Uppföljning av tidigare granskningar av IT-säkerhet

Haninge kommun

Building a better working world

Innehållsförteckning

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna följt upp två av de fördjupade granskningar som genomfördes i Haninge kommun under revisionsåren 2022 och 2023. De två fördjupade granskningarna avser "Granskning av kommunens cybersäkerhet", samt "Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur". Granskningen av kommunens cybersäkerhet har delvis följts upp inom ramen för den tidigare uppföljande granskningen 2024.

Sammanfattningsvis bedöms kommunstyrelsen i huvudsak ha åtgärdat de rekommendationer som lämnades i tidigare granskningar. Vi noterar att en omorganisation har skett sedan granskningarna genomfördes och att flera åtgärder har vidtagits med utgångspunkt från lämnade rekommendationer. Pågående utvecklingsarbete bedöms ge förutsättningar för att åtgärda rekommendationerna som bedöms vara delvis åtgärdade.

I tabellen nedan redovisas en sammanställning av uppföljningen med angivelse av huruvida tillräckliga åtgärder vidtagits till följd av lämnade rekommendationer.

Granskning	Antal rekommendationer	Åtgärdad		
		Ja	Delvis	Nej
Granskning av kommunens cybersäkerhet (2022)	9[1]	5	4	-
Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur (2023)	3	2	1	-
TOTALT	**12**	**7**	**5**	**-**

Vi bedömer att åtgärder har vidtagits med anledning av tidigare incidenter, så som till exempel incidenter rörande den externa leverantören Miljödata. Miljödata har inte upptäckt att information från Haninge kommun har läckt, men kommunen har vidtagit flera åtgärder. Detta inkluderar att kommunen har isolerat funktioner till Miljödatas olika system, gjort anmälningar till Integritetsskyddsmyndigheten (IMY) och Myndigheten för civilt försvar (MCF)[2]. Kommunen deltar även i flera forum i lärosyfte.

Av protokollgranskningen framgår att det inte har skett någon särskild återrapportering av vidtagna åtgärder kopplat till granskningarna till kommunstyrelsen. Däremot framgår det att kommunstyrelsen fått del av ärenden som avser förbättringar i linje med lämnade rekommendationer.

[1] Inom ramen för den uppföljande granskningen 2024 följdes rekommendation 1–3 upp. Sammantaget bedömdes två av revisionens tre rekommendationer ha beaktats och åtgärdats fullt ut, och en rekommendation hade delvis åtgärdats. I denna granskning följs den rekommendation som bedömdes som delvis uppfylld upp, utöver övriga sex rekommendationer.
[2] Från den 1 januari 2026 är Myndigheten för samhällsskydd och beredskap, MSB, Myndigheten för civilt försvar.

1. Inledning

1.1 Bakgrund

En viktig del i revisionens arbete är att följa upp granskningar från tidigare år i syfte att bedöma genomslag för de förbättringsförslag och rekommendationer revisionen lämnat. Kommunrevisionen har utifrån sin risk- och väsentlighetsanalys för revisionsåret 2025 därför beslutat att genomföra en uppföljning av följande granskningar:

- Granskning av kommunens cybersäkerhet (genomfördes 2022)
- Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur (genomfördes 2023)

I dessa granskningar noterades brister i kommunstyrelsens styrning, arbetssätt och interna kontroll.

Granskningen av kommunens arbete för cybersäkerhet visade på tydliga brister i kommunens mognadsgrad, i jämförelse med andra kommuner, främst när det gäller riktlinjer och processbeskrivningar för informationssäkerhetsarbetet samt en utförlig roll- och ansvarsbeskrivning. Därtill saknades processer för uppföljning/kontroll och kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Flera rekommendationer avlämnades inom ramen för granskningen.

Vad gäller granskningen av kommunens IT-infrastruktur var den samlade bedömningen att kommunstyrelsen inte i tillräcklig utsträckning säkerställt en ändamålsenlighet för de granskade områdena. Kommunstyrelsen hade inte säkerställt att relevanta styrdokument för vardera granskat område fanns framtaget. Därutöver saknades tydliga och dokumenterade riktlinjer för vissa områden. Därtill hade kommunstyrelsen inte säkerställt uppföljning och efterlevnad av kommunens riktlinjer.

1.2 Syfte och revisionsfrågor

Syftet med den uppföljande granskningen är att bedöma de åtgärder som kommunstyrelsen vidtagit utifrån revisionens tidigare rekommendationer.

I den uppföljande granskningen besvaras följande revisionsfrågor för respektive granskningsrapport:

- Har kommunstyrelsen behandlat granskningarna på nämndsmöte?
- Har kommunstyrelsen givit förvaltningen i uppdrag att vidta åtgärder med utgångspunkt från revisionens granskningar?
- Har ändamålsenliga åtgärder vidtagits med utgångspunkt från lämnade rekommendationer?
- Är vidtagna åtgärder i linje med de svar kommunstyrelsen lämnade till kommunrevisionen i samband med granskningen?
- Har åtgärder vidtagits med anledning av tidigare incidenter, så som till exempel Miljödata?
- Har åtgärderna följts upp och återrapporterats till kommunstyrelsen?

1.3 Avgränsning

Den uppföljande granskningen avser kommunstyrelsen. Granskningen avgränsas i tid till perioden från det att respektive granskning avlämnades till kommunstyrelsen, till avrapportering av denna granskning januari 2026.

1.4 Metod och genomförande

Granskningen har genomförts genom dokumentstudier, samt kompletterande intervjuer. Inhämtande av skriftliga svar från kommunstyrelseförvaltningen har även begärts in.

Utöver vår interna kvalitetssäkring får samtliga intervjuade möjlighet att sakgranska rapportutkastet. Detta för att säkerställa att revisionsrapporten bygger på korrekta fakta och uttalanden. Samtliga intervjuade funktioner och granskade underlag framgår av källförteckningen.

