

# Plan för intern kontroll 2024

---

Samhällsbyggnadsnämnd

## Innehållsförteckning

<b>1 Inledning</b> .....	<b>3</b>
1.1 Riskmatris.....	4
<b>2 Kontrollmoment- urval till intern kontrollplan</b> .....	<b>6</b>
2.1 Risk för obehörig åtkomst till information (gemensam risk).....	7
2.2 Risk att förankrade och uppdaterade krisberedskapsplaner saknas.....	7
2.3 Risk att kommunens riktlinjer inte efterföljs vid samtliga rekryteringar (gemensam risk).....	7
2.4 Risk att direktupphandlingar inte genomförs korrekt (gemensam risk).....	8
2.5 Risk att det förebyggande brandskyddsarbetet inte utförs (gemensam risk).....	8
2.6 Risk för bristfälligt skydd av personuppgifter.....	9
2.7 Risk att verksamheten inte använder sig av aktörer som upphandlats.....	9
<b>3 Förslag till beslut</b> .....	<b>9</b>

## 1 Inledning

Enligt kommunallagen 6 kap 6 § ska nämnden tillse att verksamheten bedrivs i enlighet med gällande mål, riktlinjer och föreskrifter. Detta brukar benämnas intern kontroll.

I Lomma kommuns reglemente för intern kontroll framgår det att respektive nämnd ska anta en intern kontrollplan för innevarande år senast i mars månad. Uppföljning av intern kontroll ska ske senast i februari nästkommande år. Det är nämnderna som har det yttersta ansvaret för den interna kontrollen inom respektive verksamhetsområde.

Intern kontroll ska säkerställa att följande uppnås:

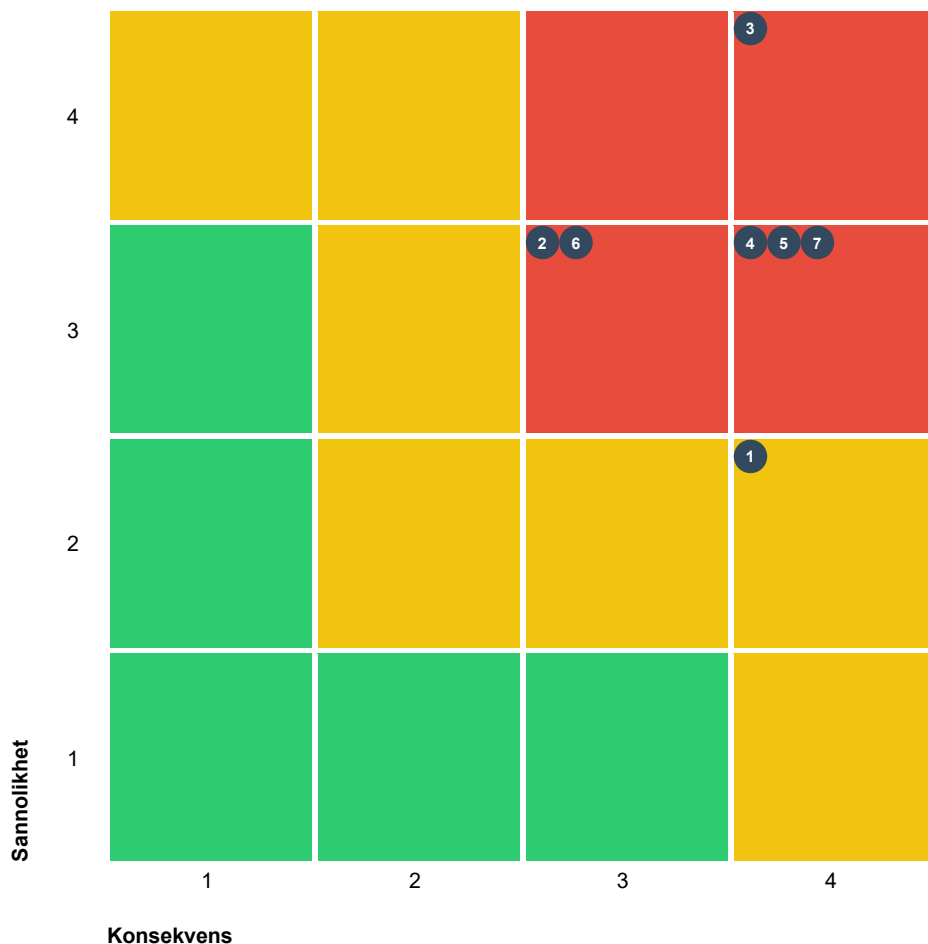
- Ändamålsenlig och kostnadseffektiv verksamhet.
- Tillförlitlig finansiell rapportering och information om verksamheten.
- Efterlevnad av tillämpliga lagar, föreskrifter, riktlinjer m.m.
- Eliminering av risker för korruption och ekonomisk svindel.

