2024-10-08

Internkontrollplan 2025

Uppsalahem AB

Innehållsförteckning

1 Analys av årets internkontroll och plan för kommande år

I reglemente för intern kontroll i Uppsala kommun och kommunens helägda bolag beskrivs hur arbetet med den interna kontrollen ska struktureras och rapporteras till kommunstyrelsen som har det övergripande ansvaret.

Enligt reglementet ska nämnder och bolagsstyrelser årligen lämna in en analys och utvärdering av sina system och rutiner för intern kontroll till kommunstyrelsen. Analysen ska användas för utveckling av den interna kontrollen inom nämndernas och bolagsstyrelsernas verksamhetsområden. Den används också för utveckling på kommunövergripande nivå.

Nämnder och bolagsstyrelser ska årligen upprätta en internkontrollplan. Planen ska vara ett stöd i styrningen av verksamheten och ett hjälpmedel för att nå verksamhetsmålen. Planen ska försäkra att:

- att verksamheten är ändamålsenlig och resurseffektiv,
- att informationen och rapporteringen om verksamheten och ekonomin är tillförlitlig och rättvisande,
- att verksamheten efterlever lagar, regler, avtal med mera.

Internkontrollplanen beskriver vad som behöver göras utifrån prioriterade risker som framkommit i riskanalyser. I riskregistret framgår om risken omhändertas i internkontrollplanen. Internkontrollplanen innehåller också tre obligatoriska kontrollmoment som identifierats i kommunstyrelsens övergripande riskanalys. Varje kontrollmoment i internkontrollplanen följs upp enligt beskriven frekvens och metod. Resultatet av uppföljningen redovisas årligen till kommunstyrelsen.

1.1 Efterlevnad av riktlinje och analys av funktionalitet

Bolagets riskidentifiering och internkontrollplan omfattar de områden som reglementet föreskriver

- Verksamhetskontroller
- Kontroller av verksamhetens arbetssätt, system och rutiner
- Kontroll av efterlevnad av regler, policys och beslut
- Finansiell kontroll

Till grund för de kontrollmoment som redovisas i interkontrollplanen finns en rikslista med 54 identifierade risker. 16 av dessa, med riskvärde på nivå 8 eller över samt obligatoriska kontrollmoment, har tagits upp i internkontrollplanen.

Bolaget har upprättat en rutin för internkontroll som finns dokumenterat i bolagets IT-system för styrande dokument, Tycho.

Bolagets internkontrollplan följs upp tre gånger per år, i april, augusti och december.

1.2 Organisation och ansvar för arbetet med intern kontroll

Styrelsen är löpande involverad i affärsplaneringen inför kommande år genom löpande information om affärsplaneringen på styrelsens agenda. Internkontrollarbetet är en integrerad del av arbetet, och styrelsens synpunkter arbetas in i bolagets riskregister, den så kallade risklistan. Risklistan uppdateras årligen, varefter ledningsgruppen värderar risker och tar fram underlag på vilka risker som bör ingå i internkontrollplanen.

För respektive risk finns utsedd, ansvarig chef för hantering av risken samt en person inom organisationen som är ansvarig för att genomföra kontroll.

1.3 Planerad utveckling av intern kontroll 2025 och framåt

Under 2024 har digitaliserade arbetssätt för riskhantering och internkontroll implementerats. Risklista och internkontrollplan finns nu i Uppsalahems digitala styrsystem. I och med detta har arbetet med uppföljning av risker och åtgärder utvecklats ytterligare genom att arbetssätt setts över och utbildningar genomförts. Under 2025 arbetas vidare med att befästa de nya arbetssätten och genomföra löpande förbättringar när behov identifieras.