2. Kommunstyrelsens behandling av tidigare granskningar

Av granskning av protokoll från kommunstyrelsens sammanträden från december 2022 till december 2025 framgår att kommunstyrelsen har behandlat en av de två granskningarna vid sammanträde. Granskningen av kommunens arbete med cybersäkerhet behandlades vid sammanträde den 15 maj 2023[3]. Av protokollen framgår att kommunstyrelsen har beslutat att kommunstyrelseförvaltningens tjänsteskrivelse godkänns som kommunstyrelsens svar på revisionsskrivelsen.

Vad gäller granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur har denna inte behandlats vid sammanträde. Vi har fått det förklarat att detta inte har skett med anledning av att rapporten belagts med sekretess. Vi har inom ramen för granskningen inte kunnat styrka om behandling av rapporten har skett muntligen eller genom annat förfarande.

Av protokollgranskningen framgår att det inte har skett någon särskild återrapportering av vidtagna åtgärder kopplat till granskningarna till kommunstyrelsen. Däremot framgår det att kommunstyrelsen fått del av ärenden som avser förbättringar i linje med lämnade rekommendationer. Av protokoll framgår exempelvis att nya styrdokument inom området eller revideringar av befintliga har gjorts under perioden. Detta inkluderar policy för säkerhet och beredskap, riktlinjer för säkerhetsskydd, informationssäkerhetspolicy, reglemente för internkontroll, samt kommunstyrelsens delegationsordning där ett nytt kapitel om säkerhetsskydd införs. Från protokollgranskningen görs även övriga noteringar att återrapportering till kommunstyrelsen har skett gällande uppföljning av beredskapsarbete, samt internkontroll inom ramen för verksamhetsuppföljningen.

[3] § 92 Svar på revisionsrapport 7 2022 Granskning av kommunens cybersäkerhetsarbete

3. Åtgärder utifrån granskning av kommunens arbete med cybersäkerhet

3.1 Sammanfattning av tidigare granskning

Granskningen av kommunens arbete med cybersäkerhet genomfördes från juni till december 2022. Syftet var att identifiera om det fanns brister i kommunens interna kontroll avseende cybersäkerhet. Revisorernas sammanfattande bedömning var att Haninge kommuns arbete med cybersäkerhet delvis var ändamålsenligt.

I granskningen konstaterades att Haninge kommun hade en genomsnittlig mognadsgrad på 2,60. Motsvarande offentliga organisationer av likande storlek och karaktär hade ett genomsnitt på 2,52. Granskningsresultatet indikerade att kommunens mognadsgrad var högst inom området personuppgiftstyrning. Kommunens lägsta mognadsgrad var inom området strategi och rutiner. Med hänvisning till den stora mängden personuppgifter och andel personuppgifter av känslig karaktär som hanteras inom Haninge kommun var bedömningen att kommunens mognadsgrad är klar lägre än vad EY rekommenderar för en kommun likt Haninge.

Det fanns ett implementerat ledningssystem för informationssäkerhet samt flertalet övergripande styrdokument, däribland säkerhetsprogram som inkluderar informationssäkerhet, digitaliseringspolicy samt riktlinjer för GDPR. Det konstaterades att riktlinjer och processbeskrivning för informationssäkerhetsarbetet samt en utförlig roll- och ansvarsbeskrivning saknades. Granskningen visade även att det saknades processer för uppföljning/kontroll och kontinuerlig rapportering till kommunstyrelse avseende hur cybersäkerhetsarbetet fortlöper. Det fanns även ett behov av en utpekad samordnare för informationssäkerhet och dokumentation som beskrivning kommunens hantering av informationssäkerhetsincidenter.

Utifrån identifierade förbättringsområden lämnades totalt nio rekommendationer till kommunstyrelsen. Vi noterar att formuleringen av rekommendationerna varierar lite mellan granskningsrapporten och revisionsskrivelsen, där de är mer utförliga i granskningsrapporten, men har samma innebörd. Främst rekommenderade EY att kommunstyrelsen i Haninge kommun skulle tillse att:

1. En samordnare rekryteras med informationssäkerhet som sitt huvudsakliga ansvarsområde för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.
2. Direktivet för informationssäkerhet färdigställs och beslutas för att säkerställa att den övergripande målbilden och ansvarsfördelningen med informationssäkerhet formaliseras och träder i kraft.
3. Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.
4. En riktlinje för hantering av informationssäkerhetsincidenter upprättas och beslutas för att formalisera arbetsmetoder och säkerställa att anställda inom kommunen följer en enhetlig process som är ändamålsenlig.
5. En ändamålsenlig kontinuitetsplan finns på plats för samtliga kommunens verksamheter. Kommunstyrelsen bör även tillse att en process upprättas som regelbundet säkerställer att kontinuitetsplanerna förblir riktiga och aktuella över tid.

Därefter rekommenderade EY även att kommunstyrelsen i Haninge kommun skulle tillse att:

6. En utbildningsplan för cybersäkerhet upprättas och beslutas. Utbildningsplanen bör innehålla obligatoriska och regelbundna utbildningar för samtliga anställda som hanterar kommunens information och deltagande bör följas upp för att säkerställa att samtliga berörda anställda har genomfört utbildningarna.
7. En formaliserad internkontrollplan upprättas, beslutas och implementeras för att granska och säkerställa att policy och riktlinjer avseende cybersäkerhet efterlevs i praktiken. Interkontrollplanen bör även inkludera uppföljning av GDPR från centralt håll som inte förlitar sig på att kommunens nämnder granskar sitt eget personuppgiftsarbete.
8. Formaliserade rapporteringskrav kring cybersäkerhet upprättas, beslutas och implementeras för att säkerställa kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Den kontinuerliga rapporteringen tillåter kommunstyrelsen att identifiera gap och kontrollera efterlevnad av policy och riktlinjer avseende cybersäkerhet.
9. En kommunikationsplan upprättas, beslutas och implementeras som innebär att anställda aktivt nås av policy och riktlinjer avseende cybersäkerhet. Kommunikationsplanen syftar till att säkerställa att anställda som hanterar kommunens information har kännedom om kommunens policy och riktlinjer avseende cybersäkerhet.

