STOCKHOLMS STADSHUS AB
En del av Stockholms stad

2022-12-02

Väsentlighets- och riskanalys samt internkontrollplan Bolagen 2023

Stockholm Globe Arena Fastigheter AB

Stockholms Stadshus AB	Org.nr 556415-1727			
Postadress	Besöksadress	Telefon	Fax	E-post
105 35 STOCKHOLM	Stadshuset, 3 tr.	08-508 290 00	08-509 290 80	info@stadshusab.se

Innehållsförteckning

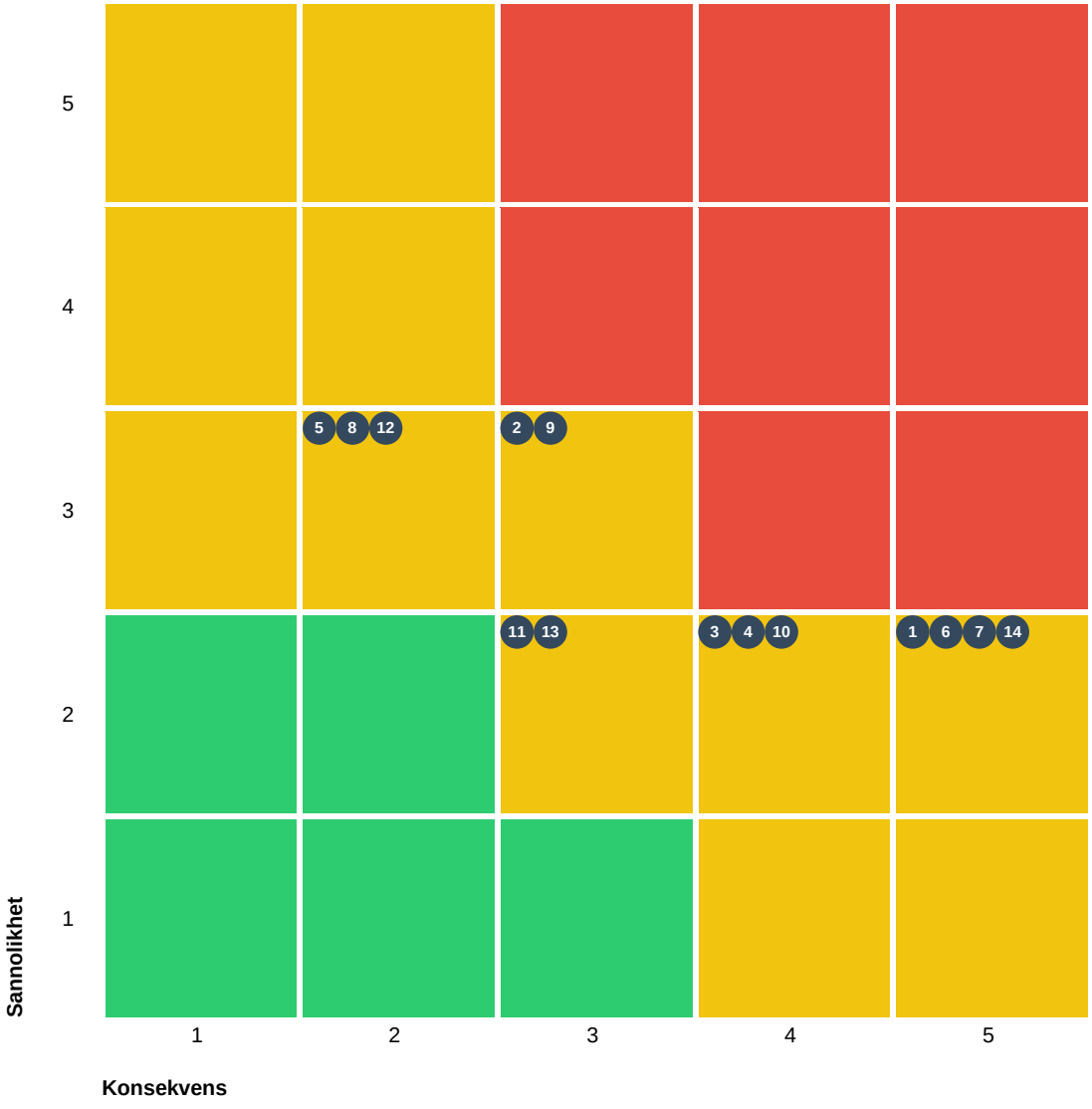
Inledning

Beskrivning av arbetet med intern kontroll

Bolagets internkontrollarbete ska bestå av tre delar. Bolaget ska ha fastställt ett aktuellt system för internkontroll, årligen genomföra en väsentlighets- och riskanalys (VoR) samt utifrån denna fastställa en internkontrollplan. Systemet för internkontroll ska ses över årligen och vid behov revideras. Väsentlighets- och riskanalysen genomförs i flera steg. Bolaget ska identifiera de viktigaste processerna/arbetssätten för att uppnå kommunfullmäktiges mål för verksamhetsområdena. Bolaget ska i arbetet beakta lagstiftning och verksamhetens uppdrag. Utifrån arbetssätten ska oönskade händelser identifieras. Dessa ska värderas (1-5) utifrån vilka konsekvenserna blir om händelsen inträffar samt hur sannolikt det är att händelserna inträffar. Utifrån riskvärdet beslutas om den oönskade händelsen/risken ska hanteras i internkontrollplanen. I internkontrollplanen planerar bolaget hur de löpande kontrollerna/arbetssätten ska följas upp. Internkontrollplanen fastställs i samband med verksamhetsplanen och följs upp i samband med verksamhetsberättelsen.

Väsentlighets- och riskanalys

I riskmatrisen nedan syns alla oönskade händelser i VoR:en. Alla som har en stjärna ⭐ samt en kontrollaktivitet finns även i Internkontrollplanen längre ner i rapporten.



