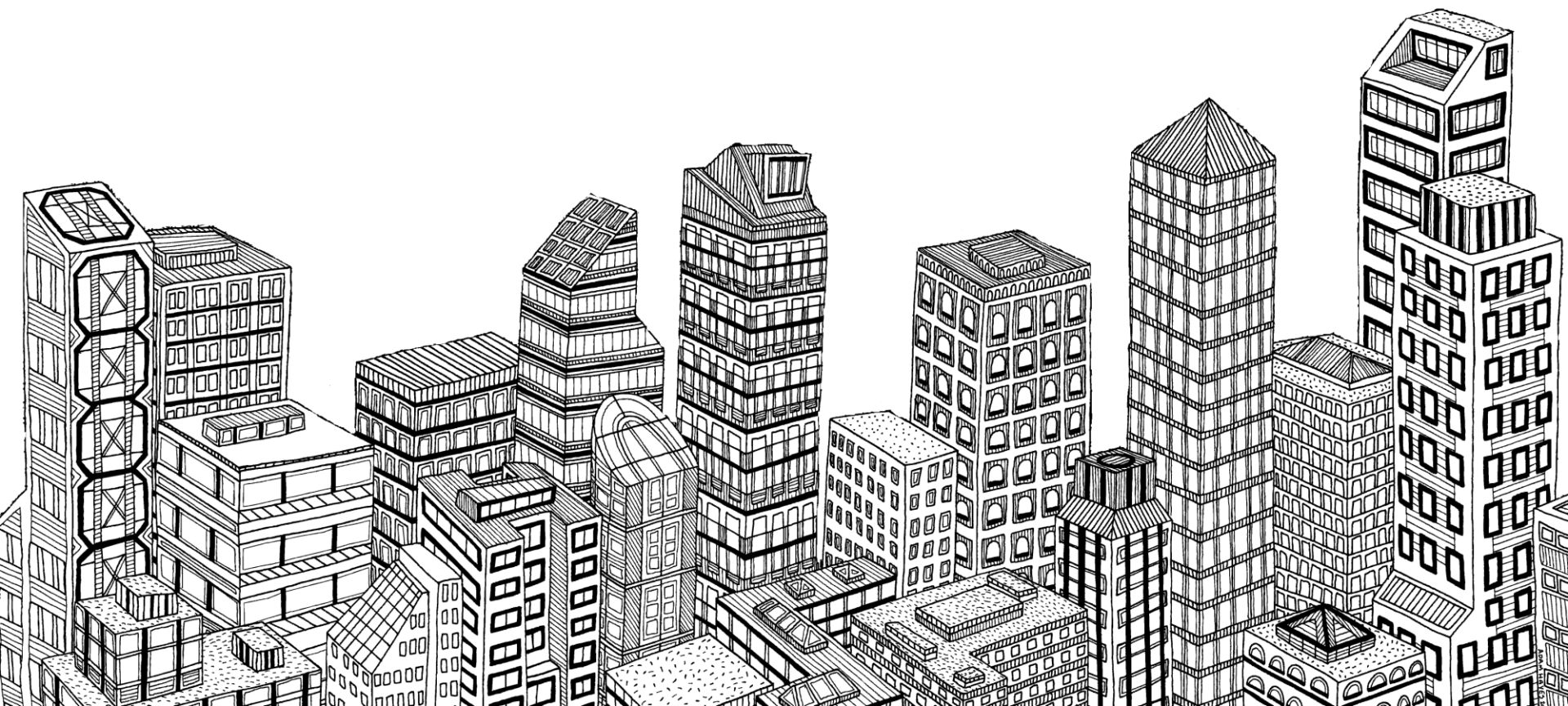


Bolagsspecifika resultat

Sektion 3



Omfattning av granskning

- ▶ EY har under 2015 genomfört en uppföljning av de observationer som noterades i samband med IT-revisionen 2014. De tidigare observationerna har prioriterats utifrån hur pass kritiska de bedöms vara för respektive bolag. Bolag med tidigare noteringar som inte ansetts vara av kritisk karaktär har inte ingått i uppföljningen 2015.
- ▶ Dotterbolagen är uppdelade och prioriterade i två olika grupper:
 - ▶ **Bolag med högre prioritering**
 - ▶ Uppföljningen av tidigare noteringar har genomförts genom intervjuer samt granskning av relevant dokumentation hos respektive bolag.
 - ▶ **Bolag med lägre prioritering (ej granskade 2015)**
 - ▶ De bolag som är exkluderade från har inte haft några iakttagelser från 2014 års granskning av någon högre dignitet och bedöms inte behöva följas upp inom ramen för 2015 års granskning.

