# Granskning av informationssäkerhet

**Hylte kommun**

Augusti 2025

# Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Hylte 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. Från år 2026 kommer lagstiftningen att skärpas inom området informationssäkerhet.

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? | Nej |
| 3. Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet? | Nej |
| 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 bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms inte 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. Hur uppsikten framgent ska struktureras styrs bland annat om nämnderna tilldelas ansvar och arbetsuppgifter inom området.
- 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.

Från år 2026 kommer lagstiftningen att skärpas inom området informationssäkerhet.

Revisorerna har i sin riskanalys för år 2025 bedömt det angeläget att genomföra en granskning inom området informationssäkerhet.

## 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:

- Informationssäkerhetssamordnare för kommunens samlade verksamhet
- Företrädare för barn- och ungdomsförvaltningen respektive samhällsbyggnadsförvaltningen

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. Informationssäkerhetspolicy (Kommunfullmäktige 2017)
2. Reglemente för kommunstyrelse och nämnden (beslutade av fullmäktige)

Granskningen visar att styrdokument nr 1, som beretts av kommunstyrelsen, inte preciserar hur ansvar för informationssäkerhet fördelas mellan kommunstyrelse och nämnder. Granskning av styrdokument 2 visar att dessa inte heller reglerar området. Här klargörs emellertid att kommunstyrelsen har ett övergripande ansvar för kommunens samlade verksamhet. Detta kan tolkas som att styrelsen ensam bär ansvaret för området informationssäkerhet.

I styrdokument som upprättats inom verksamheten framgår emellertid att respektive nämnd är ansvarig för informationssäkerheten inom sina verksamhetsområden. 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, dels möjliggöra för politiska organ att kunna utkräva ansvar inom verksamhetsorganisationen.

Följande styrdokument har noterats i granskningen:

1. Informationssäkerhetspolicy (Kommunfullmäktige 2017)
2. Rutin – informationssäkerhetsombudets roll (Informationssäkerhetssamordnare 2024)

Av dokumenten framgår att grundprincipen är att ansvaret för arbete med informationssäkerhet följer det ordinarie verksamhetsansvaret. Dokumenten ger viss vägledning vilket ansvar och vilka uppgifter

som vilar på kommunchef, förvaltningschefer, övriga chefer, informationssäkerhetssamordnare samt informationssäkerhetsombud. Dokumentationen kan dock inte betecknas som heltäckande.

Inom ramen för granskningen har vi noterat att det finns ett särskilt nätverk för arbetet med informationssäkerhet.  Nätverket består i första hand av informationssäkerhetssamordnare och informationssäkerhetsombud från respektive förvaltning. Granskningen indikerar att nätverket har en central roll i kommunens arbete med informationssäkerhet. Vi noterar att nätverkets uppdrag i viss grad har dokumenterats i befintliga styrdokument.

Vid intervjuer framkommer att det finns ett behov att i vissa avseenden tydliggöra roll- och ansvarsfördelningen inom verksamhetsorganisationen.

### 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. Informationssäkerhetspolicy (Kommunfullmäktige 2017)
2. Rutin – Informationssäkerhetsombudets roll (Informationssäkerhetssamordnare 2024)
3. Rutin och vägledning för informations- och dokumenthantering (Kommunledningsgruppen 2015)

Sammanställningen visar att endast ett styrdokument (nr 1) har beslutats på politisk nivå. Övriga styrdokument är upprättade på verksamhetsnivå.

Vid granskning av respektive styrdokument har följande noterats:

Styrdokument 1: I policydokumentet beskrivs det övergripande syftet med kommunens arbete med informationssäkerhet. Dokumentet definierar vad som avses med informationstillgång samt klargör i viss grad ansvars- och arbetsfördelning inom verksamhetsorganisationen. Dokumentet saknar mål för området informationssäkerhet och saknar även beskrivning hur kommunstyrelse och nämnder ska arbeta med området.

Styrdokument 2: I styrdokumentet ges viss styrning hur organisationen ska arbeta med informationssäkerhet. Detta gäller bland inom områdena informationsklassning, riskanalys, kontinuitetshantering samt incidentrapportering. Dokumentet saknar årshjul för arbetet med informationssäkerhet. Inte heller regleras hur kommunstyrelse och nämnder ska involveras i detta arbete.

Styrdokument 3: Dokumentet syftar till att säkerställa god kvalitet i hantering av information. Här riktas fokus i första hand på dokumenthantering. Däremot ges ingen närmare vägledning hur arbetet med informationssäkerhet ska bedrivas inom organisationen.

Företrädare för kommunledningsförvaltningen framhåller att det finns en medvetenhet inom organisationen att styrdokument inom området informationssäkerhet är i behov av utveckling. Detta bekräftas även vid genomförda intervjuer med företrädare inom förvaltningarna.

### Bedömning

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

Nej.

Bedömningen baseras på följande:

- Det finns några styrdokument som reglerar hur arbetet med informationssäkerhet ska bedrivas inom kommunen.
- Förekommande styrdokument kan 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 indikerar ett utvecklingsbehov i fråga om styrdokument för informationssäkerhet.

