Granskning av informationssäkerhet

Enköpings kommun

September 2025

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Enköpings kommun genomfört en granskning av kommunens arbete med informationssäkerhet. Granskningens syfte är att bedöma om kommunstyrelse och nämnder arbetar med informationssäkerhet på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Nedan ses bedömning för varje revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten.

Revisionsfrågor	**Bedömning**	
1. Finns en organisation med tydlig roll- och ansvarsfördelning?	Delvis	
2. Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?	Delvis	
3. Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet?	Delvis	
4. Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?	Delvis	

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelse och nämnders arbete med informationssäkerhet inte helt bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms inte helt vara tillräcklig.

För att utveckla granskningsområdet bör följande rekommendationer prioriteras:

- Att kommunstyrelsen utvecklar befintliga styrdokument. Störst utvecklingsbehov finns när det gäller styrdokument antagna på politisk nivå.
- Att kommunstyrelsen preciserar roller och ansvar inom organisationen. Detta gäller bland annat vilket eventuellt ansvar som ska läggas på nämnderna.
- Att kommunstyrelsen utvecklar sin uppsikt inom området. Detta kan exempelvis ske genom en årlig rapport från arbetet med informationssäkerhet.
- Att organisationen – på strategisk nivå – prövar hur arbetet med informationssäkerhet kan göras mer enhetligt och systematiskt. Prövningen bör ta utgångspunkt från de krav som ställs i kommande lagstiftning inom området.

Innehållsförteckning

Inledning

Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag, detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde.

Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Informations- och nätverkssystem blivit än mer centrala och nödvändiga för att människors vardagsliv, näringsliv och grundläggande samhällsfunktioner ska fungera. Samtidigt har också hotbilden mot dessa system höjts, och incidenter har både ökat och blivit mer omfattande och sofistikerade. Information är värdefull och behöver många gånger skyddas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering, vilket i sin tur skapar förtroende både internt och externt samt är en förutsättning för att organisationen ska kunna leverera ett fullgott skydd.

Under 2025 förväntas lagstiftningen skärpas inom området informationssäkerhet. Tidigare har delar av kommunal verksamhet varit skyldig att bedriva ett systematiskt arbete med informationssäkerhet. Hädanefter kommer all verksamhet att omfattas av denna lag.

Revisorerna har i sin riskanalys för år 2025 bedömt det angeläget att genomföra en granskning inom ovan rubricerat område.

Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelse och nämnder arbetar med informationssäkerhet på ett ändamålsenligt sätt och med tillräcklig intern kontroll. Följande revisionsfrågor ska besvaras:

1. Finns en organisation med tydlig roll- och ansvarsfördelning?
2. Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?
3. Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet?
4. Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Revisionsfråga 3–4 bildar underlag för om granskningsområdet hanteras på ett ändamålsenligt sätt. Övriga revisionsfrågor nyttjas för att pröva om den interna kontrollen är tillräcklig.

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.
Följande revisionskriterier används i granskningen:

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster § 11–14

- Kommunallagen (2017:725) 6:1, 6:6, 6:13
- Styrdokument inom kommunen som är relevant för granskningen, främst policy, riktlinjer och rutiner gällande informationssäkerhet.

Avgränsning

I tid avgränsas granskningen huvudsakligen till år 2025. Övrig avgränsning, se avsnitt ”Syfte och revisionsfrågor”.

Metod

Granskningen har utförts genom analys av relevanta styrdokument och protokoll. Därutöver har genomförts kompletterande intervjuer med ett urval av identifierade nyckelpersoner inom verksamheten. Följande har intervjuats:

- Informationssäkerhetsstrateg på kommunledningsförvaltningen
- Företrädare för utbildningsförvaltningen respektive upplevelseförvaltningen

De intervjuade har beretts möjlighet att sakgranska rapporten.

Revisionell bedömning av respektive revisionsfråga sker utifrån en tregradig skala: ja/uppfyllt (grön); delvis uppfyllt (gul); nej/ej uppfyllt (röd).

Rapporten har kvalitetssäkrats i enlighet med PwC:s interna rutiner och checklistor för kvalitetssäkring.

Granskningsresultat

Organisation och ansvarsfördelning

Revisionsfråga 1: Finns en organisation med tydlig roll- och ansvarsfördelning?

