Uppföljande granskning av informations- och IT-säkerhet

Rapport

Skövde kommun

2026-02-10

Antal sidor 31

1 INNEHÅLLSFÖRTECKNING

1 SAMMANFATTNING

Azets Revision & Rådgivning har av Skövde kommuns revisorer fått i uppdrag att följa upp en tidigare genomförd granskning av informations- och it-säkerhet från år 2023.

Syftet med granskningen har varit att bedöma om kommunstyrelsen, barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden beaktat och hörsammat de mest väsentliga rekommendationerna från den föregående granskningen.

Vår samlade bedömning utifrån granskningens syfte är att barn- och utbildningsnämnden i allt väsentligt vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer, att servicenämnden endast delvis vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer, men att kommunstyrelsen, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden och bygglovsnämnden inte vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer

Granskningen har visat att kommunstyrelsen, i egenskap av övergripande ansvarig för informationssäkerheten, vidtagit ett antal åtgärder i syfte att strukturera upp och lägga grund för en organisation som möjliggör ett systematiskt informationssäkerhetsarbete i hela kommunorganisationen. Ingen av de påbörjade processerna har dock implementerats i full skala av styrelsen eller något revisionsobjekt. Bedömningen är därvid att informationssäkerhetsarbetet, inte i någon mening, kan betraktas som systematiserat. Därvid kvarstår de flesta rekommendationer från föregående granskning.

En viktig iakttagelse från den tidigare granskningen var att kommunens styrdokument var föråldrade och icke ändamålsenliga. Nya styrdokument har ännu inte fastställts, vilket motiveras med att kommunen inväntat NIS2-direktivet. Det är givetvis centralt att informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning. Flera av de granskade nämnderna hänvisar emellertid till implementeringen av de uppdaterade styrdokumenten som en förutsättning för att kunna påbörja systematisering av det verksamhetsnära informationssäkerhetsarbetet. Vi anser därvid att kommunstyrelsen hade behövt formalisera den interna styrningen tidigare. Samt att det är nödvändigt att fastställande av styrdokumenten prioriteras och att pågående utvecklingsarbete fortlöper.

Bland övriga granskade nämnder bedöms endast barn- och utbildningsnämnden ha hörsammat de rekommendationer som nämnden kunnat påverka i tillräcklig omfattning.

I det följande redovisas vår bedömning av vilka rekommendationer som hörsammats av respektive revisionsobjekt.

Följande rekommendationer kvarstår helt eller delvis till kommunstyrelsen (utifrån dess övergripande samordningsansvar):

- Verka för att en informationssäkerhetspolicy upprättas av kommunfullmäktige och i samband med detta aktualisera tillhörande riktlinjer som konkretiserar policyn.
- Säkerställa att informationssäkerhetsrisker beaktas i en kommunövergripande riskanalys.
- Säkerställa att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning och klassning av kommunens informationstillgångar genomförs.
- Säkerställa att incidentrutiner upprättas med tydliggjorda eskaleringsvägar samt att inträffade incidenter dokumenteras och analyseras på en kommunövergripande nivå.
- Säkerställa att former för uppföljning av informationssäkerhetsarbete upprättas.
- Säkerställa att styrelsen erhåller tillräcklig återrapportering i syfte att kunna besluta om mål- och handlingsplan.

Följande rekommendationer kvarstår helt eller delvis till kommunstyrelsen (utifrån dess verksamhetsansvar):

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Följande rekommendationer kvarstår helt eller delvis till vård- och omsorgsnämnden och socialnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Följande rekommendation kvarstår helt eller delvis till barn- och utbildningsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

Följande rekommendationer kvarstår helt eller delvis till kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

2 BAKGRUND

Azets Revision & Rådgivning har av Skövde kommuns revisorer fått i uppdrag att följa upp tidigare genomförd granskning av IT-säkerhet från år 2023. Uppdraget ingår i revisionsplanen för år 2025.

Revisorerna genomförde under år 2023 en fördjupad granskning av kommunens arbete med informations- och IT-säkerhet. Granskningens bedömning var att kommunstyrelsen och nämnderna inte bedrev ett systematiskt och ändamålsenligt informations- och IT-säkerhetsarbete.

Enligt granskningen saknades flera delar som är fundamentala i ett systematiskt informationssäkerhetsarbete, till exempel aktuella styrdokument, tillräckliga riskhanteringsprocesser och uppföljning av arbetet.

Utifrån genomförd granskning och de brister som uppdagades ser revisorerna i sin riskanalys behov av att följa upp den tidigare granskningen. Detta i syfte att granska huruvida kommunstyrelsen och granskade nämnder beaktat granskningens resultat och mest väsentliga rekommendationer.

3 SYFTE, REVISIONSFRÅGOR OCH AVGRÄNSNING

Syftet med granskningen har varit att följa upp om kommunstyrelsen, barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden beaktat och hörsammat de mest väsentliga rekommendationerna från granskningen av informations- och IT-säkerhet från 2023.

Granskningen har avsett att besvara följande revisionsfråga:

- Har tillräckliga åtgärder vidtagits mot bakgrund av lämnade rekommendationer?

För att besvara revisionsfrågan har följande rekommendationer från den tidigare granskningen följts upp.

Rekommendationer till kommunstyrelsen utifrån dess övergripande samordningsansvar:

- Verka för att en informationssäkerhetspolicy upprättas av kommunfullmäktige och i samband med detta aktualisera tillhörande riktlinjer som konkretiserar policyn.
- Säkerställa att informationssäkerhetsrisker beaktas i en kommunövergripande riskanalys.

- Säkerställa att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning och klassning av kommunens informationstillgångar genomförs.
- Säkerställa att incidentrutiner upprättas med tydliggjorda eskaleringsvägar samt att inträffade incidenter dokumenteras och analyseras på en kommunövergripande nivå.
- Säkerställa att former för uppföljning av informationssäkerhetsarbete upprättas.
- Säkerställa att styrelsen erhåller tillräcklig återrapportering i syfte att kunna besluta om mål- och handlingsplan.

Rekommendationer till kommunstyrelsen (utifrån dess verksamhetsansvar), barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

3.1 AVGRÄNSNING

Uppföljningen avser avlämnad revisionsrapport för granskning av informations- och IT-säkerhet från 2023.

4 REVISIONSKRITERIER

Utifrån den tidigare genomförda granskningen har vi efterfrågat svar på vilka åtgärder som vidtagits med anledning av granskningen. Vidare har vi begärt att få ta del av revisionsbevis i form av styrdokument, planer och rutiner för att verifiera uppgifter.

5 METOD

Granskningen har genomförts genom:

- Dokumentstudier av relevanta revisionsbevis.

