Revisionsrapport 2025
Genomförd på uppdrag av
de förtroendevalda revisorerna
Februari 2026

Strömstads kommun

Uppföljande granskning av 2022 års fördjupade granskning

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

Building a better working world

Sammanfattning

Syftet med den uppföljande granskningen är att följa upp hur kommunstyrelsen har hanterat de rekommendationer som lämnades i den fördjupade granskningen avseende IT- och informationssäkerhet 2022. Särskilt fokus har legat på utvecklingen av styrdokument, genomförda utbildningsinsatser, rapporteringsvägar för incidenter samt uppföljning av vidtagna åtgärder. Underlaget utgörs av dokumentstudier, skriftliga frågor och intervjuer med berörd personal.

Vår övergripande bedömning är att Strömstads kommun fortfarande har brister i sitt informationssäkerhetsarbete som kan medföra betydande risker. Det har delvis tagits initiativ inom vissa rekommendationer, men arbetet domineras av pågående insatser snarare än avslutade. Vissa styrdokument har tagits fram och ansvarsfördelningen klargjorts, men dokumenten är ännu inte beslutade eller implementerade.

Vidare är arbetet med informationsklassning pågående, men flera system har fortfarande inte klassats. Resurser för informationssäkerhetsarbetet är inte fullt ut tydliggjorda. Det saknas också en formell funktion för informationssäkerhetsansvarig inom respektive nämnd.

Utbildningsinsatserna är digitala och omfattar samtliga medarbetare. Däremot saknas en långsiktig, formellt beslutad utbildningsplan. Det finns i dagsläget endast riktade utbildningar för dataskyddsombud. Övriga riskgrupper omfattas inte av riktade utbildningsinsatser och det sker ingen systematisk uppföljning av deltagande. Rutiner för upphandling har utvecklats, men en gemensam process för uppföljning av leverantörsavtal och efterlevnad av säkerhetskrav saknas. Incidenthanteringen bygger på grundläggande rutiner. Däremot saknas en sammanhållen process för uppföljning och analys av IT-incidenter. Avsaknaden av dessa processer ökar risken för att säkerhetsbrister förblir oupptäckta eller inte åtgärdas i tid.

Sammantaget har Strömstads kommun påbörjat arbete inom fyra av rekommendationsområdena. De bedöms vara delvis omhändertagna. Däremot bedöms områdena styrdokument, rapporteringsvägar, utbildning och incidenthantering fortfarande inte vara hanterade från ett styrningsperspektiv. Det finns alltså kvarstående betydande brister i arbetet med styrning och intern kontroll inom IT- och informationssäkerhet. Det kan medföra brott mot den nya cybersäkerhetslagen och i förlängningen en ökad sårbarhet och risk för till exempel dataintrång och avbrott i verksamheten. För att uppnå en fungerande styrning och ett robust informationssäkerhetsarbete behöver kommunstyrelsen nu genomföra, implementera och följa upp påbörjade åtgärder.

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

Innehållsförteckning

Sammanfattning....2
1. Inledning....4
1.1 Bakgrund....4
1.2 Syfte och revisionsfrågor....4
1.3 Metod....4
1.4 Avgränsningar....5
1.5 Revisionskriterier....5
1.6 Rekommendationer från granskningen 2022....5
2. Uppföljning av vidtagna åtgärder....6
2.1 Rekommendation 1: Färdigställ och implementera styrdokument för IT- och informationssäkerhet....6
2.2 Rekommendation 2: Genomför informationsklassning av verksamhetskritiska system....7
2.3 Rekommendation 3: Säkerställ resurser för informationssäkerhetsfunktionen....7
2.4 Rekommendation 4: Tydliggör ansvar och rutiner för kontinuitetsplanering....8
2.5 Rekommendation 5: Ta fram handlingsplan och rapporteringsvägar för informationssäkerhet....8
2.6 Rekommendation 6: Utveckla och förankra en utbildningsplan för informationssäkerhet....9
2.7 Rekommendation 7: Upprätta rutiner för informationssäkerhet vid upphandling och avtal....9
2.8 Rekommendation 8: Utforma en process för hantering och uppföljning av incidenter....9
3. Bedömning avseende åtgärdade rekommendationer....10
4. Slutsats....12
Bilaga 1: Källförteckning....14
Bilaga 2: Ordlista....15