Inom ramen för den uppföljande granskningen 2024 följdes rekommendation 1–3 upp. Sammantaget bedömdes två av revisionens tre rekommendationer ha beaktats och åtgärdats fullt ut, och en rekommendation hade delvis åtgärdats.[4] I denna granskning följs den rekommendation som bedömdes vara delvis uppfylld upp, utöver övriga sex rekommendationer.

3.1.1 Rekommendationer som bedömdes vara åtgärdade i den uppföljande granskningen 2024

Följande rekommendationer bedömdes vara åtgärdade i den uppföljande granskningen 2024. Dessa följs inte upp i denna granskning, men beskrivs nedan.

Rekommendation 1: En samordnare rekryteras med informationssäkerhet som sitt huvudsakliga ansvarsområde för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.	
Bedömning i uppföljande granskning 2024	Rekommendationen bedömdes ha åtgärdats fullt ut. En informationssäkerhetssamordnare anställdes på kommunstyrelseförvaltningen i januari 2024. Samordnaren hade tidigare erfarenhet av motsvarade arbetsuppgifter i andra offentliga organisationer och kommunstyrelseförvaltningen bedömde att bemanningen var tillräcklig.[5]

[4] Rekommendation 3: Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.
[5] Vi noterar att vid intervju nämndes att en ny informationssäkerhetssamordnare är under rekrytering.

Rekommendation 2: Direktivet för informationssäkerhet färdigställs och beslutas för att säkerställa att den övergripande målbilden och ansvarsfördelningen med informationssäkerhet formaliseras och träder i kraft.	
Bedömning i uppföljande granskning 2024	Rekommendationen bedömdes ha åtgärdats fullt ut. Kommunfullmäktige beslutade den 20 maj 2024 om policy för säkerhet och beredskap, samt igångsättningsbeslut för tillkommande styrdokument. Policyn reglerar inriktning, principer och ansvarsfördelning för Haninge kommuns arbete inom säkerhet. Detta omfattar informationssäkerhet, internt skydd, säkerhetsskydd samt beredskap (krisberedskap och civilt försvar).

3.2 Uppföljning av vidtagna åtgärder per november 2025

Nedan följer iakttagelser för rekommendationerna som kvarstod i uppföljningen 2025.

3.2.1 Iakttagelser

Styrningen har stärkts genom styrdokument och tydligare ansvarsfördelning

Av intervju framgår att det har skett en omfattande organisationsförändring sedan den tidigare granskningen genomfördes och att IT-enheten numera är sorterad inom en annan avdelning, utvecklingsavdelningen inom kommunstyrelseförvaltningen. En IT-chef har rekryterats som leder enheten. En ny funktion, IT-säkerhetsspecialist, har även rekryterats till enheten som är tillgänglig för alla kommunens förvaltningar.

I kommunstyrelseförvaltningens svar till den uppföljande granskningen 2025 framgår att en rutin för informationssäkerhet beslutades av kommundirektören den 20 december 2023. Rutinen är styrande för kommunens praktiska informationshantering. Rutinen ska tillämpas av alla förvaltningar i kommunen, samt kommunens helägda bolag där bolagen använder sig av kommunens gemensamma informationstillgångar.

Vi har tagit del av rutinen som beskriver ansvar och roller, säkerhetsrelaterad kunskap och informationstillgångar, informationssäkerhet vid rekrytering, anställning och avslut av tjänst, fysiskt skydd av informationstillgångar, åtkomst till och lagring av information, driftsäkerhet, hantering av incidenter, samt uppföljning. Kommunstyrelseförvaltningen ansvarar för att rutinen revideras senast under första året i varje mandatperiod, men även vid större förändringar eller tillkommande myndighetskrav som påtagligt påverkar kommunens informationssäkerhetsarbete. Kommunstyrelseförvaltningen följer årligen upp informationssäkerhetsarbetet enligt rutinen.

Kommunicering och förankring av rutiner

En kommunikationsplan har inte upprättats. Dock förankras policys och riktlinjer bland medarbetare genom utbildningar. I kommunstyrelseförvaltningens svar framgår att förankring och kännedom om befintliga policys och riktlinjer bland medarbetare säkerställs genom utbildningar, samt det arbete som görs inom ramen för kommunens systemförvaltningsmodell. Vi har inom ramen för granskningen kunnat bekräfta detta arbetssätt genom rutiner och underlag gällande utbildningar.

Det finns en upprättad internkontrollplan med relevanta risker

Vi har tagit del av kommunstyrelsens internkontrollplan för 2025. Internkontrollplanen inkluderar följande risker med bäring på granskningsområdet:

- Efterlevnad av lagar, föreskrifter och riktlinjer: Bristande kompetens kring informationssäkerhet kan leda till att känslig/värdefull information sprids till obehöriga och/eller förvanskas eller ändras.
- Verksamhetskontroll:
    - Bristande IT-säkerhet kan leda till att känslig/värdefull information sprids till obehöriga och/eller förvanskas eller ändras.
    - Bristande kunskap kring rapportering av incidenter, som sker i nätverk och informationssystem, kan leda till att incidenter återkommer samt att de inte rapporteras in till rätt tillsynsmyndighet.

Internkontrollplanen följs upp inom ramen för kommunens system för uppföljning av verksamhet och ekonomi.

