Kommunernas informationssäkerhetsarbete

En övergripande kartläggning av kommunernas systematiska informationssäkerhetsarbete

Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

Informations- och cybersäkerhet har fått ökad aktualitet både genom utvecklingen mot ett allt mer digitaliserat samhälle, men också genom nya former av hot och risker.

Även om det är en nationell angelägenhet att säkerställa Sveriges samlade förmåga inom informations- och cybersäkerhet, vilar ett stort ansvar på varje kommun, region, statlig myndighet och företag att vidareutveckla och stärka sitt systematiska och riskbaserade informationssäkerhetsarbete.

Sveriges Kommuner och Regioner (SKR) har som ambition att stötta alla sina medlemmar till att arbeta systematiskt och riskbaserat med informationssäkerhet, för att skydda individers integritet och bevara invånarnas förtroende för välfärdsleveransen.

Som ett led både i att utveckla SKR:s stöd inom informationssäkerhetsområdet och att skapa bättre förutsättningar för samarbete och erfarenhetsutbyte mellan landets kommuner, samt utvärdering av informationssäkerhetsarbetet och dess styrning har SKR utvecklat en webbenkät.

Denna webbenkät är en uppföljning på en tidigare webbenkät som SKR skickade ut 2019. Totalt besvarades enkäten av nästan 82% av kommunerna.

Funktion för informationssäkerhet

För att kommunerna ska lyckas med sitt systematiska och riskbaserade informationssäkerhetsarbete är det viktigt att det finns en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen.

- Av uppföljningen framgår att rollen informationssäkerhetssamordnare finns utpekad i 208 (ca 71%) av kommunerna.

För att informationssäkerhetssamordnaren ska lyckas med sitt uppdrag är en viktig aspekt att den disponibla arbetstid som informationssäkerhetssamordnaren arbetar med informationssäkerhet är så omfattande som möjligt, gärna heltid.

Det finns stora ekonomiska fördelar med att samarbeta och samverka, att kommuner går samman och gemensamt rekryterat en informationssäkerhetssamordnare ökar förutsättningarna för att informationssäkerhetssamordnaren kan arbeta heltid med uppgiften.

Information till ledningen

En viktig del i ett lyckat införande av ett systematiskt och riskbaserat informationssäkerhetsarbete är ledningens aktiva engagemang.

Ledningens årliga utvärdering av att kommunens ledningssystem för informationssäkerhet (LIS) är lämpligt, tillräckligt, effektivt och leder till en förbättring av informationssäkerheten är en central förutsättning för det systematiska och riskbaserade informationssäkerhetsarbetet inom kommunen.

- Av uppföljningen framgår att i 166 (ca 57%) av kommunerna genomförs en ledningsgenomgång med den politiska ledningen regelbundet.

Med införandet av NIS2-direktivet i svensk lag ökar kraven på kommunernas ledningar, bland annat lyfter NIS2-direktivet fram krav på att ledningen ska godkänna riskhanteringsåtgärder och genomgå utbildning, samt erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis.

Styrande dokument

Det är de styrande dokumenten som lägger grunden för ett systematiskt och riskbaserat informationssäkerhetsarbete inom kommunen. Informationssäkerhetspolicyn är ledningens viljeyttring vad avser informationssäkerhetens inriktning och ger det strategiska perspektivet.

- Av uppföljningen framgår vidare att i 232 kommuner finns fastställda övergripande strategiska styrdokument (t.ex. mål, vision, program), i 231 kommuner finns fastställda handlingsinriktade styrdokument (t.ex. policy, handlingsplan) och i 229 kommuner finns fastställda konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler).

Brister i att omsätta de styrande dokumenten (t.ex. policy, riktlinjer och anvisningar) i konkreta handlingsplaner, med aktiviteter, leder till det systematiska

och riskbaserade informationssäkerhetsarbetet i kommunerna inte ger den effekt som ledningen beslutat om i informationssäkerhetspolicyn.

Hantering av informationssäkerhetsrisker

Riskhantering är processen där kommunen på ett systematiskt sätt identifierar, bedömer, prioriterar, analyserar och förebygger potentiella risker för att skydda sina resurser och vidta lämpliga åtgärder för att minimera, övervaka och kontrollera sannolikheten eller inverkan kopplat till oönskade händelser.

- Av uppföljningen framgår att 205 (ca 71%) av kommunerna har en fastställd process för hantering av informationssäkerhetsrisker.

Brister i ett etablerat arbetssätt för hantering av informationssäkerhetsrisker gör att kommunernas medarbetarna löpande tvingas hantera risker.

NIS2-direktivet syftar till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder, vilket innebär att ledningen behöver säkerställa att riskåtgärder godkänns samt att deras genomförande övervakas.

Klassificering av informationstillgångar

Informationsklassificering är en av de grundläggande aktiviteterna inom ett systematiskt och riskbaserat informationssäkerhetsarbete.

- Av uppföljningen framgår att 211 (ca 73%) av kommunerna har en fastställd process för klassificering av informationstillgångar.

Bristen på ett etablerat arbetssätt för att klassificera kommunens informationstillgångar leder till att informationstillgångarna saknar adekvata säkerhetsåtgärder.

Hantering av informationssäkerhetsincidenter

Incidenthantering är också en av de grundläggande aktiviteterna inom ett systematiskt och riskbaserat informationssäkerhetsarbete.

- Av uppföljningen framgår att 220 (ca 76%) av kommunerna har en fastställd process för hantering av informationssäkerhetsincidenter.

Bristen på ett etablerat arbetssätt för att hantera incidenter i hela kommunens verksamhet leder till onödiga ledtider innan incidenter identifieras och hanteras,

vilket gör att kommunens verksamhet drabbas längre än nödvändigt av inträffade incidenter.

Kontinuitetshantering

Kommunen behöver ha en väl förankrad process för att säkerställa verksamhetens kontinuitet, det är väsentligt att kunna förebygga och hantera (snabbare återhämta sig från och mildra konsekvenserna av) inträffade incidenter i kommunens verksamhet.

- Av uppföljningen framgår att 208 (ca 72%) av kommunerna har en fastställd process för att säkerställa verksamhetens kontinuitet.

Med anledning av att några stora informationssäkerhetsincidenter har drabbat kommunerna de senaste åren behöver kontinuitetshantering få mer fokus i framtiden, då tillgången till information är central för att upprätthålla verksamhetens förmåga att producera och leverera oavsett vad som än händer.

Alla kommuner behöver upprätta, införa och öva (för att kontrollera att planen är genomförbar och fungerar) en kontinuitetsplan, så att kritisk verksamhet kan bedrivas även vid störningar.

Utbildning inom informationssäkerhet

Alla medarbetare i kommunen har ett kunskapsbehov när det gäller informationssäkerhet, från ledningen ner till enskilda medarbetare.

- Av uppföljningen framgår att 218 (ca 75%) av kommunerna har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande.

Utbildning i informationssäkerhet är en väsentlig del i att bygga upp och upprätthålla en hög nivå i informationssäkerhetsarbetet och en god informationssäkerhetskultur, vilket leder till att medarbetare känner ett starkare engagemang för att efterleva styrande dokument och därigenom minimeras t.ex. orsaker till incidenter (som t.ex. misstag och systemfel) och verksamhetens kontinuitet upprätthålls.

NIS2-direktivet ställer också krav på utbildning, ledningen är skyldiga att genomgå utbildning och ska uppmuntra sina anställda att genomgå utbildning för att öka medvetenheten om t.ex. cyberhot, nätfiske eller sociala manipuleringstekniker.

Informationssäkerhetsrelaterade krav vid upphandlingar

För att säkerställa att kommunens information skyddas är det viktigt att kommunen har väl förankrade processer för upphandlingar, och att informationssäkerhet är en naturlig del i dessa processer.

- Av uppföljningen framgår att 208 (ca 72%) av kommunerna har en fastställd process för att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar.

Förmågan att kunna ställa och verifiera uppfyllnad av informationssäkerhetskrav är en nödvändig förmåga i kommunernas systematiska och riskbaserade informationssäkerhetsarbete, då de lösningar som upphandlas ofta har långa livscykler och kommunen därmed kan få leva länge med dåliga lösningar.

NIS2-direktivet innebär också ökade krav på säkerhet i leveranskedjan, vilket innebär att kommunerna behöver beakta risker som härrör från leverantörer och tjänsteleverantörer.

Uppföljning

Utvärdering av kommunens informationssäkerhetsarbete, avseende dess lämplighet, tillräcklighet och verkan är en väldigt central del av kommunens systematiska och riskbaserade informationssäkerhetsarbete.

- Av uppföljningen framgår att 159 (ca 55%) av kommunerna har en fastställd process så att kommunens systematiska och riskbaserade informationssäkerhetsarbete följs upp.

Uppföljningen är viktig för att säkerställa att informationen till ledningen är korrekt och möjliggöra för kommunernas ledningar att fatta kloka och välgrundade beslut rörande kommunens framtida informationssäkerhetsarbete.

Slutsats

Kommunerna har mellan 2019 och 2023 genomfört ett gediget arbete med att säkerställa det systematiskt och riskbaserat informationssäkerhetsarbete är lämpligt, tillräckligt, effektivt och leder till en förbättring av informationssäkerheten i kommunerna.

- Det finns fler informationssäkerhetssamordnare och det arbetas fler informationssäkerhetstimmar i kommunerna.
- Informationssäkerhet har kommit högre upp på agendan, vilket tydligt framgår av att allt fler politiska ledningar regelbundet informerar sig kring kommunens informationssäkerhetsarbete.
- Kommunfullmäktige och kommunstyrelser är betydligt mer involverade i arbetet med de styrande dokumenten (t.ex. policy och handlingsplaner.
- Kommunerna har arbetat mycket med att säkerställa verksamhetens kontinuitet, en viktig faktor när vi ser att antalet cyberangrepp mot Sverige ökar.
- Kommunerna utbildar sina medarbetare i större utsträckning i informationssäkerhet, en viktig aspekt i att bygga en säkerhetskultur i kommunerna.
- Kommunerna har blivit mycket bättre på att ställa informationssäkerhetskrav vid upphandlingar, en viktig faktor för att möjliggöra en säker informationshantering inom kommunerna.
- Kommunerna behöver bli bättre på att följa upp informationssäkerhetsarbetet, inte minst när det gäller leverantörsuppföljningar.

Det är flera nya regelverk på gång, som exempel kommer Sverige att införa EU:s NIS2-direktiv i svensk lag under 2024. Denna nya reglering kommer ställa tydligare och mer omfattande krav på kommunerna att arbete systematiskt och riskbaserat med sin informations- och cybersäkerhet.

SKR ser att ett systematiskt informationssäkerhetsarbete är en nödvändig del i en framgångsrik digitalisering för kommunerna och bedömer att området kräver ett ökat fokus i samband med enskilda digitaliseringslösningar och för att öka kommunernas förmåga att stå emot hot och kunna säkerställa tillit från medborgarna.

Inledning

Bakgrund

Informations- och cybersäkerhet har fått ökad aktualitet både genom utvecklingen mot ett allt mer digitaliserat samhälle och nya former av hot och risker. Inte minst har det efter Rysslands invasion av Ukraina blivit tydligt att Sveriges förmåga att stå emot hot och angrepp behöver stärkas.

Även om det är en nationell angelägenhet att säkerställa Sveriges samlade förmåga inom informations- och cybersäkerhet, vilar ett stort ansvar på varje kommun, region, statlig myndighet och företag att vidareutveckla och stärka sitt systematiska och riskbaserade informationssäkerhetsarbete.