- Intervjuer har genomförts med följande funktioner:
  Kommunledningsstab: säkerhets- och beredskapscef.
  Sektor vård och omsorg: stabschef, informations- och GDPR-samordnare, strategisk systemsamordnare.
  Sektor socialtjänst: stabschef, systemförvaltare.
  Sektor barn och utbildning: stabschef, administrativ chef.
  Sektor service: sektorchef.
  Sektor medborgare och samhällsutveckling: sektorchef, stabschef.
  Sektor samhällsbyggnad: enhetschef verksamhetsstöd, dataskyddssamordnare.

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

Samtliga intervjuade har getts möjlighet att faktakontrollera rapporten.

6 RESULTAT AV GRANSKNINGEN

Detta rapportkapitel framställer resultatet av den uppföljande granskningen. Kapitlet inleds med uppföljning av rekommendationer till kommunstyrelsen utifrån dess övergripande samordningsansvar och dess verksamhetsansvar. På det följer en samlad bedömning avseende vidtagna åtgärder inom kommunstyrelsen.

Därefter redovisas uppföljning av rekommendationer till barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden, samt en samlad bedömning per nämnd.

6.1 REKOMMENDATIONER TILL KOMMUNSTYRELSEN UTIFRÅN DESS ÖVERGRIPANDE SAMORDNINGSANSVAR

6.1.1 Rekommendation: Verka för att en informationssäkerhetspolicy upprättas av kommunfullmäktige och i samband med detta aktualisera tillhörande riktlinjer som konkretiserar policyn.

Bakgrund

Den tidigare granskningen visade att kommunens styrande dokument inom informationssäkerhet var daterade och ofullständiga i fråga om att ge styrning åt informationssäkerhetsarbetet. Policy för säkerhet och beredskap hade antagits av fullmäktige 2018, och även om policyn beaktade informationssäkerhet konstaterades den framför allt vara inriktad mot övergripande säkerhet och beredskap. Kommunens Riktlinje för informationssäkerhet hade inte reviderats sedan 2010 och bedömdes, liksom Policy för säkerhet och beredskap, sakna reglering av det verksamhetsbaserade ansvaret för informationssäkerhet. Därtill saknade dokumenten kravställning av moment som är centrala i ett systematiskt informationssäkerhetsarbete.

Vidare konstaterades att det fanns en handlingsplan för informationssäkerhetsarbetet för perioden 2023-2027. En av aktiviteterna som ingick i planen var att upprätta styrande dokument.

Yttrande

Av kommunstyrelsens yttrande[1] som svar på granskningen framgår att IT-avdelningen samt enheten för säkerhet- och juridik hade uppdragits att fortsätta arbetet med införande av ett ledningssystem för informationssäkerhet. Som del i det ingick att ta fram erforderliga styrdokument samt genomföra översyn och revideringar av befintliga styrdokument.

I yttrandet uppmanade kommunstyrelsen samtliga nämnder att:

- Säkerställa att aktualiserade styrdokument och rutiner implementeras och efterlevs i verksamheten.

[1] 2024-04-15

- Säkerställa att det kommungemensamma ledningssystemet för informationssäkerhet, efter att det är infört, nyttjas och följs.

Vidtagna åtgärder

Både Policy för säkerhet och beredskap och Riktlinje för informationssäkerhet var under revidering då granskningen genomfördes. Dokumenten har tillhandahållits i arbetsversion, av vilka det framgår att riktlinjen förtydligats med att arbetet ska utgå från gällande lagar samt ISO/IEC 27001. Även det verksamhetsbaserade ansvaret för informationssäkerhet har tydliggjorts.

I intervju uppges att kommunen velat invänta NIS2-direktivet för att anpassa slutversionerna av styrdokumenten till den nya lagstiftningen. Av den anledningen ska dokumenten fastställas under första halvåret 2026.

Dokumenten är i stora delar färdiga varför de redan nu används av de två centrala informationssäkerhetssamordnarna som tillsammans med den nyinstiftade funktionen ”dataskyddssamordnare” koordinerar kommunens informationssäkerhetsarbete. Det arbete som bedrivs syftar i nuläget till att skapa en verksamhetsnära struktur med lokala informationssäkerhetssamordnare för det löpande informationssäkerhetsarbetet, samt till att förbereda implementering av operativa arbetsprocesser som kravställs av riktlinjen.

6.1.1.1 Bedömning

Vår bedömning är att rekommendationen inte har hörsammats i tillräcklig omfattning.

Vi konstaterar att dokument är under framtagande och att organisatoriskt arbete pågår, vilket är en förutsättning för att på sikt systematisera informationssäkerhetsarbetet. Att detta inte gjorts med hänvisning till att kommunen inväntat NIS2-direktivet har fått som konsekvens att informationssäkerhetsområdet saknar adekvat styrning. Detta är en brist som i förlängningen försvårat för kommunens nämnder att arbeta med informationssäkerheten. Kommunstyrelsen behöver formalisera den interna styrningen oberoende av NIS2-direktivet. Vi ser det som angeläget att fastställandet av styrdokumenten prioriteras och genomförs enligt tidplan.

6.1.2 Rekommendation: Säkerställa att informationssäkerhetsrisker beaktas i en kommunövergripande riskanalys.

I den tidigare granskningen framkom att IT-beroende utifrån elektronisk kommunikation hade beaktats i den kommunövergripande risk- och sårbarhetsanalysen (RSA) för åren 2024–2027. Därvid bedömdes det finnas behov av att komplettera risk- och sårbarhetsanalysen med fler risker inom informationssäkerhet. Detta i syfte att identifiera sårbarheter som kan påverka kommunens verksamhet på ett negativt sätt.

Yttrande

Kommunstyrelsens yttrande har inget innehåll som svarar mot rekommendationen.

Vidtagna åtgärder

Enligt intervjuer tillämpas fortfarande strukturen med RSA som utgångspunkt för riskanalys av informationssäkerhetsrisker. Informationsklassningar och riskbedömningar som görs per enskilt IT-system betraktas som den kontext inom vilken djupare analys av informationssäkerhetsrisker görs i förhållande till aktuell lagstiftning. Det anses inte finnas behov av någon annan slags eller ytterligare kommunövergripande riskanalys. Att RSA fastställs av fullmäktige och även hanteras av kommunstyrelsen beskrivs i intervju som ett sätt att medvetandegöra informationssäkerhetsrisker även hos de förtroendevalda.

6.1.2.1 Bedömning

Vår bedömning är att rekommendationen inte har hörsammats i tillräcklig omfattning.

I enlighet med tidigare granskning vidhåller vi att det finns behov av att komplettera RSA med en mer specifik riskanalys avseende informationssäkerhetsrisker.

6.1.3 Rekommendation: Säkerställa att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning och klassning av kommunens informationstillgångar genomförs.