14 Medium | Totalt: 14

Kritisk
Medium
Låg

	Sannolikhet	Konsekvens
5	Mycket sannolikt	Mycket allvarlig
4	Sannolikt	Allvarlig
3	Möjlig	Kännbar
2	Mindre sannolikt	Lindrig
1	Osannolikt	Försumbar

KF:s mål för verksamhetsområdet	Process	Nr		Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd	**Ekonomi**	1		**Hyresgäster ställer in betalningar**	2. Mindre sannolikt	5. Mycket allvarlig	10	★
	Inköp	2		**Anlitar leverantör med bristande ekonomisk stabilitet**	3. Möjlig	3. Kännbar	9	★
		3		**Inköp sker utan upphandling eller beställning**	2. Mindre sannolikt	4. Allvarlig	8	★
		4		**Upphandling som ej följer LOU**	2. Mindre sannolikt	4. Allvarlig	8	★
3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb	**Intern kontroll**	5		**Otillåten bisyssla**	3. Möjlig	2. Lindrig	6	★
		6		**Otillåten påverkan mutor och bestickning**	2. Mindre sannolikt	5. Mycket allvarlig	10	★
		7		**Otillåten representation**	2. Mindre sannolikt	5. Mycket allvarlig	10	★
3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden	**IT**							
	Systematiskt informationssäkerhetsarbete	8		**Bristande efterlevnad av dataskyddsförordningen**	3. Möjlig	2. Lindrig	6	★
		9		**Brister i informationssäkerheten**	3. Möjlig	3. Kännbar	9	★
3.6 Tryggheten ska öka genom förebyggande insatser	**Fysisk säkerhet**	10		**Arbetsplatsolycka**	2. Mindre sannolikt	4. Allvarlig	8	★
		11		**Bolagets krisberedskap brister**	2. Mindre sannolikt	3. Kännbar	6	★
		12		**Bristande efterlevnad av rutiner och arbetsprocesser**	3. Möjlig	2. Lindrig	6	★
		13		**Brister i hantering av passerkort**	2. Mindre sannolikt	3. Kännbar	6	★
		1		**Större olycka,**	2. Mindre	5. Mycket	10	★