Vi noterar även att sedan granskningen genomfördes 2022 har flera risker inom IT-säkerhet inkluderats i internkontrollplanerna (se avsnitt 6 för ytterligare information). Risk kring personuppgiftsbehandling enligt GDPR har ingått i internkontrollplanerna 2022 och 2023, risk för gallring av data i koncerngemensamma verksamhetssystem 2023, samt risker inom IT-säkerhet 2024.

Rutiner för hantering av incidenter har stärkts

I kommunstyrelseförvaltningens svar framgår att det finns en riktlinje, *Haninge kommuns IT-handbok – Anvisningar om hur du hanterar din IT- och telefoniutrustning*, på intranätet HINT. Vi har tagit del av riktlinjen och där framgår ett avsnitt om rapportering av säkerhetsincidenter. Riktlinjen upprättades den 1 februari 2024 av IT-enheten och reviderades senast den 5 november 2024.

IT-enheten har en mall och process för incidenthanteringsprocess och utsedd Incident Manager (IM) samt Major Incident Manager (MIM). Riktlinjen beskrivs förankras löpande inom ramen för kommunens systemförvaltningsmodell där klassning av system ingår. Systemförvaltarmöten hålls till systemförvaltare i alla verksamheter inom kommunen för att praktiskt lära ut incidenthantering. Mötena hålls av IT-enheten varannan månad och individuella möten sker även vid behov. Av intervju framgår att förvaltningen ser över frekvensen för mötena.

Det pågår arbete med att säkerställa ändamålsenliga kontinuitetsplaner

I kommunstyrelseförvaltningens svar framgår att en kontinuitetsplan är en av flera åtgärder som kontinuitetshantering kan resultera i. En ny enhet på kommunstyrelseförvaltningen, krisberedskap och civilt försvar, bildades under våren 2025. Enheten ansvarar för att administrativa processer upprättas som regelbundet säkerställer att kontinuitetsplanerna förblir riktiga och aktuella över tid. Enheten kommer under det fjärde kvartalet 2025 att påbörja arbetet med en gemensam process. Arbetet beräknas vara färdigt senast under våren 2026.

Informationssäkerhetskollen, där framtagande av kontinuitetsplanering ingår, är genomförd för samtliga verksamheter.

Utbildningsinsatser genomförs men kommer att systematiseras under 2026

I rutinen för informationssäkerhet ingår avsnitt som beskriver utbildningskrav. Kommunens regelverk för informationssäkerhet ska finnas tillgängligt på intranätet. Anställda ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att en tillfredsställande informationssäkerhetsnivå uppnås. Utbildningens omfattning ska anpassas till befattningens ansvar och befogenheter. Detsamma gäller även när tillfällig personal eller externa aktörer anlitas. Utbildning ska ske regelbundet och hållas aktuell och relevant i förhållande till ändringar i

lagar eller andra myndighetskrav. Verksamhetsansvarig/chef ansvarar för att medarbetarna får relevant utbildning och kommunövergripande information.

Det uppges finnas en digital informationssäkerhetsutbildning (DISA) tillgänglig för samtliga medarbetare. Förvaltningen beskriver att det finns en sammanställning över vilka medarbetare som har tagit del av utbildningar inom området och att arbete pågår med att implementera del 2, som ska komplettera DISA och alla medarbetare ska gå årligen. Del 2 avser IT-säkerhetsutbildningar på den digitala plattformen Nimblr. Detta ska implementeras under 2026.

På systemförvaltningsmöten förekommer även tema säkerhet med syfte att höja medvetenheten hos medarbetare som arbetar i systemen.

Simulerade tester genomförs även gällande kommunens medarbetares medvetenhet kring nätfiske. Av intervju framgår att tester inte har skickats ut under 2025, att dessa tidigare enbart har genomförts sporadiskt, men från och med 2026 årligen. Utbildning om nätfiske ska även ingå i Nimblr. Detta kommer att stärka utbildningsinsatserna avseende cybersäkerhet ytterligare, då nätfiske bedöms som ett påtagligt hot för kommunen inom detta område.

Uppföljning och rapportering till kommunstyrelsen kan fortsatt stärkas

Av intervju beskrivs uppföljning till kommunstyrelsen främst ske inom ramen för internkontrollprocessen. Av granskning av protokoll från kommunstyrelsens sammanträden från december 2022 till december 2025 framgår viss rapportering om cybersäkerhetsarbetet. Formaliserade rapporteringskrav kring cybersäkerhet bedöms inte finnas upprättade i övrigt. Övergripande uppföljning till kommunstyrelsen beskrivs ytterligare i avsnitt 6.

Vi noterar att återrapportering av uppföljningen av åtgärderna kopplade till granskningen har skett till kommunstyrelsen.

3.3 Sammanfattande bedömning

Sammantaget bedömer vi att fem av revisionens nio rekommendationer har beaktats och åtgärdats fullt ut, och fyra rekommendationer har delvis åtgärdats. Inom ramen för den uppföljande granskningen 2024 följdes rekommendation 1–3 upp. Sammantaget bedömdes två av revisionens tre rekommendationer ha beaktats och åtgärdats fullt ut, och en rekommendation hade delvis åtgärdats. I denna granskning följs den rekommendation som bedömdes som delvis uppfylld upp, utöver övriga sex rekommendationer.

Kommunstyrelsen har beaktat revisorernas iakttagelser och rekommendationer, samt vidtagit relevanta åtgärder för sju av nio lämnade rekommendationer. Vi ser positivt på det arbete som skett i kommunstyrelsen sedan granskningen genomfördes och att det finns en ny organisation på plats som har prioriterat utvecklingsarbetet och att utveckla ändamålsenliga strukturer för arbetet.