Bakgrund

Med utgångspunkt i metoder från Sveriges kommuner och regioner (SKR) och Myndigheten för samhällsskydd och beredskap (MSB) hade kommunen tagit fram en egen modell för informationsklassning, enligt den tidigare granskningen. Dock var modellen inte fullt ut implementerad i samtliga sektorer. Genomförandet av klassningar hade inte heller systematiserats utan gjordes företrädelsevis i samband med nyanskaffning av system. Därtill saknades dokumentation som visade vilka system som respektive sektor hade klassat.

Vid tid för granskning pågick införskaffande av ett verksamhetssystem med funktionalitet för att genomföra klassningar och riskbedömningar.

Yttrande

I det uppdrag som ålades IT-avdelningen samt enheten för säkerhet- och juridik ingick att ta fram ett förslag på systemstöd för att underlätta informationssäkerhetsarbetet. Vidare framgår av yttrandet att arbetet med klassningar och riskanalyser skulle fortsätta med särskild vikt på samhällsviktiga verksamheter.

Vidtagna åtgärder

Vid den uppföljande granskningen hade det nya verksamhetssystemet driftsatts och arbetssätt för att använda systemet var under utrullning. En ny klassningsmodell har tagits fram, vilken dokumenterats i en användarmanual som vi tagit del av.

Enligt intervju är klassningsarbetet ännu inte systematiserat och sektorerna har kommit olika långt i arbetet. Fokus har legat på att skapa klassningsmodellen samt att tillse ett

samordningsforum för den centrala informationssäkerhetsfunktionen och de lokala informationssäkerhetssamordnarna. Genom detta forum ska klassningsmetodiken läras ut samt stöd vid klassningar kanaliseras. Merparten av det faktiska klassningsarbetet ligger emellertid framför kommunen.

6.1.3.1 Bedömning

Vi bedömer att rekommendationen endast delvis har hörsammats i tillräcklig omfattning.

Vi ser att kommunstyrelsen har vidtagit åtgärder i enlighet med yttrandet. Genom implementering av det nya verksamhetssystemet och framtagandet av ny klassningsmodell finns förutsättningar för att systematisera klassningsarbetet. Detta behöver prioriteras då informationsklassningar är väsentliga i att säkerställa att informationstillgångar skyddas av erforderliga säkerhetsåtgärder.

6.1.4 Rekommendation: Säkerställa att incidentrutiner upprättas med tydliggjorda eskaleringsvägar samt att inträffade incidenter dokumenteras och analyseras på en kommunövergripande nivå.

Bakgrund

I föregående granskningen framkom att kommunen hade rutiner för incidenthantering, men att dessa var ofullständiga i flera avseenden. Rutinerna saknade eskaleringsvägar och angav inte heller hur incidenter skulle anmälas, analyseras eller dokumenteras för att skapa en enhetlig och sammanhållen process. Därtill konstaterades rutinerna inte vara etablerade inom hela organisationen.

Yttrande

I yttrandet angavs att incidenthanteringsprocessen skulle utvecklas. Det som en del i det uppdrag som ålades IT-avdelningen och enheten för säkerhet och juridik.

Vidtagna åtgärder

Den centrala informationssäkerhetsfunktionen har tagit fram stödjande dokumentation som utifrån ett användarperspektiv förtydligar innebörden av informationssäkerhetsincidenter och fungerar som manual vid anmälningar. Dokumentationen har tillhandahållits. I den ingår inte eskaleringsvägar eller metod för uppföljningsmetodik. Det som enligt uppgift kvarstår är att skapa motsvarande process och organisation för hantering av inträffade incidenter.

Utöver detta har en grundutbildning i personuppgiftshantering och incidentanmälningar tagits i fram som kunskapshöjande åtgärd riktad mot anställda.

6.1.4.1 Bedömning

Vår bedömning är att rekommendationen endast delvis har hörsammats i tillräcklig omfattning.

För att rekommendationen ska ses som fullt ut hörsammad behöver hela incidenthanteringsprocessen, från anmälan till incidentutredning och uppföljning, dokumenteras och göras känd. Den genomförda utbildningen bidrar till stärkt medvetenhet om informationssäkerhet, samt till att sprida kunskap om incidenter och anmälningsförfarande, vilket är positivt.

6.1.5 Rekommendation: Säkerställa att former för uppföljning av informationssäkerhetsarbete upprättas.

Bakgrund

I föregående granskning framgick att kommunens riktlinje för informationssäkerhet angav att uppföljning av informationssäkerhetsarbetet ska bevaka följande:

- att beslutade åtgärder ska vara genomförda
- att årliga mål är uppfyllda
- att instruktioner följs

Granskningen visade emellertid att uppföljning inte hade skett enligt riktlinjen, liksom att det saknades ett etablerat kommunövergripande uppföljningsarbete.

Yttrande

Kommunstyrelsens yttrande innehåller inget svar som avser uppföljning av informationssäkerhetsarbetet. Yttrandet anger däremot att en övergripande handlingsplan med åtgärder som ökar informations- och IT-säkerhet skulle tas fram.

Vidtagna åtgärder

I intervju ges bild av att systematisering av uppföljning är något som ligger framför kommunen. Enligt den struktur som beskrivs ska de lokala informationssäkerhetssamordnarna dels involveras i det nämndspecifika uppföljningsarbetet, dels vara kanal för uppföljning till central nivå. Detta genom att den centrala informationssäkerhetsfunktionen har månadsvisa samordningsmöten med de lokala informationssäkerhetssamordnarna, där respektive sektors arbete följs upp. Även om mötesforumet har sjösatts har arbetsprocesserna inte etablerats fullt ut, enligt intervju.

Vad gäller en övergripande handlingsplan med åtgärder för ökad informations- och IT-säkerhet har sådan upprättats. Planen, som har tillhandahållits, upprättades 2024 av IT-avdelningen och informationssäkerhetsfunktionen. Enligt uppgift uppdateras den löpande över tid och följs upp av chef för IT-avdelningen samt säkerhets- och beredskapschef.

6.1.5.1 Bedömning

Vår bedömning är att rekommendationen endast delvis har hörsammats i tillräcklig omfattning.

Vi konstaterar att den handlingsplan upprättats, som kommunstyrelsen enligt missivet avsåg att fastställa. Planen ger struktur åt informationssäkerhetsarbetets framdrift och uppföljning, vilket är viktigt. För att stärka uppföljning och styrning anser vi att handlingsplanen ska återrapporteras även till kommunledningen.

6.1.6 Säkerställa att styrelsen erhåller tillräcklig återrapportering i syfte att kunna besluta om mål- och handlingsplan.