Sveriges Kommuner och Regioner (SKR) har som ambition att stötta alla sina medlemmar till att arbeta systematiskt och riskbaserat med informationssäkerhet, för att skydda individers integritet och bevara invånarnas förtroende för välfärdsleveransen.

En väsentlig del av ett systematiskt och riskbaserat informationssäkerhetsarbetet är utvärdering av informationssäkerhetsarbetet och dess styrning. Genom att en organisation använder sig av en strukturerad övervakning och mätning ges förutsättningar för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder är implementerade och fungerar tillfredsställande.

Som ett led både i att utveckla SKR:s stöd inom informationssäkerhetsområdet och att skapa bättre förutsättningar för samarbete och erfarenhetsutbyte mellan landets kommuner, samt utvärdering av informationssäkerhetsarbetet och dess styrning har SKR utvecklat en webbenkät.

Det finn stora ekonomiska fördelar med att samarbeta och samverka, alla behöver inte uppfinna hjulet själva.

Uppföljningens omfattning

Ett viktigt ingångsvärde i skapandet av denna uppföljning har varit SKR:s webbenkät som skickades till kommunerna under 2019 och SKR:s webbenkät som skickades till regionerna under 2021, dessutom har frågeställningarna som

Myndigheten för samhällsskydd och beredskap (MSB) använder sig av i Infosäkkollen[1] utgjort ett underlag.

För en mer detaljerad beskrivning över uppföljningens omfattning se kapitel 6 Uppföljningens omfattning.

Mognadsmodellen

MSB presenterade en rapport[2] 2018 över landstingens informationssäkerhetsarbete inom hälso- och sjukvården, i samband med den rapporten presenterade MSB samtidigt en mognadsmodell.

Denna mognadsmodell låg också till grund för de bedömningar som gjordes under SKR:s uppföljning över kommunernas systematiska och riskbaserade informationssäkerhetsarbete 2019.

Mognadsmodellen har senare vidareutvecklats av MSB, men för spårbarhet och jämförelse mellan 2019 och 2023 väljer SKR, i denna uppföljning, att behålla den mognadsmodell som användes vid uppföljningen 2019.

För en mer detaljerad beskrivning över mognadsmodellen omfattning se kapitel 6 Uppföljningens omfattning.

Om kommunerna

Kommunerna ansvarar för en stor del av den samhällsservice som finns där vi bor. Bland de viktigaste uppgifterna är förskola, skola, socialtjänst och äldreomsorg.

Kommunerna är skyldiga att ha vissa verksamheter enligt lag. Andra verksamheter är frivilliga och beslutas av lokalpolitikerna.

Antalet anställda i kommunerna uppgick i november 2022 till nästan 900 000.

---

[1] Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter, (https://www.msb.se/infosakkollen)

[2] En bild av landstingens informationssäkerhetsarbete 2018 : kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (https://www.msb.se/sv/publikationer/en-bild-av-landstingens-informationssakerhetsarbete-2018--kartlaggning-och-analys-av-landstingens-informationssakerhetsarbete-inom-halso--och-sjukvardsverksamheten/)

För en mer detaljerad beskrivning över kommunerna se kapitel 7 Om kommunerna.

Kommungruppsindelning

För att underlätta analyser och jämförelser ur ett regionalt perspektiv har SKR sedan 1980-talet utarbetat en gruppering av landets kommuner.

SKR:s kommungruppsindelning[3] syftar till att gruppera kommuner efter deras förutsättningar ur ett perspektiv sett till befolkningsstorlek, geografiskt täthet och närhet till större städer eller tätorter.

För en mer detaljerad beskrivning över kommungrupsindelningen se kapitel 7 Om kommunerna.

Så styrs kommuner

Sverige är indelat i 290 kommuner. Kommuner är självstyrande och styrs av lokalt folkvalda politiker. Självstyret är grundlagsstadgat.

Kommunerna styrs av politiker som valts direkt av medborgarna, vilket betyder att medborgarna har stora möjligheter att påverka och kontrollera hur kommuner utför sina uppdrag.

Kommunerna styrs genom direktvalda politiska församlingar, så kallade kommunfullmäktige. Dessutom finns det politiska uppdrag inom kommunstyrelser, i olika nämnder och utskott. Det finns drygt 38 000 förtroendevalda i landets 290 kommuner. Merparten, 97 procent, är fritidspolitiker och sköter därmed sina uppdrag vid sidan av arbete eller studier.

Kommunfullmäktige är kommunens högsta beslutande organ. Kommunfullmäktige representerar folket i kommunen och tar beslut i kommunens viktigaste frågor.

För en mer detaljerad beskrivning över hur kommunerna styrs se kapitel 7 Om kommunerna.

[3] Kommungruppsindelning (https://skr.se/download/18.ef4ba7d1849a2f55db2898a/1669978414789/Kommungruppsindelning-2023.pdf)

Uppföljningens delområden och resultat

Under våren 2023 genomförde SKR en webbenkät, som en uppföljning på kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

Denna webbenkät är en uppföljning på en webbenkät SKR skickade ut 2019.

Svarsfrekvensen var god (siffrorna från 2019 inom parentes):

- 215 (242) kommuner besvarade hela enkäten och avslutade
- 19 kommuner besvarade så gott som hela enkäten, men avslutade inte
- 3 (23) kommuner besvarade delar av enkäten
- 53 (25) kommuner besvarade inte enkäten

Totalt besvarades enkäten av nästan 82% (91%) av kommunerna.

Nedan redovisas, förutom en kortare beskrivning av respektive uppföljningsområden, erhållna svar samt korta iakttagelser kopplat till dessa svar.

Det är också värt att notera att denna webbenkät endast har haft som syfte att mäta mot de två lägre nivåerna i mognadsmodellen, det går således inte att utläsa huruvida det finns någon av kommunerna som ligger på mognadsnivå 3 eller 4.

Funktion för informationssäkerhet

Beskrivning av området

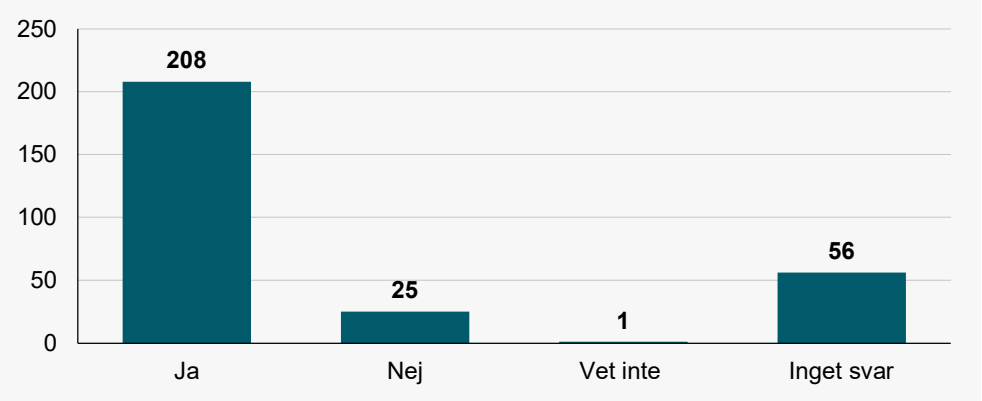
Information blir en allt viktigare resurs för kommunerna och genom en ökad digitalisering krävs ännu större fokus på säkerheten kring informationen. Det är därför viktigt att kommunen utser en funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen. Denna funktion har ofta titeln informationssäkerhetssamordnare, men titeln kan också vara CISO, informationssäkerhetschef eller liknande.

Rollen som informationssäkerhetssamordnare är bred och arbetar med t.ex.:

- att utveckla och kommunicera kommunens ledningssystem för informationssäkerheten (policys, riktlinjer och anvisningar/instruktioner),
- att stödja kommunens olika verksamheter genom rådgivning, utbildning och uppföljning inom informationssäkerhetsområdet (t.ex. informationsklassning, risk- och incidenthantering samt kravställning och -uppföljning vid upphandlingar) och
- att genomföra ledningens genomgång minst en gång om året.

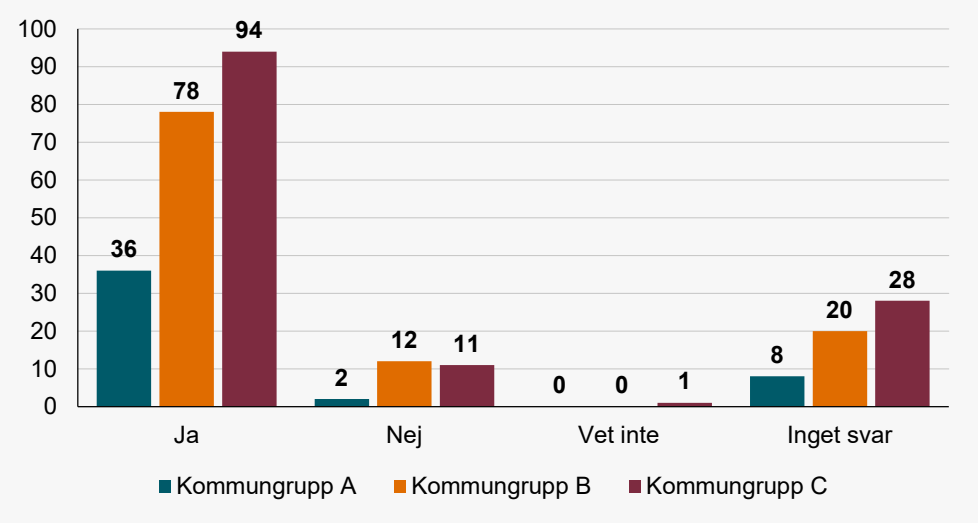
Erhållna svar

Figur 1 Har er kommun en funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen som organisation?



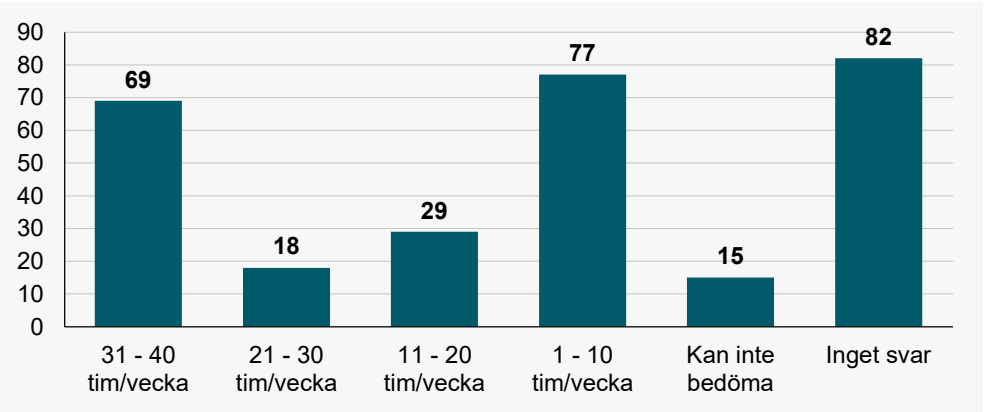
Av svaren framgår att 208 (ca 72%) av kommunerna har en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen, medans 25 (ca 9%) av kommunerna uppger att de saknar en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen.

Figur 2 Har er kommun en funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen som organisation, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att 36 (ca 78%) av kommungrupp A, 78 (ca 71%) av kommungrupp B och att 94 (ca 70%) av kommungrupp C uppger att de har en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen.

