Malmö stad
Kommunstyrelsen

Datum
2026-11-05
Adress
Kalendegatan 1
Diarienummer
STK-2025-302

Yttrande

Till
Revisorskollegiet

Granskning av IT-säkerhet
SR-2024-38

Sammanfattning
Revisorskollegiet genomförde hösten 2024 en granskning av kommunstyrelsens och servicenämndens arbete med IT-säkerhet. Syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad. Den samlade bedömningen i granskningen är att kommunstyrelsen och servicenämnden inte helt har säkerställt en tillräcklig IT-säkerhet för Malmö stad. Revisorskollegiet har begärt att kommunstyrelsen ska inkomma med ett tredje yttrande över granskningen senast den 31 december 2026.

I detta tredje yttrande framgår vad som gjorts sedan föregående yttrande samt att kommunstyrelsen omhändertar kvarstående rekommendationer genom den pågående implementeringen av de föreskrifter som trädde i kraft i oktober 2026. Kommunstyrelsen anser att detta är en prioriterad fråga och arbetet sker strukturerat i nära samarbete med servicenämnden.

Yttrande
Nedan presenteras revisorskollegiets rekommendationer, följt av kommunstyrelsens uppföljande svar och redogörelse för utförda åtgärder.

Revisorskollegiets rekommendation med kommunstyrelsens uppföljande svar
Cybersäkerhetslagen trädde i kraft i januari 2026 och föreskrifter om säkerhetsåtgärder och ledningens utbildning trädde i kraft i oktober 2026. Alla kvarstående rekommendationer från revisorskollegiet berörs på något sätt av kommunstyrelsens arbete med att omhänderta cybersäkerhetslagen och dess tillhörande föreskrifter.

En plan för att omhänderta lagkraven fastställdes i februari 2026. Planen togs fram av medarbetare från servicenämnden och kommunstyrelsen utifrån identifierade gap i analyser och mätningar som Cybersäkerhetskollen. Av planen framgår att föreskrifterna behöver beaktas i konkretiseringen av de aktiviteter som identifierats i

planen. Föreskrifterna innehåller säkerhetsåtgärder som berör hela spektrumet av cybersäkerhetsarbetet, från styrning till uppföljning och rapportering. Regler och arbetssätt i Malmö stad ses nu över utifrån planen och föreskrifterna.

Revisorskollegiet har begärt att kommunstyrelsen yttrar sig om tre punkter. Den första lyder:

- Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien

Av föreskrifterna framgår det att Malmö stad som verksamhetsutövare ska fastställa de interna regler och arbetssätt som behövs för att vidta lämpliga och proportionella säkerhetsåtgärder utifrån externa krav, interna behov och identifierade risker avseende cybersäkerhet. Kommunstyrelsen bedömer att det inte är ändamålsenligt att en ny policy tas fram enbart för att stärka informationssäkerheten.

Informationssäkerhet, inklusive cybersäkerhet, ska istället ingå i kommunens styrning av skydd av verksamheten samt digitalisering. Ett exempel på sådan styrning är Malmö stads trygghets- och säkerhetspolicy (STK-2014-233). En översyn av policystyrning relaterad till detta område kommer att initieras under 2027. I samband med översynen kommer kommunstyrelsen att utreda hur policykraven i ISO 27000-serien skulle kunna omhändertas på ett lämpligt sätt.

Den andra punkten som revisorskollegiet önskar att kommunstyrelsen yttrar sig om lyder:

- Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i Riktlinjer för informationssäkerhet samt att kontroll av efterlevnad av riktlinjerna etableras

Malmö stads riktlinjer för informationssäkerhet kommer att uppdateras utifrån föreskrifterna. Arbetet hänger ihop med den planerade översynen av policystyrning som nämns i punkten ovan. Nationellt pågår en uppdatering av uppföljningsstrukturen Cybersäkerhetskollen som Malmö stad använder sig av för att anpassa metoden till cybersäkerhetslagen och tillhörande föreskrifter. Detta väntas vara färdigt våren 2027.

Metodens tidigare utformning har haft en tydlig koppling till Malmö stads riktlinjer och anvisningar för informationssäkerhet. Kommunstyrelsen anser därför att Malmö stads behov av efterlevnadskontroller behöver bedömas i relation till kraven i föreskrifterna och den nya uppföljningsstrukturen när den tillgängliggjorts.

Kommunstyrelsen kommer att etablera årlig rapportering om cybersäkerhet i enlighet med föreskrifterna. Det utreds nu hur detta kan utformas och samordnas med övrig

rapportering. Föreskrifterna ställer krav på att ledningen blir informerad om genomförandet av säkerhetsåtgärder och verksamhetsutövarens nivå av cybersäkerhet vid behov men minst en gång per år. Syftet med rapporteringen är att skapa förutsättningar för ledningen att godkänna och övervaka genomförandet av säkerhetsåtgärder i Malmö stad.

Den tredje punkten som revisorskollegiet önskar att kommunstyrelsen yttrar sig om lyder:

- Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med Anvisning för informationshantering och säkerhetsprocesser

Malmö stads styrning om uppföljning kommer att uppdateras utifrån föreskrifterna och den nya utformningen av uppföljningsstrukturen Cybersäkerhetskollen. Föreskrifterna ställer krav på uppföljning och utvärdering av säkerhetsåtgärdernas lämplighet och proportionalitet i förhållande till externa krav, interna behov och identifierade risker. Verksamhetsutövaren ska även identifiera behov av att förbättra säkerhetsåtgärder. Implementering av kraven i föreskrifterna förväntas höja kvalitén på genomförd uppföljning och utvärdering. Kommunstyrelsen har bedömt att etablering av uppföljning behöver ha en något lägre prioritet i implementeringen av föreskrifterna eftersom det finns andra åtgärder som först behöver etableras i regler och arbetssätt för att kunna följas upp.

Kommunstyrelsen välkomnar revisorskollegiets intresse för Malmö stads informationssäkerhet och anser att det är ett viktigt och prioriterat område. I kommunstyrelsens budgetskrivelse för 2027 lyftes bland annat ett osäkert omvärldsläge, effekterna av ett högt lagstiftningstempo och ökade krav på säkerhet och beredskap. Kommunstyrelsen bedriver redan i dag ett brett arbete för att möta dessa utmaningar, bland annat genom att utveckla säkerhets- och beredskapsarbetet.

Kommunstyrelsen har identifierat ett behov av att stärka stadens förmåga, samt öka takten i det systematiska, sammanhållna och långsiktiga arbetet med säkerhet och beredskap. Det pågår ett intensivt arbete med att tolka och implementera kraven i föreskrifterna utifrån en Malmö stad-kontext. Prioritering och samordning av aktiviteter görs utifrån den framtagna planen och i samråd med Malmö stads verksamhetsansvariga för stadsövergripande informationssäkerhet och dataskydd. Kommunstyrelsen anser att det är detta arbete som behöver ligga i fokus framåt. För att möta behoven och påskynda implementeringen kommer den centrala informationssäkerhetsfunktionen att förstärkas med en tjänst.

Avslutningsvis vill kommunstyrelsen betona att det på kort sikt är svårt både att genomföra alla åtgärder som revisorskollegiet rekommenderat och att se effekterna av dem med tanke på att föreskrifterna trädde i kraft i oktober 2026.

Ordförande [Förnamn Efternamn]

[Fyll i titel] [Förnamn Efternamn]

[Här anger du om det finns reservationer/särskilda yttranden.]