ENKÖPINGS KOMMUN

Rapport
Datum: 2024-11-18
Ärendenummer: KS2025/24

Plan för internkontroll 2025

Kommunstyrelsen

Innehållsförteckning

Inledning

Enligt kommunallagen (kapitel 6, paragraf 6) ska nämnderna, var och en inom sitt ansvarsområde, se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska också se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredställande sätt.

Den interna styrningen och kontrollen är ett av flera verktyg för styrning och ledning som syftar till att säkerställa att kommunen når sina mål, genomför fattade beslut som fattats av kommunfullmäktige och trygga kommunens tillgångar. Den används även för att minimera risker, förluster och förhindra allvarliga fel.

Kommunens regler för intern styrning och kontroll bygger på COSO-ramverket, en modell som är framtaget av amerikanska "Committee of Sponsoring Organizations of the Treadway Commission" som syftar till att hantera och förutse risker i verksamheten. Fokus är inte på tillfälliga insatser utan ett ständigt pågående utvecklingsarbete som uppdateras i takt med att organisationen och omvärlden förändras, exempelvis genom ny lagstiftning, nya riktlinjer, nya mål eller när ny teknik ska införas. .

Den interna styrningen och kontrollen ska vara ett hjälpmedel och en naturlig del i verksamhetens vardagliga arbete och i det systematiska kvalitetsarbetet. Ständiga förbättringar är en grundprincip i uppföljningen.

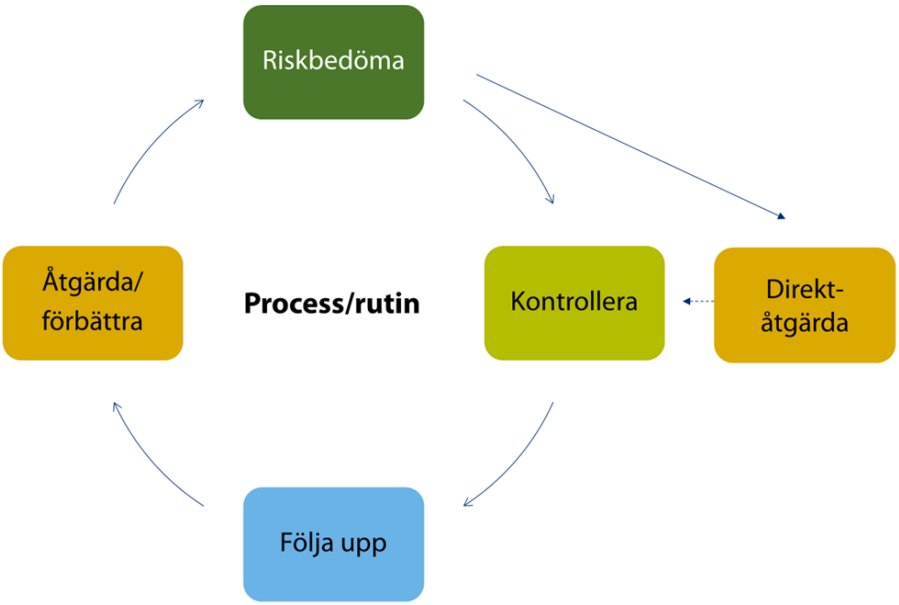
Syfte

Intern styrning och kontroll är ett hjälpmedel för att ha ordning och reda samt kontroll på både verksamhet och ekonomi. Det är ett hjälpmedel för att skydda förtroendevalda och anställda från oberättigade misstankar. Det handlar även om att säkra en effektiv förvaltning och att kunna uppnå följande mål med rimlig grad av säkerhet:

- ändamålsenlig och kostnadseffektiv verksamhet
- tillförlitlig finansiell rapportering och information om verksamheten
- efterlevnad av tillämpliga lagar, föreskrifter, riktlinjer med mera
- säkra tillgångar och förhindra förluster
- eliminera och upptäcka allvarliga fel.