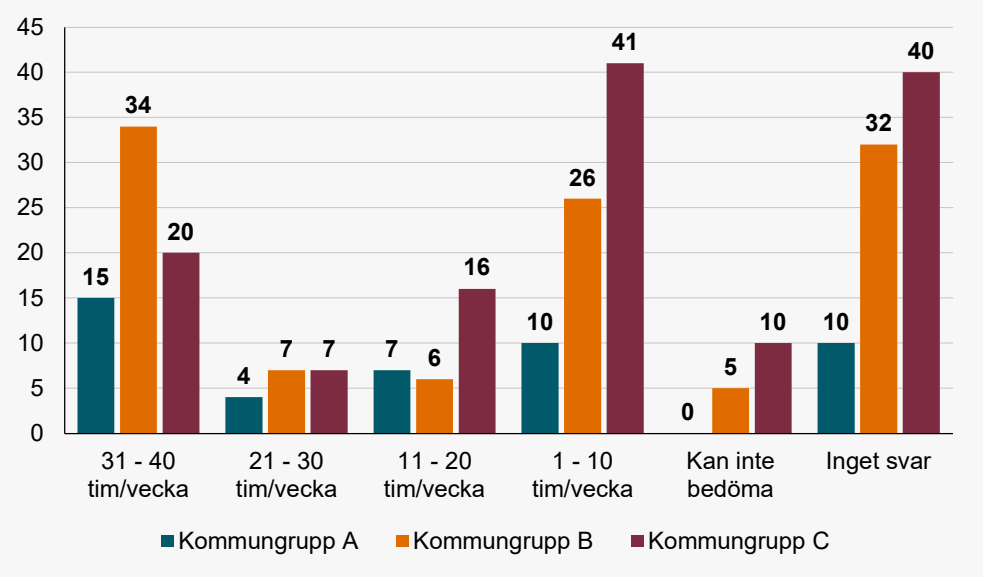
Figur 3 Ungefär hur mycket tid avsätter personen som har denna funktion av sin arbetstid till informationssäkerhetsarbete i genomsnitt per vecka?



Av svaren framgår att i 69 (ca 24%) av kommunerna disponerar den utpekade funktionen 31-40 timmar i veckan till informationssäkerhetsarbete inom

kommunen, i 18 (ca 6%) av kommunerna disponerar den utpekade funktionen 21-30 timmar i veckan till informationssäkerhetsarbete inom kommunen. I 29 (ca 10%) av kommunerna disponerar den utpekade funktionen 11-20 timmar i veckan till informationssäkerhetsarbete inom kommunen.

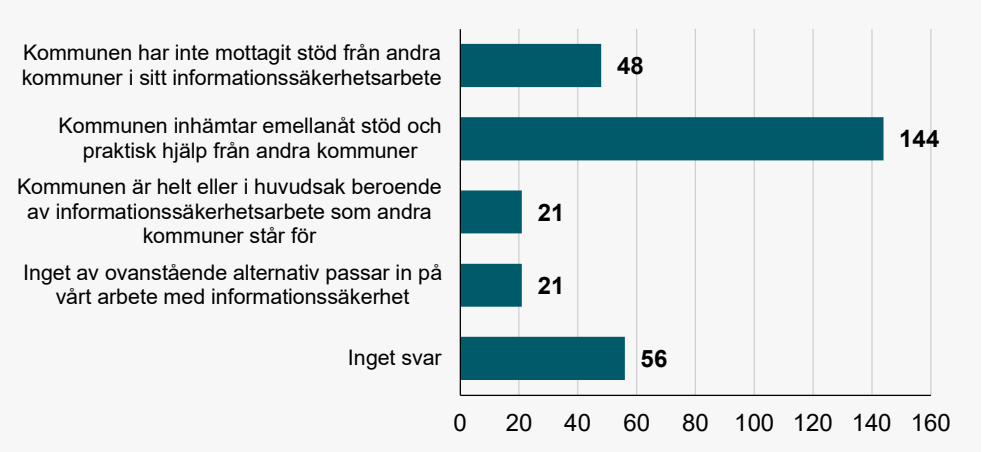
Figur 4 Ungefär hur mycket tid avsätter personen som har denna funktion av sin arbetstid till informationssäkerhetsarbete i genomsnitt per vecka, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 15 (ca 33%) av kommungrupp A och i 34 (ca 31%) av kommungrupp B disponerar den utpekade funktionen 31-40 timmar i veckan till informationssäkerhetsarbete inom kommunen, medans det framgår att i 41 (ca 31%) av kommungrupp C disponerar den utpekade funktionen 1-10 timmar i veckan till informationssäkerhetsarbete inom kommunen.

Figur 5 Kommuner kan ingå i olika samverkansrelationer med andra kommuner i sitt informationssäkerhetsarbete. Vilket av följande alternativ stämmer bäst för kommunen om du ser till de senaste tre åren?

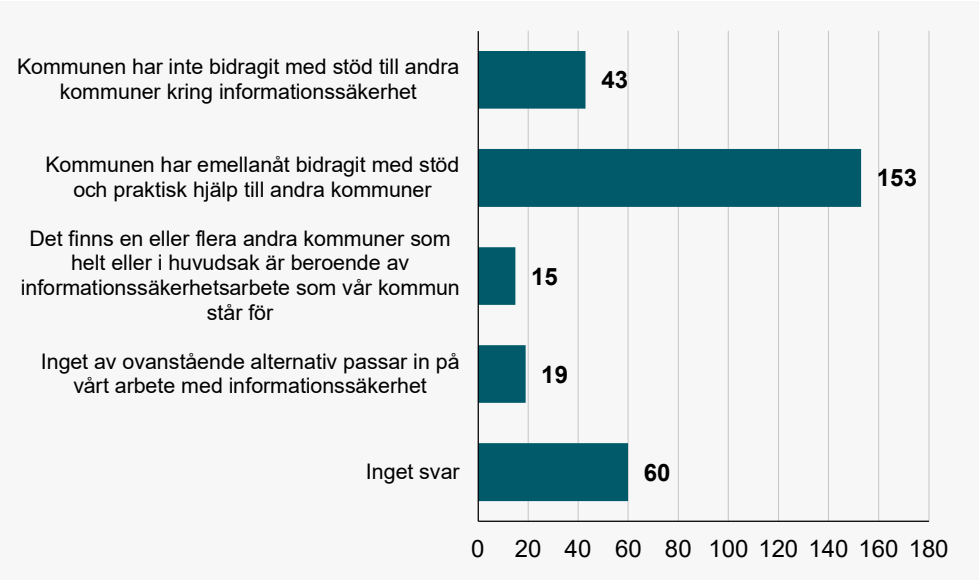
- När det gäller kommunens beroende av andra kommuner:



Av svaren framgår att i 144 (ca 50%) av kommunerna inhämtas emellanåt stöd och praktisk hjälp från andra kommuner i sitt informationssäkerhetsarbete. 48 (ca 17%) av kommunerna har inte mottagit stöd från andra kommuner i sitt informationssäkerhetsarbete.

Figur 6 Kommuner kan ingå i olika samverkansrelationer med andra kommuner i sitt informationssäkerhetsarbete. Vilket av följande alternativ stämmer bäst för kommunen om du ser till de senaste tre åren?

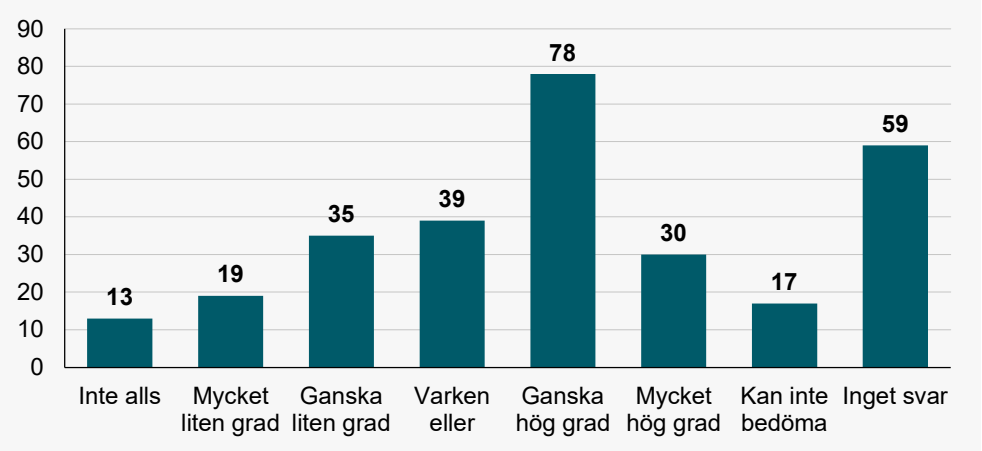
- När det gäller kommunens stöd till andra kommuner:



Av svaren framgår att 153 (ca 53%) av kommunerna har emellanåt bidragit med stöd och praktisk hjälp till andra kommuner kring informationssäkerhet. 43 (ca 15%) av kommunerna har inte bidragit med stöd till andra kommuner kring informationssäkerhet.

Figur 7 I vilken grad behöver kommunen stöd i informationssäkerhetsfrågor från följande aktörer under de kommande tre åren?

- Andra kommuner



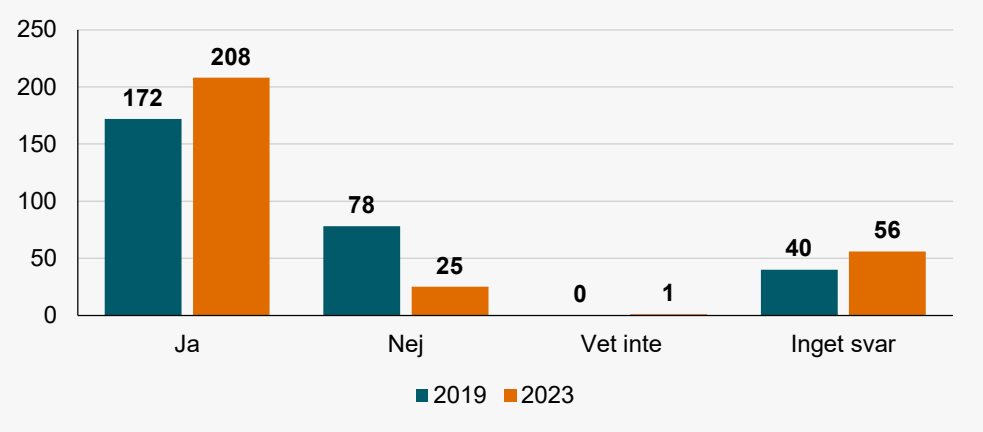
Av svaren framgår att 78 (ca 27%) av kommunerna i ganska hög grad behöver stöd i informationssäkerhetsfrågor från andra kommuner under de kommande tre åren. 39 (ca 13%) av kommunerna behöver varken eller stöd i informationssäkerhetsfrågor från andra kommuner under de kommande tre åren.

lakttagelser

Rollen som samordnare av informationssäkerhetsarbetet är en viktig funktion för att kommunerna ska lyckas med sitt systematiska och riskbaserade informationssäkerhetsarbete. Detta i sin tur är viktigt för arbetet med digitaliseringen.

Av uppföljningen framgår att rollen informationssäkerhetssamordnare finns utpekad i 208 (ca 72%) av kommunerna, vilket kan jämföras med uppföljningen från 2019 då 172 (ca 59%) kommuner uppgav att det fanns en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen.

Figur 8 har er kommun en CISO med uppdrag att samordna det övergripande informationssäkerhetsarbetet?



<u>Notera:</u> svarsalternativet "Vet inte", fanns inte med som ett svarsalternativ i uppföljningen 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en informationssäkerhetssamordnare utpekad, har ökat från 29 till 36, en ökning med 24%.
- Kommungrupp B, som har en informationssäkerhetssamordnare utpekad, har ökat från 63 till 78, en ökning med ca 24%.
- Kommungrupp C, som har en informationssäkerhetssamordnare utpekad, har ökat från 80 till 94, en ökning med ca 18%.

