Väsentlighets- och riskanalys samt internkontrollplan 2026 för Stockholm Business Region AB

Innehållsförteckning

Inledning

Syftet med intern kontroll är att med rimlig grad av säkerhet säkerställa att verksamheten bedrivs på ett ändamålsenligt och effektivt sätt, att information om verksamhet och ekonomi är tillförlitlig och rättvisande samt att gällande lagar, förordningar, föreskrifter och styrdokument följs. Bestämmelser om intern kontroll för de kommunala bolagen återfinns i aktiebolagslagen.

Väsentlighets- och riskanalysen fungerar som fundamentet för bolagets arbete med intern kontroll och är ett centralt verktyg för att identifiera och begränsa risker inom verksamheten. Identifierade risker bedöms med ett riskvärde på maximalt 16, ett riskvärden på 8 eller över tas automatiskt med i internkontrollplanen. Risker med ett värde under 8 kan accepteras eller åtgärdas omedelbart via en direktåtgård. Analysen utgår från bolagets mest betydelsefulla processer och delprocesser, varav vissa är obligatoriska. Genom att systematiskt kartlägga och bedöma risker i dessa kan bolaget arbeta förebyggande, åtgärda brister och på så sätt minska risken för fel och oegentligheter.

Internkontrollplanens huvudsakliga syfte är att säkerställa kvaliteten i bolagets processer och att minska risken för fel, brister och oegentligheter. Genom de kontroller som ingår i planen skapas ett underlag för lärande och utveckling, eftersom resultaten kan användas för att förbättra centrala processer och ge en tydligare bild av hur väl den interna kontrollen fungerar.

Arbetet med att gemensamt identifiera risker inom de mest betydelsefulla processerna bidrar dessutom till ett ökat organisatoriskt lärande. Det ger insikter som kan användas för att utveckla verksamheten på en övergripande nivå, exempelvis genom att identifiera behov av samordning eller vidareutveckling av processer inom staden.

Ansvar

Bolagsstyrelsen har ansvar för den interna kontrollen i den egna verksamheten. I likhet med nämndernas arbetssätt ska bolagsstyrelsen säkerställa att denna är tillräcklig för att förebygga fel och oegentligheter i verksamheten samt att den bedrivs på ett i övrigt tillfredsställande sätt. Detta omfattar att utforma och organisera den interna kontrollen och skapa effektiva system för uppföljning.

Bolagen ska i samband med verksamhetsplaneneringen:
• upprätta och besluta om ett system för intern kontroll.
• genomföra och besluta om en väsentlighets- och riskanalys.
• upprätta och besluta om en internkontrollplan utifrån genomförd väsentlighets- och riskanalys.

Dessa dokument ska biläggas verksamhetsplanen.

Bolaget ska under verksamhetsåret genomföra de åtgärder och kontroller som beskrivs i väsentlighets- och riskanalysen samt internkontrollplanen.

Bolaget ska i samband med verksamhetsberättelsen:
• redovisa genomförda direktåtgärder.
• redovisa resultatet av samtliga genomförda kontroller enligt internkontrollplanen.

• redovisa vilka korrigerande åtgärder som genomförts med anledning av kontrollerna.
• bedöma om bolagets interna kontroll under det föregångna året varit tillräcklig, delvis tillräcklig eller otillräcklig.