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska kännetecknas av god intern kontroll. En del i den interna kontrollen är att tydliggöra ansvar och roller inom en organisation. Detta gäller inom såväl den politiska organisationen som verksamhetsorganisationen.

Politisk nivå
Ansvarsfördelning inom den politiska organisationen ska beslutas av kommunfullmäktige. I kommunstyrelsens uppdrag ingår att bereda ärenden som ska hanteras av fullmäktige.

Inom ramen för granskningen har följande dokument granskats:

1. Reglemente för kommunstyrelse och nämnder (beslutade av kommunfullmäktige)
2. Trygghets- och säkerhetspolicy (Kommunfullmäktige 2022)

Av dessa styrdokument framgår att kommunstyrelsen har det övergripande och strategiska ansvaret för området informationssäkerhet. Nämndernas eventuella ansvar inom området har inte preciserats.

I styrdokument som upprättats inom verksamheten framgår emellertid följande:

- Nämnderna är informationsägare och informationsansvarig
- Varje nämnd har ansvaret för att säkerhetsarbetet bedrivs enligt beslutade kommunövergripande strategier

För att nämnderna formellt ska bli bundna till vad som anges ovan krävs emellertid ett beslut av fullmäktige.

Verksamhetsnivå
Det finns även ett behov att precisera hur arbetet med informationssäkerhet ska bedrivas på verksamhetsnivå. Syftet med detta är dels att klargöra roller inom organisationen, men även möjliggöra för politiska organ att kunna utkräva ansvar inom verksamhetsorganisationen.

Följande styrdokument har noterats i granskningen:

1. Roller inom informationssäkerhet, IT-säkerhet och dataskydd (framgår ej beslutsorgan eller datering)
2. Säkerhetsorganisation med befattningar (framgår ej beslutsorgan eller datering)

Av dokumenten framgår att grundprincipen är att ansvaret för arbete med informationssäkerhet följer det ordinarie verksamhetsansvaret. Här exemplifieras vilka arbetsuppgifter som vilar på bland annat kommundirektör, förvaltningschefer, övriga chefer samt informationssäkerhetsstrateg.
Granskade dokument ger en beskrivning hur arbets- och rollfördelningen ser ut inom verksamhetsorganisationen. Dokumentationen kan dock inte betecknas som heltäckande.

Inom kommunen finns exempelvis en särskild grupp för arbetet med informationssäkerhet. Gruppen utgörs av företrädare för olika förvaltningar och har återkommande möten. Granskningen indikerar att gruppen har en central roll i kommunens arbete med informationssäkerhet. Vi kan inte finna att gruppens uppdrag och ansvar har dokumenterats.

Bedömning

Finns en organisation med tydlig roll- och ansvarsfördelning?
Delvis.

Bedömningen baseras på följande:

- Roll- och ansvarsfördelningen är delvis preciserad avseende arbetet med informationssäkerhet.
- Emellertid finns otydligheter i organisationen på såväl politisk nivå som verksamhetsnivå.

För framtiden föreslås att kommunstyrelsen preciserar roller och ansvar inom organisationen. Detta gäller dels vilket eventuellt ansvar som ska läggas på nämnderna, dels tydliggöra roller och ansvar för de befattningar (centralt och på förvaltningar) som i dagsläget har nyckelpositioner för att driva kommunens arbete med informationssäkerhet framåt.

Styrdokument

Revisionsfråga 2: Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska styras genom mål, riktlinjer och planer. Mål och riktlinjer ska beslutas av den politiska organisationen.

I Myndigheten för samhällsskydd och beredskaps (MSB) uppdrag ingår att lämna råd och stöd till organisationer hur de ska arbeta med informationssäkerhet. I MSB:s vägledning beskrivs vikten av att ta fram styrdokument. Styrdokumenten kan utgöras av policy, riktlinjer, planer och instruktioner.
Syftet med ett styrdokument är att styra och vägleda hur organisationen ska arbeta inom ett specifikt område. Granskningen visar att kommunens arbete med informationssäkerhet i första hand regleras i följande styrdokument:

1. Trygghets- och säkerhetspolicy (Kommunfullmäktige 2022)

2. Riktlinjer för hantering av personuppgifter (Kommunstyrelsen 2018)
3. Riktlinjer för informationssäkerhet för anställda (Trygghets- och säkerhetschef 2023)
4. Verktyg och modell för informationsklassning samt tillhörande hanteringsregler utifrån ett informationssäkerhetsperspektiv (Trygghets- och säkerhetschef 2023)
5. Ledningssystem för informationssäkerhet (framgår ej beslutsorgan eller datering)
6. Roller inom informationssäkerhet, IT-säkerhet och dataskydd (do)
7. Säkerhetsorganisation med befattningar (do)

Sammanställningen visar att ett par av styrdokumenten (nr 1–2) är beslutade på politisk nivå. Övriga styrdokument är upprättade på verksamhetsnivå.