Plan för intern kontroll baseras på en risk- och väsentlighetsanalys av processer och rutiner som bedöms särskilt viktiga att granska. Denna plan redogör för de interna kontrollpunkter som ska utföras inom nämndens verksamhetsområde. Inför framtagandet av kontrollplanen har verksamheten utgått från förgående års uppföljning av intern kontroll, där en redogörelse av kontrollerna, dess resultat och avvikelser tagits upp. Därefter har en riskanalys för innevarande år genomförts. Kommunens ledningsgrupp identifierar förslag till kommunövergripande risker som gäller för samtliga nämnder. Kommunstyrelsen beslutar om de kommunövergripande riskerna. I uppföljningen av intern kontroll är det kommunstyrelsen som följer upp riskerna via kontrollaktiviteter samt lämnar förslag till åtgärder vid avvikelser. Nämnderna ansvarar för att åtgärderna genomförs.

Riskerna har graderats, med värdena 1-4, utifrån sannolikhet och konsekvens, där det sammanlagda värdet utgör riskbedömningen. Samtliga identifierade risker redovisas nedan i riskmatrisen. Områden där riskerna bedömts som viktiga att kontrollera har inkluderats i planen för intern kontroll. I planen tydliggörs vem som ansvarar för uppföljningen och med vilken metod kontrollen ska ske.

## 1.1 Riskmatris

I riskmatrisen nedan presenteras nämndens risker som identifierats vid riskanalys. Matrisen omfattar både kommungemensamma risker och sådana som identifierats av nämnden. Kommungemensamma risker hanteras utav samtliga nämnder och är bedömda på kommunnivå, för hela kommunen, och inte nämnden specifikt.

















6 Kritisk 1 Medel Totalt: 7

Kritisk
Medel
Låg

	Sannolikhet	Konsekvens
4	Mycket stor (Risken att den oönskade händelsen inträffar ofta är stor)	Allvarlig (Felet får i princip inte inträffa eftersom konsekvensen är för stor)
3	Stor (Risken att den oönskade händelsen inträffar är överhängande)	Kännbar (Uppfattas som besvärande för intressenter och kommun)
2	Liten (Risken att den oönskade händelsen skulle inträffa är liten, endast vid något enstaka tillfälle)	Lindrig (Uppfattas som liten av såväl intressenter som kommun)
1	Mycket liten (Risken att den oönskade händelsen skulle inträffa är praktiskt taget obefintlig)	Försumbar (Obetydlig för intressenter och kommun)

