Skellefteå kommun

Skellefteå Museum AB

Internkontroll-plan 2023

Datum: 2022-12-15

Innehåll

Sammanfattning **3**

Riskbedömning **4**

Internkontrollplan **6**

Sammanfattning

Enligt fullmäktiges riktlinjer för intern kontroll (KF 2015-09-15 § 231) ska riskbedömningar göras för att kunna rikta kontroller och uppföljning dit där de bäst behövs.

Målet med den interna kontrollen är att identifiera och förebygga risker som kan hindra att:

- verksamheten är ändamålsenlig och kostnadseffektiv (**Ändamålsenlig verksamhet**)
- den finansiella rapporteringen och information om verksamheten är tillförlitlig (**Rättvisande information**)
- lagar, regelverk, policys och principer efterlevs såväl externa som interna (**Lagar och regler**)

Intern kontroll utgår ifrån följande delar:

1. Kontrollmiljö (vilka processer och strukturer som stödjer den interna kontrollen)
2. Riskbedömning (identifiera interna och externa risker för att inte nå ovanstående mål)
3. Kontrollaktiviteter (kontroller för att upptäcka eventuella fel och motverka risken)
4. Information & kommunikation (information och kommunikation av utfallet av genomförda kontroller)
5. Uppföljning & utvärdering (Kontinuerligt utvärdera och utveckla den interna kontrollen)

Riskbedömning

Identifierade risker inom väsentliga processer har värderats utifrån konsekvens och sannolikhet. Riskvärdet (konsekvens · sannolikhet) har graderats enligt följande: grön (0-2) – låg risk, gul (3-4) – medelhög risk och röd (6, 9) – hög risk.

Vissa risker har valts ut att följas upp i internkontrollplanen medan andra risker har lämnats utan åtgärd. Vissa risker kan även kräva mer direkta åtgärder. För år 2023 kommer internkontrollen att fokuseras på redovisningskontroller, personalkostnader, betalningar, representation samt efterlevnad av attestregler samt besluts- och delegationsordning. Kommunstyrelsen har även fattat beslut om koncernövergripande granskningsområden som för år 2023 är krisberedskap, kompetensförsörjning, bisysslor, IT-säkerhet samt mutor, korruption och efterlevnad av jävsregler.

Internkontrollplanen innehåller de aktiviteter som har bedömts vara tillräckliga för att säkerställa en god intern kontroll. Planen tydliggör hur kontrollerna ska gå till och vem som är ansvarig för dem samt vem som utför kontrollerna. Resultatet av kontrollerna och en utvärdering av internkontrollarbetet ska återrapporteras för beslut i nämnden/bolaget enligt fastställd tidplan.

Samtliga kontrollaktiviteter har utförts och dokumenterats i enlighet med fastställd plan. Förbättringsområden har identifierats och noterats i förekommande fall.

Den samlade bedömningen av 2023 års internkontroll är att den varit tillräcklig och fungerat på ett tillfredställande sätt. Kontrollresultaten visar samtidigt att verksamheten i allt väsentligt drivits i enlighet med fastställda mål, lagar och regelverk.

Riskbedömning

Definitioner:

Mål: *Anges vilket mål som kontrollaktiviteterna kopplat till som riskbedömningen ska möta*

- *Ändamålsenlig och kostnadseffektiv verksamhet*
- *Rättvisande information, ekonomi och verksamhet*
- *Lagar och regler externa och interna*

Process/rutin/område: *Beskriv vilken process, rutin eller område där en risk har identifierats.*

Risk: *Beskriv risken som har identifierats som riskerar att mål inte uppnås (ändamålsenligt och kostnadseffektiv verksamhet, rättvisande information eller lagar och regler.*

Konsekvenser: *Lämna en beskrivning över vilka konsekvenser som är kopplade till identifierad risk.*

Färg används grön (0-2) – låg risk, gul (3-4) – medelhög risk och röd (6, 9) – hög risk