2 Begrepp som används i internkontrollplanen

Begrepp	Förklaring
Kontrollområde	Områden som det ska finnas kontrollmoment inom. Det finns fyra kontrollområden: 1) Kontroller av verksamhetens arbetssätt, system och rutiner 2) Kontroll av efterlevnad av regler, policyer och beslut 3) Finansiell kontroll 4) Kontroll avseende oegentligheter, mutor och jäv
Riskbeskrivning	Beskrivning av den risk som ligger till grund för kontrollmomentet. Hämtas från riskregistret.
Kontrollmoment	Konkreta åtgärder som vidtas för att motverka, minimera eller i vissa fall eliminera riskerna. Kontrollmomenten kan antingen vara förebyggande eller upptäckande och korrigerande. Förebyggande kontrollmoment är åtgärder för att undvika att brister uppstår. Upptäckande och korrigerande kontrollmoment hjälper bolagsstyrelsen att se om riskerna har lett till de händelser som kan befaras och visar på vilka åtgärder som behöver vidtas för att komma tillrätta med bristerna.
Kontrollmetod	Beskrivning av hur, när och hur frekvent kontrollmomentet ska genomföras.
Tidpunkt för rapportering	Tidpunkt då kontrollmomentet ska rapporteras till bolagsstyrelsen.

Fotnot: *Tabell 1. Begrepp som används i internkontrollplanen.*

3 Risker och kontrollmoment

Bolagsstyrelsen uppdrar åt bolaget att utse kontrollansvarig för respektive kontrollmoment.

Risk	Kontrollområde	Kontrollmoment	Kontroll-metod	Tidpunkt för rappor-tering
Bränder uppstår med uppsåt eller på grund av olycka i Uppsalahems byggnader **Riskbeskrivning** På grund av uppsåt eller olycka inträffar en brand i en lägenhet eller fastighet vilket leder till - skada på egendom - skada på människor, i värsta vall dödsfall. Ingår i Lagen om skydd mot olyckor (LSO)	Kontroll av efterlevnad av regler, policyer och beslut	Kontroll av ifyllda SBA-protokoll	Stickprov	Tertial
Leverantörer bryter mot Uppsalahems uppförandekod. **Riskbeskrivning** På grund av att våra leverantörer bryter mot vår uppförandekod finns risk för korruption och/eller otillbörliga förmåner förekommer i vår leverantörskedja. Det kan leda till: - Förtroendeskada - Varumärkesskada - Skadeståndsskyldiga - Ekonomisk förlust	Kontroll avseende oegentligheter, mutor och jäv	Kontroll av att det finns mötesprotokoll från möten för genomgång av uppförandekoden med de leverantörer som tecknat avtal direkt med Uppsalahem under 2025	Stickprov	Tertial
Uppsalahems personal blir utsatt för hot eller våld **Riskbeskrivning** Medarbetare blir utsatt för hot eller våld, vilket kan innebära både fysiska och psykiska skador, i värsta fall dödsfall. Ingår i Lagen om skydd mot olyckor (LSO)	Kontroller av verksamhetens arbetssätt, system och rutiner	Uppföljning att samtliga aktuella medarbetare har genomgått utbildning i hot och våld	Rapport	Tertial
Fel görs av misstag eller med uppsåt vid inköp och/eller upphandling **Riskbeskrivning** På grund av att medvetet eller omedvetet misstag görs vid inköp och/eller upphandling så görs köp vid sidan av upphandlade ramavtal eller entreprenörer. Det kan leda till: '- Förtroendeskada hos upphandlade leverantörer. - Felaktig leverans som inte uppfyller UHABs kravställning - Lagbrott - Ekonomiska konsekvenser, t.ex. skadeståndskrav - Försämrat anseende	Finansiell kontroll	Uppföljning över leverantörstrohet	Rapport	Tertial

