STOCKHOLMS STADSHUS AB
En del av Stockholms stad

2022-12-08

Väsentlighets- och riskanalys samt internkontrollplan Bolagen 2023

S:t Erik Försäkrings 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

Enligt kommunfullmäktiges budget ska nämnder och styrelser utarbeta en internkontrollplan. För att kunna bedöma risken för att staden inte når kommunfullmäktiges inriktningsmål och mål för verksamhetsområdena ska nämnder och bolagsstyrelser upprätta en risk- och väsentlighetsanalys för dessa mål. I riskanalysen ska även åtgärder för att minimera riskerna redovisas.
Utgångspunkten för internkontrollplanen är att
- verksamheten bedrivs i enlighet med ägarens och den egna styrelsens uppsatta mål,
- lagar, beslut och regler följs
- verksamheten bedrivs effektivt och ändamålsenligt,
- redovisningen är rättvisande och att uppföljningen av verksamheten och ekonomin är tillförlitlig,
- säkerheten i administrativa rutiner är tillfredsställande,
- bolagets tillgångar skyddas.

Bolaget skall härvidlag:
- ha ett aktuellt system för internkontroll,
- årligen genomföra en risk- och väsentlighetsanalys,
- ta fram en internkontrollplan utifrån den genomförda risk- och väsentlighetsanalysen.

.

Beskrivning av arbetet med intern kontroll

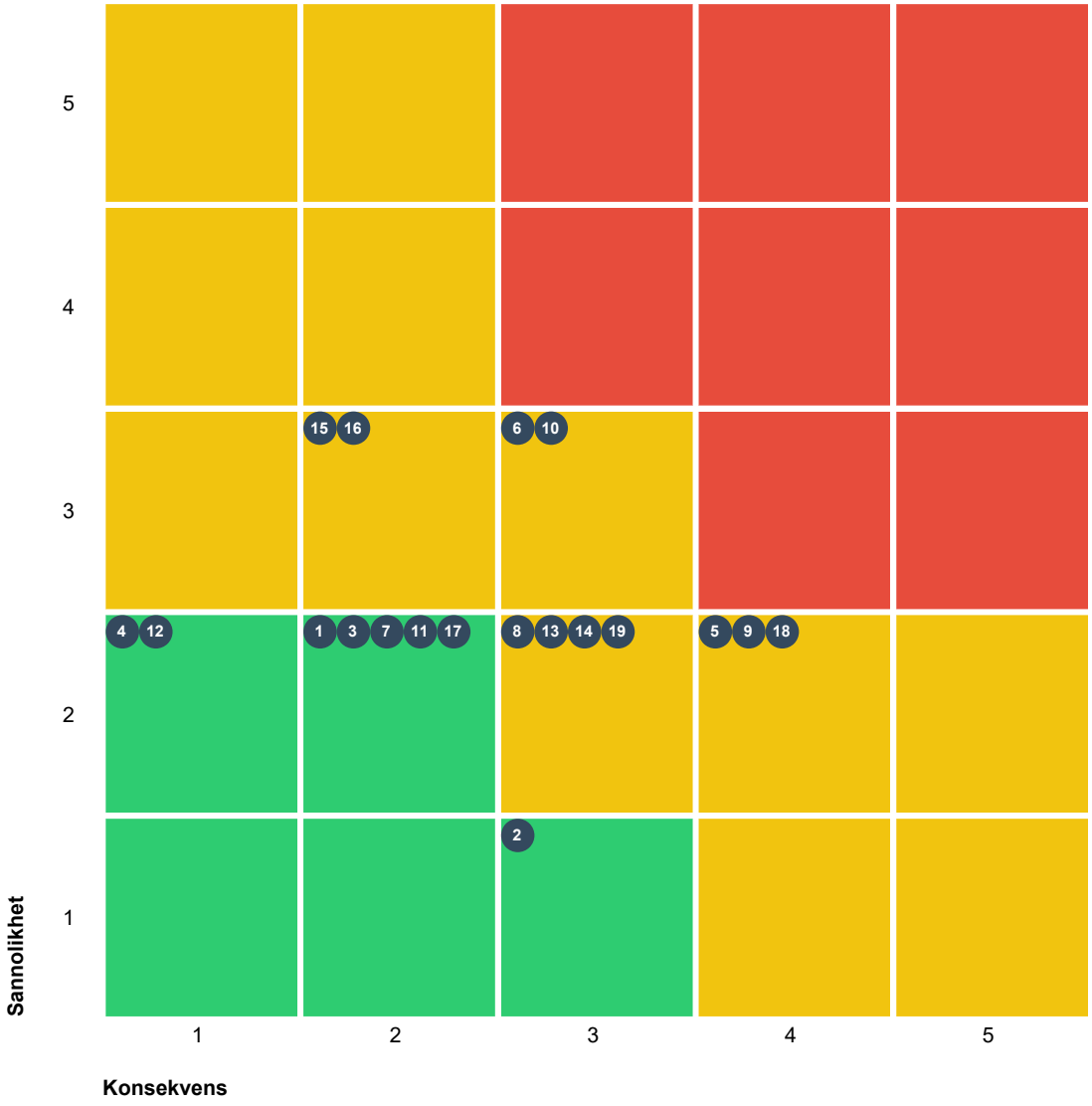
Bolagets internkontrollarbete ska bestå av tre delar. Bolaget ska ha fastställt ett aktuellt system för internkontroll, årligen genomföra en väsentlighets- och riskanalys (VoR) samt utifrån denna fastställa en internkontrollplan. Systemet för internkontroll ska ses över årligen och vid behov revideras. 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.