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

1. Inledning

1.1 Bakgrund

På uppdrag av de förtroendevalda revisorerna genomförde EY år 2022 en granskning av kommunstyrelsen arbete med IT- och informationssäkerhet. Granskningen syftade till att bedöma om styrningen och arbetet med IT- och informationssäkerhet bedrevs på ett ändamålsenligt sätt samt om den interna kontrollen var tillräcklig inom området.
Den samlade bedömningen var att kommunstyrelsen inte helt hade säkerställt att arbetet med IT- och informationssäkerhet bedrevs på ett ändamålsenligt sätt. Kommunstyrelsen ansågs dessutom inte ha etablerat en tillräcklig intern kontroll inom området. Kommunstyrelsen rekommenderades därmed utföra en rad åtgärder, vilka låg till grund för det fortsatta förbättringsarbetet inom organisationen.

Cybersäkerhetslagen, som omfattar bland annat kommuner, trädde i kraft den 15 januari 2026. Med det blev kraven på ett strukturerat och systematiskt informationssäkerhetsarbete ännu mer betydelsefulla. Lagen ställer krav på bland annat skydd av IT-system, incidentrapportering samt ett riskbaserat och dokumenterat cybersäkerhetsarbete. Det understryker vikten av att kommunstyrelsen har tydliga rutiner och en god intern kontroll inom området.

1.2 Syfte och revisionsfrågor

Syftet med den uppföljande granskningen är att följa upp hur kommunstyrelsen har hanterat de rekommendationer som lämnades i den fördjupade granskningen avseende IT- och informationssäkerhet 2022.

Granskningen har utgått från följande revisionsfråga:

- Har kommunstyrelsen vidtagit tillräckliga åtgärder utifrån de rekommendationer som lämnades i den fördjupade granskningen av IT- och informationssäkerhet?

1.3 Metod

Granskningen genomförs genom dokumentstudier samt skriftliga frågor med grund i de rekommendationer som lämnades i den fördjupade granskningen 2022. Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor. Ramverket omfattar flera områden vilka täcker in de domäner som är väsentliga utifrån ett internkontrollperspektiv för att bedöma eventuella avvikelser och risker kopplat till brister i IT- och informationssäkerhet. Information kring områdena insamlas både genom granskning av relevanta dokument och intervju med berörd tjänstepersonal.

Källförteckning återfinns i bilaga 1. Samtliga intervjuade har getts möjlighet att sakfelskontrollera rapporten.

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

1.4 Avgränsningar

Granskningen avgränsas i enlighet med den ställda revisionsfrågan. Vidare har uppföljningen genomförts genom skriftliga frågor och svar, intervjuer med berörda personer samt granskning av insamlad dokumentation. Granskningen har inte omfattat att kontrollera implementeringen av vidtagna åtgärder.

1.5 Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser, slutsatser och bedömningar. I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen kap 6. 6 § om styrelse och nämnders ansvar.
- Myndigheten för civilt försvar (MCFs) ramverk LIS, som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.
- God praxis och EY:s erfarenhet inom IT-, cyber- och informationssäkerhet i offentlig sektor.

Sammanfattning av tidigare granskning från 2022

Granskningen från 2022 fokuserade på Strömstads kommuns arbete med IT- och informationssäkerhet, särskilt hur styrdokument och rutiner fungerade i praktiken och i vilken utsträckning de efterlevdes.

Vid granskningen som genomfördes 2022 noterades att styrdokument och processer saknades eller var otillräckliga. Informationsklassning av verksamhetens system hade inte genomförts på ett strukturerat eller formaliserat sätt och resurser för detta arbete saknades. Utbildningsinsatser hade påbörjats, men det fanns ingen långsiktig utbildningsplan och det fanns ingen utbildning inom driftorganisationen. Medarbetarnas kunskapsnivåer och medvetenhet kring informationssäkerhet varierade, vilket ökade risken för bristande efterlevnad av rutiner. Vidare konstaterades att incidenthanteringsprocessen inte var tillräckligt formaliserad och att incidenter riskerade att inte upptäckas eller hanteras i tid. Ansvarsfördelningen kring kontinuitetsplanering var otydlig och uppföljning av leverantörsavtal och servicenivåavtal brast.