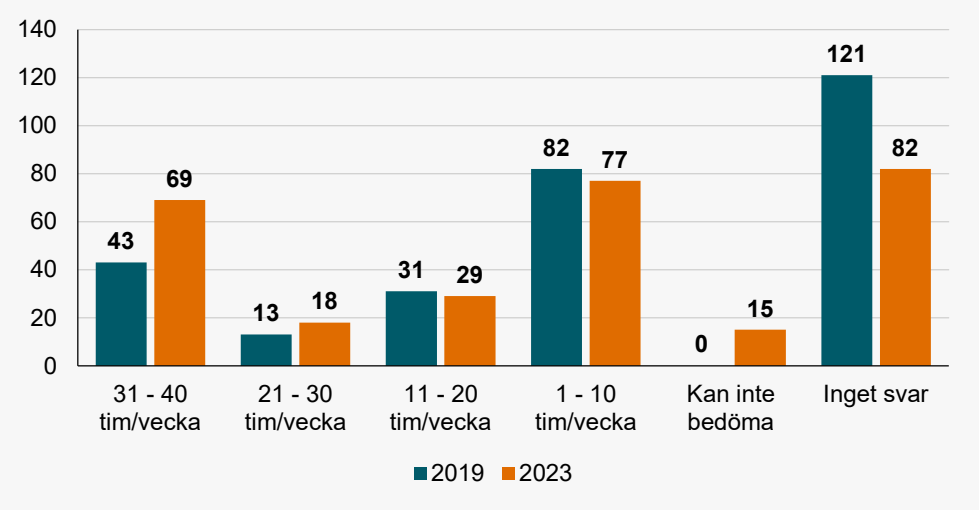
Det är positivt att nästan tre av fyra kommuner har en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen, jämfört med uppföljningen 2019 då det var nästan sex tio kommuner som uppgav att de hade en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen.

Ökningen av kommuner med en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet är relativt jämförbar mellan kommungrupp A, B och C.

Vi kan, av uppföljningen, se att antalet kommuner som har en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen har ökat, när vi tittar på den disponibla arbetstid som funktionen

med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen kan vi konstatera att också den har ökat, jämfört med uppföljningen 2019.

Figur 9 Hur mycket tid avsätter personen som har denna funktion av sin arbetstid till informationssäkerhetsarbete i genomsnitt per vecka, jämförelse mellan uppföljningen 2019 och 2023.



<u>Notera:</u> svarsalternativet "Kan inte bedöma", fanns inte med som ett svarsalternativ i uppföljningen 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en informationssäkerhetssamordnare utpekad, har ökat antalet arbetade timmar från 590 till 853, en ökning med ca 45%.
- Kommungrupp B, som har en informationssäkerhetssamordnare utpekad, har ökat antalet arbetade timmar från 1036 till 1649, en ökning med ca 59%.
- Kommungrupp C, som har en informationssäkerhetssamordnare utpekad, har ökat antalet arbetade timmar från 1165 till 1417, en ökning med ca 22%.

<u>Notera:</u> antalet arbetade timmar utgår från medianen i de olika spannen, d.v.s. för spannet 31-40 timmar räknas med 35,5 timmar.

Det är positivt att antalet kommuner som uppger att de har en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen ökar. Även den disponibla arbetstid som informationssäkerhetssamordnaren arbetar med informationssäkerhet har ökat, idag avsätter tre av tio informationssäkerhetssamordnare mer än halva av sin ordinarie arbetstid till informationssäkerhetsarbetet, vilket kan jämföras med uppföljningen från 2019 då färre än två av tio avsatte mer än halva av sin ordinarie arbetstid till informationssäkerhetsarbetet.

Av uppföljningen framgår att den disponibla arbetstid som informationssäkerhetssamordnaren arbetar med informationssäkerhet har ökat mest i kommungrupp B, följt av kommungrupp A. För kommungrupp C är ökningen något mindre, vilket kan förklaras av att merparten av informationssäkerhetssamordnarna disponerar 1-10 timmar av sin ordinarie arbetstid till informationssäkerhet.

Detta sammantaget ger kommunerna bättre förutsättningar att införa ett systematiskt och riskbaserat informationssäkerhetsarbete, som är en viktig grundförutsättning för digitaliseringsresan som kommunerna har påbörjat.

För att informationssäkerhetssamordnaren ska lyckas i uppdraget att stödja kommunens olika verksamheter (t.ex. informationsklassning, risk- och incidenthantering, utbildning och uppföljning) är en viktig aspekt att den disponibla arbetstid som informationssäkerhetssamordnaren arbetar med informationssäkerhet är så omfattande som möjligt, gärna heltid.

Det finns flera exempel där kommuner gått samman och gemensamt rekryterat en informationssäkerhetssamordnare, då de enskilt kanske inte är tillräckligt stora för att stödja en informationssäkerhetssamordnare på heltid.

Av uppföljningen framgår också att det finns ett stort intresse och behov av ett samarbete mellan kommunerna när det gäller informationssäkerhetsarbetet.

Information till ledningen

Beskrivning av området

Högsta ledningen bör minst en gång per år informera sig om verksamhetens informationssäkerhetsarbete, d.v.s. utvärdera att ledningssystem för informationssäkerhet (LIS) är lämpligt, tillräckligt, effektivt och leder till en

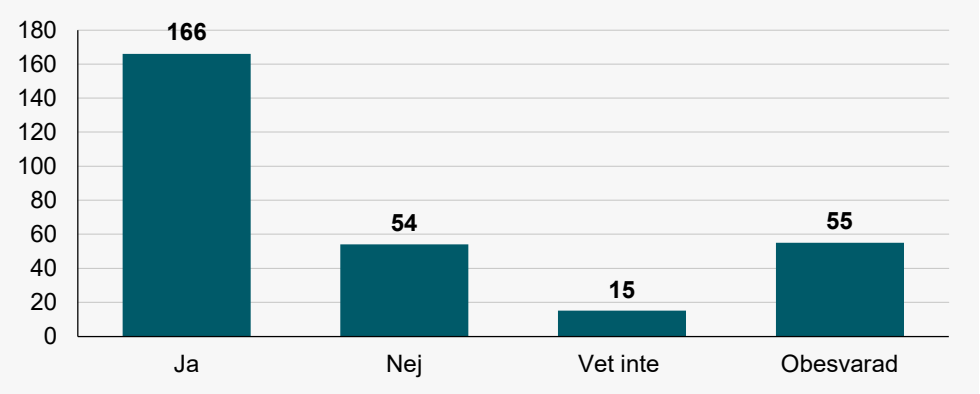
förbättring av informationssäkerheten. Denna utvärdering kallas för ledningens genomgång och syftar till att ledningen på strategisk nivå ska få kunskap om ”informationssäkerhetsläget”.

Vid ledningens genomgång informeras ledningen om viktiga händelser (kring t.ex. informationstillgångar, risker, incidenter och säkerhetsmedvetenhet) och förändringar i informationssäkerhetsarbetet som skett under den gångna perioden, samtidigt fattar ledningen strategiska beslut (t.ex. budget) och drar upp riktlinjer inför den kommande tidsperioden.

En nyckel till ett framgångsrikt informationssäkerhetsarbete inom kommunen är en god relation och kommunikation mellan ledning och informationssäkerhetssamordnaren.

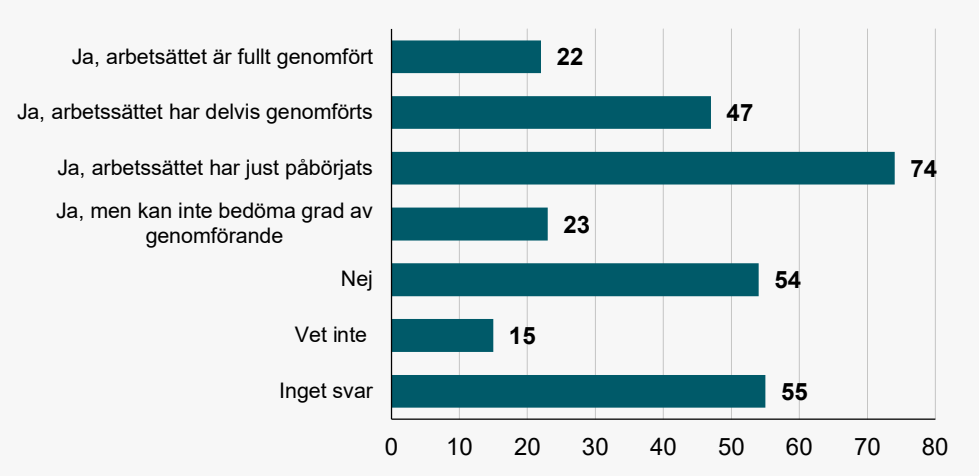
Erhållna svar

Figur 10 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor?



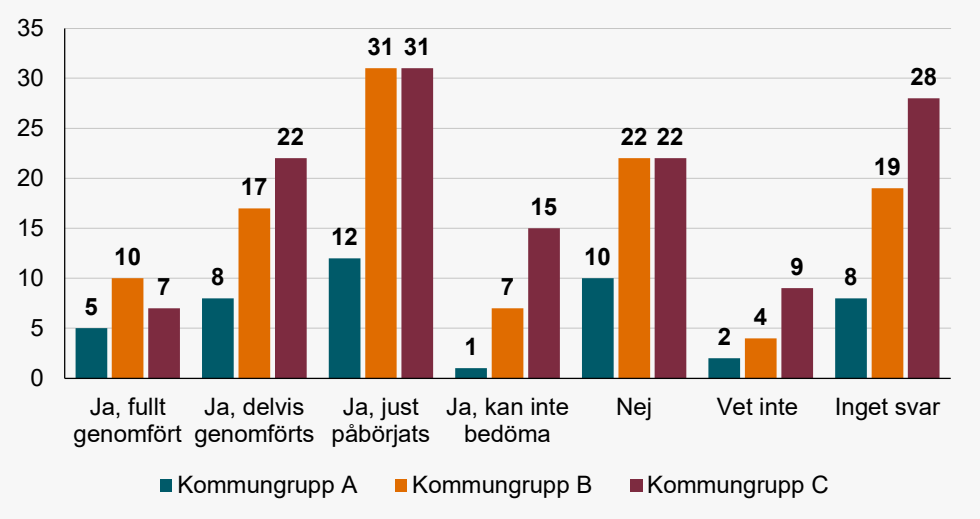
Av svaren framgår att i 166 (ca 57%) av kommunerna informeras den politiska ledningen regelbundet i informationssäkerhetsfrågor. I 54 (ca 19%) av kommunerna informeras inte den politiska ledningen regelbundet i informationssäkerhetsfrågor.

Figur 11 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor?



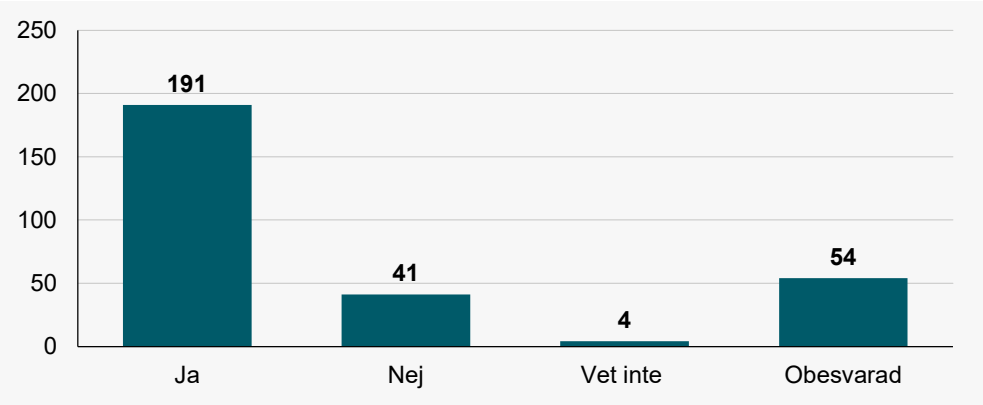
Av svaren framgår att 22 (ca 8%) av kommunerna har ett etablerat arbetssätt så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor. I 144 (ca 50%) av kommunerna pågår ett arbete med att etablera ett arbetssätt så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor.