KF:s mål för verksamhetsområdet	Process	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
		4	**större oönskad händelse, på arenaområdet**	sannolikt	allvarlig		

Internkontrollplan

Anvisning

En process kommer med i Internkontrollplanen när man har **skapat en *Kontrollaktivitet***. Med andra ord kommer **alla** processer som har en eller flera kontrollaktiviteter att synas i internkontrollplanen **oberoende** av valet *Med till upprättande av IKP?*

Vill du inte att en process ska komma med i Internkontrollplanen måste du ta bort den kopplade kontrollaktiviteten. Det räcker alltså inte att ändra valet på *Med till upprättande av IKP* till *Nej, endast VoR.*

3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd

Process	Oönskad händelse	Kontrollaktivitet
Ekonomi	**Hyresgäster ställer in betalningar** 10	**Genomgång hyresgästsstabilitet** Kontroll mot Skatteverket och ev. UC görs för att säkerställa ekonomisk stabilitet. Kontroll av hyresgästers ÅR.
Inköp	**Anlitar leverantör med bristande ekonomisk stabilitet** 9	**Kontroll av leverantörers ekonomiska stabilitet** Kontroll via skatteverket av SGAF:s 10 största leverantörer (störst inköp) av bl.a. deras ekonomiska stabilitet (t.ex. ej konkurs) i samband med detta sker även kontroll av att leverantören är korrekt upphandlad. Kontroll sker minst 1 gång per år eller utifrån behov.
	Inköp sker utan upphandling eller beställning 8	**Kontroll av leverantörsfakturor** Kontrolleras genom 5 stickprov där fakturor slumpmässigt granskas. Granskning sker gällande korrekt belopp, avtal, om LOU har följts etc. Kontroll sker 2 ggr/år i samband med tertialrapportering.
	Upphandling som ej följer LOU 8	**Kontroll av upphandling** Kontrolleras genom 5 stickprov där fakturor slumpmässigt granskas. Granskning sker gällande korrekt belopp, avtal, om LOU har följts etc. Kontroll sker 2 ggr/år i samband med tertialrapportering.

3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb

Process	Oönskad händelse	Kontrollaktivitet

Process	Oönskad händelse	Kontrollaktivitet
Intern kontroll	**Otillåten bisyssla** 6	**Kontroll av bisysslor** Kontrolleras genom att medarbetarna årligen får utskick gällande bisysslor samt kontroll av medarbetarna mot näringslivsregister för att att upptäcka ev. otillåtna bisysslor
	Otillåten påverkan mutor och bestickning 10	**Genomgång av hantering av mutor och bestickning** Kontroll av hur chefer och medarbetare hanterar frågan om mutor och bestickning samt hur informationen om detta ser ut. Kontroll sker 1 ggn/år.
	Otillåten representation 10	**Kontroll av representation** Kontroll av samtlig intern och extern representation. Sker i samband med varje delårsbokslut samt årsbokslut. Kontroll sker 3 ggr/år.

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

Process	Oönskad händelse	Kontrollaktivitet
Systematiskt informationssäkerhetsarbete	**Bristande efterlevnad av dataskyddsförordningen** 6	**Externt anlitad dataskyddsombud (DSO)** SGA Fastigheter ska anlita extern DSO för att utöka granskningen och ha oberoende från verksamheten.
		Översyn av registerförteckningen Årlig översyn och uppdatering av registerförteckningen för att denna ska vara aktuell.
	Brister i informationssäkerheten 9	**Kontrollera avslutade medarbetare och entreprenörer/leverantörer** Kontrollera att medarbetare som slutat eller entreprenörer/leverantörer som avslutat sina uppdrag inte har fortsatt behörighet eller åtkomst till system.
		Stickprov i kritiska system av behörighet Stickprov i system av att användare har rätt behörighet samt att lösenord utformats och uppdaterats kontinuerligt i enlighet med rekommendationer.
		Testa återläsning av säkerhetskopior Testa återläsning av säkerhetskopior av kritiska system. Årligen.
		Följa upp och åtgärda rekommendationer efter penetrationstest av kritiska system Följa upp och åtgärda rekommendationer efter genomfört