Högre prioritering	Bolag med lägre prioritering (ej granskade 2015)
Stockholms Hamn AB	Stockholm Business Region AB
MICASA AB	St. Eriks Livförsäkring AB
SISAB	Stockholm Parkering AB
Stockholms Stadshus AB	AB Stockholms-hem
Stockholm Vatten AB	AB Stokab
Kulturhuset / Stadsteatern AB	AB Familjebostäder
St. Eriks Försäkring AB	Svenska bostäder
Stockholms Stads Bostads-förmedling AB	Stockholm Globe Arena Fastigheter AB
	St. Eriks Markutveckling AB

Översikt bolag inom granskningen

Sektion 3

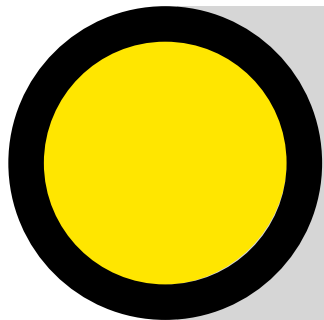
Företagsspecifika resultat

Bolag	Sida	lakttagelser 2013	lakttagelser 2014	lakttagelser 2015
Stockholm Hamn AB	4			
MICASA AB	5-6			Inga kvarstående noteringar
SISAB	7-8			
Stockholm Stadshus AB	9			Inga kvarstående noteringar
Stockholm Vatten AB	10-11			
Kulturhuset / Stadsteatern AB	12			
Sthlm Stads Bost-förm.. AB	13			Inga kvarstående noteringar
AB Stockholms-hem	14-15			Inga kvarstående noteringar

2014	lakttagelser	Status	2015
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Underhållssystemet Idus ska uppdateras vilket kommer att innebära att möjligheter för att genomföra återläsningstester förenklas då denna är planerad att användas blanda annat för detta ändamål. Vidare har vi noterat att det centralt tagits fram en rutin tillsammans med Volvo som underlättar beställning och utförande av återläsningstester. <i>lakttagelsen bedöms vara åtgärdad.</i>	
	Stockholm Hamn AB har tagit fram ett nytt testprotokoll med godkännande för införande i produktionsmiljön. Det är av vikt att den uppdaterade rutinen följs för både större och mindre programförändringar.	Stockholms Hamn AB har inte haft några signifikanta programförändringar under året därmed har vi inte kunnat verifiera att de nya rutinerna följs. Två större uppdateringar är planerade av Idus och Port IT och det är då av vikt att de uppdaterade rutinerna följs och förankras i processen för framtida programförändring. <i>lakttagelse kvarstår.</i>	
	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.	Stockholms Hamn AB har implementerat en halvårsvis periodisk kontroll av användare i samtliga system. Systemansvarig får ett mail med godkända användare i systemet, dessa användare utvärderas och godkänns alternativt termineras. <i>lakttagelsen bedöms vara åtgärdad.</i>	

2014	lakttagelser	Status	2015
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Micasa Fastigheter AB har gått över till stadens nya gemensamma Agresso system från och med 1 oktober. I och med övergången till det gemensamma ekonomisystemet har ansvaret för återläsningstester lyfts upp på den centrala systemförvaltningen inom staden. <i>lakttagelsen bedöms vara åtgärdad.</i>	
	Bristande spårbarhet i de periodiska genomgångarna av tilldelade behörigheter i Fasad.	Micasa fastigheter AB har utfört genomgång av användare i Fasad under året. Genomgången är utförd i enighet med de rutiner som finns formaliserade för behörighetskontroll på Micasa fastigheter AB. <i>lakttagelsen bedöms vara åtgärdad.</i>	
	Bristande dokumentation av rutiner för programförändringar.	Micasa Fastigheter AB har haft utvecklingsstopp i Visma under året och nu gått över till stadens nya gemensamma ekonomisystem. Det har även varit minimal utveckling av Fasad på grund av att det ska bytas ut under Q1 2018. Detta har summerat upp till att inga resurser har lagts på att utveckla nya rutiner för programförändringar till de befintliga systemen. <i>lakttagelse och rekommendation kvarstår.</i>	

MICASA: Bristande dokumentation av rutiner för programförändringar



Iakttagelse

Iakttagelsen och rekommendationen kvarstår, Micasa Fastigheter AB har haft utvecklingsstopp i Visma under året och nu gått över till stadens nya gemensamma ekonomisystem. Minimal utveckling av Fasad, det ska bytas ut under Q1 2018. Inga resurser har lagts på att utveckla nya rutiner för programförändringar till de befintliga systemen även detta år.

