STOCKHOLMS STADSHUS AB
En del av Stockholms stad

2023-11-10

Väsentlighets- och riskanalys samt internkontrollplan Bolagen 2024

Stockholm Business Region 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

Internkontroll är den process genom vilken styrelse, ägare, ledning och annan personal skaffar sig rimlig säkerhet för att uppsatta mål uppnås. Syftet är att säkerställa att policys, program, riktlinjer och processer är fullgoda och efterlevs, att säkerställa att lagstiftningen följs, att verka förebyggande så att inga risksituationer uppstår samt att minimera skadorna och ta lärdom av en incident. Internkontrollen sker genom en löpande intern granskning, uppföljning och förebyggande åtgärder.

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.

Ansvar
Styrelsen har det yttersta ansvaret för den interna kontrollen, både vad gäller utformning och utförande.

Styrelsen ska årligen:

- Besluta om systemet för den interna kontrollen.
- Besluta om en internkontrollplan utifrån väsentlighets- och riskanalysen.
- Bedöma om den interna kontrollen är tillräcklig i samband med redovisningen av genomförandet.

Verkställande direktören
Verkställande direktören ska se till att regler och anvisningar utformas som säkerställer att den interna kontrollen fungerar och att den redovisas till styrelsen en gång om året.

Övriga chefer
Cheferna svarar inom respektive verksamhetsområde för att regler och anvisningar är kända och att de följs samt för att arbetsmetoder och rutiner bidrar till en god intern kontroll. Cheferna ska även bidra till utformningen av konkreta regler och anvisningar för en god intern kontroll.

Alla medarbetare
Varje medarbetare måste vara medveten om sin betydelse när det gäller att uppnå en säker och effektiv verksamhet. Medarbetarna är skyldiga att följa gällande regler, rutiner, program, riktlinjer och policys samt anvisningar för god intern kontroll. Alla medarbetare har ett ansvar för att rapportera brister och avvikelser.

Administrativa avdelningen
Administrativa avdelningen svarar för att det finns ett fungerande regelverk inom ekonomi-, personal- och administrativa området.

Revisorernas roll
Revisorerna prövar om styrelsens internkontroll är tillräcklig. Stadens lekmannarevisorer granskar koncernen utifrån verksamheten, ägardirektiven och de fastställda målen.

De externa revisorerna granskar verksamheten utifrån den ekonomiska redovisningen och förvaltningen av bolagen, att denna är korrekt och följer gällande lagstiftning samt att all redovisning till ägare och myndigheter är till fullo korrekt och genomförd.

Rapportering
Rapportering sker löpande till bolagsledningen och en sammanfattning av genomförd internkontroll rapporteras en gång om året till styrelsen.

Väsentlighets- och riskanalys
Grunden för den planerade internkontrollen är väsentlighets- och riskanalysen. Väsentlighetsanalysen bedömer konsekvenserna ur politiskt, mänskligt, ekonomiskt och verksamhetsmässigt perspektiv. Riskanalysen är en bedömning av var de största riskerna finns, där det med en risk avses en skada, ett fel eller en brist som kan skada verksamheten, personer eller förtroendet. Analysen revideras årligen utifrån förändringar i omvärlden och den verksamhet som bedrivs inom koncernen.

Risker:

Omvärldsrisker
– Händelser i omvärlden vilket medför nya beslut fattade av regering, riksdag eller annan extern aktör som påverkar verksamheten.

Verksamhetsrisker
– Verksamheten når inte fastställda mål.
– Verksamheten inte bedrivs på ett kostnadseffektivt sätt.
– Verksamheten brister i hantering av ny lagstiftning, nya förordningar och föreskrifter.

Redovisningsrisker
– Räkenskaperna är inte rättvisande eller tillförlitliga.