Metod

Arbetet med internkontrollplanen inleds med en riskanalys av verksamhetens processer/rutiner. Utifrån riskanalysen bestäms sedan om risken ska hanteras via nämndens internkontrollplan eller inom ramen för verksamhetens grunduppdrag.



Riskbedöma - identifiera brister och avvikelser som gör det svårare att utföra sitt grunduppdrag och nå uppsatta mål. Bedömning av sannolikhet att risk ska inträffa och konsekvens om det sker.

Direktåtgärda - åtgärder som identifieras i riskanalysen och som behöver åtgärdas omgående.

Kontrollera - systematiska kontroller för av en viss process/rutin för att utvärdera ändamålsenligheten av processen/rutinen och om brister/avvikelser förekommer.

Åtgärda/förbättra - korrigerande åtgärder som identifieras utifrån utfallet av kontrollerna där processen/rutinen behöver förändras/förbättras.

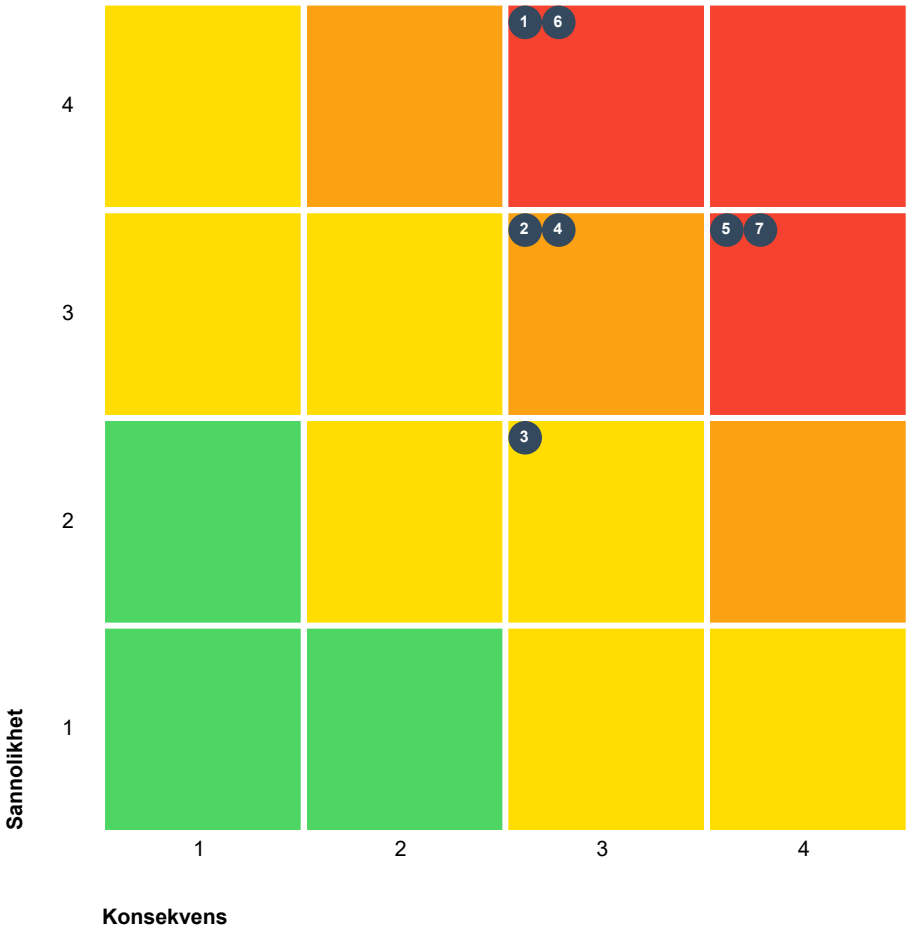
Nämndens riskanalys

Kommunstyrelsen har i sin riskanalys identifierat sju risker inom sex processer/rutiner:

- Hantering av allmän handling
- Styrning och uppföljning
- Lönekartläggning
- Ekonomiadministration/hantering av leverantörsfakturor
- Informationssäkerhet
- Krisberedskap/kontinuitetsplanering

Riskerna kommer att kontrolleras under året och återrapporteras efter augusti och december 2025.