1.6 Rekommendationer från granskningen 2022

Baserat på informationen ovan lämnades följande rekommendationer till kommunstyrelsen år 2022:

- Färdigställa och implementera de styrdokument avseende IT- och informationssäkerhet som ej är ändamålsenliga, och att upprätta de styrdokument som saknas vid tidpunkten för granskning.
- Färdigställa genomförandet av informationsklassning för kommunens verksamhetskritiska informationssystem, och upprätta de styrdokument som saknas vid tidpunkten för genomförandet av informationsklassningar..

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

- Allokera medel och resurser till informationssäkerhetsfunktionen, och se över möjligheten att stötta upp informationssäkerhetsfunktionen exempelvis genom att formellt utse en informationssäkerhetsansvarig inom respektive nämnd.
- Upprätta formella styrdokument som beskriver ansvaret för kontinuitetsplanering, och följa upp arbetet med kontinuitetsplanering och avstämning mot systemsäkerhetsplanen i enlighet med framtagna riktlinjer.
- Färdigställa en heltäckande handlingsplan för kommunens informationssäkerhetsområden, och tydliggöra rapporteringsvägar till kommunstyrelsen. Detta för att kommunstyrelsen ska ha god insyn i kommunens IT och informationssäkerhetsarbete och säkerställa att eventuella brister upptäcks och åtgärdas.
- Utforma och förankra en långsiktig utbildningsplan för informationssäkerhet och interna styrdokument, och tillse att anställda genomgår utbildning inom informationssäkerhet och interna styrdokument enligt denna plan.
- Upprätta formella rutiner och detaljera ansvar kopplat till informationssäkerhetskrav vid upphandling och uppföljning av leverantörsavtal. Detta för att säkerställa att nya och befintliga avtal med leverantörer av informationsbehandlingstjänster på ett ändamålsenligt sätt säkerställer att kommunens krav på informationsbehandling av leverantörer efterlevs.
- Utforma en process för hantering och uppföljning av informationssäkerhetsincidenter och kommunicera denna till berörda parter i verksamheten.

2. Uppföljning av vidtagna åtgärder

I avsnitten nedan redogörs för hur respektive rekommendation som lämnades 2022 hanterats.

2.1 Rekommendation 1: Färdigställ och implementera styrdokument för IT- och informationssäkerhet

Sedan granskningen från 2022 har kommunen enligt skriftliga svar tagit fram dokumenten *Regler för informationssäkerhet* och *Riktlinje för systemförvaltning*. Dessa dokument har dock inte beslutats än eller fått någon plan för implementering. Enligt *Riktlinje för systemförvaltning* framgår att systemförvaltaren ansvarar för behörighetsadministration, men någon detaljerad processbeskrivning för behörighetshantering finns inte dokumenterad. Vid genomgång av skriftliga svar, uppföljande frågor och dokumentet *Cybersäkerhetslagen_vad behöver vi göra Q4 2025,* noteras att det saknas en formaliserad och dokumenterad process för incidenthantering.

Vidare uppgavs i den tidigare granskningen från 2022 att riktlinjer så som kommunövergripande rutiner för kontinuitetsplanering, granskning och uppföljning av leverantörsavtal, hantering av programförändringar samt ett formellt ledningssystem för informationssäkerhet saknades. Dokumentet *Riktlinje för systemförvaltning*, beskriver

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

ansvarsfördelning, krav på dokumentation och nämner att dessa områden ska omfattas. I intervju uppges även att de arbetar enligt MCF:s (Myndigheten för Civilt Försvar) metodstöd för LIS (Ledningssystem för informationssäkerhet).

Enligt de intervjuade har en beredningsgrupp under det senaste året granskat beslutsnivåer och styrdokument, och resultatet av denna översyn har antagits under hösten 2025. Enligt skriftligt svar publiceras de nya styrdokumenten på intranätet, och den närmaste chefen ansvarar för att informera nya medarbetare samt följa upp vid arbetsplatsträffar. Uppföljning avseende styrdokumenten sker genom diarieförda ärenden. Ett exempel på publicering om informationsklassning har granskats och dokumentet beskriver syfte, kriterier, process och ansvarsfördelning.

