STOCKHOLMS STADSHUS AB
En del av Stockholms stad

2023-03-07

Väsentlighets- och riskanalys samt internkontrollplan 2023

Moderbolaget Stockholms Stadshus 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

Inledning
Den interna kontrollen ska vara utformad för att med rimlig grad av säkerhet kunna uppnå följande:

- att verksamheten är ändamålsenlig och effektiv
- att information om verksamhet och ekonomi är tillförlitlig
- att lagar, förordningar och styrdokument följs

Genom en tillräcklig intern kontroll skapas förutsättningar för att upptäcka och förebygga oönskade händelser i verksamheten samt säkra tillgångar, förhindra förluster och oegentligheter.
Varje bolag ansvarar för att utforma och organisera den interna kontrollen och skapa effektiva system för uppföljning

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.

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.

System för intern kontroll
Intern kontroll är en ständigt pågående process där styrelse, VD och övrig personal samverkar. Syftet med intern kontroll är att säkerställa att bolaget bedriver en effektiv verksamhet och undgår allvarliga fel och skador. Intern kontroll är ett vitt begrepp som innefattar allt från rättvisande räkenskaper till styrning och uppföljning mot uppsatta mål. Den interna kontrollen ska bidra till en ändamålsenlig och kostnadseffektiv verksamhet, tillförlitlig finansiell rapportering och information om verksamheten samt efterlevnad av tillämpliga styrdokument. Detta ska sammantaget bidra till effektiv användning av skattemedel samt service med hög kvalitet till kommuninnevånarna.

Roller, ansvarsfördelning och rapporteringsrutiner
En förutsättning för en tillräcklig intern kontroll är en tydlig delegation av ansvar och befogenheter i organisationen. Nedan beskrivs roller och ansvar i arbetet med intern kontroll.

Styrelsen
Styrelsen har det yttersta ansvaret för den interna kontrollen i den egna verksamheten och ska årligen:

- upprätta, dokumentera och besluta om ett system för intern kontroll. Detta görs i samband med verksamhetsplan.
- upprätta och besluta om en internkontrollplan utifrån genomförd väsentlighets- och riskanalys. Detta görs i samband med verksamhetsplan.
- bedöma huruvida den interna kontrollen är tillräcklig. Detta görs i samband med verksamhetsberättelse.

VD/Vice vd:

- ser till att medarbetarna har förståelse för vad tillräcklig intern kontroll innebär i verksamheten.
- skapar förutsättningar för ett arbetsklimat som främjar tillräcklig intern kontroll.
- verkar för att de arbetssätt som används bidrar till tillräcklig intern kontroll.
- rapporterar snarast möjligt väsentliga avvikelser till styrelse. Vid väsentliga avvikelser ska åtgärder vidtas.

Administrativ chef

- samordnar arbetet med intern kontroll för bolaget.
- samordnar granskningsresultat och rapportering till styrelse.
- rapporterar avvikelser till vice vd.

Medarbetare

- ansvarar för att bidra med sin kompetens i arbetet med intern kontroll.
- ansvarar för att rapportera brister och avvikelser till överordnad chef.

Väsentlighets och riskanalys
Bolaget ska årligen genomföra en väsentlighets- och riskanalys. Bolaget identifierar de viktigaste *processerna* för att uppnå kommunfullmäktiges mål för verksamhetsområdena. Processerna utgår från bolagets klassificeringsstruktur och stadens obligatoriska processer. O*önskade händelser identifieras* och värderas utifrån konsekvens och sannolikhet. I analysen, bedöms sannolikheten för att oönskade händelser kan inträffa och vilka konsekvenser de skulle kunna få.

Utifrån den genomförda väsentlighets- och riskanalysen ska en internkontrollplan tas fram. I internkontrollplanen beskrivs *arbetssätt och systematisk kontroll.* Vilka *kontrollaktiviteter* som ska utföras under året dokumenteras. Åtgärder ska alltid identifieras för oönskade händelser med totalt riskvärde 9 eller högre. Bolaget bedömer hur övriga oönskade händelser ska hanteras, ibland tas oönskade händelser med lägre riskvärde med för att bolagets analys är att en kontrollaktivitet kan vara relevant.