Nr	Mål	Process/rutin/område	Risk	Konsekvenser - beskrivning	Konsekvens 0-3	Sannolikhet 0-3	Riskvärde 0-9	Åtgärd J/N	IK-plan J/N
1	Lagar och regler	Krisberedskap	Risk att bolaget saknar krisberedskap.	Kan leda till ökad risk vid olyckor.	3	1	3	N	J
2	Lagar och regler	Mutor, korruption och efterlevnad av jävsregler.	Risk att bolagets VD, styrelse eller anställda saknar kunskap om, eller följer inte kommunens riktlinjer samt att beslut fattas av person som inte anmält jäv.	Kan leda till att personer som utsätts för eller misstänker att detta förekommer i verksamheten inte har vägledning i hur de skall agera.	3	1	3	N	J
3	Lagar och regler	IT-säkerhet	Risk att styrdokument inte är kända för chefer och anställda samt otillräckligt skydd mot intrång och sabotage.	Kan leda till att styrning av IT-säkerhet ej lever upp till fattade beslut samt att externa parter får tillgång till information.	2	2	4	J	J
4	Ändamålsenlig och kostnadseffektiv	Kompetensförsörjning	Risk att kritiska funktioner försvinner.	Kan leda till att funktioner blir sårbara om medarbetare, som är ensamma på sin position, lämnar bolaget.	2	1	2	N	J
5	Lagar och regler	Bisysslor	Olämpliga bisysslor hos personer i ledande/beslutande ställning.	Kan leda till förtroendeskadliga och konkurrerande bisysslor.	3	1	3	N	J
6	Lagar och regler	Regler och anvisningar	Risk att någon ny regel eller anvisning inte uppmärksammas eller implementeras.	Kan leda till felaktiga räkenskaper.	2	1	2	N	N

7	Ändamålsenlig och kostnadseffektiv	Försäkringsärenden	Risk för att museets kulturhistoriska byggnader och andra försäkringspliktiga tillgångar saknas adekvat försäkringsskydd.	Kan leda till att bolaget belastas med stora kostnader i samband med försäkringsärenden.	3	2	6	N	N
8	Rättvisande information	Redovisningskontroller	Risk för att redovisningen inte är korrekt eller komplett.	Kan leda till felaktiga räkenskaper.	2	1	2	N	J
9	Lagar och regler	Personalkostnader	Risk för att personalens ersättning betalas ut felaktigt.	Förtroendeskada och skattemässiga konsekvenser.	2	1	2	N	J
10	Lagar och regler	Delegation	Risk för brister i efterlevnad i delegationsordning.	Kan leda till att verksamhetsärenden fattas av felaktiga beslutsorgan.	3	1	3	N	J
11	Lagar och regler	Betalningar	Risk för brister i säkerheten kring betalningar.	Kan leda till otillåtna utbetalningar.	3	1	3	J	J
12	Lagar och regler	Efterlevnad attestregler	Risk för att fakturor och verifikat inte attesteras korrekt.	Kan leda till att fakturor och verifikat attesteras av anställda utan någon attesträtt.	2	1	2	N	J
13	Lagar och regler	Representation	Risk för att representationsreglerna inte följs.	Förtroendeskada och skattemässiga konsekvenser.	2	1	2	N	J
14	Ändamålsenlig och kostnadseffektiv	Mål- och resultatstyrning	Risk för att företaget inte styr mot uppsatta mål och resultat.	Kan leda till att bolaget inte styrs i enlighet med ägardirektivet.	2	1	2	N	N

Kommentarer: Risker som har ett högt riskvärde (rödmarkerade och vissa gulmarkerade) och anses prioriterade medför ***kontroller ska genomföras som en del av internkontrollplanen vilket markeras med J i rutan för IK-plan***. Om det anses att åtgärder behöver vidtas för ***att förbättra process, rutin etc markeras ett J i rutan för åtgärd***. Risker med lägre riskvärde (grönmarkerade och vissa gulmarkerade) lämnas utan åtgärd markeras med N i rutan för åtgärd och N i rutan för IK-plan.