Vad gäller att säkerställa en ändamålsenlig kontinuitetsplan, samt att tillse en process som regelbundet säkerställer att kontinuitetsplanerna förblir riktiga och aktuella över tid kan det kopplas till pågående utvecklingsarbete, men vi har inte sett implementering av detta fullt ut. Arbetet beräknas vara klart under våren 2026.

Vidare pågår utvecklingsarbete vad gäller att säkerställa IT-säkerhetsutbildningar på en digital plattform (Nimblr). Vår bild är att arbetet inte är på plats fullt ut, men att det finns långtgående planer för implementeringen. Vi bedömer att rapportering kring cybersäkerhetsarbetet delvis sker inom ramen för internkontrollprocessen, samt till viss del vid kommunstyrelsens sammanträden. Dock har formaliserade rapporteringskrav inte implementerats vid denna granskning. Detta kan fortsatt stärkas.

Vad gäller rekommendationen gällande att en kommunikationsplan upprättas, har det inte gjorts, men det finns ett arbete i syfte att säkerställa att personal aktivt nås av information gällande riktlinjer avseende cybersäkerhet, bland annat genom utbildningar, samt det arbete som görs inom ramen för kommunens systemförvaltningsmodell.

3.3.1 Bedömning av vidtagna åtgärder

Nedan framgår vår bedömning kring vidtagna åtgärder för vardera rekommendation.

Rekommendation 3: Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas. Riktlinjerna bör konkretisera processer och rutiner för att leva upp till målbilden som beskrivs i direktivet för informationssäkerhet.	
Bedömning i uppföljande granskning 2024	Rekommendationen bedömdes **delvis** ha åtgärdats.
Vår bedömning	Rekommendationen bedöms ha åtgärdats, genom att ny rutin för informationssäkerhet har beslutats om och implementerats.

Rekommendation 4: En riktlinje för hantering av informationssäkerhetsincidenter upprättas och beslutas för att formalisera arbetsmetoder och säkerställa att anställda inom kommunen följer en enhetlig process som är ändamålsenlig.	
Vår bedömning	Rekommendationen bedöms ha åtgärdats, genom riktlinje och mall för incidenthantering som sätter ramar för arbetet, samt genom systemförvaltarmöten för att säkerställa kännedom om processen.

Rekommendation 5: En ändamålsenlig kontinuitetsplan finns på plats för samtliga kommunens verksamheter. Kommunstyrelsen bör även tillse att en process upprättas som regelbundet säkerställer att kontinuitetsplanerna förblir riktiga och aktuella över tid.	
Vår bedömning	Rekommendationen bedöms delvis ha åtgärdats, då verksamheterna har egna kontinuitetsplaner, men utveckling av en gemensam process är under utveckling och beräknas vara klar under våren 2026.

Rekommendation 6: En utbildningsplan för cybersäkerhet upprättas och beslutas. Utbildningsplanen bör innehålla obligatoriska och regelbundna utbildningar för samtliga anställda som hanterar kommunens information och deltagande bör följas upp för att säkerställa att samtliga berörda anställda har genomfört utbildningarna.	
Vår bedömning	Rekommendationen bedöms delvis ha åtgärdats, genom att IT-säkerhetsutbildningar på den digitala plattformen Nimblr kommer att implementeras i större skala under 2026.

Rekommendation 7: En formaliserad internkontrollplan upprättas, beslutas och implementeras för att granska och säkerställa att policy och riktlinjer avseende cybersäkerhet efterlevs i praktiken. Interkontrollplanen bör även inkludera uppföljning av GDPR från centralt håll som inte förlitar sig på att kommunens nämnder granskar sitt eget personuppgiftsarbete.	
Vår bedömning	Rekommendationen bedöms ha åtgärdats, genom att risker med bäring på informationssäkerhet har inkluderats i internkontrollplaner sedan granskningen genomfördes 2022.

Rekommendation 8: Formaliserade rapporteringskrav kring cybersäkerhet upprättas, beslutas och implementeras för att säkerställa kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper. Den kontinuerliga rapporteringen tillåter kommunstyrelsen att identifiera gap och kontrollera efterlevnad av policy och riktlinjer avseende cybersäkerhet.	
Vår bedömning	Rekommendationen bedöms delvis ha åtgärdats. Rapportering kring cybersäkerhetsarbetet sker till viss del inom ramen för internkontrollprocessen, samt till viss del vid kommunstyrelsens sammanträden. Dock har formaliserade rapporteringskrav inte implementerats vid den uppföljande granskningen 2025.

Rekommendation 9: En kommunikationsplan upprättas, beslutas och implementeras som innebär att anställda aktivt nås av policy och riktlinjer avseende cybersäkerhet. Kommunikationsplanen syftar till att säkerställa att anställda som hanterar kommunens information har kännedom om kommunens policy och riktlinjer avseende cybersäkerhet.	
Vår bedömning	Rekommendationen bedöms delvis ha åtgärdats. En kommunikationsplan har inte upprättats. Dock förankras policys och riktlinjer bland medarbetare genom utbildningar, samt det arbete som görs inom ramen för kommunens systemförvaltningsmodell.

4. Åtgärder utifrån granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur

4.1 Sammanfattning av tidigare granskning

Granskningen av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur genomfördes 2023. Granskningen omfattade behörighetshanteringen, programförändringshanteringen, samt IT-driftshanteringen inom fyra av kommunens IT-system.

Syftet var att bedöma om kommunstyrelsen hade säkerställt en ändamålsenlig intern kontroll och uppföljning avseende hantering av programförändringar, behörighetshantering och driftrutiner för system som är centrala för den finansiella rapporteringen.

Den samlade bedömningen var att kommunstyrelsen inte i tillräcklig utsträckning hade säkerställt en ändamålsenlig hantering av de granskade områdena.