Bakgrund

Av den tidigare granskningen framgick att riktlinjerna för informationssäkerhet omfattade sju informationssäkerhetsmål. Målen hade emellertid inte följts upp, och det samma gällde det samlade informationssäkerhetsarbetet som inte hade återrapporterats till vare sig ledningsgrupp eller kommunstyrelsen.

Yttrande

Kommunstyrelsens yttrande innehåller inget svar som avser uppföljning av informationssäkerhetsarbetet.

Vidtagna åtgärder

Arbetsversionerna av policy för säkerhet och beredskap samt riktlinje för informationssäkerhet anger att uppföljning ska ske i enlighet med ISO 27001[2]. I praktiken innebär det att en sammanfattning av genomfört och kommande informationssäkerhetsarbete ska tas fram årligen och delges kommunstyrelsen. Då granskningen genomfördes hade arbetssättet ännu inte implementerats.

6.1.6.1 Bedömning

Vår bedömning är att rekommendationen inte har hörsammats i tillräcklig omfattning.

I linje med föregående granskning ser vi det som relevant att kommunstyrelsen erhåller återrapportering i syfte att kunna besluta om erforderliga åtgärder för att stärka kommunens informationssäkerhet.

6.2 REKOMMENDATIONER TILL KOMMUNSTYRELSEN UTIFRÅN DESS VERKSAMHETSANSVAR

6.2.1 Rekommendation: Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

Bakgrund

Den föregående granskningen underströk behovet av att upprätta aktuella styrande dokument, vilket även var en av aktiviteterna i handlingsplanen för

[2] Standard för systematiskt informationssäkerhetsarbete

informationssäkerhetsarbetet 2023-2027. I granskningen rekommenderades därvid styrelsen och nämnderna att implementera de uppdaterade dokumenten.

Yttrande

Enligt kommunstyrelsens yttrande uppmanas samtliga nämnder (inklusive kommunstyrelsen utifrån dess verksamhetsansvar) att säkerställa att aktualiserade styrdokument och rutiner implementeras och efterlevs.

Åtgärd

Som redovisats tidigare i rapporten har aktualiserade styrdokument ännu inte fastställts. När de finns kommer implementeringen faciliteras av enheten för säkerhet och beredskap, enligt intervjuuppgifter.

6.2.1.1 Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte har hörsammats i tillräcklig omfattning.

Bedömningen är avhängig att kommunstyrelsen, utifrån sitt övergripande ansvar för informationssäkerhet, inte tillsett att styrdokumenten aktualiserats.

6.2.2 Rekommendation: Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.

Bakgrund

Den tidigare granskningen visade att styrelsen inte genomfört någon verksamhetsspecifik riskanalys med bäring på informationssäkerhetsrisker. Kommunstyrelsen hade dock inkluderat risker med koppling till granskningsområdet i riskanalysen för internkontrollplanen för 2023. Vid granskningens genomförande hade dock ingen uppföljning av internkontrollmomenten genomförts.

Yttrande

Kommunstyrelsens yttrande innehåller ingen utfästelse vad avser verksamhetsövergripande riskanalyser.

Åtgärd

I intervju framförs att risk- och sårbarhetsanalysen (RSA) är det sammanhang där verksamhetsövergripande informationssäkerhetsrisker identifieras. Dessa riskanalyser har delgetts kommunstyrelsen och ses på så vis som ett sätt att tydliggöra risker för styrelsen.

Gällande uppföljning av internkontrollplanen för 2023, som belystes i den föregående granskningen, visar dokumentstudier att de utpekade riskerna ingick i riskanalysen som föregick upprättandet av internkontrollplanen. Riskerna inkluderades inte i den slutgiltiga internkontrollplanen varför de inte har följts upp.

6.2.2.1 Bedömning

Vår bedömning är att rekommendationen inte har hörsammats i tillräcklig omfattning.

I enlighet med tidigare granskning vidhåller vi att det finns behov av att komplettera RSA med en mer specifik riskanalys avseende informationssäkerhetsrisker.

6.2.3 Rekommendation: Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.

Enligt den tidigare granskningen var kommunens informationsklassningsmodell inte fullt ut implementerad i samtliga sektorer. Som exempel angavs att sektor barn och utbildning använt en annan klassningsmodell, och de klassningar som genomfördes av styrelsen och nämnderna betraktades inte heller som systematiska. Klassningar genomfördes företrädelsevis i samband med nyanskaffning av system, men det saknades dokumentation som visade vilka system som respektive sektor hade klassat.

Yttrande

I kommunstyrelsens yttrande uttrycktes att arbete med informationsklassningar och riskanalyser skulle fokuseras till verksamheter som omfattas av NIS2-direktivet.

Åtgärd

Informationsklassning av system som tillhör kommunstyrelsens verksamhetsområde hade inte systematiserats då granskningen genomfördes. Enligt intervju hade ungefär en fjärdedel av systemen klassats och riskbedömts enligt den nya kommungemensamma klassningsmodellen. Den centrala informationssäkerhetsfunktionens fokus beskrivs ha varit att stötta samhällsviktiga verksamheter vid klassningar. Därför har andra sektorer setts som mer angelägna varför merparten av kommunstyrelsens verksamheter inte genomfört klassningar.

6.2.3.1 Bedömning

Vi bedömer att rekommendationen inte har hörsammats i tillräcklig omfattning.

Som tidigare påpekat är informationsklassningar väsentliga moment för att säkerställa att informationstillgångar skyddas av erforderliga säkerhetsåtgärder. Klassningar behöver därför genomföras och dokumenteras i det nya verksamhetssystemet.

6.2.4 Rekommendation: Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Bakgrund

Enligt den tidigare granskningen skulle årliga informationssäkerhetsmål fastställas och integreras i verksamhetsplanering, utifrån vad som angavs i riktlinjerna för

informationssäkerhet. Granskning av kommunstyrelsens verksamhetsplan visade att så inte skett. Styrelsen hade heller inte följt upp informationssäkerhetsarbetet. Tanke fanns om att kommunens informationssäkerhetssamordnare skulle upprätta en informationssäkerhetsrapport, vilken skulle distribueras till styrelsen och samtliga nämnder.

Yttrande

Kommunstyrelsens yttrande benämner inte uppföljning.

Åtgärd

Enligt intervju har kommunstyrelsen ännu inte systematiserat någon uppföljning, men det ska göras i enlighet med vad som anges av ISO27001-standarden, det vill säga en årlig genomgång av genomfört arbete.

Den uppföljning som genomförts var en rapport[3] framtagen av den centrala informationssäkerhetsfunktionen, vilken redovisar hur långt kommunledningssektorns enheter har kommit i informationssäkerhetsarbetet. Rapporten har delgivits berörda chefer för kännedom. Dock ej kommunstyrelsen.

6.2.4.1 Bedömning

Vår bedömning är att rekommendationen inte har hörsammats i tillräcklig omfattning.