Risk

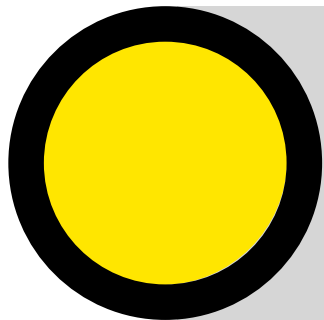
Bristande dokumentation av rutiner kan leda till att det inte finns ett gemensamt arbetssätt för exempelvis testförfarande eller produktionssättning och därmed kan viktiga kontroller utebli eller kringgås.

Rekommendation

Eftersom utveckling 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.

2014	lakttagelser	Status	2015
	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.	SISAB har under året implementerat nya rutinerna i systemet för felanmälan av beställning (Feber). Övriga system har inte infört de nya rutinerna och det är av vikt att även de inkluderas. <i>lakttagelsen kvarstår med modifikation.</i>	
	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.	Ansvar har enligt bolaget legat för högt upp i organisationen vilket lett till att genomgångarna ej har genomförts. Ambitionen från SISAB är fortfarande att delegera ansvaret till systemansvariga under 2016. <i>lakttagelse och rekommendation kvarstår.</i>	

SISAB: Periodiska genomgångar av tilldelade behörigheter



Iakttagelse

Inom SISAB finns en nyligen framtagna instruktion för hur periodiska genomgångar av tilldelade behörigheter ska genomföras och vem som ansvarar för dessa. Någon genomgång har ej utförts under 2015.

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.

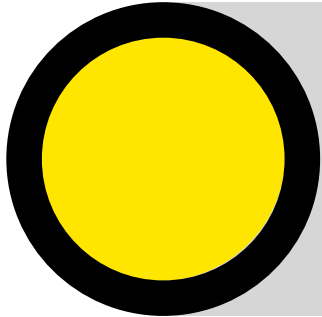
Rekommendation

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

2014	lakttagelser	Status	2015
	Tieto genomför med jämna mellanrum återläsningstester för Cognos. Dock finns det ej några dokumenterade resultat.	Stockholms Stadshus AB har beställt ett återläsningstest av Cognos och dokumenterat resultatet. <i>lakttagelsen bedöms vara åtgärdad.</i>	✓
	Det existerar ett fåtal konton med grupp access i Cognos.	Stockholm Stadshus AB har mininerat tillgången till de berörda kontona som fortfarande existerar och kartlagt vilka individer som har access. <i>lakttagelsen bedöms vara åtgärdad.</i>	✓

2014	lakttagelser	Status	2015
	Återläsningstester genomförs inte för servrar hos Volvo IT.	Vi bedömer att bolaget i samband med serverbyten och uppsättning av testsystem verifierat att processen kring återläsning fungerar för Stockholm Vatten hos Volvo IT. <i>lakttagelsen bedöms vara åtgärdad.</i>	
	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 privilegierade användare samt användare som bytt arbetsuppgifter inte omfattas av denna granskning.	Vi har verifierat att rutinen som har tagits fram täcker avslut av behörighet inom bolaget inkluderat höga behörigheter. Dock täcker rutinen inte eventuella användare som byter arbetsuppgifter inom bolaget och som därmed bör ha en förändrad behörighet. <i>lakttagelsen kvarstår med modifikation.</i>	
	Gruppkonton förekommer i Agresso.	Inga åtgärder har utförts för att minska eller helt ta bort gruppkonton för Agresso supporten. <i>lakttagelse och rekommendation kvarstår.</i>	