S:t Erik Försäkring lyder under försäkringsrörelselagen (2010:2043) och de riktlinjer som Finansinspektionen utfärdar. I 10 kap. Försäkringsrörelselagen, Förordning (EU) 2015/35 artikel 256, Riktlinjer företagsstyrning (EIOPA) 14/253 artikel 40-45 samt Finansinspektionens föreskrifter 2015:8, 2016:3, 2016:28 och 2017:5 ställs specifika krav på intern styrning och kontroll. Bolagets interna kontroll har därför utformats i enlighet med dessa regelverk och återfinns i flertalet av bolagets riktlinjer.

S:t Erik Försäkring ska årligen genomföra en riskinventering av sin verksamhet utifrån risken att verksamheten inte kan utföra de mål som ägaren och styrelsen fastslagit för året. Arbetet ska inledas med en riskinventering som innebär att företagets anställda och närstående intervjuas om vilka risker de ser i verksamheten som kan äventyra bolagets uppsatta mål. Resultatet av inventeringen ska därefter sammanställas och rangordnas av styrelsen utifrån en samlad bild av sannolikhet och konsekvenser vid ett inträffande. När riskerna är rangordnade ska VD utarbeta en handlingsplan för hur riskerna i möjligaste mån ska elimineras och upprätta en granskningsplan. Efter årets utgång ska VD därefter presentera vilka åtgärder som vidtagits under året samt vilken effekt åtgärderna fått på verksamheten. I de fall styrelsen anser att det inte skett någon förändring av riskbilden sedan föregående år har styrelsen möjlighet att avstå från den årliga riskinventeringen för att i stället ge VD i uppdrag att vidta ytterligare förebyggande åtgärder utifrån föregående års prioriterade risker.

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.



11 Medium 8 Låg | Totalt: 19

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
1.3 Stockholms stad ska ge stöd och omsorg där	**1. Identifiera kommunkoncernens risker**	1	**Inget gehör i organisationen för att genomföra**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast

KF:s mål för verksamhetsområdet	Process	Nr		Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
behoven är som störst				**arbetet**				VoR
	2. Förebygga kommunkoncernens risker	2		**S:t Erik Försäkring har inte allokerat tillräckligt med resurser för att kunna genomföra arbetet**	1. Osannolikt	3. Kännbar	3	Nej, endast VoR
	4. Analysera och följa upp kommunkoncernens riskhanteringsarbete	3		**Rapport kan inte färdigställas pga bristande underlag.**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
2.1 Stockholm ska bli klimatpositivt – genom minskade utsläpp och ökad koldioxidlagring	**10. Miljömål**	4		**Bolaget bidrar inte till stadens miljöprograms genomförande**	2. Mindre sannolikt	1. Försumbar	2	Nej, endast VoR
3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd	**3. Försäkra kommunkoncernens risker**	5		**En försäkrad risk har inte någon återförsäkring alternativt betalar inte återförsäkraren någon ersättning**	2. Mindre sannolikt	4. Allvarlig	8	★
	5. Lönsamhetsmål	6		**Skadekostnaderna blir för höga i förhållande till premieintäkterna**	3. Möjlig	3. Kännbar	9	★
	6. Effektivitetsmål	7		**Driftskostnaderna stiger på grund av oförutsedda händelser**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb	**7. Kvalitetsmål**	8		**Bolaget följer inte lagar och regler inklusive Finansinspektionens förordningar**	2. Mindre sannolikt	3. Kännbar	6	★
		9		**Bolaget har bristande rutiner som leder till fel**	2. Mindre sannolikt	4. Allvarlig	8	★
		10		**Högt personberoende av ett fåtal individer gör att bolaget sårbart om någon skulle sluta**	3. Möjlig	3. Kännbar	9	★
	8. Servicemål	11		**Bristande service leder till missnöjda kunder**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
	9. CSR-mål	12		**Bolaget lever inte upp till sina CSR-**	2. Mindre sannolikt	1. Försumbar	2	Nej, enda