2.2 Rekommendation 2: Genomför informationsklassning av verksamhetskritiska system

Enligt skriftligt svar från Strömstads kommun har informationsklassning genomförts för verksamhetskritiska IT-system. En förteckning över klassificerade system har tillhandahållits, där det framgår att klassning av system och informationsmängder görs i SKR:s (Sveriges kommuner och regioner) verktyg KLASSA. Förteckningen visar att klassning har genomförts för förvaltningar och system.

Sedan den tidigare granskningen 2022 har kommunen tagit fram en instruktion för informationsklassning på intranätet. Denna beskriver syfte, vilka informationsmängder som ska klassas samt att klassningen ska baseras på konfidentialitet, riktighet och tillgänglighet. Enligt de intervjuade använder de sig av Sveriges Kommuner och Regioners (SKR) verktyg KLASSA för att genomföra informationsklassningen. Flera system är dock fortfarande inte klassade. Enligt uppgift har alla verksamhetschefer fått i uppdrag att lista sina system och bedöma kritikalitet, men arbetet är ännu inte fullföljt.

Vidare hänvisar kommunen till styrdokumenten *Informationssäkerhetspolicy* och *Informationssäkerhetsinstruktion – Användare Strömstads kommun* som grund för informationsklassning. Dessa principer och krav var redan etablerade vid granskningen 2022 och har inte förändrats sedan dess.

Enligt skriftligt svar finns ingen skillnad i rutiner för klassning av befintliga system jämfört med nya system vid upphandling. Uppföljning och revidering sker genom diarieförda ärenden som tidsätts för aktualisering och notifieras till ansvarig.

2.3 Rekommendation 3: Säkerställ resurser för informationssäkerhetsfunktionen

Enligt skriftligt svar från Strömstads kommun ingår medel och resurser för informationssäkerhetsfunktionen i budgeten för avdelningen för kansli och kommunikation, samt IT-enheten. Kommunen uppger att det finns en

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

informationssäkerhetssamordnaremen att det inte finns någon specifik budgetpost för informationssäkerhetsarbetet.

2.4 Rekommendation 4: Tydliggör ansvar och rutiner för kontinuitetsplanering

Strömstads kommun har tagit fram dokumentet *Riktlinje för systemförvaltning* som beskriver att varje verksamhetssystem ska ha en utsedd systemägare och systemförvaltare samt att dokumentation och rutiner ska finnas för bland annat kontinuitetsplaner, informationsklassning och hantering av driftstörningar. Dokumentet är dock ännu inte beslutat eller färdigställt. Syftet är att säkerställa tillgång till information och skapa förutsättningar för ett proaktivt och säkert IT-stöd. Systemägaren ska även säkerställa att kontinuitetsplaner upprättas och att personalen har den utbildning som krävs för att använda systemet effektivt och säkert.

Under intervjun uppges att några av kommunens medarbetare har genomgått processledarutbildning enligt MCF:s metodstöd för kontinuitetsplanering och att denna grupp planerar att arrangera workshops i samhällsviktiga verksamheter, där IT ingår.

2.5 Rekommendation 5: Ta fram handlingsplan och rapporteringsvägar för informationssäkerhet

Vad gäller rapporteringsvägar är dessa angivna och beskrivna i dokumentet *Informationssäkerhetspolicy*, dessa är oförändrade sedan den tidigare granskningen från 2022. Enligt skriftligt svar har IT-avdelningen påbörjat arbetet med dokumentet *Security Roadmap*, som enligt uppgift ska innehålla planerade aktiviteter och en tidplan fram till 2027. Dokumentet är inte färdigställt och har inte tillhandahållits av EY. Sedan 2023 har informationssäkerhetsarbetet haft fokus på den kommande cybersäkerhetslagen. Säkerhetsåtgärderna i lagförslaget har brutits ned till en checklista som löpande uppdateras och har kommunicerats till kommundirektör och förvaltningschef.

I skriftligt svar uppges även att rapportering och uppföljning av informationssäkerhetsarbetet sker i ledningens genomgång till kommunstyrelsen, kommundirektörens ledningsgrupp, förvaltningschefer och berörda enhetschefer två gånger per år. Vidare skriver de att de årligen genomför cybersäkerhetskollen.