Granskningen visade att kommunstyrelsen inte hade säkerställt att relevanta styrdokument för vart och ett av de granskade områdena har tagits fram. Det saknades även tydliga och dokumenterade riktlinjer för vissa områden. Kommunen hade inte säkerställt uppföljning och efterlevnad av Haninge kommuns riktlinjer.

Utifrån granskningens iakttagelser lämnades följande rekommendationer till kommunstyrelsen:

1. Relevanta styrdokument finns framtagna och att tillhörande riktlinjer implementeras.
2. Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.
3. Säkerhetsinställningarna avseende lösenord bör uppdateras i enlighet med gällande praxis.

4.2 Uppföljning av vidtagna åtgärder per november 2025

Nedan följer iakttagelser från uppföljningen av rekommendationerna 2025.

4.2.1 Iakttagelser

Styrdokument finns framtagna som även omfattar säkerheten och IT-strukturen

En rutin för informationssäkerhet har tagits fram. Inom ramen för de implementerade rutinerna finns även en ny systemförvaltningsmodell på plats. Av intervju framgår att den nya systemförvaltarmodellen är indelad i tre nivåer: strategisk, taktisk och operativ. Syftet med modellen har varit att förtydliga ansvarsfördelningen och rollbeskrivningar med tydligare ägarskap kring system. Ansvaret för system och kostnad har kopplats till ansvarig chef på ett tydligare sätt. Dessa delar stärker säkerheten och efterlevnad av denna.

Enligt intervjuade sker uppföljning av att systemägare följer rutiner och fastställer planer, bland annat vid systemägarmöten, men de ser behov av att systematisera uppföljningen framåt. Det finns ett inarbetat arbetssätt och en befintlig struktur för detta.

IT-enheten har kartlagt kommunens samtliga system. Enheten ansvarar även för att säkerställa att samtliga har en systemägare och systemförvaltningsplan. Uppföljningen av detta har gjorts utifrån riskbedömning kring systemets väsentlighet vad gäller information och behov av skydd. En struktur finns på plats för alla system som bedömts väsentliga. Uppföljningen från IT-enheten fokuserar på dessa system.

Styrningen av lösenordshantering kan stärkas ytterligare

Lösenordshantering beskrivs i kommunens IT-handbok och flera anvisningar presenteras.

Vi noterar att Myndigheten för civilt försvars (MCF:s) föreskrifter har förändrats sedan den tidigare granskningen. Enligt MCF:s aktuella föreskrifter[6] rekommenderas 14 tecken, men fler och både numeriska, versaler, gemena och specialtecken minskar risken för att någon ska knäcka lösenordet.

Uppföljningen har stärkts genom internkontrollplan och systemförvaltarskap

I kommunstyrelseförvaltningens svar framgår att uppföljning sker inom ramen för kommunens system för planering och uppföljning av verksamhet och ekonomi, samt internkontrollprocessen. Vi noterar även att ett utvecklingsarbete har skett inom ramen för systemförvaltarmodellen där en del av de systemtekniska planerna hanteras. Vidare noterar vi att penetrationstester har genomförts, samt att övervakning av brandväggar finns. Detta utgör olika delar i kommunens rutiner och arbetssätt för att följa upp efterlevnad av befintliga rutiner och riktlinjer.

4.3 Sammanfattande bedömning

Sammantaget bedömer vi att två av revisionens tre rekommendationer har beaktats och åtgärdats fullt ut, och att en rekommendation delvis har åtgärdats.

Kommunstyrelsen har beaktat revisorernas iakttagelser och rekommendationer, samt vidtagit relevanta åtgärder för två av tre lämnade rekommendationer. Vi ser positivt på det arbete som skett i kommunstyrelsen sedan granskningen genomfördes.

I intervjuer sker hänvisning till omvärldsbevakning och dialog med vissa säkerhetsaktörer. Vi bedömer att detta bör bygga på en riskbedömning kring respektive system och konto, samt att det bör finnas ett dokumenterat ställningstagande. Vi har i granskningen inte fått del av något dokumenterat ställningstagande med riskbedömning och bakgrund till kommunens nuvarande praxis. Detta kan stärkas.

4.3.1 Bedömning av vidtagna åtgärder

Nedan framgår vår bedömning kring vidtagna åtgärder för vardera rekommendation.

Rekommendation 1: Relevanta styrdokument finns framtagna och att tillhörande riktlinjer implementeras.	
Vår bedömning	Rekommendationen bedöms ha åtgärdats, genom ny rutin för informationssäkerhet och ny systemförvaltningsmodell som sätter ramar för området.

Rekommendation 2: Processer för uppföljning av efterlevnaden av kommunens riktlinjer och rutiner implementeras och genomförs.	
Vår bedömning	Rekommendationen bedöms ha åtgärdats, genom att uppföljning sker inom ramen för kommunens system för planering och uppföljning av verksamhet och ekonomi. Vi noterar även från protokollgranskning att viss uppföljning sker vid kommunstyrelsens sammanträden.

[6] "Säkra dina lösenord", MCF, 2025. Tillgänglig: Säkra dina lösenord

Rekommendation 3: Säkerhetsinställningarna avseende lösenord bör uppdateras i enlighet med gällande praxis.	
Vår bedömning	Rekommendationen bedöms ha delvis åtgärdats. Vi noterar att MCF:s föreskrifter har uppdaterats sedan den ursprungliga granskningen, men att kommunens lösenordskrav är lägre än MCF:s gällande föreskrifter.

5. Vidtagna åtgärder med anledning av tidigare incidenter

Miljödata, som är leverantör av systemen Adato och Novi för att hantera personal- och rehabiliteringsärenden i Haninge kommun, utsattes för ett cyberangrepp under 2025. Händelsen upptäcktes lördagen den 23 augusti 2025 och utreds av Miljödata tillsammans med externa experter.