I linje med rekommendationens syfte är uppföljning relevant för att beslutsfattare ska ha en bild över nuläge och utifrån den kunna fatta välunderbyggda beslut för att stärka informationssäkerheten. Därvid är det av vikt att kommunstyrelsen fullföljer den uttalade ambitionen om att systematisera uppföljningen.

6.2.5 Samlad bedömning – uppföljning av rekommendationer till kommunstyrelsen

Vår bedömning är att kommunstyrelsen inte hörsammat rekommendationerna från den föregående granskningen i tillräcklig omfattning. Bedömningen avser kommunstyrelsen både utifrån dess övergripande samordningsansvar och kommunstyrelsen utifrån dess verksamhetsansvar.

Granskningen visar att kommunstyrelsen, sedan föregående granskning, vidtagit ett antal åtgärder i syfte att systematisera kommunens övergripande informationssäkerhetsarbete. Den bild som ges är att dessa processer är under utveckling och att fullskalig implementering av strukturer och rutiner återstår att göra. Kommunen har avvaktat revidering av föråldrade styrdokument med hänvisning till nya regulatoriska bestämmelser. Att kommunens styrning utgår från aktuellt lagrum är givetvis centralt. Grunden i styrningen är dock att fastställa tillräcklig och uppdaterade styrdokument, varför detta behöver prioriteras och arbetet därefter operationaliseras.

[3] Status KLS informationssäkerhet 251120

Vad gäller åtgärder vidtagna från kommunstyrelsen utifrån dess verksamhetsansvar konstaterar vi att samtliga rekommendationer kvarstår. Detta är i stora delar hänförligt till att den övergripande styrningen ännu inte implementerats, något som understryker vikten av att säkerställa att styrdokumenten fastställs.

Följande rekommendationer kvarstår helt eller delvis till kommunstyrelsen (utifrån dess övergripande samordningsansvar):

- Verka för att en informationssäkerhetspolicy upprättas av kommunfullmäktige och i samband med detta aktualisera tillhörande riktlinjer som konkretiserar policyn.
- Säkerställa att informationssäkerhetsrisker beaktas i en kommunövergripande riskanalys.
- Säkerställa att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning och klassning av kommunens informationstillgångar genomförs.
- Säkerställa att incidentrutiner upprättas med tydliggjorda eskaleringsvägar samt att inträffade incidenter dokumenteras och analyseras på en kommunövergripande nivå.
- Säkerställa att former för uppföljning av informationssäkerhetsarbete upprättas.
- Säkerställa att styrelsen erhåller tillräcklig återrapportering i syfte att kunna besluta om mål- och handlingsplan.

Rekommendationer till kommunstyrelsen (utifrån dess verksamhetsansvar):

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

6.3 Rekommendationer till barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden, bygglovsnämnden

6.3.1 Rekommendation: Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

Bakgrund

Den föregående granskningen underströk behovet av att upprätta aktuella styrande dokument, vilket även var en av aktiviteterna i handlingsplanen för informationssäkerhetsarbetet 2023-2027. I granskningen rekommenderades därvid styrelsen och nämnderna att implementera de uppdaterade dokumenten.

Yttrande

Yttrandena från barn- och utbildningsnämnden[4], socialnämnden[5], kultur- och fritidsnämnden[6], servicenämnden[7] och bygglovsnämnden[8] anger att nämnderna ska säkerställa att dokumentationen implementeras i respektive del av organisationen.

I yttrandet från vård- och omsorgsnämnden[9] hänvisas till framtagandet av de kommungemensamma styrdokumenten.

Vidtagna åtgärder

Vård- och omsorgsnämnden: Då aktualiserade styrdokument ännu inte fastställts har implementering inte skett. Enligt intervju utgår arbetet i stället direkt från gällande lagstiftning samt att förvaltningen har ett nära samarbete med den centrala informationssäkerhetsfunktionen, vilket beskrivs som ett värdefullt stöd.

Socialnämnden: Då aktualiserade styrdokument ännu inte fastställts har implementering inte skett. Enligt intervju utgår arbetet i stället direkt från lagstiftning samt att förvaltningen har ett nära samarbete med den centrala informationssäkerhetsfunktionen, vilket beskrivs som ett värdefullt stöd.

Barn- och utbildningsnämnden: I väntan på de kommungemensamma styrdokumenten har sektor barn och utbildning tagit fram egen dokumentation som ska fungera som stöd till de anställda, enligt intervju. Dokumentationen har förevisats och finns publicerad på sektorns intranätssida och reglerar processer som avser personuppgiftshantering i första hand, men som i viss utsträckning även beaktar informationssäkerhet.

Servicenämnden: Till följd av resultatet från den tidigare granskningen har sektor service tagit fram en användarmanual med förhållningssätt, användarregler och läshänvisningar till

[4] 2024-05-27
[5] 2024-05-30
[6] 2024-05-22
[7] 2024-04-25
[8] 2024-05-23
[9] 2024-05-30

styrdokument samt en lathund för riktlinjen för informationssäkerhet. Dokumentationen har tillhandahållits vid granskning. Syftet uppges i intervju vara att underlätta för medarbetarna och höja kunskapsnivån. Sektorn har vidare utsett avdelningsvisa kontaktpersoner för informationssäkerhet. Dessa ska driva respektive avdelnings informationssäkerhetsarbete samt fungera som stöd till medarbetare och chefer i både stab och verksamhet, och även höja kunskap om kommunens styrning och regelverk när detta implementeras.

Kultur- och fritidsnämnden: Då aktualiserade styrdokument ännu inte fastställts har implementering inte skett.

Bygglovsnämnden: Då aktualiserade styrdokument ännu inte fastställts har implementering inte skett. Intervjuade framför att sektor samhällsbyggnads rutin för implementering av styrdokument kommer att följas när dokumenten väl har fastställts. Förvaltningen har ett nära samarbete med den centrala informationssäkerhetsfunktionen, vilket beskrivs som ett värdefullt stöd.

6.3.1.1 Bedömning

Vår bedömning är att ingen av de granskade nämnderna har hörsammat rekommendationen i tillräcklig omfattning.

Bedömningen är avhängig att kommunstyrelsen inte tillsett att styrdokumenten aktualiserats.

6.3.2 Rekommendation: Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.

Bakgrund

Den tidigare granskningen visade att varken styrelsen eller de granskade nämnderna hade genomfört någon verksamhetsspecifik riskanalys med bäring på informationssäkerhetsrisker inom respektive verksamhetsområden. Kommunstyrelsen och fyra av de granskade nämnderna hade dock inkluderat risker och kontrollmoment med koppling till granskningsområdet i internkontrollplanen för 2024: sektor barn och utbildning, sektor medborgare och samhällsutveckling, sektor service, sektor vård och omsorg. Vid granskningens genomförande hade dock ingen uppföljning av internkontrollmomenten genomförts.