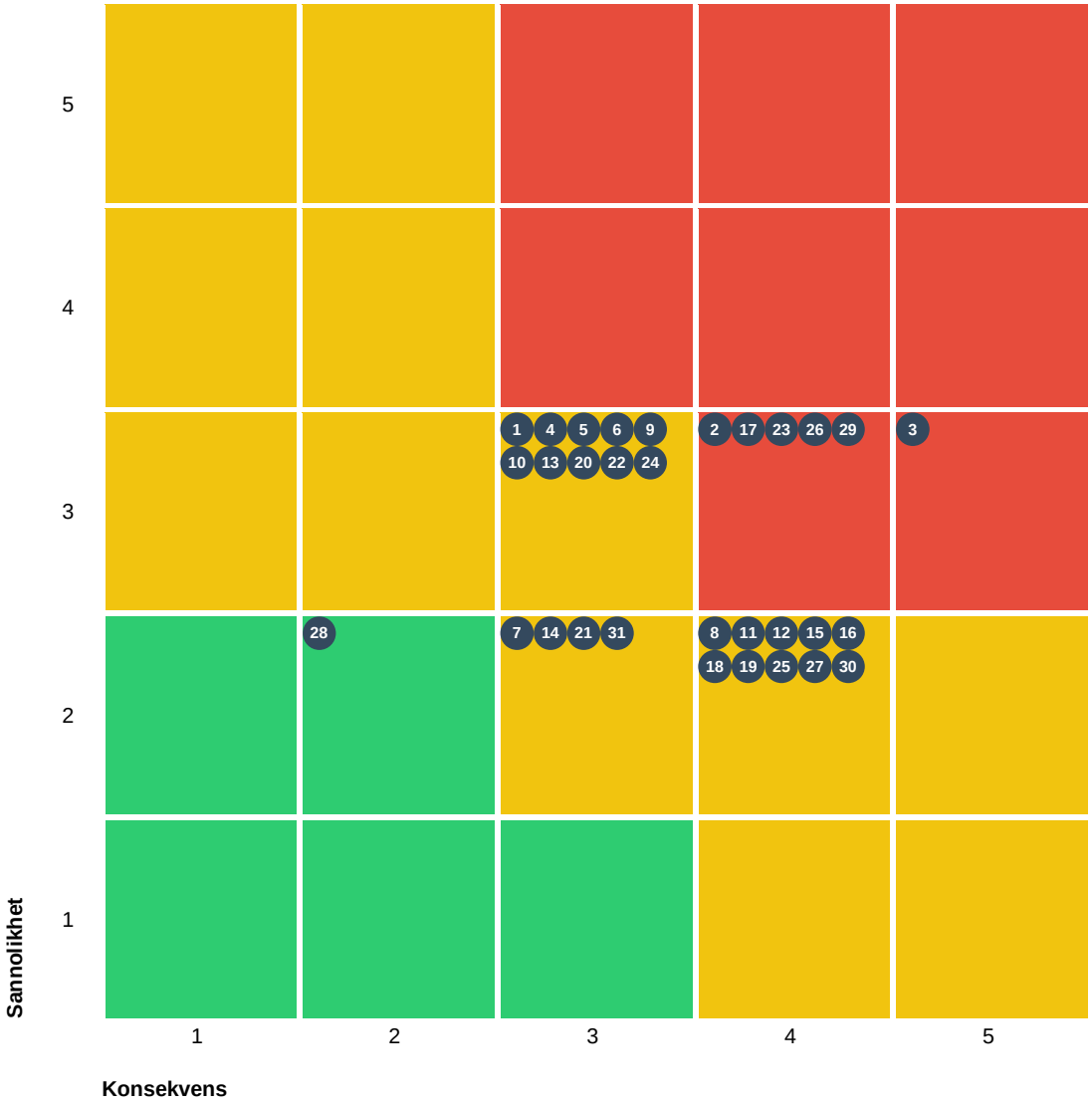
Internkontrollplanen
Internkontrollplanen är upprättad med utgångspunkt i att de av fullmäktige fastställda målen uppfylls. Utifrån bedömningen om påverkbara och icke påverkbara risker är fokus i internkontrollplanen att granska efterlevnad av lagar och policys, program, riktlinjer och ekonomistyrning samt uppföljning av verksamhetens mål, effektivitet och resultat.

Inom följande områden bedöms sannolikheten för att fel, brist eller skada uppstår som stor och/eller konsekvenserna så allvarliga att de kan bedömas som riskområden. De största skadorna bedöms kunna uppstå för medarbetare som befinner sig på tjänsteresa och inom informationssäkerheten och då främst rörande personuppgifter. En förtroendeskada för staden och varumärket Stockholm bedöms också som allvarlig. Dessa områden har prioriterats i internkontrollarbetet.

- Styrning och uppföljning av verksamheten.
- Anskaffning av varor och tjänster.
- Finansförvaltning.
- Förmögenhetsskydd samt skydd av dokument och arbetspapper.
- Personaladministration och hantering av löneunderlag/ lönerapporter.
- Hantering av representation, personalförmåner, gåvor etc.
- Fysisk säkerhet.

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.