Risk	Kontrollområde	Kontrollmoment	Kontroll-metod	Tidpunkt för rappor-tering
Risker inom arbetsmiljö både internt och i entreprenad- och underhållsprojekt hanteras ej på ett adekvat sätt **Riskbeskrivning** På grund av att risker inom arbetsmiljö inte hanteras på ett adekvat sätt så uppstår skador och/eller allvarlig arbetsplatsolycka för egen eller kontrakterad personal vilket leder till: - Personskada. - Dödsfall. - Uppsalahem blir skadeståndsskyldiga.	Kontroll av efterlevnad av regler, policyer och beslut	Kontroll av att det finns arbetsmiljöplan i projekten	Stickprov	Tertial
Ökad social oro och otrygghet i staden **Riskbeskrivning** Allmän otrygghet i samhället ökar. Det kan leda till ökad förekomst av utanförskap och vidare till ökad segregation. Områdets attraktivitet kan minska i segregerade områden, vilken kan innebära att hyresgäster vill flytta därifrån och/eller att få vill flytta dit. Det leder i sin tur till lägre nöjdhet hos hyresgäster och sjunkande marknadsvärden för våra fastigheter. Ingår i Lagen om skydd mot olyckor (LSO)	Kontroller av verksamhetens arbetssätt, system och rutiner	Uppföljning av Trygghetsindex i Affärsplanen	Rapport	Tertial
Felaktig hantering av personuppgifter **Riskbeskrivning** På grund av felaktig hantering av personuppgifter riskerar Uppsalahem att bryta mot GDPR och röja individers personuppgifter vilket leder till: - Lagbrott mot GDPR - Förtroendeskada - risk för individers säkerhet om känsliga uppgifter röjs	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut	Kontroll av PUB-avtal	Stickprov	Halvår
	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut	Informationssäkerhetssamordnare träffar inköp varje kvartal	Stickprov	Kvartal

Risk	Kontrollområde	Kontrollmoment	Kontroll-metod	Tidpunkt för rappor-tering
Klimatförändringar leder till konsekvenser i klimatet i Uppsala, som t.ex. ökad förekomst och frekvens av extremväder i form av skyfall och höga temperaturer. **Riskbeskrivning** Skyfall leder till stora vattenmängder som kan - skada Uppsalahems fastigheter. Höga temperaturer kan leda till höga inomhus-temperaturer - minskad komfort/trivsel för hyresgäster. Extremväder kan innebära t.ex. skyfall med stora vatten-/snömängder och översvämningar, vilket kan leda till: - skador på egendom. Högre temperaturer kan leda till att inomhustemperaturen i lägenheter blir oacceptabelt höga, vilket kan leda till: - ökade kostnader ökad energianvändning för att hantera detta. Högre temperaturer kan även innebära att: - odlade ytor kräver mer bevattning, ökad vattenanvändning - förändring i vad som planteras. Ingår i Lagen om skydd mot olyckor (LSO)	Kontroll av efterlevnad av regler, policyer och beslut	Uppföljning av beslutade åtgärder i Affärsplanen	Rapport	Tertial
Kontrollerat användande av priviligierade konton **Riskbeskrivning** Priviligierade kontons åtgärder spåras och kontrolleras inte i den utsträckning som de borde göras. Det finns risk för att individers säkerhet om känsliga personuppgifter röjts. Det leder till brott mot GDPR, sanktionsavgifter, förtroendeskada.	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut	Avstämning med produktägare	Stickprov	Halvår
Uppsalahems personal blir utsatt för kränkande särbehandling **Riskbeskrivning** På grund av att medarbetare blir utsatt för kränkande särbehandling upplever medarbetaren psykisk skada vilket kan leda till: - fysiska och/eller psykiska men - i värsta fall dödsfall	Kontroll av efterlevnad av regler, policyer och beslut	Uppföljning av ifall frågor under området Rättvisa i GPTW har röda resultat. Om det finns ska en handlingsplan finnas framtagen.	Utredning	År