Figur 12 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.



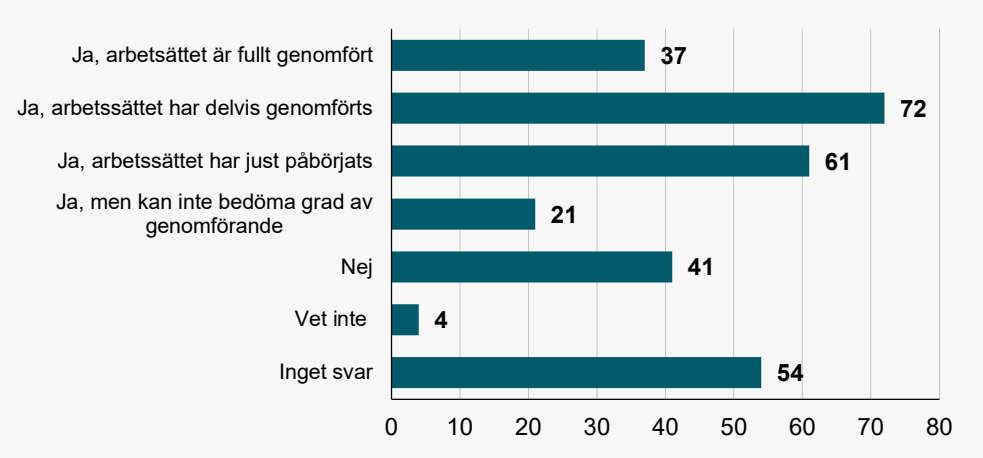
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 12 (ca 26%) av kommungrupp A, i 31 (ca 28%) av kommungrupp B och i 31 (ca 23%) av kommungrupp C har ett arbetssätt just påbörjats så att den politiska ledningen regelbundet informeras i informationssäkerhetsfrågor.

Figur 13 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor?



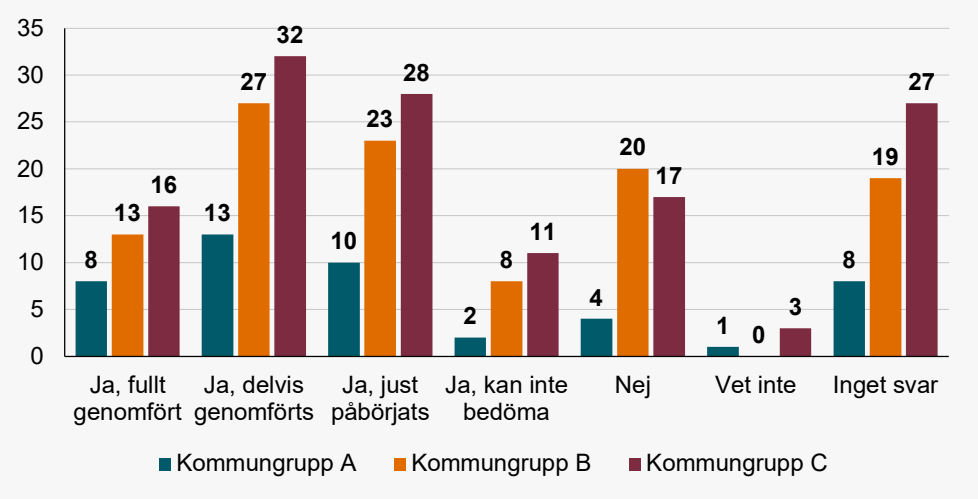
Av svaren framgår att i 191 (ca 66%) av kommunerna informeras förvaltningsledningen/-arna regelbundet i informationssäkerhetsfrågor. I 41 (ca 14%) av kommunerna informeras inte förvaltningsledningen/-arna regelbundet i informationssäkerhetsfrågor.

Figur 14 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor?



Av svaren framgår att 37 (ca 13%) av kommunerna har ett etablerat arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor. I 154 (ca 53%) av kommunerna pågår ett arbete med att etablera ett arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor.

Figur 15 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.



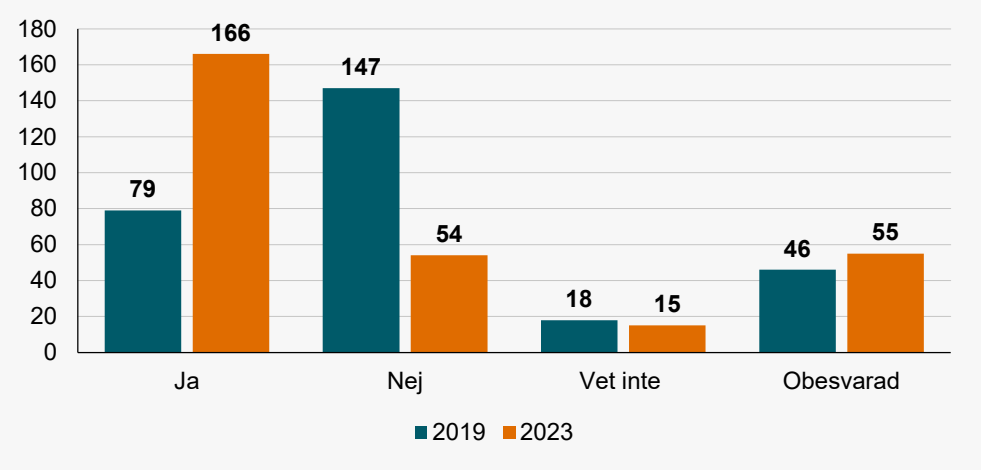
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 13 (ca 28%) av kommungrupp A, i 27 (ca 25%) av kommungrupp B och i 32 (ca 24%) av kommungrupp C har ett delvis etablerat arbetssätt så att förvaltningsledningen/-arna regelbundet informeras i informationssäkerhetsfrågor.

lakttagelser

Högsta ledningens utvärdering av att kommunens ledningssystem för informationssäkerhet (LIS) är lämpligt, tillräckligt, effektivt och leder till en förbättring av informationssäkerheten är en central förutsättning för att skapa tillit till den digitalisering som sker inom kommunen, d.v.s. att digitaliseringen sker på ett sådant sätt att den inte skapar osäkerhet, men också att det faktiskt verifieras att säkerhet inte blir en onödigt stor bromskloss, utan att det blir proportionerligt.

Av uppföljningen framgår att ledningens genomgång för den politiska ledningen genomförs regelbundet i 166 (ca 57%) av kommunerna, motsvarande siffra vid uppföljningen 2019 var 79 (ca 27%) av kommunerna.

Figur 16 Information till ledningen, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

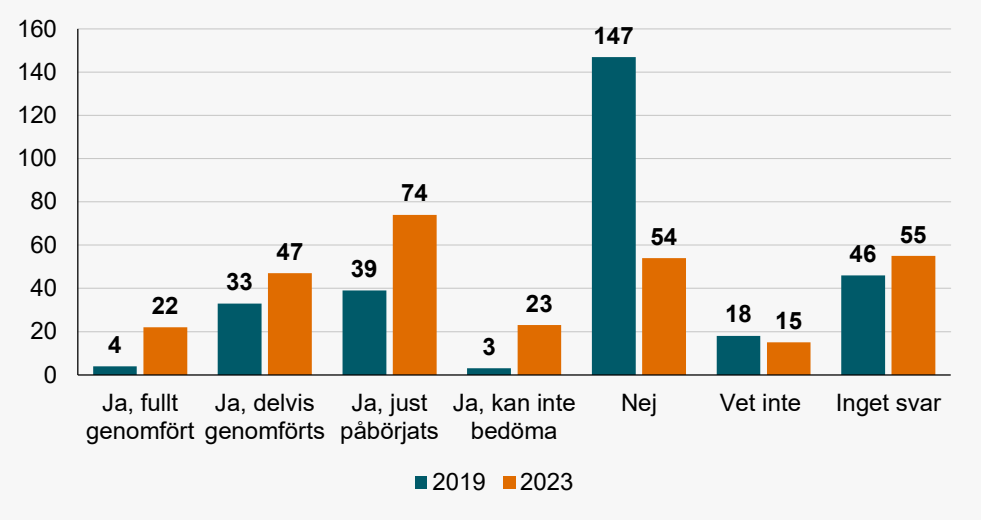
- Kommungrupp A, som genomför ledningens genomgång, har ökat från 8 till 26, en ökning med ca 325%.
- Kommungrupp B, som genomför ledningens genomgång, har ökat från 30 till 65, en ökning med ca 217%.

- Kommungrupp C, som genomför ledningens genomgång, har ökat från 41 till 75, en ökning med ca 83%.

Den positiva utvecklingen i trenden, att fler politiska ledningar informerar sig regelbundet i informationssäkerhetsfrågor, är viktig och behöver fortsätta för att möjliggöra för kommunernas systematiska och riskbaserade informationssäkerhetsarbete att skapa tillit till kommunernas digitaliseringsresa.

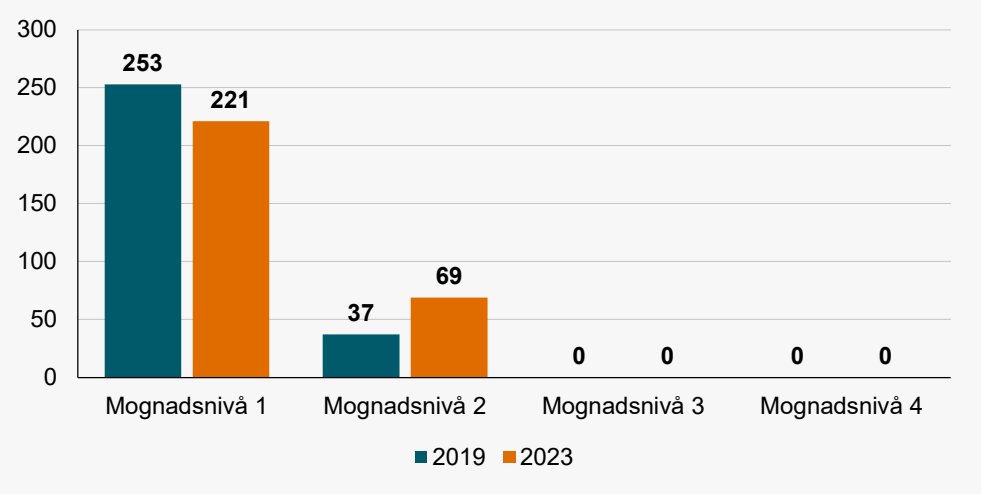
När vi bryter ner resultatet baserat på Kommungruppsindelningen blir det tydligt att den politiska ledningen insett vikten av ett systematiskt och riskbaserat informationssäkerhetsarbete och vilken roll de spelar.

Figur 17 Information till ledningen, jämförelse mellan uppföljningen 2019 och 2023.