KF:s mål för verksamhetsområdet	Process	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
			mål				st VoR
3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden	Krisplanering	13	Planer ej uppdaterade eller övade	2. Mindre sannolikt	3. Kännbar	6	★
	Systematiskt informationssäkerhetsarbete	14	Incidenter registreras inte	2. Mindre sannolikt	3. Kännbar	6	★
		15	Infoklassning bristfällig	3. Möjlig	2. Lindrig	6	★
		16	Infosäk bristfälligt reglerat	3. Möjlig	2. Lindrig	6	★
		17	Lokal anvisning är inte uppdaterad och kommunicerad	2. Mindre sannolikt	2. Lindrig	4	★
		18	Obehörig får tillgång till system	2. Mindre sannolikt	4. Allvarlig	8	★
	Systematiskt informationssäkerhetsarbete i övrigt sk IKT	19	Bolagets utsätter sig för IKT- och/eller säkerhetsincidenter som allvarligt stör verksamheten	2. Mindre sannolikt	3. Kännbar	6	★

Internkontrollplan

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

Process	Oönskad händelse	Kontrollaktivitet
3. Försäkra kommunkoncernens risker	8 En försäkrad risk har inte någon återförsäkring alternativt betalar inte återförsäkraren någon ersättning	**Avstämning återförsäkringsansvarig samt fastställande av premier och signering återförsäkring.** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.
5. Lönsamhetsmål	9 Skadekostnaderna blir för höga i förhållande till premieintäkterna	**Resultatuppföljning i ordinarie rapportering från ekonomi till staden och Finansinspektionen.** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.

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

Process	Oönskad händelse	Kontrollaktivitet
7. Kvalitetsmål	6 Bolaget följer inte lagar och regler inklusive Finansinspektionens förordningar	**Avstämning med centrala funktioner samt ekonomifunktionen** Bolaget har endast 8 st anställda och en

Process	Oönskad händelse	Kontrollaktivitet
		VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.
	Bolaget har bristande rutiner som leder till fel 8	**Avstämning med centrala funktioner samt ekonomifunktionen** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.
	Högt personberoende av ett fåtal individer gör att bolaget sårbart om någon skulle sluta 9	**Uppdaterade krisplaner och utförda utvecklingssamtal.** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

Process	Oönskad händelse	Kontrollaktivitet
Systematiskt informationssäkerhetsarbete	**Incidenter registreras inte** 6	**Arbetsmiljö tas upp på måndagsmöten samt incidentrapport från riskhanteringsfunktionen.** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma
	Infoklassning bristfällig 6	**Avstämning med IT-ansvarig samt DSO** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma
	Infosäk bristfälligt reglerat 6	**Avstämning med upphandlingsansvarig** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma
	Lokal anvisning är inte uppdaterad och kommunicerad 4	**Avstämning med IT-ansvarig att anvisning uppdateras och kommuniceras** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma
	Obehörig får tillgång till	**Avstämning med systemansvariga**

Process	Oönskad händelse	Kontrollaktivitet
	8 **system**	Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma
Systematiskt informationssäkerhetsarbete i övrigt sk IKT	6 **Bolagets utsätter sig för IKT- och/eller säkerhetsincidenter som allvarligt stör verksamheten**	**Avstämning med IT-ansvarig och centrala funktioner (riskhanterings, regelefterlevnad** Bolaget har endast 8 st anställda och en VD, ingen ledningsgrupp eller underchefer. Den systematiska kontrollen och VD/lednings kontroll blir således samma.