Internkontrollplan

Nr	Process/rutin	Risk	Kontrollaktivitet	Frekvens/tidpunkt	1.Ansvarig för process 2.Kontroll utförs av
1	Krisberedskap	Risk att bolaget saknar krisberedskap.	Inventera om bolaget har en aktuell krisberedskapsplan.	En ggr år/höst.	1. VD 2. Ekonomichef
Beskrivning av utförd granskning: Skellefteå Museum arbetar strukturerat med policyarbetet utifrån ett årshjul. Vid varje ledningsgruppsmöte tas tillämpliga policys upp utifrån ett beslutat årshjul och extra viktiga policys gås igenom vid nästkommande APT (arbetsplatsträff). På APT delas medarbetarna in i grupper och diskuterar policyn och kommer med synpunkter. Därefter kan eventuell justering göras i ledningsgruppen. På arbetsplatsträffen 230301 gick krishanteringsplanen igenom. *Resultat av utförd granskning:* Granskat uppdaterad krishanteringsplan daterad 2023-02-07. 230301 presenterades denna på APT för all personal. *Slutsats av utförd granskning:* Med tanke på att krishanteringsplanen gås igenom gruppvis så är risken att någon medarbetare ska missa vad det är som gäller väldigt liten. *Rekommenderad åtgärd:* Ingen åtgärd bedöms vara nödvändig					
2	Mutor, korruption och efterlevnad av jävsregler.	Risk att bolagets VD, styrelse eller anställda saknar kunskap om, eller följer inte kommunens riktlinjer samt att beslut fattas av person som inte anmält jäv.	Kontrollera om bolaget känner till och följer kommunens riktlinjer. Samt om organisationen känner till jävsreglerna. Kontrollera hur organisationen har informerats och påmints.	En ggr år/höst.	1. VD 2. Ekonomichef
Beskrivning av utförd granskning: Efter kontroll har av Skellefteå Museums årshjul och konstateras att policyn inte tas upp som en separat policy. Däremot så tas jäv och korruption upp i dokumentet Allt du behöver veta om Skellefteå museum, som även har granskats. Dokumentet är uppdaterat 23-09-20. *Resultat av utförd granskning:* I och med att det finns med i dokumentet Allt du behöver veta så får alla nyanställda ta del av den informationen när de börjar och årsvis gås dokumentet igenom i ledningsgrupp samt på APT för alla anställda.					

Slutsats av utförd granskning: Utifrån gjord granskning hittas ingenting som indikerat att bolaget inte följer reglerna för mutor och korruption. *Rekommenderad åtgärd:* Ingen åtgärd bedöms vara nödvändig					
3	IT-säkerhet	Risk att styrdokument inte är kända för chefer och anställda samt otillräckligt skydd mot intrång och sabotage.	Kontrollera om bolagets IT-säkerhet är tillfredsställande och om styrdokument har kommunicerats i organisationen.	En ggr år/höst.	1. VD 2. Ekonomichef
Beskrivning av utförd granskning: Efter en kontroll av Skellefteå Museums årshjul konstateras att policyn inte tas upp som en separat policy i årshjulet. Däremot så har organisationen informerats via dokumentet Kravkatalog av informationssäkerhetsåtgärdet för IT-system som har förmedlats till alla anställda. *Resultat av utförd granskning:* Utifrån granskningen framkom inget annat än att bolaget följer policyn och alla anställda informeras kontinuerligt i vad det är som gäller. *Slutsats av utförd granskning:* Eftersom att det inte finns någon anställd som enbart arbetar med IT-frågor ligger ansvaret på VD och ekonomichef. Det föreligger en risk i att dessa frågor inte prioriteras i den utsträckning som behövs då andra mer akuta frågor behöver åtgärdas. Det inbokade mötet med kommunens IT säkerhetsavdelning och medverkan i digitaliseringsrådet är viktigt utifrån att minska risken att anställda inte har tillräcklig kunskap i att skydda mot intrång och sabotage. Framöver kan det vara läge att se över möjligheten att ha ett mer nära samarbete med kommunen i dessa frågor. *Rekommenderad åtgärd:* Ta diskussion i digitaliseringsrådet om hur vi bör gå vidare för att säkerhetsställa att Skellefteå Museum följer kommunens gällande IT-policys då utvecklingen gällande IT-frågor går väldigt snabbt och VD och ekonomichef har svårt att prioriteras dessa frågor i den omfattning som kommer att behövas framöver.				