Risk	Sannolikhet	Konsekvens	Riskvärde	Ska kontrolleras	Kontrollaktivitet
8 Risk att delegationsordningen inte följs och att delegationsbeslut inte anmäls Samhällsbyggnadsnämnd			—		Kontroll av att beslut är fattade enligt delegationsordningen.
1 Risk att det förebyggande brandskyddsarbetet inte utförs (gemensam risk) Samhällsbyggnadsnämnd	2. Liten	4. Allvarlig	8	Ja	Kontroll av utdrag från kommunens system för SBA
9 Risk att försäkringar inte uppdateras Samhällsbyggnadsnämnd			—		Är alla objekt (byggnader, skog, tillgångar) försäkrade
10 Risk att investeringskalkyler inte hålls och att kommunen får högre driftkostnader än budgeterat Samhällsbyggnadsnämnd			—		Uppföljning av investeringsprojekt
2 Risk att kommunens riktlinjer inte efterföljs vid samtliga rekryteringar (gemensam risk) Samhällsbyggnadsnämnd	3. Stor	3. Kännbar	9	Ja	Kontroll att utbildning implementeras samt förstärkt HR-stöd till nya chefer i samband med att de ska genomföra sin första rekrytering.
11 Risk att kommunikation i driftprojekt inte är tillräcklig Samhällsbyggnadsnämnd			—		Uppföljning av kommunikationsårshjulet
12 Risk att medarbetare har bristfälligt kännedom om kommunens vision och mål Samhällsbyggnadsnämnd			—		
13 Risk att nämnden inte följer LOU och LUF vid upphandling Samhällsbyggnadsnämnd			—		Kontroll att riktlinjer vid upphandlingar följs.
3 Risk för bristfälligt skydd av personuppgifter Samhällsbyggnadsnämnd	4. Mycket stor	4. Allvarlig	16	Ja	Kontroll av anställdas e-postsignatur
					Kontroll att konsekvensbedömning skett utifrån GDPR vid avtalsskrivning vid införande av system
					Kontroll av förekomst av tredjeländöverföringar i befintliga system
14 Risk för driftavbrott Samhällsbyggnadsnämnd			—		
4 Risk för obehörig åtkomst till information	3. Stor	4. Allvarlig	12	Ja	Kontroll att kontinuitetsplaner finns för respektive system

Risk	Sannolikhet	Konsekvens	Riskvärde	Ska kontrolleras	Kontrollaktivitet
(gemensam risk) Samhällsbyggnadsnämnd					Kontroll att information är klassificerat i enlighet med KLASSA Kontroll av kommunens motståndskraft för ransomware/malware/hacking
5 Risk att verksamheten inte använder sig av aktörer som upphandlats Samhällsbyggnadsnämnd	3. Stor	4. Allvarlig	 12	 Ja	Stickprovskontroll
15 Risk att det systematiskt arbetsmiljöarbetet inte utförs Samhällsbyggnadsnämnd					Uppföljning av handlingsplan (SAM)
6 Risk att direktupphandlingar inte genomförs korrekt (gemensam risk) Samhällsbyggnadsnämnd	3. Stor	3. Kännbar	 9	 Ja	Kontroll av inköp under gränsvärdet
16 Risk att intäkter inte faktureras Samhällsbyggnadsnämnd					Stickprov utifrån avtalshanteringssystemet av de avtal som ska faktureras.
17 Risk för mutor och bestickning. Samhällsbyggnadsnämnd					Informationsinsats
18 Risk att anställda har otillåten bisyssla Samhällsbyggnadsnämnd					En avstämning sker vid årets slut att samtliga anställda har fått informationen om riktlinjer vid bisyssla och hur detta ska anmälas
19 Risk att leverantörsbetalningar inte sker i tid Samhällsbyggnadsnämnd					Kontroll att fakturor betalas i tid
7 Risk att förankrade och uppdaterade krisberedskapsplaner saknas Samhällsbyggnadsnämnd	3. Stor	4. Allvarlig	 12	 Ja	Översyn och uppdatering av krisberedskapsplanen
20 Risk att tid-och faktureringsmodulen inte fylls i som det ska Samhällsbyggnadsnämnd					Kontrollera bokföring från tid och projektmodulen i Agresso
21 Risk för höga elpriser Samhällsbyggnadsnämnd					Kontrollera utfall mot budget kontinuerligt
22 Risk att nämnden inte har tillgång till bostäder utifrån anvisningsantal Samhällsbyggnadsnämnd					Kontroll av anvisningstakt och att bostäder finns till förfogande

## 2 Kontrollmoment- urval till intern kontrollplan

Nedanstående områden har identifierats som särskilt viktiga att undersöka i årets plan för intern kontroll.