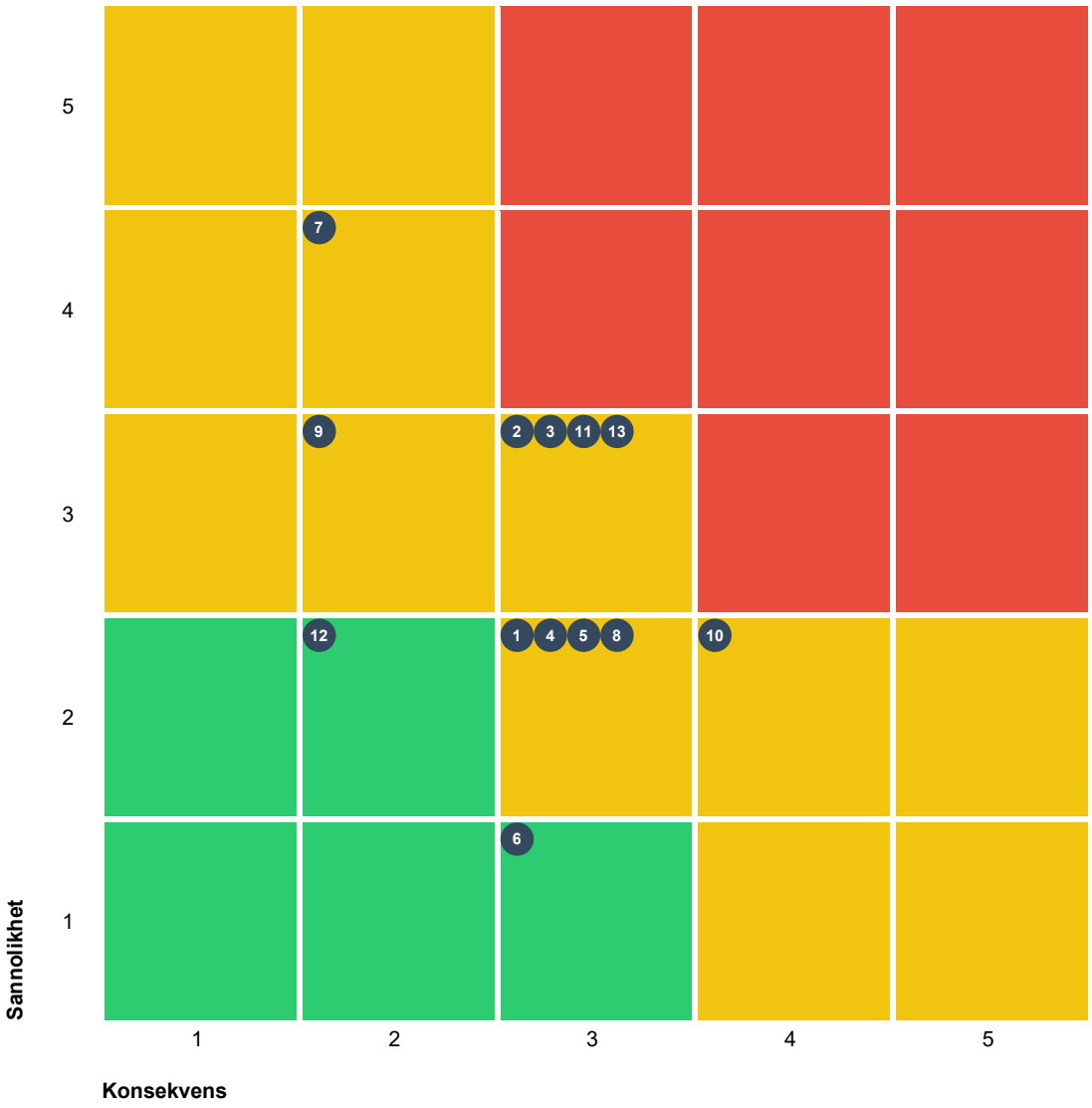
Lagstiftning och styrande dokument
Det finns ingen särskild associationsform för kommunägda aktiebolag och därför omfattas bolagen i Stockholms Stadshus AB av flera olika lagstiftningar. Kommunallagen och aktiebolagslagen är de övergripande lagar som bolagen, inklusive moderbolaget, ska följa. Därutöver styrs bolaget även av regler i bland annat tryckfrihetsförordningen, offentlighets- och sekretesslagen, årsredovisningslagen, arkivlagen, dataskyddsförordningen samt lagen om offentlig upphandling. Vissa av bolagen lyder även under speciallagstiftning som reglerar deras verksamhet. Det ställer höga krav på staden och dess bolag att analysera och tolka olika uppdrag, beslut och händelser och att anpassa sig efter detta.

