

Väsentlighets- och riskanalys samt internkontrollplan Bolagen 2023 Stockholm Business Region AB

Innehållsförteckning

Inledning	3
Beskrivning av arbetet med intern kontroll	3
Väsentlighets- och riskanalys	4
Internkontrollplan	8
3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd	8
3.2 I Stockholm ska alla ges möjlighet till ett eget jobb	9
3.4 Medarbetare i Stockholm ska ges goda förutsättningar att göra ett bra jobb	9
3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden	9
3.6 Tryggheten ska öka genom förebyggande insatser	10

Inledning

Stockholm Business Region AB med dotterbolagen Visit Stockholm AB och Invest Stockholm Business Region AB bildar koncernen Stockholm Business Region (SBR). I syfte att främja en effektiv organisation är koncernens administration samlad i moderbolaget som upprättar en gemensam internkontrollplan för alla tre bolagen.

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/arbetsätten för att uppnå kommunfullmäktiges mål för verksamhetsområdena. Bolaget ska i arbetet beakta lagstiftning och verksamhetens uppdrag. Utifrån arbetsätten 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/arbetsätten 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 koncernledningen 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

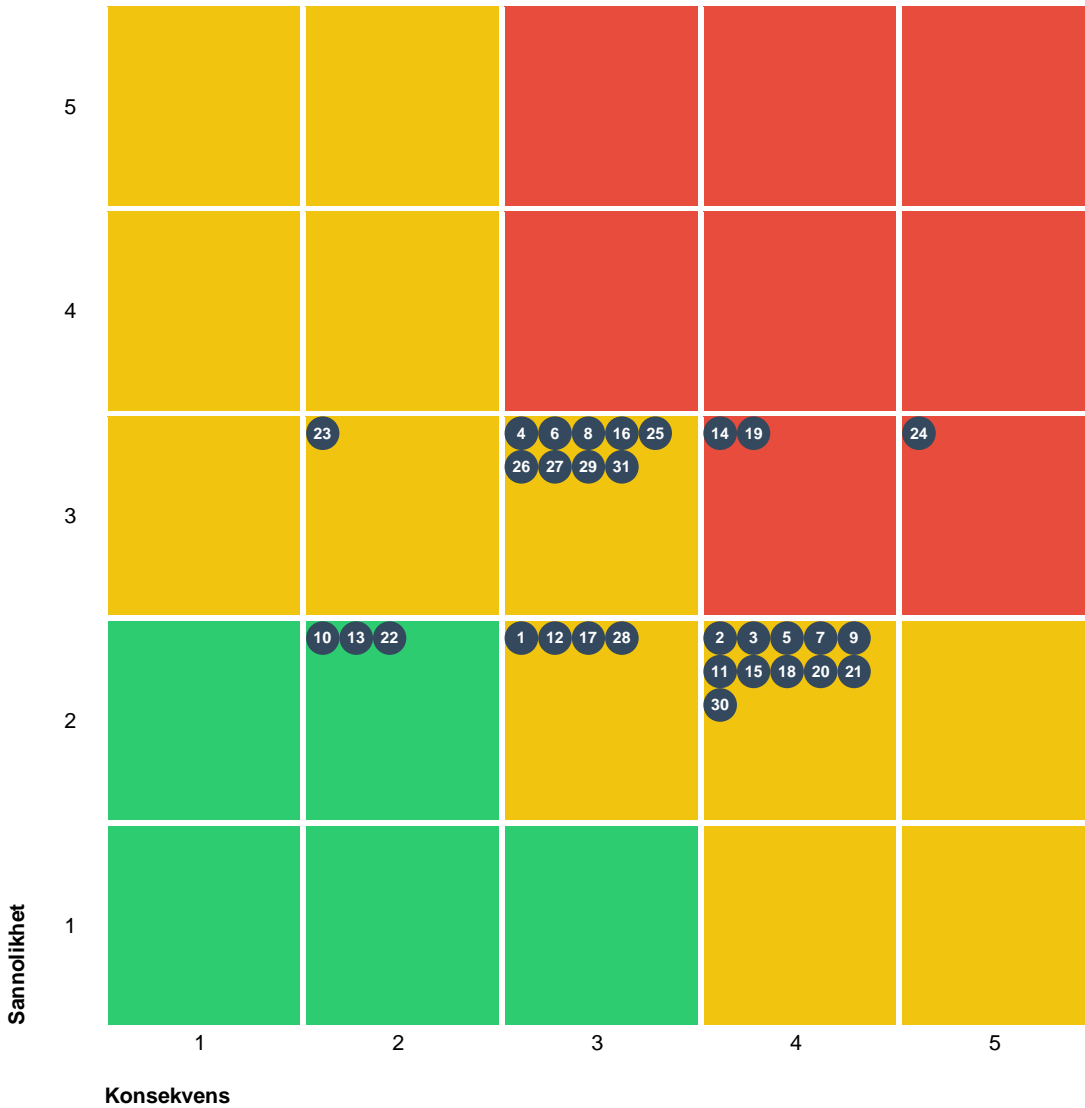
Internkontrollplanen är upprättad med utgångspunkt i att de av fullmäktige fastställda målen uppfylls. Utifrån bedömningen om påverkbara och icke påverkbara risker är fokus i internkontrollplanen att granska efterlevnad av lagar och policys, program, riktlinjer och ekonomistyrning samt uppföljning av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