Enligt kommunens hemsida framgår att Miljödata har meddelat att de hittills inte har konstaterat att information från Haninge kommun har läckt. Kommunen följer utvecklingen tillsammans med leverantören och övriga kommuner. Vidare framgår att Miljödata har isolerat sina IT-system och arbetar med återställning. Isoleringen innebär att systemet tillfälligt har kopplats bort från övriga system för att skydda information och förhindra att angreppet sprider sig. Det betyder att ingen ny information skickas till eller från systemet just nu. Kommunen har stängt kopplingen till Miljödatas olika system. En anmälan har gjorts till Integritetsskyddsmyndigheten (IMY), ett lagkrav enligt GDPR. I anmälan beskriver kommunen vad som har hänt, vilka uppgifter som kan ha påverkats, vilka åtgärder som har vidtagits och hur kommunen hanterar riskerna.[7]

Av intervju framgår att kommunen även har anmält incidenten till CERT-SE, Sveriges nationella CSIRT (Computer Security Incident Response Team) som bedrivs via Myndigheten för civilt försvar (MCF). CERT-SE är mottagare av IT-incidentrapporter enligt MSBFS 2020:8 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet. Kommunen deltar i flera forum i lärosyfte. Detta inkluderar samverkansforum Miljödata, SKR:s Handslaget och forum för cybersäkerhet.

Vid upphandling ställer kommunen strikta säkerhetskrav på IT-leverantörer med behörighetsstyrning. Under våren har IT-enheten arbetat med att utveckla de tekniska kraven och säkerhetskraven. Intervjuade ser behov av att följa upp gamla avtal, vilket är inkluderat i plan framöver, även om risker fångas i klassning och behörighetsstyrning.

IT-enheten använder en leverantör för detta, Security Operations Center, som återrapporterar statistik över incidenter och intrångsförsök. IT-enheten har möten varje vecka med IT-leverantören gällande säkerhetsfrågor.

5.1 Bedömning

Åtgärder har vidtagits med anledning av tidigare incidenter, så som till exempel Miljödata. Miljödata har inte konstaterat att information från Haninge kommun har läckt, men kommunen har vidtagit flera åtgärder. Detta inkluderar att kommunen har stängt kopplingen till Miljödatas olika system, gjort anmälningar till IMY och MCF. Kommunen deltar även i flera forum i lärosyfte.

[7] Haninge kommuns hemsida, 2025. Tillgänglig: https://www.haninge.se/aktuellt/2025/augusti/miljodata-utsatt-for-cyberangrepp_/

6. Uppföljning och återrapportering till kommunstyrelsen

Arbetet med informationssäkerhet följs till viss del upp inom ramen för kommunstyrelsens verksamhetsuppföljning (delårsrapporter, årsredovisning, sammanträden, samt internkontroll).

Av kommunstyrelsens årsredovisningar 2022–2024 framgår ökad rapportering 2024 gällande informations- och cybersäkerhet. Det saknas rapportering för 2023, utöver det som rapporteras inom ramen för internkontrollen. I årsredovisningen för 2024 framgår att kommunen i början av året beslutade att införa bakgrundskontroller på chefer i samband med nyrekrytering samt vid rekrytering av andra nyckelpositioner som kan eller ska ha åtkomst till känslig eller konfidentiell information. Bakgrundskontroller började genomföras från och med den 1 september 2024. Kommunen genomförde även cybersäkerhetskollen via Myndigheten för civilt försvar (MCF), vilken identifierade förbättringsbehov kopplade till digitala beroenden. Ytterligare styrdokument för civilt försvar är under framtagande.

Av kommunstyrelsens delårsrapporter för 2025 framgår rapportering främst kopplat till mål och uppdrag inom trygghet, civil beredskap och säkerhet, men även internkontroll. Under 2025 har kommunstyrelsen prioriterat arbetet inom krisberedskap och civilt försvar. Kommunstyrelsen har förstärkt säkerhetsskyddsarbetet bland annat genom utökade resurser, utbildning av berörda verksamheter och medarbetare samt framtagande av styrande dokument.

Under perioden har risker kopplat till IT-säkerhet ingått i internkontrollplanerna som har beskrivits under avsnitt 3.2.1.

År	2022	2023	2024	2025
Risk	**Efterlevnad av lagar, föreskrifter, riktlinjer:** Personuppgiftsbehandling enligt GDPR (kommungemensamt kontrollmoment)	**Efterlevnad av lagar, föreskrifter, riktlinjer:** Personuppgiftsbehandling enligt GDPR (kommungemensamt kontrollmoment)	**Verksamhetskontroll:** Risk att kommunen köper in system, support och IT-lösningar som inte långsiktigt passar in i helheten.	**Efterlevnad av lagar, föreskrifter och riktlinjer:** Bristande kompetens kring informationssäkerhet kan leda till att känslig/värdefull information sprids till obehöriga och/eller förvanskas eller ändras.
		Ändamålsenlig och kostnadseffektiv verksamhet: Gallring av data i koncerngemensamma verksamhetssystem	**Verksamhetskontroll:** Risk för intrång i kommunens IT-miljö och IT-system, vilket kan innebära att IT-miljön skadas, att det blir driftstopp eller att kommunens information stjäls eller görs obrukbar.	**Verksamhetskontroll:** Bristande IT-säkerhet kan leda till att känslig/värdefull information sprids till obehöriga och/eller förvanskas eller ändras.
				Verksamhetskontroll: Bristande kunskap

				kring rapportering av incidenter, som sker i nätverk och informationssystem, kan leda till att incidenter återkommer samt att de inte rapporteras in till rätt tillsynsmyndighet.