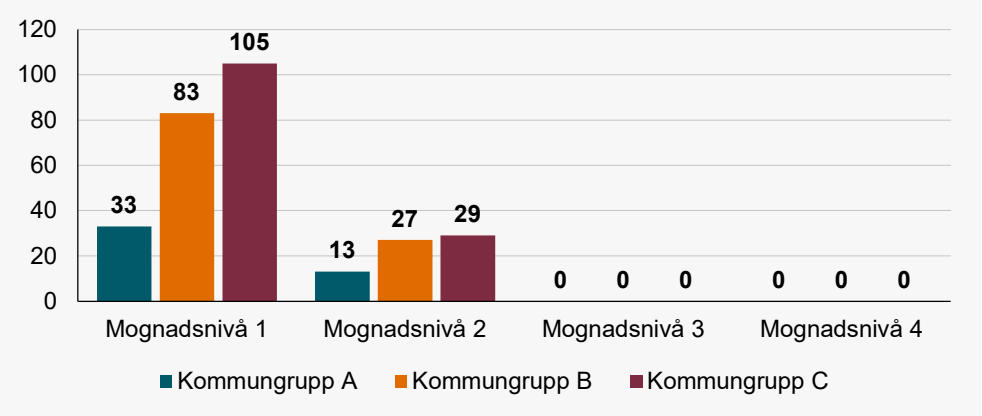
Införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete i kommunerna, där information till högsta ledningen spelar en viktig roll, har tagit flera kliv mellan 2019 och 2023.

Figur 18 Mognadsnivån för information till ledningen, jämförelse mellan uppföljningen 2019 och 2023.



Av denna uppföljning framgår att nästan en av fyra kommuner befinner sig på nivå 2 i mognadsmodellen avseende ledningens engagemang. Detta ska jämföras med att en av tio kommuner befann sig på denna nivå 2019.

Figur 19 Mognadsnivån för information till ledningen, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som genomför ledningens genomgång, har ökat från 6 (ca 13%) till 13 (ca 28%) på mognadsnivå 2, vilket motsvarar en ökning med ca 217%.

- Kommungrupp B, som genomför ledningens genomgång, har ökat från 11 (ca 10%) till 27 (ca 25%) på mognadsnivå 2, vilket motsvarar en ökning med ca 246%.
- Kommungrupp C, som genomför ledningens genomgång, har ökat från 20 (ca 15%) till 29 (ca 22%) på mognadsnivå 2, vilket motsvarar en ökning med ca 45%.

Av mätningen framgår att genomförandet av ledningens genomgång har ökat mest i kommungrupp B, följt av kommungrupp A. För kommungrupp C är ökningen inte fullt lika stor, vilket kan förklaras av att merparten av politikerna utgörs, i större omfattning, av personer med andra jobb eller studier som sin huvudsakliga syssla.

Kommunerna är på väg i rätt riktning, men har fortsatt mycket arbete framför sig.

Styrande dokument

Beskrivning av området

Det är de styrande dokumenten som lägger grunden för ett systematiskt och riskbaserat informationssäkerhetsarbete inom kommunen. De styrande dokumenten bör följa den interna strukturen gällande alla styrdokument inom kommunen.

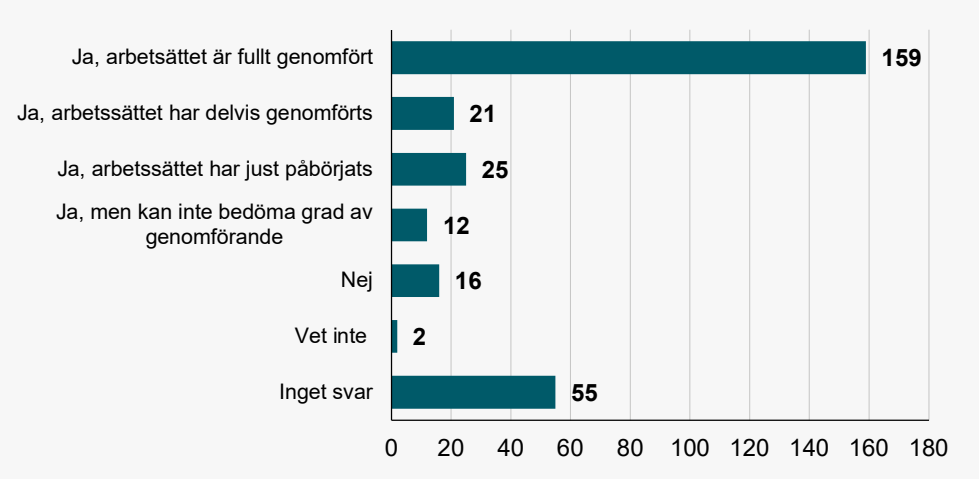
Informationssäkerhetspolicyn är ledningens viljeyttring vad avser informationssäkerhetens inriktning och ger det strategiska perspektivet. Informationssäkerhetspolicyn, som är vägledande för de andra styrdokumenten, svarar på frågor såsom vad informationssäkerhet är, ambitioner och mål, vem som ansvarar för vad på övergripande nivå.

Policyn konkretiseras genom övriga styrande dokument, t.ex. riktlinjer, anvisningar, rutiner eller vägledningar för informationssäkerhet. Dessa dokument berättar mer i detalj vad som gäller för organisationens systematiska och riskbaserade informationssäkerhetsarbete för olika målgrupper i verksamheten.

De styrande dokumenten ger förutsättningar för att det systematiskt och riskbaserat informationssäkerhetsarbete ska få en djup förankring i verksamheten. Dessa dokument är grunden för att säkerhetsarbetet genomförs på ett strukturerat sätt. De är också viktiga att ha för att kunna granska informationssäkerhetsarbetet.

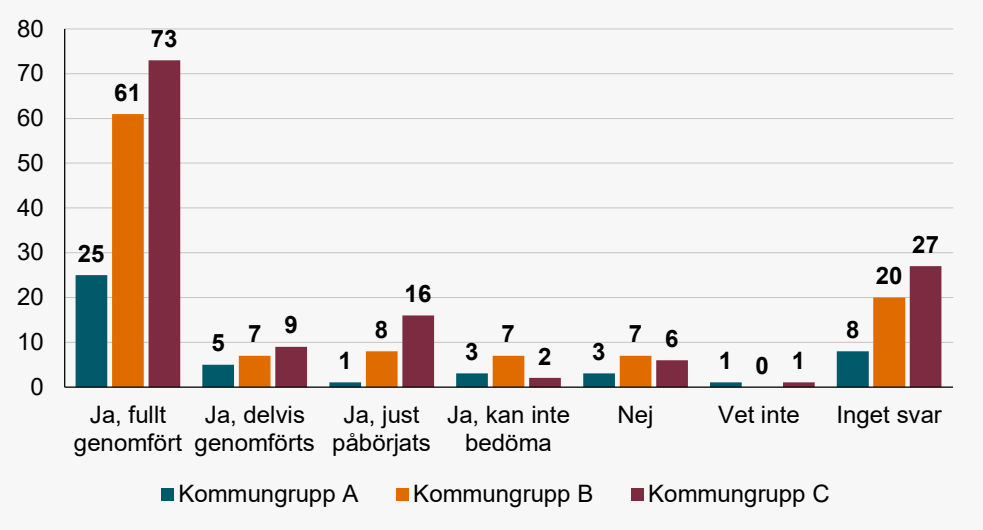
Erhållna svar

Figur 20 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att kommunens informationssäkerhetspolicy fastställs?



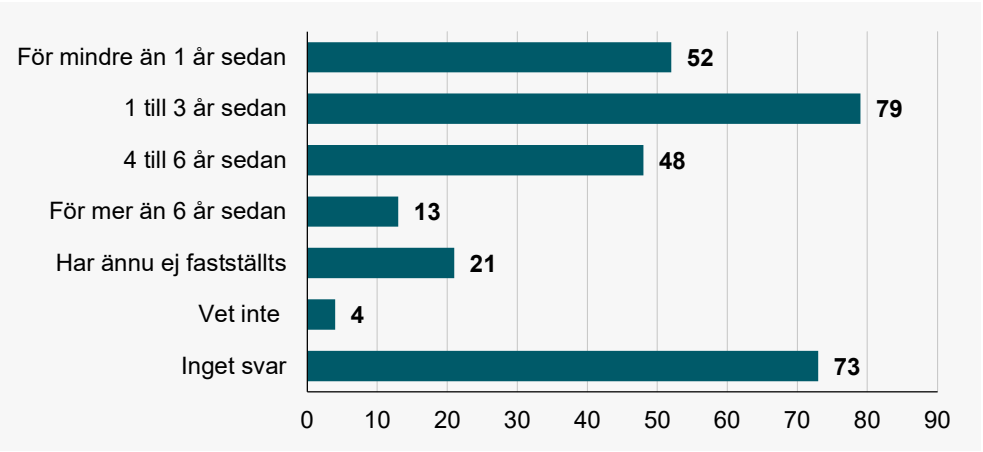
Av svaren framgår att i 159 (ca 55%) av kommunerna har kommunen fullt etablerat en informationssäkerhetspolicy. I 21 (ca 7%) av kommunerna har kommunen delvis genomfört ett arbete med att ta fram och besluta om informationssäkerhetspolicyn. I 25 (ca 9%) av kommunerna har kommunen påbörjat ett arbete med att ta fram och besluta om informationssäkerhetspolicyn.

Figur 21 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att kommunens informationssäkerhetspolicy fastställs, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 25 (ca 54%) av kommungrupp A, i 61 (ca 56%) av kommungrupp B och i 73 (ca 55%) av kommungrupp C har kommunen en fullt etablerat informationssäkerhetspolicy.

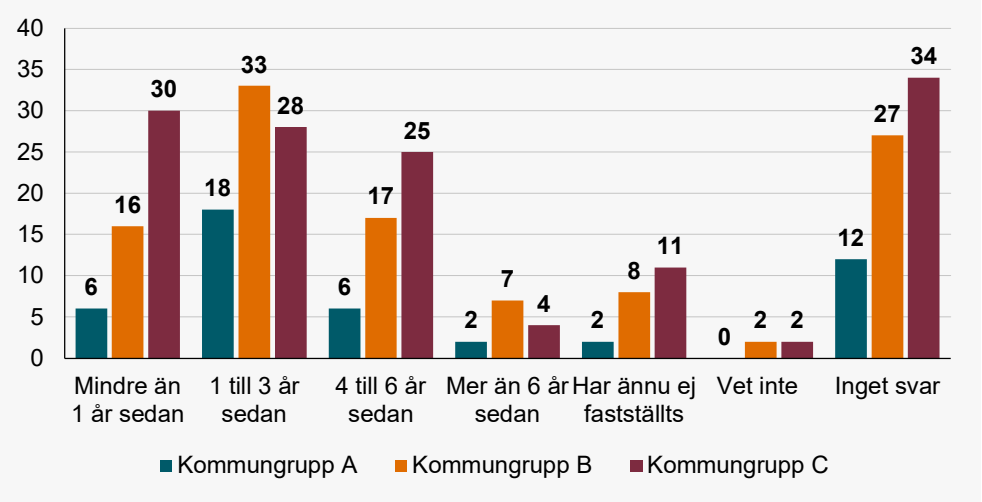
Figur 22 När fastställdes/reviderades kommunens nuvarande informationssäkerhetspolicy?



Av svaren framgår att i 52 (ca 18%) av kommunerna har kommunens informationssäkerhetspolicy fastställts för mindre än ett år sedan. I 79 (ca 27%) av

kommunerna har kommunens informationssäkerhetspolicy fastställts för 1 till 3 år sedan.