Risköversikt



4 Mycket hög risk | 2 Hög risk | 1 Medelhög risk | Totalt: 7

Mycket hög risk	
Hög risk	
Medelhög risk	
Låg risk	

	Sannolikhet	Konsekvens
4	Sannolik	Allvarlig
3	Möjlig	Betydande
2	Mindre sannolik	Lindrig
1	Osannolik	Försumbar

Process/rutin		Risk	Risknivå
Hantering av allmänna handlingar Offentlighetsprincipen kommer till uttryck på olika sätt i Sveriges grundlagar, exempelvis genom rätten till yttrandefrihet, meddelarfriheten för tjänstemän och genom allmänna handlingars offentlighet. Huvudregeln är att allmänna handlingar är offentliga. Rätten att ta del av allmänna handlingar kan begränsas genom sekretess, som innebär ett förbud att muntligen eller på annat sätt röja uppgifter. Det kan vara så att vissa uppgifter i en allmän handling omfattas av sekretess och att andra är offentliga. Bestämmelser om sekretess finns framför allt i offentlighets- och sekretesslagen (2009:400).	1	**Ärendehantering** Risk för att ärenden inte diarieförs korrekt av verksamheten med följd att handlingar inte kan hittas eller spåras i ett ärende.	4. Sannolik 3. Betydande
Styrning och uppföljning Kommunstyrelsen ansvarar för att kommunen har en god styrning. Det innebär bl.a. en ändamålsenlig planering- och uppföljningsprocess, hög budgetdisciplin, god internkontroll samt kvalitativa beslutsunderlag och styrdokument. Kommunstyrelsen ansvarar även för att ha uppsikt över kommunens övriga nämnder och bolag/förbund och bland annat säkerställa att efterlevnaden av beslutade styrdokument och mål efterlevs.	2	**Brister i hantering av delegationsbeslut** Risk att beslut fattas av fel delegat eller att det saknas/finns felaktig information i delegationsbeslutet om delegatens behörighet.	3. Möjlig 3. Betydande
Lönekartläggning Alla arbetsgivare ska göra en lönekartläggning varje år enligt diskrimineringslagen. Syftet är att säkerställa att lönerna är jämställda. Om arbetsgivaren är fler än tio anställda ska lönekartläggningen dokumenteras.	3	**Diskriminering vid lönesättning** Risken är att förekommande löneskillnader mellan män och kvinnor motiveras med hänvisning till andra anställningsvillkor som inte är könsneutrala, om inte lönekartläggning genomförs tillsammans med en analys. Detta kan leda till att kommuner ha osakliga löneskillnader mellan kvinnor och män.	2. Mindre sannolik 3. Betydande
Ekonomiadministration/hantering av leverantörsfakturor Kommunen ställer krav på leverantörers fakturor om betalningsvillkor på 30 dagar efter fakturadatum. Det innebär att kommunen har 30 dagar att	4	**Leverantörsfakturor betalas inte inom 30 dagar** I det fall kommunen inte betalar sina fakturor inom 30 dagar kan det leda till kostnader för dröjsmålsränta enligt räntelagen. Det leder även till mer administrativt arbete då ytterligare en	3. Möjlig 3. Betydande