6 Kritisk 24 Medium 1 Låg | Totalt: 31

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	**Finansförvaltning.**	**Hantering och av leverantörsfakturor och intäkter i Agresso samt utlägg som**	14	**Att allegat som styrker inköpet (utlägget) inte finns i samtliga fall.**	2. Mindre sannolikt	3. Kännbar	6	★
			12	**Att attestinstruktionerna inte följs.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR

KF:s mål för verksamhetsområdet	Process	Arbetssätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
		hanteras i lönesystemet.	15	**Att försäljningsintäkterna inte faktureras korrekt.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
			13	**Att instruktioner om hur hanteringen av inköp genom utlägg ska ske är otydliga.**	3. Möjlig	3. Kännbar	9	⭐
			16	**Att redovisningssystemet inte följs upp genom regelbundna avstämningar.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
	Förmögenhetsskydd samt skydd av dokument och arbetspapper.	**Hantering av dokument i eDok och inom registraturet**	17	**Att dokument inte diarieförs och arkiveras enligt gällande regler.**	3. Möjlig	4. Allvarlig	12	⭐
	Personaladministration och hantering av löneunderlag / lönerapporter.	**Hantera personuppgifter och löneuppgifter till lönesystemet**	18	**Att anställning och löneändringar inte registreras korrekt i lönesystemet och loggas.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
		Löpande arbete inom HR med processer och utbildningar	20	**Att personalpolicyn inte efterlevs.**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
		Löpande arbete med utläggsredovisningar i lönesystemet	19	**Att arbetsordning, delegationsordning och attestinstruktion inte följs.**	2. Mindre sannolikt	4. Allvarlig	8	⭐
3.2 I Stockholm ska alla ges möjlighet till ett eget jobb	**Styrning och uppföljning av verksamheten.**	**Hantera budget och verksamhetsplanering**	30	**Att verksamhetens åtaganden inte är väl kommunicerade och implementerade.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
		Hantera den digitala infrastrukturen	31	**Att den digitala infrastrukturen brister vilket medför att verksamheten inte kan leverera mot sina åtaganden.**	2. Mindre sannolikt	3. Kännbar	6	Nej, endast VoR
		Hantera styr- och stöddokument	28	**Att organisationen saknar tydligt förtecknade ansvarsområden som framgår av arbetsordning, delegationsordning och attestinstruktion.**	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR

KF:s mål för verksamhetsområdet	Process	Arbetssätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
			29	**Att verksamhetens styrdokument är otydliga eller rutiner är bristfälligt kommunicerade och att det kan medföra utmaningar och bekymmer för medarbetare på tjänsteresa i Sverige eller utomlands.**	3. Möjlig	4. Allvarlig	12	⭐
3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb	**Anskaffning av varor och tjänster.**	**Väl kända rutiner och processer för upphandling och inköp av varor och tjänster**	23	**Att attestinstruktionen inte följs för utläggsredovisningar.**	3. Möjlig	4. Allvarlig	12	Nej, endast VoR
			22	**Att attestinstruktionens regelverk inte är känt och inte följs av såväl godkännare som attestant i Agresso.**	3. Möjlig	3. Kännbar	9	⭐
			24	**Att avtalsuppföljningen brister och medför att inköp görs på felaktiga grunder**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
			21	**Att upphandling inte görs enligt LOU (lagen om offentlig upphandling) och stadens program för inköp.**	2. Mindre sannolikt	3. Kännbar	6	Nej, endast VoR
	Hantering av representation, personalförmåner, gåvor etc.	**Hantera representation och andra förtroendekänsliga poster**	25	**Att attestinstruktionerna inte följs.**	2. Mindre sannolikt	4. Allvarlig	8	⭐
			26	**Att riktlinje om mutor och representation, personalförmåner, gåvor etc. inte är känd och följs.**	3. Möjlig	4. Allvarlig	12	⭐
			27	**Att uppföljning och efterkontroll av poster rörande representation, personalförmåner och gåvor inte sker löpande.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden	**Stockholms stads säkerhetsprogram.**	**Hantera rutiner och rutinbeskrivningar för krisledningsarbetet**	8	**Bristfällig krisledningsförmåga och beredskap.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
	Systematiskt informationssäkerhetsarbete	**Behörighetshantering**	6	**Behörighet till verksamhetssystem avslutas inte i samband med att en anställning upphör eller förändrat arbetsinnehåll**	3. Möjlig	3. Kännbar	9	Nej, endast VoR

KF:s mål för verksamhetsområdet	Process	Arbetssätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	RV	IKP
		Implementering av lokal anvisning	1	**Att verksamheten brister i arbetet med informationssäkerhet**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
		Incidenthantering	3	**Att en personuppgiftsincident inträffar**	3. Möjlig	5. Mycket allvarlig	15	⭐
			2	**Att verksamheten brister i arbetet med informationssäkerhet och en incident inträffar**	3. Möjlig	4. Allvarlig	12	⭐
		Informationsklassning	4	**Att gällande lagar, regler, policys, program, riktlinjer inte är kända och följs.**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
			5	**Att åtgärdslistan efter genomförd informationsklassning inte hanteras och åtgärder inte vidtas**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
		Informationssäkerhet inom upphandlingsförfarande	7	**Att bristande eller felaktiga krav ställs i en upphandling**	2. Mindre sannolikt	3. Kännbar	6	Nej, endast VoR
3.6 Tryggheten ska öka genom förebyggande insatser	**Systematiskt arbetsmiljöarbete (SAM).**	**Hantera rutiner och rutinbeskrivningar för oönskade händelser.**	9	**Att policys, program, riktlinjer, regler och rutiner är otydliga.**	3. Möjlig	3. Kännbar	9	Nej, endast VoR
	Systematiskt brandskyddsarbete (SBA)	**Hantera brandskydd och beredskap för oväntade olyckshändelser**	11	**Att det inte finns förebyggande brandskyddsinstruktioner.**	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
		Hantera rutiner och rutinbeskrivningar för brandskyddet	10	**Att policys, program, riktlinjer, regler och rutiner är otydliga.**	3. Möjlig	3. Kännbar	9	⭐