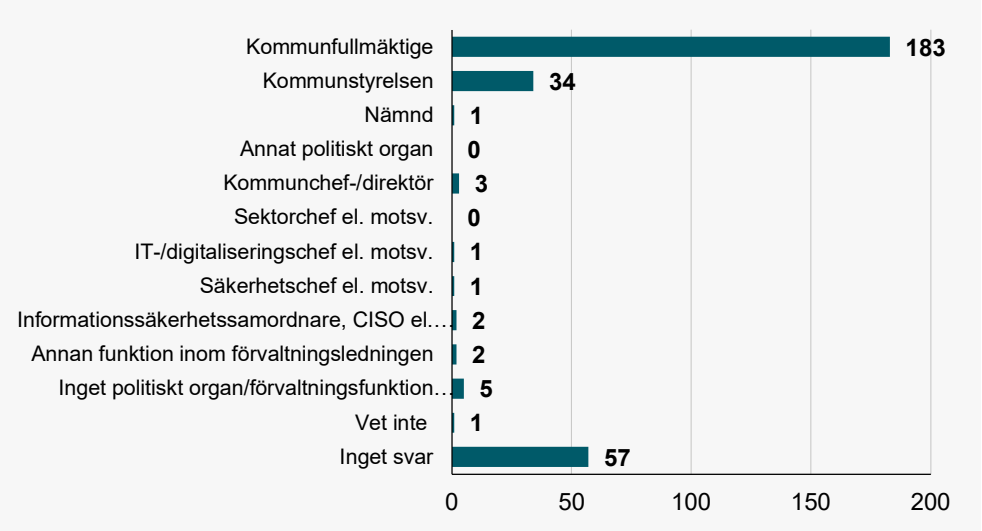
Figur 23 När fastställdes/reviderades kommunens nuvarande informationssäkerhetspolicy, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 18 (ca 39%) av kommungrupp A och i 33 (ca 30%) av kommungrupp B har kommunens informationssäkerhetspolicy fastställts för ett till tre år sedan, medans det framgår att i 30 (ca 8%) av kommungrupp C har kommunens informationssäkerhetspolicy fastställts för mindre än ett år sedan.

Figur 24 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor?

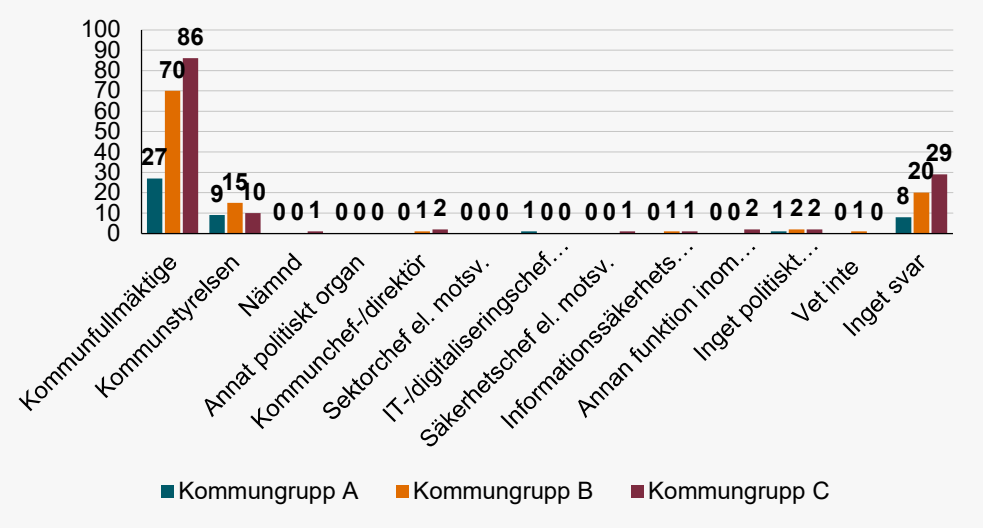
- Övergripande strategiska styrdokument (t.ex. mål, vision, program)



Av svaren framgår att i 183 (ca 63%) av kommunerna är det Kommunfullmäktige som beslutat om övergripande strategiska styrdokument (t.ex. mål, vision, program) och i 34 (ca 12%) av kommunerna är det Kommunstyrelsen som beslutat om övergripande strategiska styrdokument (t.ex. mål, vision, program).

Figur 25 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.

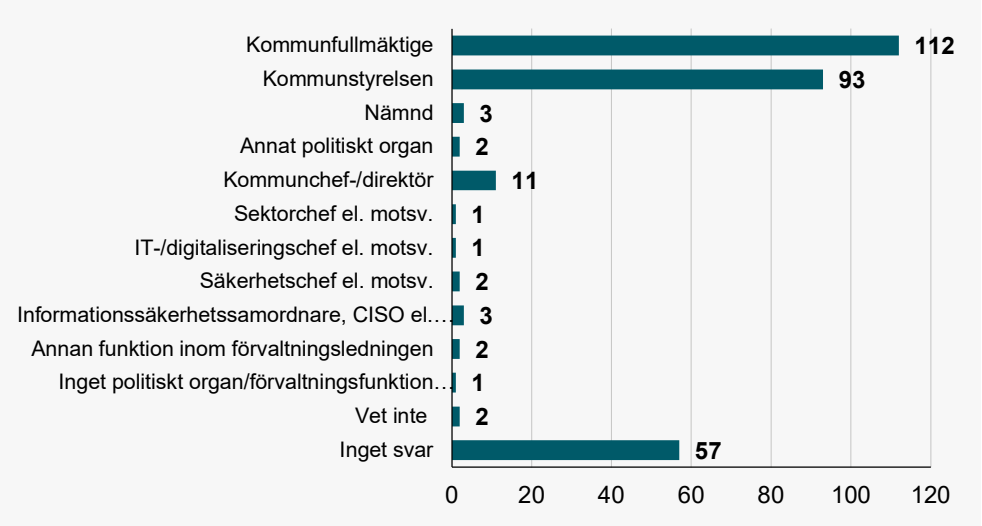
- Övergripande strategiska styrdokument (t.ex. mål, vision, program)



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 27 (ca 59%) av kommungrupp A, i 70 (ca 64%) av kommungrupp B i 86 (ca 64%) av kommungrupp C är det Kommunfullmäktige som beslutat om övergripande strategiska styrdokument (t.ex. mål, vision, program).

Figur 26 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor?

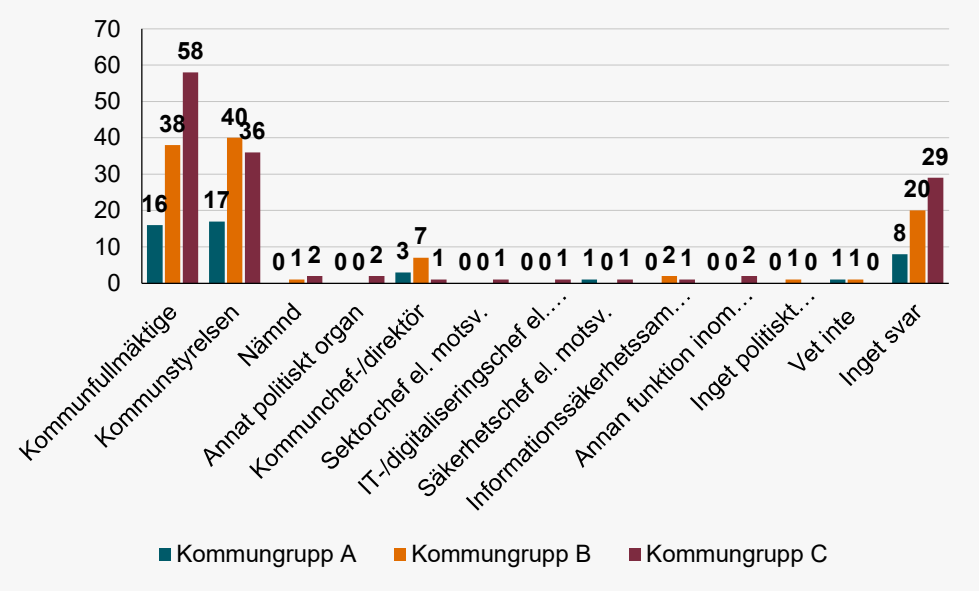
- Handlingsinriktade styrdokument (t.ex. policy, handlingsplan)



Av svaren framgår att i 112 (ca 39%) av kommunerna är det Kommunfullmäktige som beslutat om handlingsinriktade styrdokument (t.ex. policy, handlingsplan). I 93 (ca 32%) av kommunerna är det Kommunstyrelsen som beslutat om handlingsinriktade styrdokument (t.ex. policy, handlingsplan).

Figur 27 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.

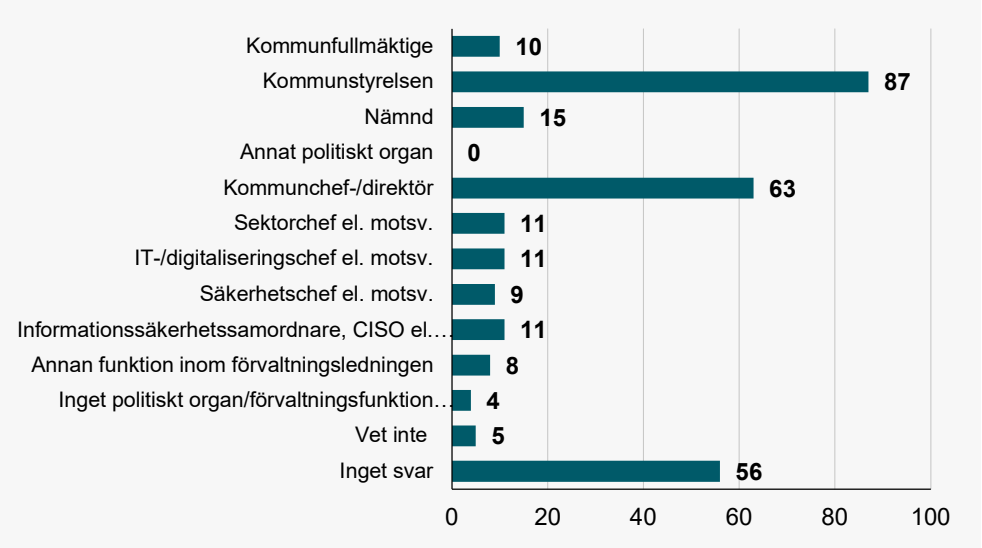
- Handlingsinriktade styrdokument (t.ex. policy, handlingsplan)



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 17 (ca 37%) av kommungrupp A och i 40 (ca 36%) av kommungrupp B är det Kommunstyrelsen som beslutat om handlingsinriktade styrdokument (t.ex. policy, handlingsplan), medans det framgår att i 58 (ca 43%) av kommungrupp C är det Kommunfullmäktige som beslutat om handlingsinriktade styrdokument (t.ex. policy, handlingsplan).

Figur 28 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor?

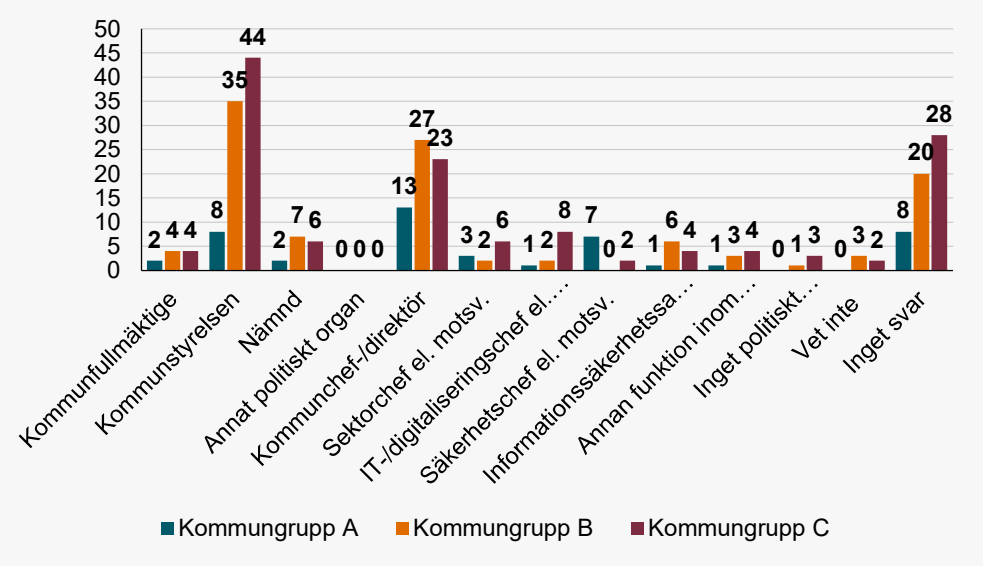
- Konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler)



Av svaren framgår att i 87 (ca 30%) av kommunerna är det Kommunstyrelsen som beslutat om konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler). I 63 (ca 22%) av kommunerna är det Kommunchef-/direktör som beslutat om konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler).

