

Beslutsfattare: Bolagsstyrelse Uppsalahem AB
Beslutsdatum: 2025-11-12
Diarienummer: UH-2025-000487
Dokumentansvarig: Verksamhetscontroller Uppsalahem AB
Dokumentidentitet: 1

Internkontrollplan 2026

Uppsalahem AB



UPPSALAHEM

Uppsalahem AB Postadress: Box 136, 751 04 Uppsala Växel: 018-727 34 00
Webb: www.upsalahem.se Org.nr.: 556137-3589

Innehållsförteckning

1 Syfte	3
2 Analys av internkontroll föregående år	4
2.1 Efterlevnad av riktlinje och analys av funktionalitet	4
2.2 Organisation och ansvar för arbetet med intern kontroll	4
2.3 Planerad utveckling av intern kontroll 2026 och framåt	4
3 Begrepp som används i internkontrollplanen	5
4 Risker och kontrollmoment	6

1 Syfte

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.

2 Analys av internkontroll föregående år

2.1 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 internkontrollplanen finns en rikslista med knappt 50 identifierade risker. 14 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.

2.2 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.

2.3 Planerad utveckling av intern kontroll 2026 och framåt

Under 2025 har det digitaliserade arbetssättet för riskhantering och internkontroll befasts och blivit en del i det löpande arbetet. Risklista och internkontrollplan finns i Uppsalahems digitala styrsystem och följs upp tre gånger per år. Förbättringar i processen för arbetssätt kopplade till risker och intern kontroll införs löpande.



3 Begrepp som används i internkontrollplanen

Begrepp	Förklaring
Kontrollområde	Områden som det ska finnas kontrollmoment inom. Det finns fyra obligatoriska 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	Vilken kontroll 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 nämnden/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 metoden för att genomföra kontrollen. En bra kontrollmetod ska uppfylla följande kriterier: · Validitet: mäter det som är avsett att mäta · Reliabilitet: mäter på ett tillförlitligt sätt · Utförs på samma sätt varje gång Möjlig att genomföra med en rimlig arbetsinsats/till en rimlig kostnad
Ansvarig	Den som ansvarar för att kontrollen genomförs. Anges som roll, ej personnamn.
Tidpunkt för uppföljning	Tidpunkt då kontrollmomentet ska följas upp inför rapportering till nämnd/bolagsstyrelse.

Fotnot: Tabell 1. Begrepp som används i internkontrollplanen.



4 Risker och kontrollmoment

Bolagsstyrelsen uppdrar åt bolaget att utse kontrollansvarig för respektive kontrollmoment. Kontrollansvariga anges i bolagets verksamhetssystem för Risk och kontroll.

Eventuella obligatoriska kontrollmoment från Uppsala kommun kan tillkomma när dessa beslutats.

Risk	Kontrollområde	Kontrollmoment	Kontrollmetod	Tidpunkt för rapportering
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 fall dödsfall. Ingår i Lagen om skydd mot olyckor (LSO)	Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Förvaltningschef	Kontroll av ifyllda SBA-protokoll	Stickprov	Tertial
Intrång av obehörig till enskilda personers konton Uppsalahems IT-miljö Riskbeskrivning På grund av intrång av obehöriga till enskilda personers konton i Uppsalahems IT-miljö får utomstående få tillgång till bolagets uppgifter vilket leder till att: -Risk att känslig information röjs, exempelvis personuppgifter -Bryter mot lagstiftning som dataskyddsförordningen med de påföljder som det kan innebära -Uppsalahem blir mindre attraktiv som arbetsgivare.	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Chef IT- och digitalisering	Kontrollera användande av privilegierade konton	Intervjuer	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 Ansvar för att kontroll genomförs Chef Ekonomi	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

Risk	Kontrollområde	Kontrollmoment	Kontrollmetod	Tidpunkt för rapportering
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 Ansvar för att kontroll genomförs Chef Fastighets-utveckling	Kontroll av att det finns arbetsmiljöplan i projekten	Stickprov	Tertial
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. - risk för påverkan på hälsan hos hyresgäster. 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 Ansvar för att kontroll genomförs Chef Hållbarhet	Uppföljning av att klimatrisk-screening är genomförd.	Rapport	Tertial
Cyberangrepp och bedrägeri mot medarbetare lyckas Riskbeskrivning Bristar 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 Ansvar för att kontroll genomförs Chef IT- och digitalisering	Obligatoriskt kontrollmoment: Kontroll av att samtliga medarbetare har genomfört obligatorisk utbildning i informations-säkerhet	Rapport	År

Risk	Kontrollområde	Kontrollmoment	Kontrollmetod	Tidpunkt för rapportering
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 Ansvar för att kontroll genomförs Chef Personal	Uppföljning att samtliga medarbetare har genomgått utbildning avseende mutor och korruption.	Rapport	Tertial
Om information hos Bolagsverket är ofullständig eller inaktuell kan det leda till rättsliga, administrativa och ekonomiska konsekvenser. Det leder också till risk för att det kommunala bolagets trovärdighet och förtroende hos invånare, kunder, leverantörer med flera försämrar. Riskbeskrivning På grund av att information hos Bolagsverket är ofullständig eller inaktuell kan det leda till: - Rättsliga, administrativa och ekonomiska konsekvenser - Trovärdighet och förtroende hos invånare, kunder, leverantörer med flera försämrar.	Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Chef Ekonomi	Obligatoriskt kontrollmoment för kommunala bolagen: Kontroll av att uppgifter som ska registreras hos Bolagsverket finns registrerade där, och att uppgifterna är korrekta, aktuella och fullständiga	Utredning	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 Ansvar för att kontroll genomförs Chef IT- och digitalisering	Obligatoriskt kontrollmoment: Kontroll av att bolagsledningen genomfört mognadsdialogen informations-säkerhet.	Stickprov	År



Risk	Kontrollområde	Kontrollmoment	Kontrollmetod	Tidpunkt för rapportering
Kontroll av system och rutiner för hantering av avbrott och störningar saknas, är okända eller oprövade Riskbeskrivning Nödvändiga rutiner och planer för hantering av avbrott och störningar saknas, är okända eller oprövade vilket gör att ett avbrott i informationsförsörjningen medför stora störningar i produktionen och svårigheter vid återgång till normal verksamhet. (Obligatorisk risk)	Kontroller av verksamhetens arbetssätt, system och rutiner Ansvar för att kontroll genomförs Chef Hållbarhet	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
	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Chef IT- och digitalisering	Verifiera överenskomna servicenivåer (SLA)	Stickprov	År
	Kontroller av verksamhetens arbetssätt, system och rutiner Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Chef IT- och digitalisering	Använd standardiserad kravställning vid inköp av IT-system	Stickprov	År



Risk	Kontrollområde	Kontrollmoment	Kontrollmetod	Tidpunkt för rapportering
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 Ansvar för att kontroll genomförs Chef Hållbarhet	Kontroll av att processer, riktlinjer och rutiner är uppdaterade och kommunicerade till berörda	Rapport	År
	Kontroll av efterlevnad av regler, policyer och beslut Ansvar för att kontroll genomförs Chef Ekonomi	Kontroll av att obligatoriska utbildningar i GO+ avseende policyer och riktlinjer har gåtts igenom av samtliga medarbetare	Utredning	År