Nr	Process/rutin	Risk	Kontrollaktivitet	Frekvens/tidpunkt	1.Ansvarig för process 2.Kontroll utförs av
4	Kompetensförsörjning	Risk att kritiska funktioner försvinner.	Inventera om bolaget har rutinbeskrivningar.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning
Kontrollerat om uppdaterade rutinbeskrivningar finns.

Resultat av utförd granskning:
Inga uppdaterade rutinbeskrivningar har framkommit vid granskning

Slutsats av utförd granskning:
Skellefteå Museum saknar rutinbeskrivningar och processdokumentationer.

Rekommenderad åtgärd:
VD bör se över behovet och eventuellt upprätta rutinbeskrivningar för kritiska funktioner.

5	Bisysslor	Olämpliga bisysslor hos personer i ledande/beslutande ställning.	Inventeras centralt för hela kommunkoncernen med hjälp av registeranalys.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning:
KPMGs bisysslokollen har använts för att kontrollera samtliga anställda och styrelseledamöter förekomst i bolagsregistret.

Resultat av utförd granskning: Ingen person i ledande/beslutande ställning har identifierats med olämplig bisyssla enligt genomförd registeranalys. Skellefteå Museum följer Skellefteå Kommuns policy gällande bisysslor.

Slutsats av utförd granskning: Skellefteå Museum bedöms följa policyn för bisysslor.

Rekommenderad åtgärd: Inga ytterligare åtgärder bedöms behövas.

8	Redovisningskontroller	Risk för att redovisningen inte är korrekt eller komplett.	Stickprovskontroll av en period i redovisningen, med avseende på relevans, riktighet, attest och kontering.	En ggr år/höst.	1. VD 2. Ekonomichef

*Beskrivning av utförd granskning**:*** Granskning av samtliga fakturor i maj med avsikt att granska relevant, riktighet, attest och kontering.
Kundfaktura nummer: 30020-30024 Levfakturanummer 30345-30421 samt verifikat 30072-30086.
Alla fakturor attesteras i turordning av avdelningschef som kontrollerar med beställare om riktigheten och leverans, därefter vd som slutattesterar. Innan vd:s slutattest går inte fakturan att betala, via en spärr i systemet.

Resultat av utförd granskning: Vid granskningen konstaterades inga felaktigheter, inga saknade attestering eller felaktig kontering.

Slutsats av utförd granskning: Utifrån den granskning som gjort är bedömningen att delegationsordningen följs.

Rekommenderad åtgärd: Inga ytterligare åtgärder bedöms behövas.

Nr	Process/rutin	Risk	Kontrollaktivitet	Frekvens/tidpunkt	1.Ansvarig för process 2.Kontroll utförs av
9	Personalkostnader	Risk för att personalens ersättning betalas ut felaktigt.	Stickprovskontroll av en periods personalkostnader är korrekta utifrån aktuella underlag.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning
Stickprovsgranskat mars lönekörning i Visma Lön mot tidrapporterad tid i Visma Tid samt mot löneutbetalningen.
Tidrapportering sker av varje anställd i Visma Lön Anställd, innan överföring av uppgifter till löneprogrammet granskas och godkänns rapporten av avdelningschef. Ekonomen upprättar lönespecifikationer utifrån den inlagda tiden i Visma tid. Den totala lönekörningen granskas därefter av ekonomichef innan den attesteras av VD för att sedan betalas ut.

Resultat av utförd granskning:
Granskning av majs löner, mot tidrapportering samt fysiska underlag (kvitton mm). Inga felaktigheter har upptäckts vid 5 stickprov.

Slutsats av utförd granskning:
Risken för stora fel är mycket liten och förväntas upptäckas i kontrollfunktionerna.

Rekommenderad åtgärd: Inga ytterligare åtgärder bedöms behövas.