Process/rutin		Risk	Risknivå
kontrollera och betala fakturan. Kommunen ställer även krav på leverantörer att fakturorna ska skickas digitalt vilket underlättar hanteringen i kommunens system. Samtliga fakturor ska mottagningsattesteras och beslutsattesteras inom de 30 dagarna enligt gällande regler för attest.		faktura måste hanteras. Förutom onödiga kostnader för dröjsmålsränta och merarbete kan det leda till sämre förtroende för kommunen och skapa negativ publicitet.	
Informationssäkerhet Information ska vara tillgänglig, riktig och endast läsbar för behöriga, varje dag, för varje informationsbärare, samt i enlighet med verksamhetens behov. Arbetet inkluderar informationshantering utifrån säkerhetsskyddslagen och dataskyddsförordningen (GDPR).	5	**Lagkrav och målbild uppfylls inte** NIS2 direktivet syftar till att uppnå en hög EU-gemensam cybersäkerhetsnivå ska införas i svensk lagstiftning. NIS2 kravställer bland annat att kommuer ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. I dagsläget når inte kommunen upp till den nivå som föreskrifter för statliga myndigheter anger (dessa föreskrifter motsvarar de föreskrifter MSB tar fram för kommunerna.). Kommundirektörens ledningsgrupp beslutade därför om en färdplan för att förbättra kommunens informationssäkerhet men målbilden att nå upp till föreskriften under kvartal tre år 2025. Stora delar av Enköpings kommuns dataskyddsarbete ingår i informationssäkerhetsarbetet. Återstående delar, såsom till exempel förutsättningar för dataskyddsombudets roll, dataskyddsorganisation, dokumentation och identifiering av risker kopplat till personuppgiftshantering ligger utanför och ska enligt plan följas upp i kommunens system för uppföljning.	3. Möjlig 4. Allvarlig
	6	**Dataintrång** Vid ett potentiellt intrång i kommunens IT-system riskerar kommunen att förlora känslig information och data, exempelvis genom kryptering av information. Lösenord, personuppgifter och annan känslig data kan läcka ut eller säljas vidare. Åtkomst till vitala IT-system, inklusive de som hanteras av kommunens IT-personal, kan blockeras eller begränsas av en extern tredje-part. Ett sådant intrång kan medföra mycket	4. Sannolik 3. Betydande

Process/rutin		Risk	Risknivå
		stora kostnader för att återställa systemen, och dessutom kan kommunen åläggas viten för eventuella brott mot dataskyddsregler och andra säkerhetskrav	
Krisberedskap/ kontinuitetsplanering Enköpings kommuns verksamheter är en viktig del i samhällets robusthet och totalförsvarets civila förmåga lokalt. För att kunna hantera ett kraftigt försämrat omvärldsläge finns ett stort behov av robusta verksamheter och i det arbetet är kontinuitetsplanering är en grundförutsättning. Kontinuitetsplanering är ett verktyg för verksamheterna att kartlägga och ta ansvar för den egna organisationens förmåga att stå emot störningar. Fördelen med kontinuitetsplanering är att det förbereder verksamheten oavsett vilken oönskad händelse eller störning som kan inträffa. Verksamheternas kontinuitetsplaner utgör också en viktig bas för att vi som organisation ska kunna kraftsamla och bygga upp rätt gemensamma förmågor för de stora störningarna. I detta arbete finns centralt stöd i form av beredskapsstrateger som kan bistå verksamheterna i deras framtagande av kontinuitetsplaner och bära vidare eventuella behov av centrala lösningar.	7	**Kontinuitetsplaner saknas** Utan en kontinuitetsplan blir verksamheterna sårbara vid störningar/avbrott av något kritiskt beroende (tex elbortfall, IT-bortfall, personalbortfall). Som kommun riskerar vi då också att inte uppfylla krav som finns kopplade till krisberedskap och civilt försvar, eller för den delen förväntningar från kommunmedlemmarna.	3. Möjlig 4. Allvarlig