För bolaget finns flera övergripande program, riktlinjer, regler och anvisningar som styr bolagets verksamhet. När det gäller arbetet med intern kontroll är det, utöver stadens budget, vision, representationspolicy och allmänna styrdokument framförallt stadens säkerhetsprogram, informationssäkerhetsriktlinje, personalpolicy samt upphandlingsprogram som berör riskerna nämnda i nedan väsentlighets och riskanalys samt internkontrollplan. Även bolagets attestinstruktion, arbetsordning och bolagsordning är styrdokument relevanta för internkontrollplanen.

Uppföljning
I samband med verksamhetsberättelsen ska det interna kontrollarbetet följas upp och rapporteras till styrelsen. Vid eventuella avvikelser ska vidtagna åtgärder beskrivas.

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 2 Låg | Totalt: 13

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	Arbetssätt	Nr		Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd	**Köpa in och beställa**	**Inköp hanteras och avrop och beställningar sker enligt rutiner och beslut**	1		**Felaktigheter uppstår vid inköp eller fakturering**	2. Mindre sannolikt	3. Kännbar	6	
	Planera och följa upp verksamheten	**Anvisningar tas fram för bolagens arbete med verksamhetsplan utifrån beslutad budget och ägardirektiv**	2		**Uppdrag i budgeten hanteras otillräckligt**	3. Möjlig	3. Kännbar	9	
		Finanspolicy beslutas och följs och kontinuerlig omvärldsbevakning sker.	3		**Händelser i samhällsekonomin får oförutsedda negativa följder för koncernens bolag.**	3. Möjlig	3. Kännbar	9	
		Uppföljning av ekonomisk-, löne-, avtalshantering och förtroendekänsliga frågor inom koncernen.	4		**Brister i uppföljningen gör att en förtroendekris uppstår**	2. Mindre sannolikt	3. Kännbar	6	
	Styra och leda verksamheten	**Framtagande av anvisningar och rutiner för bolagskoncernen**	5		**Styrningen av koncernen har brister/är ej tillräcklig för att målen ska uppnås**	2. Mindre sannolikt	3. Kännbar	6	
3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb	**Hantera arbetsmiljö och gemensamma personalfrågor**	**Regler och riktlinjer kring arbetsmiljö följs**	6		**Brister i arbetsmiljön uppstår**	1. Osannolikt	3. Kännbar	3	Nej, endast VoR
	Utveckla verksamheten	**Arbetssätt och rutiner ses över kontinuerligt**	7		**Verksamheten är personberoende och utveckling i vissa processer kan avstanna vilket medför sårbarhet**	4. Sannolikt	2. Lindrig	8	Nej, endast VoR
3.5 Hög beredskap och stark rådighet ska råda i alla	**Systematiskt informationssäkerhetsarbete**	**Behörighetshantering**	8		**Obehöriga har åtkomst till material**	2. Mindre sannolikt	3. Kännbar	6	
		Implementering av lokal	9		**Arbete, ansvar, roller och hantering av**	3. Möjlig	2. Lindrig	6	