3 Kritisk 25 Medium 3 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	Arbetsätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	R V	IKP
3.1 Stockholms ekonomi är stark, hållbar och lägger grunden för en jämlik välfärd	Finansförvaltning.	Hantering och av leverantörsfakturer och intäkter i Agresso samt utlägg som	1	Att allegat som styrker inköpet (utlägg) inte finns i samtliga fall.	2. Mindre sannolikt	3. Kännbar	6	★
			2	Att attestinstruktionerna inte följs.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR

KF:s mål för verksamhetsområdet	Process	Arbetsätt	Nr	Oönskad händelse	Sannolihet	Konsekvens	R V	IKP		
		hanteras i lönesystemet.	3	Att försäljningsintäkterna inte faktureras korrekt.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR		
			4	Att instruktioner om hur hanteringen av inköp genom utlägg ska ske är otydliga.	3. Möjlig	3. Kännbar	9	★		
			5	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	6	Att dokument inte diarieförs och arkiveras enligt gällande regler.	3. Möjlig	3. Kännbar	9	★		
			Personaladministration och hantering av löneunderlag / lönerapporter.	Hantera personuppgifter och löneuppgifter till lönesystemet	7	Att anställning och löneändringar inte registreras korrekt i lönesystemet och loggas.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
					8	Att personalpolicyn inte efterlevs.	3. Möjlig	3. Kännbar	9	Nej, endast VoR
	Löpande arbete inom HR med processer och utbildningar	9	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	10	Att anställda inte har rätt kompetens.	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
	11				Att verksamhetens åtaganden inte är väl kommunicerade och implementerade.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR	
Hantera den digitala infrastrukturen	12			Att den digitala infrastrukturen brister vilket medför att verksamheten inte kan leverera mot sina åtaganden.	2. Mindre sannolikt	3. Kännbar	6	Nej, endast VoR		
	13			Att organisationen saknar tydligt förtecknade ansvarsområden som framgår av	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR		

KF:s mål för verksamhetsområdet	Process	Arbetsätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	R V	IKP
				arbetsordning, delegationsordning och attestinstruktion.				
			14	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	1 2	★
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	15	Att attestinstruktionen inte följs för utläggsredovisningar.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
			16	Att attestinstruktionens regelverk inte är känt och inte följs av såväl godkännare som attestant i Agresso.	3. Möjlig	3. Kännbar	9	★
			17	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	18	Att attestinstruktionerna inte följs.	2. Mindre sannolikt	4. Allvarlig	8	★
			19	Att riktlinje om mutor och representation, personalförmåner, gåvor etc. inte är känd och följs.	3. Möjlig	4. Allvarlig	1 2	★
			20	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	21	Bristfällig krisledningsförmåga och beredskap.	2. Mindre sannolikt	4. Allvarlig	8	Nej, endast VoR
	Systematiskt informations säkerhetsarbete	Behörighetshantering	22	Behörighet till verksamhetssystem avslutas inte i samband med att en anställning upphör eller förändrat arbetsinnehåll	2. Mindre sannolikt	2. Lindrig	4	Nej, endast VoR
		Implementering av lokal	23	Att verksamheten brister i arbetet med	3. Möjlig	2. Lindrig	6	Nej, endast VoR