Vidare konstaterade den tidigare granskningen att IT-beroende utifrån elektronisk kommunikation hade beaktats i den kommunövergripande risk- och sårbarhetsanalysen (RSA) för åren 2024–2027. Därvid bedömdes det finnas behov av att komplettera risk- och sårbarhetsanalysen med fler risker inom informationssäkerhet. Detta i syfte att identifiera sårbarheter som kan påverka kommunens verksamhet på ett negativt sätt.

Yttrande

Yttrandena från barn- och utbildningsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden hänvisar samtliga till kommunstyrelsens yttrande, vilket ska förtydliga vilka aktiviteter och åtgärder som ska genomföras. Yttranden innehåller därutöver ingen utfästelse vad avser verksamhetsövergripande riskanalyser.

I vård- och omsorgsnämndens yttrande uttrycks behov av kommungemensamma mallar och metoder för riskanalyser, så att dessa blir likvärdiga inom hela kommunen.

Vidtagna åtgärder

Vård- och omsorgsnämnden, socialnämnden och bygglovsnämnden: Hänvisar till den kommungemensamma RSA, men har utöver den inte genomfört någon specifik riskanalys avseende informationssäkerhet.

Barn- och utbildningsnämnden: Sektor barn och utbildning har beaktat informationssäkerhetsrisker inom ramen för RSA-arbetet. De intervjuade anser inte att de analysmoment som avser informationssäkerhet speglar hela riskspektrat fullt ut. Ytterligare en upplevd brist är att det tidigare inte har funnits någon tydlig kommungemensam styrning kring riskanalysarbete inom just informationssäkerhetsområdet. Detta i kombination med den tidigare granskningen av informationssäkerhet, som bedömde riskanalysarbetet som bristfälligt, beskrivs ha legat till grund för initiativet att göra en mer omfattande riskanalys inom sektorn. I den riskanalysen inkluderades fler operativa risker som träffar verksamheten i högre utsträckning. Underlaget förevisas vid granskningen varvid vi konstaterar att sektorn analyserat olika informationssäkerhetsrisker och identifierat behov av åtgärder. Underlaget har inte delgivits nämnden.

Servicenämnden: I intervju framförs att sektor service inväntar central samordning gällande hur riskanalyser ska genomföras. Hittills riskarbete har genomförts inom ramen för den riskanalys som föregår framtagandet av den årliga internkontrollplanen. I den riskanalysen ingår informationssäkerhet som en stående risk. Risken genererade inget kontrollmoment i internkontrollplanen för 2025.

Kultur- och fritidsnämnden: Ingen verksamhetsövergripande riskanalys avseende informationssäkerhet har genomförts. Detta då sektor medborgare och samhällsutveckling har inväntat införandet av det nya verksamhetssystemet för informationssäkerhetsarbete. Enligt de intervjuade ska riskanalys göras under 2026, inom ramen för arbetet med den övergripande risk- och sårbarhetsanalysen (RSA). Resultatet av RSA ska sedan ligga till grund för fastställande av internkontrollplan, där de intervjuade menar att informationssäkerhet kommer att ingå.

6.3.2.1 Bedömning

Vi bedömer att barn- och utbildningsnämnden har hörsammat rekommendationen i tillräcklig omfattning. Detta då nämnden genomfört en riskanalys som specifikt avser informationssäkerhet, vilken genererat åtgärder.

Vi bedömer att servicenämnden endast delvis har hörsammat rekommendationen i tillräcklig omfattning. Nämnden beaktar informationssäkerhetsrisker genom internkontrollarbetet, vilket är ett sätt att medvetandegöra sådana risker. En specifik riskanalys avseende informationssäkerhet fördjupar insikterna ytterligare, vilket understryks av det faktum att inget kontrollmoment avseende informationssäkerhet var inkluderat i internkontrollplanen för 2025.

Vi bedömer att vård- och omsorgsnämnden, socialnämnden, servicenämnden och kultur- och fritidsnämnden inte har hörsammat rekommendationen i tillräcklig omfattning. Ingen av nämnderna har genomfört någon riskanalys med specifikt avseende på informationssäkerhet. Som föregående granskning påpekade är den riskanalys som görs inom ramen för RSA varken tillräckligt frekvent eller omfattande för att ge en tillräcklig bild av informationssäkerhetsriskerna.

6.3.3 Rekommendation: Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.

Bakgrund

Enligt den tidigare granskningen var kommunens informationsklassningsmodell inte fullt ut implementerad i samtliga sektorer. Som exempel angavs att sektor barn och utbildning använt en annan klassningsmodell, och de klassningar som genomfördes av styrelsen och nämnderna betraktades inte heller som systematiska. Klassningar genomfördes företrädelsevis i samband med nyanskaffning av system, men det saknades dokumentation som visade vilka system som respektive sektor hade klassat.

Yttrande

I kommunstyrelsens yttrande uttrycktes att samtliga verksamheters arbete med informationsklassningar och riskanalyser skulle fokuseras till verksamheter som omfattas av NIS2-direktivet.

Yttrandena från barn- och utbildningsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden hänvisar samtliga till kommunstyrelsens yttrande, vilket ska förtydliga vilka aktiviteter och åtgärder som ska genomföras. Yttranden innehåller därutöver ingen utfästelse vad avser verksamhetsövergripande riskanalyser.

Yttrandet från vård- och omsorgsnämnden påpekar behov av kommungemensamma metoder för informationsklassning och riskbedömning.

Vidtagna åtgärder

Vård- och omsorgsnämnden: Vid intervju förevisas riskanalyser och informationsklassningar som gjorts på nämndens prioriterade verksamhetssystem och väsentliga processer. Riskanalyserna och klassningarna följer en metodik där information har klassats utifrån

perspektiven ”konfidentialitet”, ”riktighet” och ”tillgänglighet”, och risker har bedömts utifrån konsekvens och sannolikhet. Övriga system ska, enligt uppgift, klassas i ett senare skede då det nya verksamhetssystemet för informationssäkerhet har implementerats fullt ut.

Socialnämnden: Vid granskningen delges dokumentation som visar underlag från klassning av nämndens två största verksamhetssystem. Då granskningen genomfördes kvarstod vissa moment i klassningen av det ena systemet. Enligt de intervjuade ska andra befintliga system också klassas efter att kommunens nya verksamhetssystem för informationssäkerhet har implementerats fullt ut.

Barn- och utbildningsnämnden: Erhållen dokumentation visar underlag från klassning av några av sektorns största system. Enligt intervjuer ska klassning genomföras av samtliga system, men hittills har fokus legat på de system som prioriterats som mest kritiska.