Internkontrollplan

Internkontrollplanen är upprättad med utgångspunkt i att de av fullmäktige fastställda målen uppfylls. Utifrån bedömningen om påverkbara och icke påverkbara risker är fokus i internkontrollplanen att granska efterlevnad av lagar och policys, program, riktlinjer och ekonomistyrning samt uppföljning av verksamhetens mål, effektivitet och resultat.

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

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Finansförvaltning.	Hantering och av	Kontroll av	Att allegat som	Stickprovskontroll

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
	leverantörsfakturor och intäkter i Agresso samt utlägg som hanteras i lönesystemet.	utläggsredovisningar innan de skickas för attest	6 styrker inköpet (utlägget) inte finns i samtliga fall.	varje månad i bolagen.
			9 Att instruktioner om hur hanteringen av inköp genom utlägg ska ske är otydliga.	Stickprovskontroller i utläggsredovisningarna varje månad.
Förmögenhetsskydd samt skydd av dokument och arbetspapper.	Hantering av dokument i eDok och inom registraturet	Utbildning och information om eDok	1 2 Att dokument inte diarieförs och arkiveras enligt gällande regler.	Genom eDok-stugor ge stöd och utbildning till medarbetare
Personaladministration och hantering av löneunderlag/ lönerapporter.	Löpande arbete med utläggsredovisningar i lönesystemet	Utläggsredovisningar kontrolleras av ekonomiansvarig inför utbetalning	8 Att arbetsordning, delegationsordning och attestinstruktion inte följs.	Stickprovskontroller genomförs löpande under året

3.2 I Stockholm ska alla ges möjlighet till ett eget jobb

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Styrning och uppföljning av verksamheten.	Hantera styr- och stöddokument	Löpande uppföljning av ägardirektiv, kompletterande ägardirektiv samt ändringar i lagar och regelverk	1 2 Att verksamhetens styrdokument är otydliga eller rutiner är bristfälligt kommunicerade och att det kan medföra utmaningar och bekymmer för medarbetare på tjänsteresa i Sverige eller utomlands.	En översyn av styr- och stöddokument för resor och representation.

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

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Anskaffning av varor och tjänster.	Väl kända rutiner och processer för upphandling och inköp av varor och tjänster	Leverantörsfakturor kontrolleras i extrakontrollen och beloppskontrollen i Agresso.	9 Att attestinstruktionens regelverk inte är känt och inte följs av såväl godkännare som attestant i Agresso.	Stickprovskontroller genomförs löpande under året.
Hantering av representation, personalförmåner, gåvor etc.	Hantera representation och andra förtroendekänsliga poster	Leverantörsfakturor granskas i extrakontrollen och beloppskontrollen i Agresso	8 Att attestinstruktionerna inte följs.	Stickprovskontroller genomförs löpande under året.
		Utläggsredovisningar granskas löpande innan de skickas för attest i lönesystemet	1 2 Att riktlinje om mutor och representation, personalförmåner, gåvor etc. inte är känd och följs.	Stickprovskontroll varje månad i bolagen.

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Systematiskt informationssäkerhets	Incidenthantering	Löpande uppföljning av arbetet med	1 Att en personuppgiftsinciden	Årlig uppföljning av arbetet med

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
arbete		registerförteckningen	5 t inträffar	registerförteckningen
		Regelbundna utbildningar inom informationssäkerhet och GDPR	1 2 Att verksamheten brister i arbetet med informationssäkerhet och en incident inträffar	Löpande uppföljning av genomförda utbildningar för alla medarbetare

3.6 Tryggheten ska öka genom förebyggande insatser

Process	Arbetssätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Systematiskt brandskyddsarbete (SBA)	Hantera rutiner och rutinbeskrivningar för brandskyddet	Årlig uppföljning av verksamhetens rutiner för brandskyddet.	9 Att policys, program, riktlinjer, regler och rutiner är otydliga.	En uppföljning av brandskyddsinstruktioner och säkerhetsföreskrifter efter flytt till nya kontorslokaler.