Vid granskning av respektive styrdokument har följande noterats:

Styrdokument 1: I policydokumentet – som beretts av kommunstyrelsen - beskrivs det övergripande syftet med kommunens trygghets- och säkerhetsarbetet. Vidare framhålls vikten av att arbetet ska bedrivas på ett enhetligt sätt inom kommunens verksamheter. Policyn ger även uttryck för att policyn ska kompletteras med riktlinjer, rutiner samt andra styrdokument. Dokumentet saknar mål för området informationssäkerhet och saknar även beskrivning hur kommunstyrelse och nämnder ska arbete med området.

Styrdokument 2: I styrdokumentet ges viss styrning hur organisationen ska arbeta med informationssäkerhet. Detta gäller bland annat inom områdena riskanalys och incidentrapportering. Dokumentet reglerar inte närmare hur kommunstyrelse och nämnder ska involveras i detta arbete.

Styrdokument 3: Här ges vägledning till anställda bland annat i fråga om informationsklassning och incidentrapportering. Styrdokumenten ger dock inte en heltäckande bild av hur ett systematiskt arbete med informationssäkerhet ska vara utformat.

Styrdokument 4: I dokumentet beskrivs verktyg och modell för informationsklassning.

Styrdokument 5: I dokumentet beskrivs på övergripande nivå hur arbetet med informationssäkerhet ska bedrivas. Dokumentet omfattar följande delar: 1) Ledning och styrning, 2) Informationssäkerhetsmål och handlingsplaner, 3) Riskhantering, 4) Klassa information och välj säkerhetsåtgärder samt 5) Kontinuitetshantering för informationstillgångar. I jämförelse med övriga styrdokument får detta dokument betecknas som mest heltäckande. Dokumentet beskriver inte hur styrelse och nämnder ska utöva styrning och kontroll inom området.

Styrdokument 6–7: Här beskrivs primärt rollfördelning inom verksamhetsorganisationen. Dokumenten ger även uttryck för att arbetet med informationssäkerhet ska ske genom mål och prioriteringar, årsplaner som upprättas, verkställs samt följs upp.

Genomförda intervjuer med företrädare för förvaltningarna indikerar att vissa upplever att förekomsten av interna styrdokument är tillräcklig, medan andra efterlyser mer styrning genom styrdokument. I

intervjuer framkommer även att det finns ett behov att skapa en ökad tydlighet vilka dokument som finns i kommunen och att göra dessa lättillgängliga för berörda medarbetare.

Företrädare för kommunledningsförvaltningen ger uttryck för att det finns en medvetenhet inom organisationen att kommunens styrdokument inom området informationssäkerhet är i behov av utveckling.

Bedömning

Finns i tillräcklig grad styrande riktlinjer för informationssäkerhet och är dessa väl implementerade i verksamheten?

Delvis.

Bedömningen baseras på följande:

- Det finns ett flertal styrdokument som reglerar hur arbetet med informationssäkerhet ska bedrivas inom kommunen.
- Förekommande styrdokument kan dock inte betecknas som heltäckande. Bland annat saknas en samlad beskrivning hur arbetet med informationssäkerhet ska bedrivas inom organisationen. Detta gäller på såväl politisk nivå som verksamhetsnivå.
- Genomförda intervjuer med företrädare förvaltningar indikerar ett visst behov att göra förekommande styrdokument mer kända inom organisationen.

För framtiden föreslås att kommunstyrelsen utvecklar befintliga styrdokument. Störst utvecklingsbehov finns när det gäller styrdokument antagna på politisk nivå. Dokumenten kan med fördel innehålla tydliga mål för området informationssäkerhet.

Systematiskt arbetssätt

Revisionsfråga 3: Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet?