Inför den kommande cybersäkerhetslagen, som beräknas träda i kraft den 15 januari 2026, har Strömstads kommun identifierat ett antal åtgärder i dokumentet *Cybersäkerhetslagen_vad behöver vi göra Q4 2025*. Dokumentet beskriver att verksamheterna har ansvar för att aktualisera sina systemlistor och definiera kritiska verksamhetssystem. För system som saknar informationsklassning, risk- och sårbarhetsanalys eller kontinuitetsplan ska en plan tas fram, med särskild prioritet för kritiska verksamhetssystem.

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

2.6 Rekommendation 6: Utveckla och förankra en utbildningsplan för informationssäkerhet

Enligt skriftligt svar innehåller dokumentet *Security Roadmap* en utbildningsplan för IT-personal. Vi har endast fått information om dokumentet via intervju och skriftliga svar, men inte fått ta del av det och kan därför inte bekräfta ett en utbildningsplan inom informationssäkerhet är upprättad och förankrad enligt den rekommendation som lämnades i granskningen 2022.

Vid intervju med personal på Strömstads kommun framkom att utbildningsplattformen Nimblr används för utbildning inom IT- och cybersäkerhet för samtliga medarbetare. Detta arbete har pågått i tre år. Det finns dock inte specifika utbildningar för IT-personal. Det finns enligt de intervjuade beslut om att alla arbetstagare, förtroendevalda och uppdragstagare ska genomgå kommunens informationssäkerhetsutbildning, som genomförs via mejl med utskick var fjortonde dag. De berättar även att kontaktombud löpande får riktad utbildning inom sitt ansvarsområde under året, vilket ingår i Dataskyddsombudets uppdrag.

Statistik över deltagande finns tillgänglig i Nimblr och kan enligt intervjuade tas fram manuellt. Sådan statistik har enligt de intervjuade tagits fram och rapporterats till kommundirektörens ledningsgrupp. I dagsläget sker dock ingen systematisk uppföljning av deltagande och utbildningarnas effekt, vilket var en av de rekommendationer som lämnades 2022.

2.7 Rekommendation 7: Upprätta rutiner för informationssäkerhet vid upphandling och avtal

Sedan granskningen 2022 har dokumentet *förstudieprocess* införts, vilket vi har tagit del av. Det beskriver informationssäkerheten och omfattar inventering av information, risk- och sårbarhetsanalys, informationsklassning, konsekvensbedömning samt hantering av personuppgiftsbiträdesavtal. Processen används vid upphandling av nya IT-system, applikationer eller större digitala förändringar. I dagsläget sker ingen uppföljning av efterlevnaden och det saknas en gemensam rutin för uppföljning av leverantörsavtal.

Förstudieprocessen är uppdelad i tre delar: behovsanalys, informationsanalys och kravanalys. Informationsanalysen omfattar inventering av information och definiering av säkerhetskrav inför upphandling. Syftet är att säkerställa att upphandlingar uppfyller krav på informations- och IT-säkerhet.

2.8 Rekommendation 8: Utforma en process för hantering och uppföljning av incidenter

Enligt skriftligt svar rapporteras IT- och informationssäkerhetsincidenter i IT:s ärendehanteringssystem som beskrivet i dokumentet *Informationssäkerhetsinstruktion – Användare Strömstads kommun,* och följer samma som process som beskrivs i

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

granskningen 2022. Ingen fastställd process för uppföljning och analys av incidenter finns i dagsläget. Vidare uppges att arbetet med en mer omfattande incidenthanteringsprocess och kontinuitetsplanering för IT-drift har påbörjats. Kommunen har tecknat avtal med en extern aktör för incidenthantering med målet att minimera konsekvenser, identifiera rotorsaker, åtgärda säkerhetsbrister och återställa normal drift.

I granskningen 2022 framkom att *Informationssäkerhetspolicyn* anger att uppföljning ska ske regelbundet och vid behov, vilket fortfarande gäller.

I dokumentet *Cybersäkerhetslagen – vad behöver vi göra Q4 2025* framgår att kommunledningsförvaltningen ansvarar för att en process för incidenthantering ska finnas.