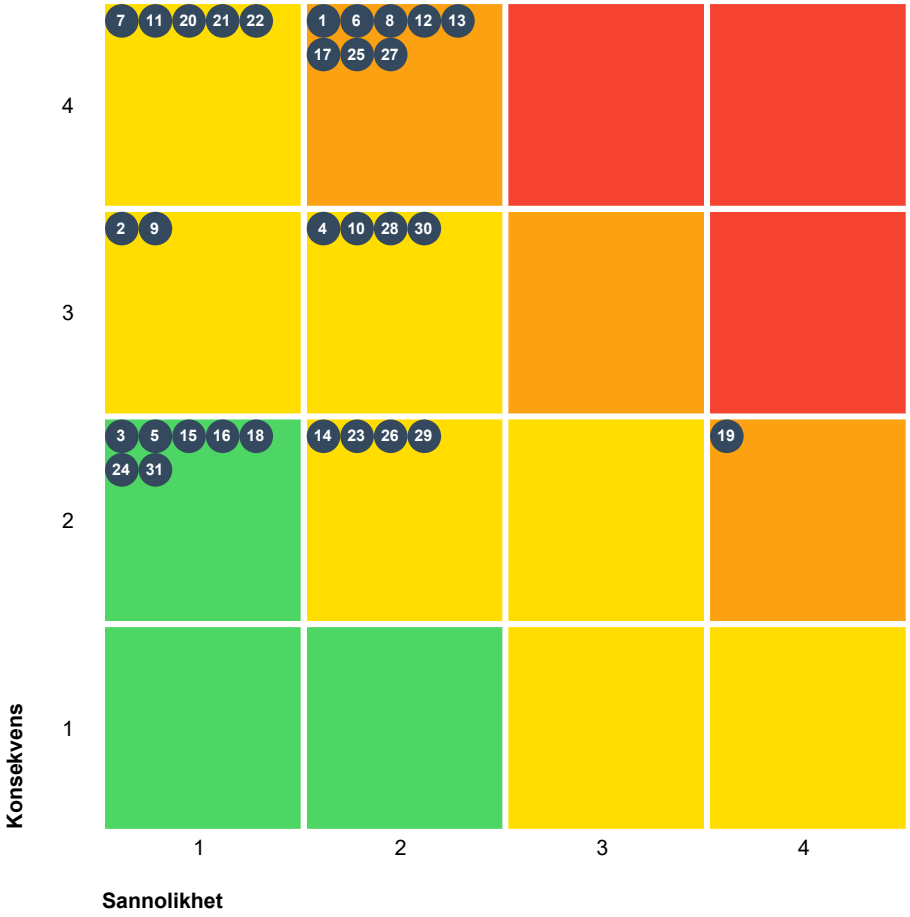
Verkställande direktör
VD ska:
• rapportera till bolagsstyrelsen hur den interna kontrollen fungerar samt föreslå nödvändiga åtgärder.
• säkerställa att bolagets chefer och medarbetare har kunskap om de lagar, föreskrifter, riktlinjer och rutiner som gäller för verksamheten samt om hur brister och avvikelser ska rapporteras.
• inom bolaget skapa förutsättningar för en arbetsplatskultur som främjar god intern kontroll.

Chefer
Samtliga chefer ska:
• säkerställa att deras underställda medarbetare har kunskap om de lagar, föreskrifter, riktlinjer och rutiner som gäller för verksamheten samt om hur brister och avvikelser ska rapporteras.
• skapa förutsättningar för en arbetsplatskultur som främjar god intern kontroll.
• rapportera brister och avvikelser i enlighet med bolagets system för intern kontroll.

Medarbetare
Samtliga medarbetare ska:
• följa de lagar, föreskrifter, riktlinjer och rutiner som gäller för verksamheten.
• bidra till att skapa en arbetsplatskultur som främjar god intern kontroll.
• rapportera brister och avvikelser i enlighet med bolagets system för intern kontroll.

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

Riskö̈versikt



9 Hög 15 Medium 7 Låg | Totalt: 31

Kritisk	
Hög	
Medium	
Låg	

	Konsekvens	Sannolikhet
4	Allvarlig	Mycket hög
3	Betydande	Hög
2	Måttlig	Medelhög
1	Försumbar	Låg

Process	Delprocess	Nr	Risk	Risknivå	Förebyggande hantering	Direktåtgärder
Ekonomistyrning	**Budget och uppföljning, investeringsstyrning**	1	**Att försäljningsintäkterna inte faktureras korrekt.**	Hög (8)	Regelbunden avstämning av relevanta huvudbokskonton	

Process	Delprocess	Nr	Risk	Risknivå	Förebyggande hantering	Direktåtgärder
		2	**Att verksamhetens åtaganden inte är väl kommunicerade och implementerade.**	Medium (3)	Löpande prognos och uppföljning i ILS	
	Penninghantering, fakturering, fakturahantering och medelsförvaltning	3	**Att allegat som styrker inköpet (utlägget) inte finns i samtliga fall.**	Låg (2)	Systematisk kontroll av leverantörsfakturor i Agresso och av utläggen i Visma Expense.	
		4	**Att arbetsordning, delegationsordning och attestinstruktionerna inte följs.**	Medium (6)	Systematisk kontroll av leverantörsfakturor i Agresso och utlägg i Visma Expense	
	Redovisning	5	**Bolagets redovisning inte följs upp genom regelbundna avstämningar och kontroller.**	Låg (2)	Regelbunden avstämning av relevanta huvudbokskonton	
Fysisk säkerhet	**Hantera rutiner och rutinbeskrivningar för brandskyddet**	6	**Att policys, program, riktlinjer, regler och rutiner är otydliga.**	Hög (8)	Årlig uppföljning av verksamhetens rutiner för brandskyddet.	
	Löpande brandskydds- och säkerhetsarbete	7	**Systematiskt arbete sker inte enligt regler och krav vilket ökar risken för brandskydds- och/eller säkerhetsbrister.**	Medium (4)	Systematiskt brandskyddsarbete utförs enligt gällande regelverk	
Inköp	**Avrop**	8	**Felaktiga avrop genomförs på befintliga avtal**	Hög (8)	Tydliga beställningsrutiner kopplat till avtal.	
	Avtal	9	**Avtal utformas felaktigt exempelvis kopplat till takvolymer.**	Medium (3)	Tillräcklig information och stöd kring takvolymer.	
	Kategoristyrning					