10	Delegation	Risk för brister i efterlevnad i delegationsordning.	Kontroll att verksamhetsärenden av större vikt har beslutats enligt delegationsordningen.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning
Vid granskningen har ett antal avtal och större inköp under året kontrollerats ifall de följt delegationsordningen. Granskningen gjordes av nytt hyresavtal, ny kassahantering samt inköp av truck.

Resultat av utförd granskning:
Granskningen visar att delegationsordningen följs vid samtliga kontrollerade ärenden.

Slutsats av utförd granskning:

Bolaget bedöms följa delegationsordningen *Rekommenderad åtgärd*: Inga ytterligare åtgärder bedöms behövas.					
11	Betalningar	Risk för brister i säkerheten kring betalningar.	Kontroll av eventuellt förekommande manuella utbetalningar under året samt att bolaget har upprättat dubbelattest avseende denna hantering.	En ggr år/höst.	1. VD 2. Ekonomichef
Beskrivning av utförd granskning: Betalning sker vanligtvis genom fil från systemet till banken. Betalfilen hanteras av ekonomen innan ekonomichef godkänner betalfilen i banken. Vid manuella betalningar som inte går via fil läggs betalningen manuellt upp av ekonom i banken och därefter godkänns den av ekonomichef. Vid granskningen har det kontrollerats dubbelattest finns på alla manuella betalningar samt har även banken kontaktats för att säkerställa korrekta behörigheter för de inblandade. *Resultat av utförd granskning:* De förekommande manuella betalningarna under året efter att ny ekonomichef tillträtt i mars månad är samtliga attesterade med dubbelattest i banken. Behörighetsinställningarna i banken gör att det krävs attest av både ekonomi samt ekonomichef för att betalningen ska gå igenom. *Slutsats av utförd granskning:* Åtgärden om att lägga till dubbelsignering har fungerat. Rekommenderad åtgärd: Inga ytterligare åtgärder bedöms behövas.					

Nr	**Process/rutin**	**Risk**	**Kontrollaktivitet**	**Frekvens/tidpunkt**	**1.Ansvarig för process 2.Kontroll utförs av**
12	Efterlevnad attestregler	Risk för att fakturor och verifikat inte attesteras korrekt.	Stickprovskontroll av en periods inköp/leverantörsfakturor med avseende på korrekta sak kontroller och behöriga attester.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning:
Granskning har utförts på perioden maj 2023. Leverantörsfakturanummer 30345-30421 har granskats med avsikt på sakkontroll och attest.

Resultat av utförd granskning:
Vid granskningen så framkom inga brister i efterlevnad av attestreglerna utan granskade fakturor har attesterats av korrekta personer utifrån fastställda attestregler.

Slutsats av utförd granskning:
Utifrån granskningsresultatet bedöms attestreglerna följas.

Rekommenderad åtgärd:
Inga ytterligare åtgärder bedöms behövas.

13	Representation	Risk för att representationsreglerna inte följs.	Stickprovsgranska representationskostnaderna med avseende på korrekt hantering.	En ggr år/höst.	1. VD 2. Ekonomichef

Beskrivning av utförd granskning
Skellefteå Museum har en egen policy för representation uppdaterad 2023-03 och gås igenom i ledningsgruppen och med personalen årsvis. Granskning av policyn utförd samt stickprovgranskat hanteringen av representation vid tre tillfällen under året.

Resultat av utförd granskning:
Granskningen visar att vid samtliga tillfällen så följer Skellefteå Museum sin uppsatta representationspolicy samt de gällande representationsreglerna.

Slutsats av utförd granskning:
Bedömningen är att representationsreglerna följs.

Rekommenderad åtgärd:
Inga ytterligare åtgärder bedöms behövas.

Kommentarer:

Gällande IT-säkerhet så fortsätter Skellefteå Museum delta i digitaliseringsrådet och hålla tät kontakt med kommunens IT- funktion för att komma fram till vilket stöd Skellefteå Museum i framtiden kan få från kommunens sida gällande IT-frågor.

När vi kommer till risken för att tappa kritiska funktioner behöver VD se över behovet och eventuellt upprätta rutinbeskrivningar för kritiska funktioner alternativt skapa processbeskrivningar eller på annat sätt minska risken.

www.skelleftea.se