## 2.1 Risk för obehörig åtkomst till information (gemensam risk)

Riskbedömning

■ 12. Allvarlig

Beskrivning av risk och kontrollaktivitet

Intrång i kommunens system kan leda till stora konsekvenser beroende på vilken information som obehöriga kommer åt. Att organisationen har en medvetenhet inom IT-säkerhet och informations säkerhet är viktigt för kommunens, medborgarnas samt andra aktörers säkerhet. Att obehöriga kommer åt vår information kan leda till brister i skydd av integritet, skapa störningar i verksamheten samt få stora ekonomiska konsekvenser. Bra förutsättningar för informationshantering är också viktigt för kommunens utveckling.

Lagar som berör kommunens information är GDPR, NIS-direktivet, PDL (patientsäkerhetslagen), arkivlagen samt offentlighet- och sekretesslagen. Informationen kan vara konfidentiell och behöva åtkomstbegränsas, den ska vara riktig och tillförlitlig samt tillgänglig för rätt personer med rätt behörighet.

Detta är en gemensam risk beslutad av kommunstyrelsen.

Kontrollaktiviteterna är att genom externa tester kontrollera kommunens motståndskraft för ransomware/malware och hacking samt kontrollera att kontinuitetsplaner finns om kritiska system inte skulle fungera. Det kommer även genomföras kontroll på att informationen som finns i våra system är klassificerade i enlighet med SKR:s verktyg KLASSA för systematisk informations säkerhet. IT-avdelningen samordnar kontrollen med stöd av övriga nämnder.

## 2.2 Risk att förankrade och uppdaterade krisberedskapsplaner saknas

Riskbedömning

■ 12. Allvarlig

Beskrivning av risk och kontrollaktivitet

Om en kommun inte har en uppdaterad och väl förankrad krisberedskapsplan kan det leda till en rad negativa konsekvenser vid en kris eller nödsituation. Krisberedskapsplanering är avgörande för att effektivt hantera olika typer av kriser, såsom naturkatastrofer, stora olyckor, pandemier eller terrorattacker. Exempel på problem och konsekvenser som kan uppstå om en adekvat krisberedskapsplan saknas är: otydlig ansvarsfördelning, brister i kommunikationen, försenad insats, förtroendeförlust, ekonomiska förluster samt ökat sårbarhet. För att undvika dessa konsekvenser är det viktigt att nämnden regelbundet reviderar och uppdatera sina krisberedskapsplaner samt säkerställer att de är väl förankrade hos aktuella medarbetare och att övningar genomförs regelbundet för att testa och förbättra beredskapen.

## 2.3 Risk att kommunens riktlinjer inte efterföljs vid samtliga rekryteringar (gemensam risk)

Riskbedömning

■ 9. Kännbar

## Beskrivning av risk och kontrollaktivitet

Det finns en risk att kommunens riktlinjer för rekrytering inte följs vid samtliga rekryteringar, på grund av bristande kunskap och/eller tidsbrist hos rekryterande chefer. Konsekvensen kan bli att medarbetare som rekryteras inte fullt ut matchar kravprofil, vilket i sin tur kan leda till bland annat kvalitetsproblem eller bristande effektivitet i verksamheten samt högre personalomsättning. Vid kontrollaktivitet under 2023 konstaterades att det finns kunskapsbrister kring rekryteringsprocessen hos kommunens chefer som behöver åtgärdas för att minska risken.

Detta är en gemensam risk beslutad av kommunstyrelsen.