3. Bedömning avseende åtgärdade rekommendationer

Strömstads kommun har vidtagit åtgärder inom flera rekommendationsområden från granskningen 2022, men arbetet anses inte vara färdigställt för att uppnå en robust och långsiktig styrning.

Styrdokument har till viss del utvecklats och ansvarsfördelning klargjorts, men implementeringen är ännu inte genomförd. Det innebär att styrningen fortfarande är teoretisk och inte tillämpas i praktiken. Arbetet med informationsklassning pågår, men omfattar fortfarande inte alla relevanta system. Arbetet behöver fortsätta arbetas med och följas upp mer systematiskt för att se till att känslig information hanteras korrekt och att risker mitigeras. Vidare finns en samordningsfunktion och resurser har avsatts, men eftersom finansieringen saknar en egen budgetpost finns det ingen garanti för att arbetet kan drivas kontinuerligt och prioriteras över tid.

Vidare saknas en beslutad utbildningsplan, riktade insatser för riskgrupper och systematisk uppföljning. Utan plan, riktning och kontroll riskerar kommunen att inte kunna säkerställa att utbildningen ger effekt, vilket ökar risken för brister i informationssäkerheten.

Rutinerna vid upphandling har stärkts, men det saknas en gemensam process för att följa upp leverantörers efterlevnad av säkerhetskrav. Detta gör att kommunen riskerar att inte fullt ut kunna kontrollera att avtalade säkerhetsnivåer hålls, vilket ökar risken för sårbarheter.

Sedan den tidigare granskningen har kommunen inlett ett arbete avseende incidenthantering med tredje part. Grundläggande rutiner för incidenthantering och en sammanhållen process för analys och uppföljning saknas dock fortsatt. Detta innebär att lärdomar från inträffade incidenter inte tas tillvara, vilket försvårar ett proaktivt arbete och ökar risken för upprepade incidenter.

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

Tabell 1: Uppföljande granskning

Rekommendation till Strömstads kommun	Bedömning
► Färdigställa och implementera de styrdokument avseende IT- och informationssäkerhet som ej är ändamålsenliga, och att upprätta de styrdokument som saknas vid tidpunkten för granskning.	
► Färdigställa genomförandet av informationsklassning för kommunens verksamhetskritiska informationssystem, och upprätta de styrdokument som saknas vid tidpunkten för genomförandet av informationsklassningar.	
► Allokera medel och resurser till informationssäkerhetsfunktionen, och se över möjligheten att stötta upp informationssäkerhetsfunktionen.	
► Upprätta formella styrdokument som beskriver ansvaret för kontinuitetsplanering, och följa upp arbetet med kontinuitetsplanering och avstämning mot systemsäkerhetsplanen i enlighet med framtagna riktlinjer.	
► Färdigställa en heltäckande handlingsplan för kommunens informationssäkerhetsområden, och tydliggöra rapporteringsvägar till kommunstyrelsen.	
► Utforma och förankra en långsiktig utbildningsplan för informationssäkerhet och interna styrdokument, och tillse att anställda genomgår utbildning inom informationssäkerhet och interna styrdokument enligt denna plan.	
► Upprätta formella rutiner och detaljera ansvar kopplat till informationssäkerhetskrav vid upphandling och uppföljning av leverantörsavtal.	
► Utforma en process för hantering och uppföljning av informationssäkerhetsincidenter och kommunicera denna till berörda parter i verksamheten.	

	Rekommendationen har omhändertagits i sin helhet
	Rekommendationen har delvis omhändertagits
	Rekommendationen har inte omhändertagits

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

4. Slutsats

Den uppföljande granskningen visar att Strömstads kommun inte har vidtagit tillräckliga åtgärder utifrån de rekommendationer som lämnades i den fördjupade granskningen av IT- och informationssäkerhet 2022. Kommunen har tagit initiativ för att stärka IT- och informationssäkerhetsarbetet, och flera utvecklingsinsatser pågår. Samtidigt visar granskningen att arbetet fortfarande till stor del består av pågående processer snarare än fullföljda åtgärder.