Tidigare använde sektorn KLASSA[10] som informationsklassningsmodell. Numera används den kommungemensamma klassningsmodellen som togs fram under 2024. Dock upplevs det fortfarande saknas ett enhetligt arbetssätt med den nya klassningsmodellen.

De klassningar som sektorn genomfört enligt den nya modellen har gjorts i kommunens nya verksamhetssystem för informationssäkerhetsarbete. I systemet finns en modul som genererar en lista med IT-säkerhetsåtgärder baserade på resultatet från klassningen. Intervjuade uppger att åtgärdslistorna ligger till grund för dialog med systemleverantörerna kring behov av nödvändiga IT-säkerhetsåtgärder.

Servicenämnden: Samtliga av system som används inom sektorn, liksom informationstillgångar som hanteras i respektive system, har inventerats och sammanställts i informationshanteringsplan. Planen ska vara utgångspunkt för kommande klassningsarbete som uppges ligga framför sektorn. Enligt intervjuer har klassningsarbetet varit vilande till följd av att sektorn inväntar att en kommungemensam klassningsmodell fastställs.

Hittills har endast sektor services huvudsakliga system informationsklassats och riskbedömts, vilket verifierats genom tillhandahållet underlag.

Kultur- och fritidsnämnden: Har inte genomfört några informationsklassningar enligt den nya klassningsmodell som tagits fram inom kommunen. Hittills arbete har handlat om att läsa in befintliga system i verksamhetssystemet för informationssäkerhetsarbete, där klassningar senare ska göras. Detta ska enligt uppgift ske under 2026.

Bygglovsnämnden: Enligt muntlig uppgift informationsklassades sektor samhällsbyggnads stora verksamhetssystem för cirka fem år sedan, återklassning har inte gjorts sedan dess. Ambitionen är att klassa systemet enligt kommunens nya modell för informationsklassning under 2026. Den information som finns i verksamhetssystemet har kartlagts i sektorns dokumenthanteringsplan.

[10] Informationsklassningsmodell framtagen av Sveriges kommuner och regioner (SKR).

Sektorns övriga system uppges inte innehålla några känsliga informationstillgångar, och ska klassas efter verksamhetssystemet.

6.3.3.1 Bedömning

Vår bedömning är att vård- och omsorgsnämnden, socialnämnden och barn- och utbildningsnämnden i allt väsentligt har hörsammat rekommendationen i tillräcklig omfattning. Nämnderna har använt kommunens nya klassningsmodell och prioriterat klassning av sina kritiska system. För att rekommendationen ska ses som fullt ut hörsammad behöver klassningar systematiseras och omfatta samtliga system.

Vår bedömning är att servicenämnden, kultur- och fritidsnämnden och bygglovsnämnden inte har hörsammat rekommendationen i tillräcklig omfattning. Servicenämnden har klassat ett system, i övrigt har ingen av nämnderna påbörjat klassningsarbetet enligt kommunens nya modell. Detta är väsentligt då informationsklassning och riskanalys bidrar till att identifiera behov av erforderliga IT-säkerhetsåtgärder som skydd för informationstillgångar.

6.3.4 Rekommendation: Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Bakgrund

Enligt den tidigare granskningen skulle årliga informationssäkerhetsmål fastställas och integreras i verksamhetsplanering, utifrån vad som angavs i riktlinjerna för informationssäkerhet. Granskning av verksamhetsplaner visade dock att ingen av de granskade nämnderna hade formaliserat dylika mål.

Ingen av nämnderna hade heller följt upp informationssäkerhetsarbetet. Tanke fanns om att kommunens informationssäkerhetssamordnare skulle upprätta en informationssäkerhetsrapport, vilken skulle distribueras till samtliga nämnder.

Yttrande

Av vård- och omsorgsnämnden yttrande framgår att informationssäkerhetsarbetet kan sammanställas och analyseras som grund inför planeringen för 2025 års arbete.

Yttrandena från barn- och utbildningsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden hänvisar samtliga till kommunstyrelsens yttrande, vilket ska förtydliga vilka aktiviteter och åtgärder som ska genomföras. Yttranden innehåller därutöver ingen utfästelse vad avser uppföljning.

Varken kommunstyrelsen eller någon av de granskade nämnderna har besvarat rekommendationen i respektive granskningsobjekts yttrande.

Vidtagna åtgärder

Vård- och omsorgsnämnden: Har inte följt upp informationssäkerhetsarbetet.

Socialnämnden: Har inte följt upp informationssäkerhetsarbetet.

Barn- och utbildningsnämnden: Till följd av den föregående granskningen av informationssäkerhet fastställde också nämndens arbetsutskott i maj 2025 ”Handlingsplan för dataskyddsarbete inom sektor barn och utbildning”[11]. Handlingsplanen innehåller aktiviteter som identifierats utifrån den genomförda riskanalysen och den tidigare granskningen. Status på handlingsplanen ska återrapporteras till arbetsutskottet i maj 2026. Den kommungemensamma informationssäkerhetsrapporten har inte delgivits nämnden.

Servicenämnden: Har inte följt upp informationssäkerhetsarbetet. I intervjuer uttrycks en avsikt att systematisera uppföljning av informationssäkerhetsarbetet och slå samman den med uppföljning av dataskyddsarbetet.

Kultur- och fritidsnämnden: Har inte följt upp informationssäkerhetsarbetet. Enligt intervjuer är anledningen att implementeringen av det nya verksamhetssystemet för informationssäkerhet har inväntats. Detta då systemet ses som en förutsättning för att kunna arbeta strukturerat med informationssäkerhet.

Bygglovsnämnden: Nämnden har inte följt upp informationssäkerhetsarbetet. På tjänstepersonsnivå har sektor samhällsbyggnad följt upp det interna deltagandet i den kommunövergripande utbildningen inom informationssäkerhet som genomfördes under 2025. Erhållen uppföljningsdata visar att majoriteten av sektorns anställda har avslutat eller påbörjat utbildningen.

6.3.4.1 Bedömning

Vår bedömning är att barn- och utbildningsnämnden i allt väsentligt har hörsammat rekommendationen i tillräcklig omfattning. Det finns en tidsplan för nämndens uppföljning av den fastställda handlingsplanen. Dataskydd är dock en del i informationssäkerhetsarbetet, varför planen bör adressera hela området, i synnerhet som den innehåller aktiviteter som avser informationssäkerhet.

Vår bedömning är att bygglovsnämnden endast delvis har hörsammat rekommendationen i tillräcklig omfattning. Det är positivt att sektorn följer upp genomförd utbildning. Uppföljningen är emellertid inte tillräcklig för att svara mot rekommendationen.

Vår bedömning är att vård- och omsorgsnämnden, socialnämnden, servicenämnden och kultur- och fritidsnämnden inte har hörsammat rekommendationen i tillräcklig omfattning. Bedömningen utgår från att ingen av nämnderna har genomfört någon uppföljning.

