Malmö stad
Stadskontoret

Tjänsteskrivelse

Datum
2026-11-05

Vår referens
Evelina Cederholm
Utvecklingssamordnare
evelina.cederholm@malmo.se

Revisorskollegiets granskning av IT-säkerhet; uppföljande yttrande

STK-2025-302

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.

Kommunstyrelsen inkom med ett första yttrande i april 2025. Av yttrandet framkom att kommunstyrelsen i huvudsak instämmer i revisorskollegiets slutsatser och att åtgärderna i stort låg i linje med redan planerade utvecklingsinsatser.

Kommunstyrelsen inkom med ett andra yttrande i februari 2026. Av yttrandet framkom att kommunstyrelsen som en åtgärd har tillgängliggjort och marknadsfört en grundläggande informationssäkerhetsutbildning. Kommunstyrelsen framförde att övriga rekommendationer behöver omhändertas utifrån kommande förskrifter som tydliggör kraven i cybersäkerhetslagen.

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. Nu arbetar stadskontoret intensivt för att tolka och implementera kraven utifrån en Malmö stad-kontext i nära samarbete med servicenämnden.

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

SIGNERAD
2026-11-18

1. Kommunstyrelsen godkänner förslag till yttrande och skickar yttrandet till Revisorskollegiet.

Beslutsunderlag

- Revisorskollegiet beslut 260325 § 27
- G-Tjänsteskrivelse KSAU 261123 Revisorskollegiets granskning av IT-säkerhet; uppföljande yttrande

Beslutsplanering

Kommunstyrelsens arbetsutskott 2025-03-17
Kommunstyrelsen 2025-04-02
Kommunstyrelsens arbetsutskott 2026-01-26
Kommunstyrelsen 2026-02-04
Kommunstyrelsens arbetsutskott 2026-11-23
Kommunstyrelsen 2026-12-02

Beslutet skickas till

Revisorskollegiet
Stadskontorets handläggare

Ärendet

Bakgrund

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. Med tillräcklig IT-säkerhet avsågs i granskningen att den bedrivs i enlighet med lagstiftning, föreskrifter och kommunfullmäktiges beslut. Revisorskollegiet gav kommunstyrelsen i uppdrag att yttra sig vid två tillfällen. Det första yttrandet lämnades i april 2025 och det uppföljande yttrandet lämnades i februari 2026.

I det första yttrandet framgick att kommunstyrelsen i huvudsak instämmer i revisorskollegiets slutsatser och att både insatser för medvetenhet och utbildning samt uppföljning och utvärdering ingick i verksamhetsplanen för 2025. Kommunstyrelsen bedömde däremot att det inte nödvändigtvis är ändamålsenligt att en ny policy tas fram enbart för att öka informationssäkerheten, men att man i samband med översynen av Malmö stads trygghets- och säkerhetspolicy kommer att utreda hur policykraven i ISO 27000-serien skulle kunna omhändertas på ett lämpligt sätt.

Kommunstyrelsen bedömde även att den systematiska uppföljning, som genomförs i hela organisationen med stöd av den nationella uppföljningsstrukturen Cybersäkerhetskollen, har en tydlig koppling till efterlevnaden av Malmö stads riktlinjer och anvisningar för informationssäkerhet. Vidare bedömde kommunstyrelsen att

ytterligare uppföljning av efterlevnad inte säkert ger önskad effekt. Kommunstyrelsen betonade att det på kort sikt är svårt att se effekterna av vidtagna åtgärder när det handlar om ett långsiktigt systematiskt arbete.

I det andra yttrandet angav kommunstyrelsen att en grundläggande informationssäkerhetsutbildning i Malmö stads lärplattform Malmö Lär hade tillgängliggjorts och marknadsförts under informationssäkerhetsmånaden i oktober 2025. Kommunstyrelsen framförde även att övriga rekommendationer behövde omhändertas utifrån de förskrifter som ännu inte tagits fram för att tydliggöra kraven i cybersäkerhetslagen som trädde i kraft i januari 2026. Detta eftersom stadskontoret ansåg det lämpligt att ta fram nya regler och arbetssätt först när det stod klart vad som skulle behöva ingå.

Revisorskollegiets bedömning

Revisorskollegiets samlade bedömning är att kommunstyrelsen inte helt har säkerställt en tillräcklig IT-säkerhet för Malmö stad. Revisorskollegiet menar att för att styrelsen ska kunna redovisa vidtagna åtgärder enligt ny lagstiftning krävs ett uppföljande yttrande från kommunstyrelsen om följande rekommenderade åtgärder:

- Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien.
- Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i Riktlinjer för informationssäkerhet samt att kontroll av efterlevnad av riktlinjerna etableras..
- Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med Anvisning för informationshantering och säkerhetsprocesser.

Stadskontorets bedömning

Kommunstyrelsens olika svar har lämnats till revisorskollegiet med tio månaders mellanrum. Stadskontoret anser att det på så kort sikt inte är möjligt att genomföra alla åtgärder av det slag som revisorskollegiet rekommenderat och att se effekterna av dem. Som jämförelse är premissen i den nationella uppföljningsstrukturen Cybersäkerhetskollen att en åtgärd behöver ha funnits på plats kontinuerligt under två år för att räknas in i mätningen. Anledningen till detta är att nivån på organisationens cybersäkerhetsarbete är resultatet av arbete och val som har gjorts över tid.

Stadskontoret bedömer vidare att rekommendationerna från revisorskollegiet i stort blev överflödiga efter att cybersäkerhetslagen med tillhörande föreskrifter trätt i kraft i januari respektive oktober 2026. Detta eftersom föreskrifterna innehåller

säkerhetsåtgärder som berör hela spektrumet av cybersäkerhetsarbetet, från styrning till uppföljning och rapportering.

Sedan föregående yttrande lämnats till revisorskollegiet i februari 2026 har stadskontoret deltagit i remissarbetet för föreskrifternas utformning, fastställt en plan för Malmö stads omhändertagande av cybersäkerhetslagen och påbörjat genomförandet av denna i nära samarbete med framförallt servicenämnden. 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. Stadskontoret 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.

Revisorskollegiets rekommendation med stadskontorets uppföljande svar

- 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. Stadskontoret 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 stadskontoret att utreda hur policykraven i ISO 27000-serien skulle kunna omhändertas på ett lämpligt sätt. Detta förväntas tydliggöra Malmö stads inriktning för arbetet med informationssäkerhet.

- 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. Stadskontoret anser därför att Malmö stads behov av efterlevnadskontroller behöver bedömas i relation till kraven i föreskrifterna och den nya uppföljningsstrukturen när den tillgängliggjorts.

Stadskontoret kommer att etablera årlig rapportering om cybersäkerhet till kommunstyrelsen i enlighet med föreskrifterna. Just nu utreder stadskontoret hur rapporteringen kan utformas och samordnas med annan 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.

- 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. Stadskontoret 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.

Stadskontorets avslutande kommentar

Stadskontoret delar revisorskollegiets uppfattning om att det är viktigt att ytterligare åtgärder för att stärka stadens arbete med informationssäkerhet, inklusive cybersäkerhet, kommer på plats. Detta arbete är högt prioriterat, men stadskontoret bedömer inte att det är rimligt att redan nu rapportera om effekter för föreskrifter som trätt i kraft i oktober 2026.

Ansvariga

Isabelle Henningsson Nämndsekreterare
Ana Maria Deliv Avdelningschef
Tomas Bärring Chefsjurist
Jonas Rosenkvist Stadsdirektör