Nämndens plan för internkontroll 2025

Internkontrollplan

	Risk	Kontroll	Genomförande av kontroll	Ansvarig
1	**Ärendehantering**	**Kontroll av ärenden i diariet** Kontroll av att de handlingar inklusive e-post som ska finnas i ett ärende finns diarieförda.	**Hur sker kontrollen?** Stickprov på 10 ärenden i diariet. **När sker kontrollen?** Inför delårs- och helårsuppföljning **Vem kontrollerar?** Registrator	**Ansvarig** Maria Ekblad
2	**Brister i hantering av delegationsbeslut**	**Uppföljning av delegationsordningen** Kontroll av ärenden och fattade beslut, att delegationsbeslut fattats och att de tagits av rätt delegat.	**Hur sker kontrollen?** Stickprov på 10 ärenden i diariet Stickprov på 10 delegationsbeslut **När sker kontrollen?** Inför delårs- och helårsuppföljning **Vem kontrollerar?** Enhetschef kansli och kontorsstöd	**Ansvarig** Maria Ekblad
3	**Diskriminering vid lönesättning**	**Lönekartläggning** Löneskillnader mellan män och kvinnor som utför likvärdigt/lika arbete.	**Hur sker kontrollen?** Datadriven kontroll **När sker kontrollen?** Årligen **Vem kontrollerar?** Förhandlingschef	**Ansvarig** Linda Ahlsén
4	**Leverantörsfakturor betalas inte inom 30 dagar**	**Antal fakturor betalade efter 30 dagar** Kontroll av hur många fakturor per förvaltning och ansvar som betalas efter 30 dagar	**Hur sker kontrollen?** Underlag som visar antalet fakturor betalade efter 30 dagar per förvaltning och ansvar. **När sker kontrollen?** Två gånger per år, i samband med delårs- och årsuppföljningen. **Vem kontrollerar?** Enhetschef Ekonomistöd	**Ansvarig** Thina Lindgren
5	**Lagkrav och målbild uppfylls inte**	**Cybersäkerhetskollen** Kontroll av nämndens resultat enlig MSB:s föreskrift inom tio områden: - analys och hantering av informationssäkerhetsrisk	**Hur sker kontrollen?** Redovisning utifrån MSB:s verktyg cybersäkerhetskollen. **När sker kontrollen?** 2 gånger per år **Vem kontrollerar?**	**Ansvarig** Marcus Wennerström

	Risk	Kontroll	Genomförande av kontroll	Ansvarig
		er - incident- och kontinuitetshantering - informationsklassning - inventering, undersökning och omvärldsbevakning - ledningens styrning och kontroll - medarbetarnas kunskap och utbildningsverksamhet - säkerhetsåtgärder och förbättringsarbete - uppföljning och utvärdering - upphandling - upprättande och utveckling av säkerhetskultur	Trygghets- och säkerhetschef	
		Personuppgifts-hantering Kontroll av nämndens hantering av personuppgifter enligt krav i dataskyddsförordningen (GDPR).	**Hur sker kontrollen?** Övervakning genomförs i enlighet med plan för övervakning av dataskyddsombudet. **När sker kontrollen?** Årligen genom en rapport under december. **Vem kontrollerar?** Dataskyddsombudet för kommunstyrelsen	**Ansvarig** Marcus Wennerström
6	**Dataintrång**	**Penetrationstest** - Sårbarheter i kommunens IT-infrastruktur - Applikationers versioner - Uppgifter som finns tillgänglig externt och som kan nyttjas vid en skadlig intension mot kommunens IT - Scanning och sårbarhetsbedömning	**Hur sker kontrollen?** Externa penetrationstest **När sker kontrollen?** En gång per år **Vem kontrollerar?** Kontroll sker genom penetrationstest	**Ansvarig** Magnus Nideborn, Marcus Wennerström
7	**Kontinuitetsplaner saknas**	**Kontinuitetsplaner finns hos förvaltningens verksamheter** Förvaltningens avdelningschefer svarar på frågan om det finns en aktuell kontinuitetsplan	**Hur sker kontrollen?** Uppföljning sker genom att frågan "Har verksamheten en uppdaterad kontinuitetsplan?" ställs till ansvarig chef två	**Ansvarig** Marcus Wennerström

Risk	Kontroll	Genomförande av kontroll	Ansvarig
	för verksamheten - Att det finns en plan - Att den är aktualiserad - Att den är övad och känd i verksamheten - Att lagarna följs	gånger per år. **När sker kontrollen?** I samband med delår- och årsuppföljningen. **Vem kontrollerar?** Trygghets- och säkerhetsavdelningen	