KF:s mål för verksamhetsområdet	Process	Arbetssätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
verksamhetsområden		**anvisning**		**informationssäkerhet är otydligt**				
		Incidenthantering	10	**Brister uppstår kring inrapportering av allvarliga informationssäkerhetsincidenter, bolaget får anmärkningar och böter**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
		Informationsklassning	11	**Brister i rutiner kring hantering av bolagets informationstillgångar uppstår**	3. Möjlig	3. Kännbar	9	⭐
		Informationssäkerhet inom upphandlingsförfarande	12	**Brister i informationssäkerhet uppstår hos leverantör eller i upphandlad tjänst**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
		Registerförteckningen över bolagets personuppgiftsbehandlingar hålls uppdaterat.	13	**Personuppgifter behandlas felaktigt och bolaget får anmärkningar gällande bristande följsamhet av dataskyddsförordningen**	3. Möjlig	3. Kännbar	9	⭐
3.6 Tryggheten ska öka genom förebyggande insatser								

Internkontrollplan

Åtgärder ska alltid identifieras för oönskade händelser med totalt riskvärde 9 eller högre i väsentlighets- och riskanalysen. Bolaget bedömer hur övriga oönskade händelser ska hanteras, ibland tas oönskade händelser med lägre riskvärde med för att bolagets analys är att en kontrollaktivitet kan vara relevant.

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

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Köpa in och beställa	Inköp hanteras och avrop och beställningar sker enligt rutiner och beslut	Då behov av vara/tjänst uppstår kontrolleras om avtal/ramavtal finns	Felaktigheter uppstår vid inköp eller fakturering 6	Avtalsinventering sker och integration mellan avtalsystemet Kommers och ärendehanteringssystemet eDok genomförs
Planera och följa upp verksamheten	Anvisningar tas fram för bolagens arbete med verksamhetsplan utifrån beslutad budget och ägardirektiv	Genomgång av bolagens verksamhetsplaner inför beslut	Uppdrag i budgeten hanteras otillräckligt 9	Granskning av dotterbolagens verksamhetsplaner och rapportering
	Finanspolicy beslutas och följs och kontinuerlig omvärldsbevakning sker.	Framtagande av finansiell månadsrapport samt annan ekonomisk redovisning till styrelsen.	Händelser i samhällsekonomin får oförutsedda negativa följder för koncernens bolag. 9	Omvärldsbevakning och analys
	Uppföljning av ekonomisk-, löne-, avtalshantering och förtroendekänsliga frågor inom koncernen.	Uppföljning och stickprover görs löpande av koncernledningen, revisorer samt lekmannarevisorer.	Brister i uppföljningen gör att en förtroendekris uppstår 6	Kontroll av bisysslor för verkställande direktörer
Styra och leda verksamheten	Framtagande av anvisningar och rutiner för bolagskoncernen	Att anvisningar följs kontrolleras kontinuerligt.	Styrningen av koncernen har brister/är ej tillräcklig för att målen ska uppnås 6	Bolagsordningar ses över och revideras under året
				Uppföljning efterlevnad av tillämpningsanvisningar för investeringar i bolagskoncernen

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Systematiskt informationssäkerhetsarbete	Behörighetshantering	Behörigheter i verksamhetssystem och gruppdiskar gås igenom och uppdateras årligen	Obehöriga har åtkomst till material 6	Stickprovskontroll
	Implementering av lokal anvisning	Den lokala anvisningen för informationssäkerhet fastställs och gås igenom årligen eller vid behov	Arbete, ansvar, roller och hantering av informationssäkerhet är otydligt 6	Kontroll av att den lokala anvisningen implementerats i verksamheten.

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
	Informationsklassning	Koncernledningen arbetar med kompetensutveckling inom området och överväger att ta in konsulthjälp för informationsklassning.	9 Brister i rutiner kring hantering av bolagets informationstillgångar uppstår	Kontroll att bolagets lönesystem informationsklassats.
	Registerförteckningen över bolagets personuppgiftsbehandlingar hålls uppdaterat.	Dataskyddsombudets årsrapport	9 Personuppgifter behandlas felaktigt och bolaget får anmärkningar gällande bristande följsamhet av dataskyddsförordningen	Stickprovskontroll personuppgiftsbehandlingar