HR-avdelningen genomför kunskapshöjande åtgärd för samtliga nämnder genom att skapa en digital rekryteringsutbildning som görs obligatorisk för samtliga chefer. HR-avdelningen ger även ett förstärkt HR-stöd till nya chefer i samband med att de ska genomföra sin första rekrytering. Nya kontroller av stickprov kommer att genomföras under 2025 för att kontrollera att åtgärderna gett effekt.

### **2.4 Risk att direktupphandlingar inte genomförs korrekt (gemensam risk)**

#### Riskbedömning

 9. Kännbar

#### Beskrivning av risk och kontrollaktivitet

Inköp och upphandling som genomförs av kommunens verksamheter regleras av lag om offentlig upphandling (LOU) och fullmäktiges beslutade upphandlingspolicy. Enligt lag (2016:1145) om offentlig upphandling kan brister i följsamhet även leda till skadestånd och/eller upphandlingsskadeavgift vid otillåten direktupphandling. Om direktupphandlingar inte genomförs korrekt kan köpet eller avtalet ogiltigförklaras av domstol och kommunen dömas till att betala upphandlingsskadeavgift.

Detta är en gemensam risk beslutad av kommunstyrelsen.

Kontrollaktiviteten utförs av ekonomiavdelningen som analyserar inköp under gränsvärdet via stickprov.

### **2.5 Risk att det förebyggande brandskyddsarbetet inte utförs (gemensam risk)**

#### Riskbedömning

 8. Kännbar

#### Beskrivning av risk och kontrollaktivitet

Om det förebyggande arbetet inte fungerar ökar risken för incidenter och olycksfall exempelvis bränder. Under 2023 gjordes en kontrollaktivitet på kommunens SBA vilket visade på vissa brister. Bristerna var bland annat:

- Funktioner inom SBA var inte namngivna
- Utbildning vara bristfällig
- Vissa rutiner fanns inte nedskrivna



Merparten av bristerna är redan åtgärdade medan andra kommer att åtgärdas under 2024. Det finns riktlinjer att verksamheternas SBA ska följas upp årligen vilket är förankrat och kommer att ske under hösten 2024. En kontroll av stickprov från kommunens system för SBA kommer att genomföras under senhösten för att se att åtgärderna gett effekt.

Detta är en gemensam risk beslutad av kommunstyrelsen.  
Kontrollaktiviteten utförs av nämnderna med stöd av säkerhetschefen.

## **2.6 Risk för bristfälligt skydd av personuppgifter**

Riskbedömning

■ 16. Mycket Allvarlig

Beskrivning av risk och kontrollaktivitet

Kommunen hanterar dagligen en stor mängd personuppgifter, inklusive känslig information om medborgare, anställda och andra intressenter. Det finns en risk att de befintliga processerna och IT-systemen inte tillhandahåller ett adekvat skydd för dessa personuppgifter, vilket kan leda till obehörig åtkomst, förlust, ändring eller otillbörlig spridning av personuppgifter. Otillräckligt skydd av personuppgifter kan resultera i brott mot GDPR, vilket inte bara medför risken för betydande böter utan också skadar kommunens rykte och förtroendet hos medborgarna.

## **2.7 Risk att verksamheten inte använder sig av aktörer som upphandlats**

Riskbedömning

■ 12. Allvarlig

Beskrivning av risk och kontrollaktivitet

Om en kommun väljer att inte använda sig av upphandlade aktörer, det vill säga aktörer som valts genom en offentlig upphandlingsprocess, kan det uppstå flera problem och negativa konsekvenser. Offentlig upphandling i Sverige styrs av Lag om offentlig upphandling (LOU), som syftar till att främja effektiv användning av offentliga medel, säkerställa rättvis konkurrens och motverka korrupktion. En brist på användning av upphandlade aktörer kan således leda till en rad juridiska och ekonomiska risker till förlorat förtroende och sämre kvalitet på inköpta varor och tjänster.

## **3 Förslag till beslut**

Se tjänsteskrivelse.