Iakttagelser

Myndigheten för samhällsskydd och beredskap (MSB) betonar vikten av att svenska myndigheter och organisationer bedriver ett systematiskt arbete med informationssäkerhet. Ett systematiskt arbetssätt kännetecknas vanligtvis av följande moment:

1. Inventering och bedömning av risker
2. Mål och aktivitetsplaner
3. Uppföljning
4. Utvärdering

Som tidigare nämnts saknar kommunen i dagsläget ett heltäckande styrdokument som innefattar samtliga moment i ett systematiskt arbetssätt.

Granskningen visar att det genomförs insatser för att utveckla det systematiska arbetet med informationssäkerhet. Följande har noterats vid genomförda intervjuer:

- Informationsklassning: Har i hög grad genomförts och dokumenterats inom organisationen.
- Incidentrapportering: Sker på ett mer systematiskt sätt än tidigare. Finns skillnader mellan olika förvaltningar.
- Riskanalys: Det finns ett etablerat arbetssätt att genomföra riskanalyser på såväl kommunövergripande nivå som på förvaltningsnivå.
- Handlingsplan: Det upprättas kommunövergripande årsplan för arbetet med informationssäkerhet. Utifrån denna plan upprättas förvaltningsspecifika planer.
- Uppföljning: Det finns en etablerad rutin att följa upp handlingsplaner. Detta sker två gånger per år. Uppföljning sker på såväl förvaltningsnivå som på kommunövergripande nivå. Detta sker genom ledningsgrupp (förvaltningsnivå resp. kommunövergripande nivå).
- Det finns skillnader mellan förvaltningar när det gäller prioriteringar och resurser för att driva ett systematiskt arbete med informationssäkerhet.

Vi kan av rapportering från kommundirektörens ledningsgrupp se att det har skett en stor förbättring mellan åren 2021 och 2024, men noterar samtidigt att kommunen har långt kvar innan verksamheten når den målbild för 2025 som beslutades av gruppen (2023-11-06). Av rapporteringen framgår även att det är stor spridning i hur långt de olika förvaltningarna har kommit i sitt arbete. Den bild som framträder i den skriftliga uppföljningen bekräftas även i genomförda intervjuer.

I övrigt framhålls kommunens förvaltningsstyrningsmodellen EM3 som en framgångsfaktor för att kunna etablera ett systematiskt arbete med informationssäkerhet. EM3 tar utgångspunkt från PM3 som är en beprövad modell för styrning och samverkan av en organisations digitala utveckling.

Myndigheten MSB erbjuder samtliga kommuner att medverka i undersökningen *Infosäkkollen*. Syftet med undersökningen är dels få en bild över hur långt respektive kommun kommit i sitt arbete med informationssäkerhet och dels till att kunna göra jämförelser med andra kommuner. Granskningen visar att Enköpings kommun sedan år 2022 har medverkat i denna undersökning. Av resultatet framgår att det skett en positiv utveckling inom kommunen, men att arbetet ännu inte kan betecknas som fullt ut systematiskt.

Generella utvecklingsområden som framkommer i MSB:s undersökning är delområdena *Ledningens styrning och kontroll* respektive *Uppföljning och utvärdering*.

Bedömning

Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet?
Delvis.

Bedömningen baseras på följande:

- Det finns etablerade rutiner inom verksamheten för att bedriva ett systematiskt arbete med informationssäkerhet. Detta gäller bland annat i fråga om riskanalys, informationsklassning, incidentrapportering samt årliga handlingsplaner.
- Arbetet med informationssäkerhet har kommit olika långt inom förvaltningarna.
- Genomförda intervjuer indikerar att det finns skillnader mellan förvaltningar när det gäller prioriteringar och resurser för att driva ett systematiskt arbete med informationssäkerhet.

För framtiden föreslås att organisationen – på strategisk nivå – prövar hur arbetet med informationssäkerhet kan göras mer enhetligt och systematiskt. Prövningen bör ta utgångspunkt från de krav som ställs i kommande lagstiftning inom området.

Kommunstyrelsens uppsikt

Revisionsfråga 4: Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Iakttagelser

I kommunstyrelsens uppdrag ingår att utöva uppsikt över kommunens samlade verksamhet. Av styrelsens reglemente framgår att styrelsen har det övergripande och strategiska ansvaret för området informationssäkerhet.