Till följd av att kommunen i hög grad saknar styrdokument inom granskningsområdet, saknas förutsättningar för revisionen att granska om dessa är implementerade på ett tillfredsställande sätt.

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: Ett arbete har påbörjats inom förvaltningarna men har ännu inte slutförts. Det saknas tydlig tidsplan när arbetet ska vara färdigt.
- Riskanalys: Ett arbete har påbörjats inom förvaltningarna men har ännu inte slutförts.
- Incidentrapportering: Under år 2024 har det tillskapats en digital rutin för anmälan av incidenter. Ses som ett viktigt framtida verktyg att vidareutveckla analys inom området.
- Handlingsplan:  På kommunövergripande nivå pågår ett arbete för att ta fram handlingsplan för att möta krav i skärpt lagstiftning. Vi kan inte finna att det på förvaltningsnivå – som en del i systematiska arbetet – tas fram årliga handlingsplaner för arbetet med informationssäkerhet.
- Uppföljning: Vi kan se att det på kommunövergripande nivå sker årlig uppföljning av arbetet med informationssäkerhet. Uppföljningen kan dock inte betecknas som heltäckande.

- Det finns skillnader mellan förvaltningar när det gäller prioriteringar och resurser för att driva ett systematiskt arbete med informationssäkerhet. Exempelvis noteras att inom vissa förvaltningar, under perioder, saknats ett informationssäkerhetsombud. I ombudets uppdrag ingår att leda det operativa arbetet med informationssäkerhet.

Granskningen visar att det genomförts olika typer av utbildningsinsatser inom området IT- och informationssäkerhet. Utbildningen har omfattat såväl anställda som förtroendevalda.

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. Undersökningen syftar även till att kunna göra jämförelser med andra kommuner. Granskningen visar att Hylte kommun har medverkat i denna undersökning vid ett flertal tillfällen. Av resultatet framgår att det skett en viss utveckling inom kommunen, men att arbetet inte kan betecknas som systematiskt.

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

### Bedömning

*Bedriver verksamhetsorganisationen ett systematiskt arbete med informationssäkerhet?*

Nej.

Bedömningen baseras på följande:

- Det har inom organisationen påbörjats ett inledande arbete inom området informationssäkerhet. Detta gäller bland annat i fråga om riskanalys, informationsklassning, incidentrapportering och handlingsplaner.
- Arbetet med informationssäkerhet kan inte i dagsläget betecknas som systematiskt.
- 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. Uppsikten ska bland annat omfatta 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.

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

- Information och rapporter (§ 35/25). Denna ärendepunkt innehåller totalt sju rapporter varav en avser området informationssäkerhet. Vid mötet i mars 2025 presenteras ett bildspel samt kompletterande muntlig information. Fokus riktas mot genomförda insatser under år 2024, däribland kommunens resultat i MSB:s *Infosäkkollen*. Viss information lämnas även om planerade insatser/åtgärder. Däremot sker ingen tydlig utvärdering av arbetet inom området. Av beslutet framgår att styrelsen har tagit del av informationen.
- Uppföljning av intern kontroll 2024 (§ 56/25). Kommunstyrelsen har i 2024 års internkontrollplan med ett (1) kontrollmoment som rör IT-säkerhet (kontinuitetsplanering). Ingen avvikelse har noterats, men här framhålls behovet att ajourhålla kontinuitetsplan. Styrelsens beslutar att ha tagit del av uppföljningen.
- Internkontrollplan för kommunstyrelsen 2025 (§ 59/25). Här återfinns ett kontrollmoment som rör IT-säkerhet (kontinuitetsplanering). Samma kontrollmoment finns även i plan 2024. Uppföljning ska ske vid delårsrapport respektive årsbokslut 2025. Styrelsen beslutar att anta planen.

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 rapportering som är hänförlig till området. Rapporteringen har i första hand skett vid ett (1) tillfälle under punkten ”Information och rapporter”.
- Styrelsens uppföljning/uppsikt kan inte betecknas som heltäckande.

För framtiden föreslås att kommunstyrelsen utvecklar sin uppsikt inom området. Hur denna uppsikt ska vara strukturerad styrs i hög grad om fullmäktige tilldelar nämnderna ansvar för informationssäkerhet inom sina verksamhetsområden. I styrelsens uppdrag ingår att utöva uppsikt över nämnderna.

# Avslutning

## Samlad bedömning

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

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

Utifrån genomförd granskning är vår samlade bedömning att kommunstyrelse och nämnders arbete med informationssäkerhet inte bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms inte vara 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.
- Att kommunstyrelsen utvecklar sin uppsikt inom området. Hur uppsikten framgent ska struktureras styrs bland annat om nämnderna tilldelas ansvar och arbetsuppgifter inom området.
- 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.

2025-08-18

| | |
|---|---|
| ***Carl-Magnus Stenehav*** | ***Bo Rehnberg*** |
| *Uppdragsledare* | *Projektledare* |

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av förtroendevalda revisorer i Hyltes kommun enligt de villkor och under de förutsättningar som framgår av projektplan daterad 2025-02-03. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.