Flera områden är fortfarande inte fullt implementerade, saknar systematisk uppföljning eller formella beslut. Det finns en ambition att förbättra styrning, ansvarsfördelning, rapporteringsvägar och utbildning, men grunden för ett långsiktigt arbete är ännu inte helt på plats. I ljuset av de skärpta krav som den nya cybersäkerhetslagen innebär blir det särskilt viktigt att kommunen fortsätter att utveckla och stärka sitt informationssäkerhetsarbete.

Granskningen indikerar att det fortsatt krävs ett strategiskt fokus på att slutföra och förankra styrdokument, säkerställa resurser och roller, samt utveckla rutiner för uppföljning och analys. Först när dessa grundläggande delar är på plats kan kommunens informationssäkerhetsarbete bedömas som tillräckligt och hållbart över tid.

Följande fyra rekommendationer bedöms delvis kvarstå:

- Färdigställa genomförandet av informationsklassning för kommunens verksamhetskritiska informationssystem, och upprätta de styrdokument som saknas vid tidpunkten för genomförandet av informationsklassningar.
- Upprätta formella styrdokument som beskriver ansvaret för kontinuitetsplanering, och följa upp arbetet med kontinuitetsplanering och avstämning mot systemsäkerhetsplanen i enlighet med framtagna riktlinjer.
- Allokera medel och resurser till informationssäkerhetsfunktionen, och se över möjligheten att stötta upp informationssäkerhetsfunktionen exempelvis genom att formellt utse en informationssäkerhetsansvarig inom respektive nämnd.
- Upprätta formella rutiner och detaljera ansvar kopplat till informationssäkerhetskrav vid upphandling och uppföljning av leverantörsavtal. Detta för att säkerställa att nya och befintliga avtal med leverantörer av informationsbehandlingstjänster på ett ändamålsenligt sätt säkerställer att kommunens krav på informationsbehandling av leverantörer efterlevs.

Följande fyra rekommendationer bedöms som inte omhändertagna:

- Färdigställa och implementera de styrdokument avseende IT- och informationssäkerhet som ej är ändamålsenliga, och att upprätta de styrdokument som saknas vid tidpunkten för granskning.
- Färdigställa en heltäckande handlingsplan för kommunens informationssäkerhetsområden, och tydliggöra rapporteringsvägar till kommunstyrelsen. Detta för att kommunstyrelsen ska ha god insyn i kommunens IT

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

och informationssäkerhetsarbete och säkerställa att eventuella brister upptäcks och åtgärdas.

- Utforma och förankra en långsiktig utbildningsplan för informationssäkerhet och interna styrdokument, och tillse att anställda genomgår utbildning inom informationssäkerhet och interna styrdokument enligt denna plan.
- Utforma en process för hantering och uppföljning av informationssäkerhetsincidenter och kommunicera denna till berörda parter i verksamheten.

Stockholm den 22 januari 2026

_____

David Asplund, Partner, EY

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

Bilaga 1: Källförteckning

Intervjuade roller:

- Informationssäkerhetssamordnare & utvecklingsstrateg, 2025-11-21.
- IT-driftchef, 2025-11-21.
- Kommunikationschef, 2025-11-21.

Dokumentation:

- Cybersäkerhetslagen_vad behöver vi göra Q4 2025
- Förstudieprocess
- Informationsklassning Info på intranät
- Informationsklassningar
- Informationssäkerhetsinstruktion - Användare Strömstads kommun
- Informationssäkerhetspolicy
- Riktlinje för systemförvaltning 251121
- Riktlinjer för Strömstads kommuns styrdokument
- Svar på intervjufrågorna som ställts i denna granskning

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY

Bilaga 2: Ordlista

- Servicenivåavtal: Ett avtal som reglerar vilken servicenivå en leverantör ska hålla.
- KLASSA: Ett verktyg från SKR för att klassificera information och system utifrån hur känsliga de är.
- Informationsklassning: En process för att bedöma hur känslig information är och hur den ska skyddas.
- Applikation: Ett datorprogram eller en mjukvara som används för att utföra specifika uppgifter, till exempel e-post eller bokningssystem.

Penneo dokumentnyckel: 1EY55-STCVX-W45Y3-JLC6D-OKA7J-QO3PY