Risk	Kontrollområde	Kontrollmoment	Kontroll-metod	Tidpunkt för rappor-tering
Uppsalahems personal bryter medvetet eller omedvetet mot företagets interna uppförandekod gällande mutor och korruption. **Riskbeskrivning** På grund av att personal utsätts för eller utövar otillbörlig påverkan bryter de mot företagets interna uppförandekod gällande mutor och korruption vilket leder till: - Förtroendeskada - Varumärkesskada - Skadeståndsskyldiga - Ekonomisk förlust	Kontroll avseende oegentligheter, mutor och jäv	Uppföljning att samtliga medarbetare har genomgått utbildning avseende mutor och korruption.	Rapport	Tertial
Bristande kontroll av system och rutiner **Riskbeskrivning** Ledningen saknar en aktuell bild över verksamhetens systematiska arbete med informationssäkerhet vilket leder till bristfälliga underlag för prioritering av nödvändiga säkerhetsåtgärder. Detta i sin tur medför risker för: - störningar i verksamhetens uppdrag - kan också medföra sanktionsavgifter från tillsynsmyndigheter. (Obligatorisk risk)	Kontroller av verksamhetens arbetssätt, system och rutiner	Obligatoriskt kontrollmoment: Kontroll av att bolagsledningen genomfört mognadsdialogen informations-säkerhet.	Utredning	År
Cyberangrepp och bedrägeri mot medarbetare lyckas **Riskbeskrivning** Brister i medarbetarnas motståndskraft mot cyberangrepp och bedrägerier medför att en medarbetares agerande möjliggör att en attack lyckas vilket i sin tur medför: - omfattande störningar och avbrott i samtliga it-leveranser. (Obligatorisk risk)	Kontroller av verksamhetens arbetssätt, system och rutiner	Obligatoriskt kontrollmoment: Kontroll av att samtliga medarbetare har genomfört obligatorisk utbildning i informations-säkerhet	Rapport	År
Kontroll av system och rutiner för hantering av avbrott och störningar saknas, är okända eller oprövade **Riskbeskrivning** På grund av att kontroll av system och rutiner för hantering av avbrott och störningar saknas, är okända eller oprövade sker ett avbrott i informationsförsörjningen vilket leder till: - stora störningar i produktionen - svårigheter vid återgång till normal verksamhet. (Obligatorisk risk)	Kontroller av verksamhetens arbetssätt, system och rutiner	Obligatoriskt kontrollmoment: Kontroll av att behovet av rutiner och planer för analogt arbete vid avbrott och störningar är inventerat inom verksamheten. Nödvändiga rutiner och planer är dokumenterade, kända och övade.	Utredning	År

Risk	Kontrollområde	Kontrollmoment	Kontroll-metod	Tidpunkt för rappor-tering
	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut	Verifiera SLAer	Stickprov	År
	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut	Använd standardiserad kravställning vud inköp av IT-system	Stickprov	År
Följer ej beslutade processer, riktlinjer, rutiner och beslut **Riskbeskrivning** På grund av att vi inte följer beslutade processer, riktlinjer, rutiner och beslut sker avvikelser inom alla delar av verksamheten vilket leder till: - högre pris - ineffektivitet - kvalitetsbrister m.m.	Kontroller av verksamhetens arbetssätt, system och rutiner	Kontroll av att processer, riktlinjer och rutiner är uppdaterade och kommunicerade till berörda	Rapport	År
	Kontroll av efterlevnad av regler, policyer och beslut	Kontroll av att obligatoriska utbildningar i GO+ avseende policyer och riktlinjer har gåtts igenom av samtliga medarbetare	Utredning	År
Uppsalahem klarar inte av det förändringstempo som krävs för att nå bolagets mål **Riskbeskrivning** På grund av den höga förändringstakten som påverkar många medarbetare så mäktar vi inte med det strategiska arbetet eller gör fel saker, vilket leder till att vi inte når våra mål.	Kontroller av verksamhetens arbetssätt, system och rutiner	Kontroll av att Uppsalahem når sina ettåriga fokusmål	Utredning	År