Process	Oönskad händelse	Kontrollaktivitet
		penetrationstest av kritiska system. Informationsklassning av alla tekniska system samt införande av PM3 förvaltningsmodell för tekniska system.
		Informera medarbetarna på gemensamma personalmöten Informera och påminna medarbetarna om informationssäkerhet i samband med månadsmöten. Se till att de får en grundläggande förståelse och uppdaterad omvärldsinformation gällande aktuella risker utifrån ett informationssäkerhetsperspektiv. Minst 1 ggr/år och annars löpande utifrån behov. Krav och uppföljning av att medarbetare genomför Stockholm Stads tester.
		Hantera ev. upptäckta brister från incidentsrapporteringssystemet Genomgång av rapport för att upptäcka ev. brister från incidentsrapporteringsystemet. Kontrollen görs årsvis.
		Följa upp om leverantör åtgärdar brister Kontrollera om leverantörer har åtgärdat brister som upptäckts i samband med uppföljningsmöten. Uppföljningen sker årsvis i samband med upptäckter.

3.6 Tryggheten ska öka genom förebyggande insatser

Process	Oönskad händelse	Kontrollaktivitet
Fysisk säkerhet	**Arbetsplatsolycka** 8	**Arbetsmiljögruppen genomför möten enligt plan** Arbetsmiljögruppens möten hålls 4 ggr/år. Möten dokumenteras och kontinuerliga förbättringar genomförs.
		Genomgång av rutiner med personal Årlig genomgång i början av året av rutiner och diskussion rörande säkerhet och trygghet i arenorna och i arenaområdet för all personal. Sker på månadsmöte. Därutöver sker olika utbildningar t.ex. säkra fall och klätterutbildning/hög höjd.
	Bolagets krisberedskap brister 6	**Kontrollera att krisplanen är uppdaterad** Se till att ha en uppdaterad krisplan. Genomgång med personal för att förebygga och agera på rätt sätt, 1 ggr per år på månadsmöte. Kontroll sker tertialvis (dvs 3 ggr/år), i samband med övrig tertialrapportering.

Process	Oönskad händelse	Kontrollaktivitet
	Bristande efterlevnad av rutiner och arbetsprocesser 6	**Analys av ärenden i PondusPro** Övergripande analys av ärenden i fastighetssystemet PondusPro för att se om det finns några indikationer på systematiska problem/förekomster, som bolaget behöver ta hänsyn till för att förebygga risker på ett systematiskt sätt. Kontroll sker genom stickprov av ärenden månadsvis samt mätning/uppföljning av tid som det tar att rapportera och följa upp ärenden. Resultat rapporteras till ledningsgruppen.
	Brister i hantering av passerkort 6	**Kontroll av lista över passerkort** Uttag lista från centralvakt för översyn av samtliga giltiga passerkort (både anställda och entreprenörer). Kontroll sker 1-2 ggr/år, per 1 april och 1 oktober.
	Större olycka, större oönskad händelse, på arenaområdet 10	**Genomgång av rutiner med personal** Årlig genomgång i början av året av rutiner och diskussion rörande säkerhet och trygghet i arenorna och i arenaområdet för all personal. Sker på månadsmöte. Därutöver sker olika utbildningar t.ex. säkra fall och klätterutbildning/hög höjd.
		Krisledningsövning och krisövning. Varje år genomför krisledningen en övning, minst i form av skrivbordsövning med scenario. Därutöver genomförs olika praktiska krisövningar, t.ex. utrymning av Skyview.