Process	Delprocess	Nr	Risk	Riskvå	Förebyggande hantering	Direktåtgärder
	Upphandling	10	**Upphandlingsprocessen påbörjas inte i tid.**	Medium (6)	Information kring upphandlingsprocessen process och tidsåtgång.	
Motverka otillåten påverkan	**Förebygga otillåten påverkan**	11	**Att riktlinje om mutor och representation, personalförmåner, gåvor etc. inte är känd och följs.**	Medium (4)	Information och rutiner finns och är kända i verksamheten gällande otillåten påverkan	
	Hantera otillåten påverkan	12	**Att uppföljning och efterkontroll av poster rörande representation, personalförmåner och gåvor inte sker löpande.**	Hög (8)	Löpande uppföljning och efterkontroll av poster rörande representation, personalförmåner och gåvor.	
Motverka välfärdsbrott	**Förebygga välfärdsbrott**	13	**Kunskap kring hur det förebyggande arbetet kan genomföras är inte känt.**	Hög (8)	Stärka informationen kring hur välfärdsbrott kan förebyggas.	
	Hantera välfärdsbrott	14	**Inga rutiner kring hanteringen av välfärdsbrott finns och/eller är väl kända**	Medium (4)	Tydlig information och rutiner gällande välfärdsbrott.	
	Upptäcka välfärdsbrott	15	**Ingen information kring hur välfärdsbrott upptäcks finns alternativt är inte kända i bolaget**	Låg (2)	Tydlig information kring hur välfärdsbrott upptäcks.	
Personalhantering	**Arbetsmiljö**	16	**Att personalpolicyn inte efterlevs.**	Låg (2)	Ha en löpande dialog om personalpolicyn på t.ex. APT och gemensamma möten	
	Lönehantering	17	**Att frånvaro inte registreras korrekt vilket medför att en lön blir felaktig**	Hög (8)	Regelbunden avstämning av lönerna före utbetalning	
	Rekrytering	18	**Att anställning och personuppgifter inte registreras korrekt i lönesystemet och loggas.**	Låg (2)	Tydliga rutiner vid registrering i lönesystemet.	

Process	Delprocess	Nr	Risk	Risknivå	Förebyggande hantering	Direktåtgärder
Skydd och bevarande av digitala och analoga dokument.	**Hantering av dokument i eDok och inom registraturet**	19	**Att dokument inte diarieförs och arkiveras enligt gällande regler.**	Hög (8)	Tydliga rutiner och information gällande diarieföring.	
Stockholms stads säkerhetsprogram.	**Hantera rutiner och rutinbeskrivningar för krisledningsarbetet**	20	**Bristfällig krisledningsförmåga och beredskap.**	Medium (4)	Tydliga och kommunicerade rutiner.	
Styrning och uppföljning av verksamheten.	**Hantera styr- och stöddokument**	21	**Att organisationen saknar tydligt förtecknade ansvarsområden som framgår av arbetsordning, delegationsordning och attestinstruktion.**	Medium (4)	Tillse att berörda dokument är tydliga och kommunicerade.	
		22	**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.**	Medium (4)	Tydliga och kommunicerade styrdokument och rutiner.	
	Säkerställa och hantera den digitala infrastrukturen	23	**Att den digitala infrastrukturen brister vilket medför att verksamheten inte kan leverera mot sina åtaganden.**	Medium (4)	Säkerställ och arbeta förebyggande med den digitala infrastrukturen.	
Systematiskt informationssäkerhetsarbete	**Fastställa krav genom informationsklassning**	24	**Att gällande lagar, regler, policys, program, riktlinjer inte är kända och följs.**	Låg (2)	Utföra åtgärder för att höja kunskapen inom området, såsom utbildning, informationsklassning enligt årshjul.	
		25	**Att åtgärdslistan efter genomförd informationsklassning inte hanteras och åtgärder inte**	Hög (8)	Uppföljning enligt av alla informationsklassningar enligt årshjulet.	