KF:s mål för verksamhetsområdet	Process	Arbetsätt	Nr	Oönskad händelse	Sannolikhet	Konsekvens	R V	IKP
		anvisning		informationssäkerhet				ast VoR
		Incidenthantering	2 4	Att en personuppgiftsincident inträffar	3. Möjlig	5. Mycket allvarlig	1 5	★
			2 5	Att verksamheten brister i arbetet med informationssäkerhet och en incident inträffar	3. Möjlig	3. Kännbar	9	★
		Informationsklassning	2 6	Att gällande lagar, regler, policys, program, riktlinjer inte är kända och följs.	3. Möjlig	3. Kännbar	9	Nej, end ast VoR
			2 7	Att åtgärdslistan efter genomförd informationsklassning inte hanteras och åtgärder inte vidtas	3. Möjlig	3. Kännbar	9	Nej, end ast VoR
		Informationssäkerhet inom upphandlingsförfarande	2 8	Att bristande eller felaktiga krav ställs i en upphandling	2. Mindre sannolikt	3. Kännbar	6	Nej, end ast VoR
3.6 Tryggheten ska öka genom förebyggande insatser	Systematiskt arbetsmiljöarbete (SAM).	Hantera rutiner och rutinbeskrivningar för oönskade händelser.	2 9	Att policys, program, riktlinjer, regler och rutiner är otydliga.	3. Möjlig	3. Kännbar	9	Nej, end ast VoR
		Systematiskt brandskyddsarbete (SBA)	Alla medarbetare ska ha kunskap om brandskydd och beredskap för oväntade olyckshändelser	3 0	Att det inte finns förebyggande brandskyddsinstruktioner.	2. Mindre sannolikt	4. Allvarlig	8
	Hantera rutiner och rutinbeskrivningar för brandskyddet	3 1	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	Arbetsätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
Finansförvaltning.	Hantering och av	Kontroll av	Att allegat som	Stickprovskontroll

Process	Arbetsätt	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. 9 Att instruktioner om hur hanteringen av inköp genom utlägg ska ske är otydliga.	varje månad i bolagen. Stickprovskontroller i utläggsredovisningarna varje månad kopplat till manualer och instruktioner.
Förmögenhetsskydd samt skydd av dokument och arbetspapper.	Hantering av dokument i eDok och inom registraturet	Utbildning och information om eDok	9 Att dokument inte diarieförs och arkiveras enligt gällande regler.	Översyn av strukturen för hantering av digitala dokument.
Personaladministration och hantering av löneunderlag/lönerapporter.	Löpande arbete med utläggsredovisningar i lönesystemet	Utläggredovisningar 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	Arbetsätt	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 Att verksamhetens styrdokument är otydliga eller rutiner är bristfälligt 2 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	Arbetsätt	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.
		Utläggredovisningar granskas löpande innan de skickas för attest i lönesystemet	1 Att riktlinje om mutor och representation, personalförmåner, gåvor etc. inte är känd och följs. 2	Stickprovskontroll varje månad i bolagen.

3.5 Hög beredskap och stark rådighet ska råda i alla verksamhetsområden

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

Process	Arbetsätt	Systematisk kontroll	Oönskad händelse	Kontrollaktivitet
arbete		registerförteckningen	1 5 t inträffar	registerförteckningen
		Regelbundna utbildningar inom informationssäkerhet och GDPR	9  Att verksamheten brister i arbetet med informationssäkerhet och en incident inträffar	Årlig uppföljning av genomförda utbildningar

3.6 Tryggheten ska öka genom förebyggande insatser

Process	Arbetsätt	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 översyn och revidering av brandskyddsinstruktioner och säkerhetsföreskrifter samt implementering av dessa i samband med flytt till nya kontorslokaler