Granskningen visar att styrelsen i låg grad utfärdat direktiv hur den ska utöva uppsikt inom området informationssäkerhet. Följande har noterats:

- De styrdokument som redovisas under revisionsfråga 2 reglerar inte hur kommunstyrelsen ska utöva uppsikt inom området.
- Vissa direktiv för uppföljning/rapportering finns emellertid i styrelsens årliga plan för internkontroll.
- Plan för uppsiktsaktiviteter (KS 2025-01-28 § 12) reglerar inte hur kommunstyrelsen ska utöva uppsikt inom området.

Inom ramen för granskningen har det skett en genomgång av styrelsens sammanträdesprotokoll för perioden juni 2024 – maj 2025. Granskningen visar följande:

- Verksamhetsberättelse för kommunstyrelsen 2024 (§ 42/25). Här lämnas viss information om kommunens arbete med informationssäkerhet. Informationen rör dels åtgärder/aktiviteter som vidtagits under året, dels viss information om planerade åtgärder.
- Uppföljning av intern kontroll 2024 (§ 35/25). Kommunstyrelsen hade under 2024 års interkontrollplan med två moment inom informationssäkerhet. Ett om användare med för hög behörighet, kontrollen visade inga avvikelser. Ett om att lagkrav och målbild inom informationssäkerhet uppfylls inte. Information lämnas även vilka åtgärder som vidtagits på verksamhetsnivå.
- Internkontrollplan för kommunstyrelsen 2025 (§ 17/25). Här återfinns ett par kontrollmoment som rör informationssäkerhet. Dessa avser Informationshantering respektive Dataintrång. Kontrollmomenten tar utgångspunkt från genomförd riskanalys. Av planen framgår det vem som är ansvarig för kontrollen, hur den ska ske, när den ska ske och vem som genomför kontrollen.

Vid intervjuer framhålls att återrapportering till styrelsen avseende informationssäkerhet blivit något mer omfattande över tid, men att det alltjämt kan betecknas som ett utvecklingsområde.

Bedömning

Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Delvis.

Bedömningen baseras på följande:

- Kommunstyrelsen har i låg grad preciserat hur den ska utöva uppsikt inom området informationssäkerhet.
- Styrelsen kan verifiera att den under granskningsperioden fått viss rapportering som är hänförlig till området. Rapporteringen har i första hand skett genom verksamhetsberättelse respektive uppföljning av intern kontroll.
- Styrelsens uppföljning/uppsikt kan inte betecknas som heltäckande.

För framtiden föreslås att kommunstyrelsen utvecklar sin uppsikt inom området. Detta kan exempelvis ske genom en årlig rapport från arbetet med informationssäkerhet.

Avslutning

Samlad bedömning

Nedan redovisas revisionell bedömning för de områden som omfattats av granskningen:

Delområde	Bedömning	
1. Organisation och ansvarsfördelning	Delvis	
2. Styrdokument	Delvis	
3. Systematiskt arbetssätt	Delvis	
4. Kommunstyrelsens uppsikt	Delvis	

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelse och nämnders arbete med informationssäkerhet inte helt bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms vara inte helt tillräcklig.

Rekommendationer

För att utveckla granskningsområdet bör följande rekommendationer prioriteras:

- Att kommunstyrelsen utvecklar befintliga styrdokument. Störst utvecklingsbehov finns när det gäller styrdokument antagna på politisk nivå. Dokumenten kan med fördel innehålla tydliga mål för området informationssäkerhet.
- Att kommunstyrelsen preciserar roller och ansvar inom organisationen. Detta gäller dels vilket eventuellt ansvar som ska läggas på nämnderna, dels tydliggöra roller och ansvar för de befattningar (centralt och på förvaltningar) som i dagsläget har nyckelpositioner för att driva kommunens arbete med informationssäkerhet framåt.
- Att kommunstyrelsen utvecklar sin uppsikt inom området. Detta kan exempelvis ske genom en årlig rapport från arbetet med informationssäkerhet.
- Att organisationen – på strategisk nivå – prövar hur arbetet med informationssäkerhet kan göras mer enhetligt och systematiskt. Prövningen bör ta utgångspunkt från de krav som ställs i kommande lagstiftning inom området.

2025-09-17

Kristian Damlin	***Bo Rehnberg***
Uppdragsledare	*Projektledare*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av förtroendevalda revisorer i Enköpings kommun enligt de villkor och under de förutsättningar som framgår av projektplan daterad 2025-02-12. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.