Av kommunstyrelsens uppföljning av internkontrollplanerna 2022–2024 framgår att kontrollmoment har utförts för riskerna. Resultatet av kontrollerna visar att åtgärder har presenterats för vissa risker, där utvecklingsområden kvarstår. Åtgärder inkluderar bland annat framtagande av nya rutiner och arbetssätt, informationsinsatser, samt fortsatta kontroller.

6.1 Bedömning

Arbetet med informationssäkerhet följs till viss del upp inom ramen för kommunstyrelsens verksamhetsuppföljning (delårsrapporter, årsredovisning, sammanträden, samt internkontroll). Av protokollgranskningen framgår att det inte skett någon särskild återrapportering av vidtagna åtgärder kopplat till granskningarna till kommunstyrelsen. Däremot framgår det att kommunstyrelsen fått del av ärenden som avser förbättringar i linje med lämnade rekommendationer.

7. Svar på revisionsfrågor

Revisionsfrågor	Svar
Har kommunstyrelsen behandlat granskningarna på nämndsmöte?	Delvis. Kommunstyrelsen har behandlat en av två granskningar vid sammanträde. Granskningen av kommunens arbete med cybersäkerhet behandlades vid sammanträde den 15 maj 2023.
Har kommunstyrelsen givit förvaltningen i uppdrag att vidta åtgärder med utgångspunkt från revisionens granskningar?	Delvis. Av protokollgranskning framgår att kommunstyrelsen har beslutat att kommunstyrelseförvaltningens tjänsteskrivelse godkänns som kommunstyrelsens svar på revisionsskrivelsen.
Har ändamålsenliga åtgärder vidtagits med utgångspunkt från lämnade rekommendationer?	Delvis. Vi noterar att en omorganisation har skett sedan granskningarna genomfördes och att flera åtgärder har vidtagits med utgångspunkt från lämnade rekommendationer. Pågående utvecklingsarbete bedöms ge goda förutsättningar för att åtgärda rekommendationerna.
Är vidtagna åtgärder i linje med de svar kommunstyrelsen lämnade till kommunrevisionen i samband med granskningen?	Ja. Vidtagna åtgärder är i linje med de svar som kommunstyrelsen lämnade till kommunrevisionen i samband med granskningen. Dock bedöms vissa rekommendationer ha delvis åtgärdats, samt ett utvecklingsarbete pågår vid granskningens genomförande.
Har åtgärder vidtagits med anledning av tidigare incidenter, så som till exempel Miljödata?	Ja. Miljödata har inte upptäckt att information från Haninge kommun har läckt, men kommunen har vidtagit flera åtgärder. Detta inkluderar att kommunen har stängt kopplingen till Miljödatas olika system, gjort anmälningar till IMY och MCF. Kommunen deltar även i flera forum i lärosyfte.
Har åtgärderna följts upp och återrapporterats till kommunstyrelsen?	Delvis. Arbetet med informationssäkerhet följs till viss del upp inom ramen för kommunstyrelsens verksamhetsuppföljning (delårsrapporter, årsredovisning, sammanträden, samt internkontroll). Av protokollgranskningen framgår inte om återrapportering av uppföljningen av åtgärderna kopplade till granskningarna har skett till kommunstyrelsen.

Haninge den 21 januari 2026

Madeleine Gustafsson
EY

Bianca Cattermole
EY

Bilaga 1 – Källförteckning

Intervjuade funktioner

- Utvecklingsdirektör, utvecklingsavdelningen, kommunstyrelseförvaltningen
- IT-chef, IT-enheten, utvecklingsavdelningen, kommunstyrelseförvaltningen

Dokumentation

- Revisionsrapport – Granskning av kommunens cybersäkerhet
- Missiv – Granskning av kommunens cybersäkerhet
- Revisionsrapport – Granskning av kommunstyrelsens rutiner för säkerhet i IT-infrastruktur
- Kommunstyrelsens svar till den uppföljande granskningen 2025
- Kommunstyrelsens årsredovisningar 2022–2024
- Kommunstyrelsens delårsrapporter 2025
- Reviderad kommunstyrelsens nämnd- och verksamhetsplan med budget 2025
- Kommunstyrelsens uppföljning av internkontroll 2022–2024
- Protokoll från kommunstyrelsens sammanträden 2022–2025
- Rutin för informationssäkerhet
- Haninge kommuns IT-handbok – Anvisningar om hur du hanterar din IT- och telefoniutrustning

Bilaga 2 – Rekommendationer i granskning av kommunens cybersäkerhetsarbete

Nedan presenteras rekommendationerna som de är återgivna i revisionsskrivelsen:

1. En samordnare rekryteras inom informationssäkerhetsområdet för att säkerställa att informationssäkerhetsfunktionen är tillräckligt bemannad med kompetent personal.
2. Direktivet för informationssäkerhet färdigställs och beslutas.
3. Riktlinjer för informationssäkerhet som kompletterar direktivet för informationssäkerhet upprättas och beslutas.
4. En riktlinje för hantering av informationssäkerhetsincidenter upprättas och beslutas för att formalisera arbetsmetoder.
5. En ändamålsenlig kontinuitetsplan finns på plats för samtliga kommunens verksamheter, samt att dessa förblir riktiga och aktuella över tid.
6. En utbildningsplan för cybersäkerhet upprättas och beslutas.
7. En formaliserad internkontrollplan upprättas, beslutas och implementeras för att granska och säkerställa att policy och riktlinjer avseende cybersäkerhet efterlevs i praktiken.
8. Formaliserade rapporteringskrav kring cybersäkerhet upprättas, beslutas och implementeras för att säkerställa kontinuerlig rapportering till kommunstyrelsen avseende hur cybersäkerhetsarbetet fortlöper.
9. En kommunikationsplan upprättas, beslutas och implementeras som innebär att anställda aktivt nås av policy och riktlinjer avseende cybersäkerhet.