Process	Delprocess	Nr	Risk	Risknivå	Förebyggande hantering	Direktåtgärder
			vidtas			
	Fastställa lokal anvisning för informationssäkerhet	26	**Att de olika rollerna med tillhörande ansvar inte är tydligt kommunicerat**	Medium (4)	Regelbunden uppföljning av årshjulet och det ansvar som är fördelat mellan de olika rollerna	
		27	**Att verksamheten brister i arbetet med informationssäkerhet**	Hög (8)	Uppföljning enligt årshjulet.	
	Informationssäkerhet inom upphandlingsförfarande	28	**Att bristande eller felaktiga krav ställs i en upphandling**	Medium (6)	Kontakt med Informationssäkerhetssamordnare (ISAM) tidigt i upphandlingsförförande.	
	Lokal rutin för behörighetshantering	29	**Behörighet till verksamhetssystem avslutas inte i samband med att en anställning upphör eller förändrat arbetsinnehåll**	Medium (4)	Hanteras i processen för off-boarding. Löpande uppföljning genom stickprover och årshjul.	
	Rutin för incidenthantering	30	**Att en personuppgiftsincident inträffar**	Medium (6)	Processerna kring personuppgiftshantering finns och är väl kommunicerade.	
		31	**Att verksamheten brister i förmåga att hantera en förfrågan om registerutdrag**	Låg (2)	Säkerställa löpande att processer finns och fungerar för personuppgiftsincidenter.	

Internkontrollplan

Process	Delprocess	Risk	Riskvärde	Förebyggande hantering	Kontroll
Ekonomistyrning	**Budget och uppföljning, investeringsstyrning**	**Att försäljningsintäkterna inte faktureras korrekt.**	Hög (8)	Regelbunden avstämning av relevanta huvudbokskonton	**Regelbundna avstämningar av intäkterna.**
Fysisk säkerhet	**Hantera rutiner och rutinbeskrivningar för brandskyddet**	**Att policys, program, riktlinjer, regler och rutiner är**	Hög (8)	Årlig uppföljning av verksamhetens rutiner för brandskyddet.	**Säkerställ att den årliga uppföljning av verksamhetens rutiner för**

Process	Delprocess	Risk	Riskvärde	Förebyggande hantering	Kontroll
		otydliga.			**brandskyddet är genomförd.**
Inköp	**Avrop**	**Felaktiga avrop genomförs på befintliga avtal**	Hög (8)	Tydliga beställningsrutiner kopplat till avtal.	**Kontroll av att det finns beställningsrutiner kopplat till avtal.**
Motverka otillåten påverkan	**Hantera otillåten påverkan**	**Att uppföljning och efterkontroll av poster rörande representation, personalförmåner och gåvor inte sker löpande.**	Hög (8)	Löpande uppföljning och efterkontroll av poster rörande representation, personalförmåner och gåvor.	**Kontrollera att löpande uppföljning och efterkontroll av poster för representation, personalförmåner och gåvor har gjorts.**
Motverka välfärdsbrott	**Förebygga välfärdsbrott**	**Kunskap kring hur det förebyggande arbetet kan genomföras är inte känt.**	Hög (8)	Stärka informationen kring hur välfärdsbrott kan förebyggas.	**Kontrollera att information kring det förebyggande arbetet kopplat till välfärdsbrott är kommunicerat och känt.**
Personalhantering	**Lönehantering**	**Att frånvaro inte registreras korrekt vilket medför att en lön blir felaktig**	Hög (8)	Regelbunden avstämning av lönerna före utbetalning	**Stickprovskontroller i utbetalda löner**
Skydd och bevarande av digitala och analoga dokument.	**Hantering av dokument i eDok och inom registraturet**	**Att dokument inte diarieförs och arkiveras enligt gällande regler.**	Hög (8)	Tydliga rutiner och information gällande diarieföring.	**Stickprovskontroller enligt årshjulet**
Systematiskt informationssäkerhet sarbete	**Fastställa krav genom informationsklassning**	**Att åtgärdslistan efter genomförd informationsklassning inte hanteras och åtgärder inte vidtas**	Hög (8)	Uppföljning enligt av alla informationsklassningar enligt årshjulet.	**Stickprovskontroll av åtgärdslistan.**
	Fastställa lokal anvisning för informationssäkerhet	**Att verksamheten brister i arbetet med informationssäkerhet**	Hög (8)	Uppföljning enligt årshjulet.	**Stickprovskontroller av processer i årshjulet**