Stockholm Vatten AB: 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

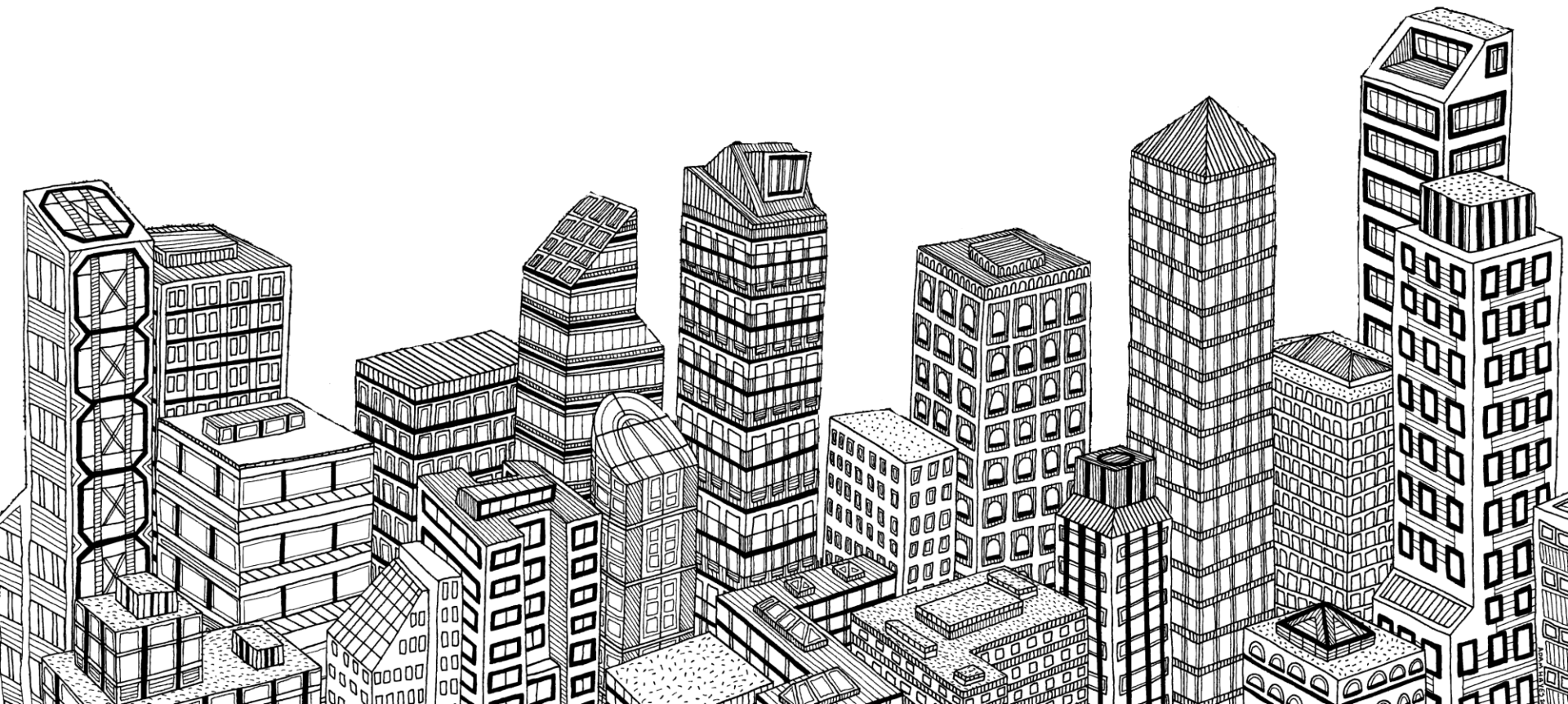
Stockholm Vatten AB bör eftersträva att enbart personliga konton används för åtkomst till samtliga applikationer, databaser och servrar. I de undantagsfall detta inte är möjligt bör en rutin tas fram för att monitorera externa användares aktiviteter i systemet. För Agresso bör Stockholm Vatten AB överväga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

2014	lakttagelser	Status	2015
	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.	Kulturhuset Stadsteatern AB har inkorporerat den nya processen för större programförändringar men bör också inkludera mindre ändringar, så kallade "quick fixes". <i>lakttagelsen kvarstår med modifikation.</i>	
	Lösenord för användarkonton i biljettkasse systemet följer inte Stockholms Stads ritlinjer för informations säkerhet.	Kulturhuset Stadsteatern AB har lyft över majoriteten av användarna i biljettkassesystemet till en single sign on lösning. Det finns ett fåtal konton kvar (5 stycken) men dessa konton kommer att byggas bort med hjälp av projektet Klara 2,0. <i>lakttagelsen bedöms vara åtgärdad.</i>	✓
	Avsaknad av rutin för periodisk genomgång av användare.	Kulturhuset Stadsteatern AB har tagit fram nya rutiner med ansvarsfördelning för periodisk genomgång av användare för samtliga kritiska system. Det är av vikt att de nya rutinerna kommuniceras och införs. <i>lakttagelsen kvarstår med modifikation.</i>	

2014	lakttagelser	Status	2015
	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. Det är av vikt att den uppdaterade rutinen kommuniceras och införs.	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. <i>lakttagelsen bedöms vara åtgärdad.</i>	
	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.	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. <i>lakttagelsen bedöms vara åtgärdad.</i>	

Granskningsdetaljer

Sektion 4



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 vår granskning 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	Mats Kings, IT
MICASA AB	Kristian Arenander, IT
SISAB	Mee Nilsson, IT
Stockholms Stadshus AB	Sara Feinberg, Inger Johansson Kjaerboe, IT
Stockholm Vatten AB	Lars Storm, IT
Kulturhuset / Stadsteatern AB	Åke Wetterblad, IT & Malin Dahlberg, EA
St. Eriks Försäkring AB	Maria Scheele
Stockholms Stads Bostads-förmedling AB	David Mancilla, IT

Tack!