[11] Ej daterad

6.3.5 Samlad bedömning – uppföljning av rekommendationer till barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden:

Att granskade nämnder inte hörsammat rekommendationen som avser implementering av styrdokument, och som följd av det inte strukturerat upp informationssäkerhetsarbetet ytterligare, är i stora delar hänförligt till att kommunstyrelsens övergripande styrning och samordning inte implementerats fullt ut. Att så sker är en förutsättning för att det verksamhetsnära informationssäkerhetsarbetet ska kunna bedrivas enligt fastslagna strukturer.

Därutöver är vår bedömning att de granskade nämnderna hörsammat lämnade rekommendationer enligt följande:

Vård- och omsorgsnämnden och socialnämnden har informationsklassat sina kritiska system, men har utöver det inte fullföljt någon av de avlämnade rekommendationerna. Därmed kvarstår övriga tre rekommendationer från den föregående granskningen.

Dessa nämnder har varken genomfört någon specifik riskanalys avseende informationssäkerhet eller följt upp arbetet mot nämnden. Detta medför en risk att det inte finns en bild av aktuella risker eller pågående arbete inom dessa nämnder. Nämnderna bedöms inte ha vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

Barn- och utbildningsnämnden har genomfört en specifik riskanalys avseende informationssäkerhet, klassat de mest väsentliga systemen samt fastställt en handlingsplan som ska följas upp av nämnden. Nämnden bedöms därvid i allt väsentligt ha hörsammat samtliga rekommendationer från den föregående granskningen i tillräcklig omfattning samt vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

Servicenämnden har, i väntan på implementering av kommungemensamma styrdokument, tagit fram intern dokumentation till stöd för medarbetare samt informationsklassat sitt huvudsakliga verksamhetssystem. Nämnden har därutöver inte hörsammat några av de övriga rekommendationerna, vilka kvarstår. Nämnden bedöms endast delvis ha vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

Kultur- och fritidsnämnden och bygglovsnämnden har inte hörsammat någon av rekommendationerna i tillräcklig omfattning. Samtliga rekommendationer kvarstår härvid. Dessa nämnder bedriver inte samhällsviktig verksamhet vilket är en förklaring till att informationsklassningar inte påbörjats. Vi ser dock behov av att riskanalys och uppföljning av informationssäkerhetsarbetet genomförs. Som tidigare påpekats finns risk att bild över pågående arbete och befintliga risker saknas, vilket kan ligga till grund för kommande insatser i syfte att stärka informationssäkerhetsarbetet. Nämnderna bedöms inte ha vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

Följande rekommendationer kvarstår helt eller delvis till vård- och omsorgsnämnden och socialnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Följande rekommendation kvarstår helt eller delvis till barn- och utbildningsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

Följande rekommendationer kvarstår helt eller delvis till kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

7 SAMLAD BEDÖMNING OCH REKOMMENDATIONER

Syftet med granskningen har varit att bedöma om kommunstyrelsen, barn- och utbildningsnämnden, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden beaktat och hörsammat de mest väsentliga rekommendationerna från den föregående granskningen.

Vår samlade bedömning utifrån granskningens syfte är att barn- och utbildningsnämnden i allt väsentligt vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer, att servicenämnden endast delvis vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer, men att kommunstyrelsen, vård- och omsorgsnämnden, socialnämnden, kultur- och fritidsnämnden och bygglovsnämnden inte vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer

Granskningen har visat att kommunstyrelsen, i egenskap av övergripande ansvarig för informationssäkerheten, vidtagit ett antal åtgärder i syfte att strukturera upp och lägga grund för en organisation som möjliggör ett systematiskt informationssäkerhetsarbete i hela kommunorganisationen. Ingen av de påbörjade processerna har dock implementerats i full skala av styrelsen eller något revisionsobjekt. Bedömningen är därvid att informationssäkerhetsarbetet, inte i någon mening, kan betraktas som systematiserat. Därvid kvarstår de flesta rekommendationer från föregående granskning.

En viktig iakttagelse från den tidigare granskningen var att kommunens styrdokument var föråldrade och icke ändamålsenliga. Nya styrdokument har ännu inte fastställts, vilket motiveras med att kommunen inväntat NIS2-direktivet. Det är givetvis centralt att informationssäkerhetsarbetet bedrivs i enlighet med gällande lagstiftning. Flera av de granskade nämnderna hänvisar emellertid till implementeringen av de uppdaterade styrdokumenten som en förutsättning för att kunna påbörja systematisering av det verksamhetsnära informationssäkerhetsarbetet. Vi anser därvid att kommunstyrelsen hade behövt formalisera den interna styrningen tidigare. Samt att det är nödvändigt att fastställande av styrdokumenten prioriteras och att pågående utvecklingsarbete fortlöper.

Bland övriga granskade nämnder bedöms endast barn- och utbildningsnämnden ha hörsammat de rekommendationer som nämnden kunnat påverka i tillräcklig omfattning.

Följande rekommendationer kvarstår helt eller delvis till kommunstyrelsen (utifrån dess övergripande samordningsansvar):

- Verka för att en informationssäkerhetspolicy upprättas av kommunfullmäktige och i samband med detta aktualisera tillhörande riktlinjer som konkretiserar policyn.
- Säkerställa att informationssäkerhetsrisker beaktas i en kommunövergripande riskanalys.

- Säkerställa att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning och klassning av kommunens informationstillgångar genomförs.
- Säkerställa att incidentrutiner upprättas med tydliggjorda eskaleringsvägar samt att inträffade incidenter dokumenteras och analyseras på en kommunövergripande nivå.
- Säkerställa att former för uppföljning av informationssäkerhetsarbete upprättas.
- Säkerställa att styrelsen erhåller tillräcklig återrapportering i syfte att kunna besluta om mål- och handlingsplan.

Följande rekommendationer kvarstår helt eller delvis till kommunstyrelsen (utifrån dess verksamhetsansvar):

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Följande rekommendationer kvarstår helt eller delvis till vård- och omsorgsnämnden och socialnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Följande rekommendation kvarstår helt eller delvis till barn- och utbildningsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.

Följande rekommendationer kvarstår helt eller delvis till kultur- och fritidsnämnden, servicenämnden och bygglovsnämnden:

- Säkerställa att aktualiserade kommunövergripande styrdokument implementeras i organisationen.
- Säkerställa att informationssäkerhet beaktas i en verksamhetsövergripande riskanalys.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs, som sedan ligger till grund för implementering av tekniska säkerhetsåtgärder.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Datum som ovan

Azets Revision & Rådgivning AB

Mikael Lind	Jenny Thörn	Sofie Ernerudh
Certifierad kommunal revisor	*Specialist*	*Verksamhetsrevisor*