Figur 29 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.

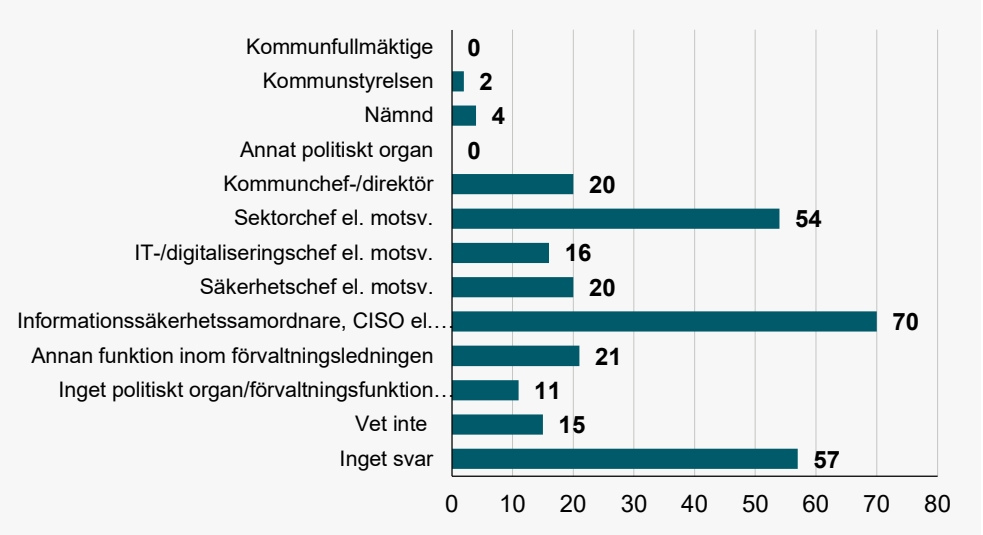
- Konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler)



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 13 (ca 28%) av kommungrupp A är det Kommunchef-/direktör som beslutat om konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler), medans det framgår att i 35 (ca 32%) av kommungrupp B och i 44 (ca 33%) av kommungrupp C är det Kommunstyrelsen som beslutat om konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler).

Figur 30 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor?

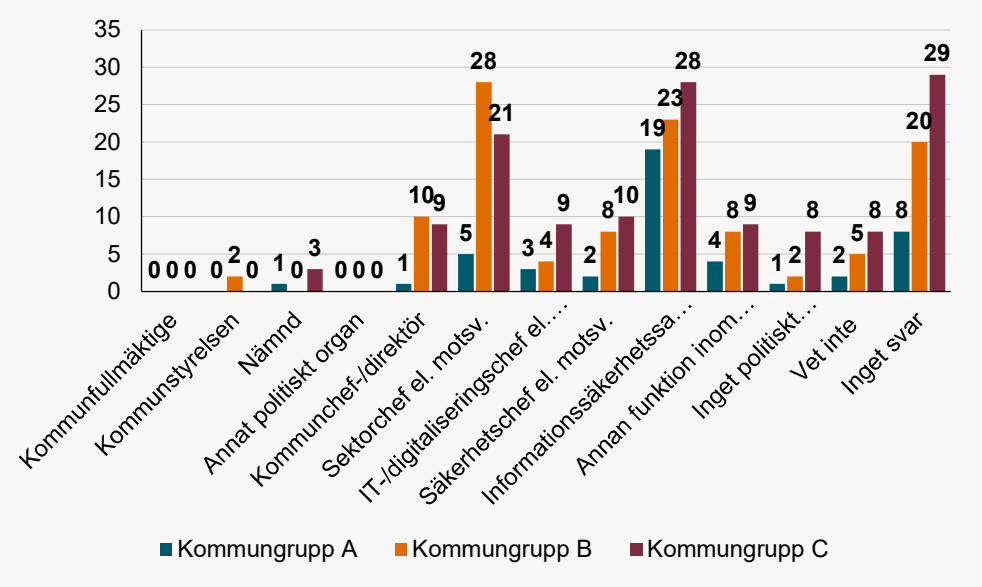
- Praktiska frågor i den löpande verksamheten



Av svaren framgår att i 70 (ca 24%) av kommunerna är det Informationssäkerhetssamordnare, CISO el. motsv. som beslutat i praktiska frågor i den löpande verksamheten och i 54 (ca 19%) av kommunerna är det Sektorchef el. motsv. som beslutat i praktiska frågor i den löpande verksamheten.

Figur 31 Vilket politiskt organ eller förvaltningsfunktion inom kommunen beslutar främst i nedanstående informationssäkerhetsfrågor, uppdelat enligt Kommungruppsindelning.

- Praktiska frågor i den löpande verksamheten



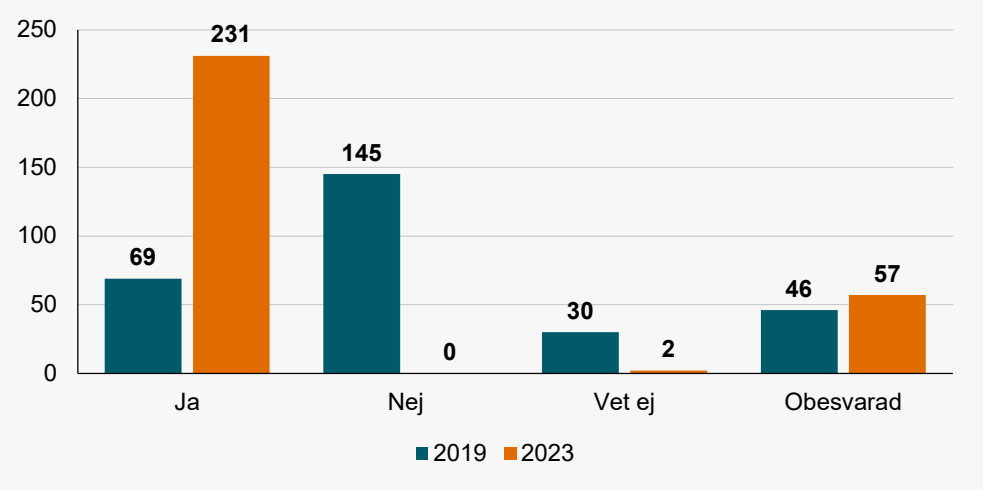
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 19 (ca 41%) av kommungrupp A och i 28 (ca 21%) av kommungrupp C är det Informationssäkerhetssamordnare, CISO el. motsv. som beslutat i praktiska frågor i den löpande verksamheten, medans det framgår att i 28 (ca 26%) av kommungrupp B är det Sektorchef el. motsv. som beslutat i praktiska frågor i den löpande verksamheten.

lakttagelser

För att kommunerna ska lyckas i sitt införande av ett systematiskt och riskbaserat informationssäkerhetsarbete är det avgörande att det styrande dokumenten (t.ex. policy, riktlinjer och anvisningar) omsätts i konkreta handlingsplaner, med aktiviteter.

Av uppföljningen framgår att handlingsinriktade styrdokument (t.ex. policy, handlingsplan) fastställs av Kommunfullmäktige i 112 (ca 39%) av kommunerna och av Kommunstyrelsen i 93 (ca 32%) av kommunerna.

Figur 32 Fastställs handlingsinriktade styrdokument (t.ex. policy, handlingsplan) i kommunen, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som fastställer handlingsinriktade styrdokument, har ökat från 11 (ca 24%) till 37 (ca 80%), vilket motsvarar en ökning med ca 336%.
- Kommungrupp B, som fastställer handlingsinriktade styrdokument, har ökat från 25 (ca 23%) till 89 (ca 81%), vilket motsvarar en ökning med ca 356%.
- Kommungrupp C, som fastställer handlingsinriktade styrdokument, har ökat från 33 (ca 24%) till 105 (ca 78%), vilket motsvarar en ökning med ca 318%.

Den positiva utvecklingen i att det inte bara är fler politiska ledningar som informerar sig regelbundet i informationssäkerhetsfrågor, utan också fastställer övergripande strategiska styrdokument (t.ex. mål, vision, program), ger en bra grund för det fortsatta arbetet för kommunernas systematiska och riskbaserade informationssäkerhetsarbete. Det är med fördel längre ner i kommunens ledningsstruktur som handlingsinriktade styrdokument (t.ex. handlingsplan) och konkreta normerande styrdokument (t.ex. riktlinjer och instruktioner) fastställs.

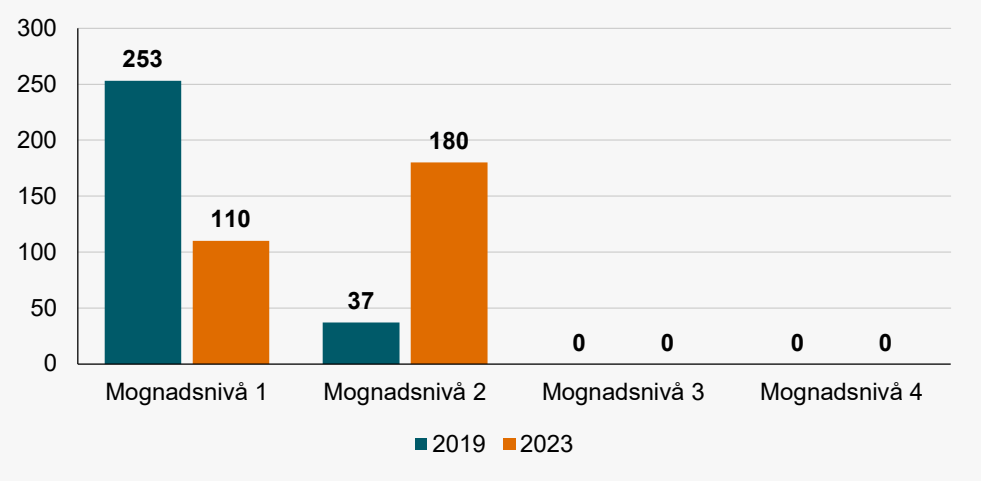
Av uppföljningen framgår att i 232 kommuner finns fastställda övergripande strategiska styrdokument (t.ex. mål, vision, program), i 231 kommuner finns fastställda handlingsinriktade styrdokument (t.ex. policy, handlingsplan) och i 229

kommuner finns fastställda konkreta normerande styrdokument (t.ex. riktlinje, instruktion, regler).

Det framgår av uppföljningen att ökningen av kommuner som fastställer handlingsinriktade styrdokument är relativt jämförbar mellan kommungrupp A, B och C.

Genom att applicera uppskattat genomförandevärde för fastställande av kommunens informationssäkerhetspolicy på fastställande av handlingsinriktade styrdokument (t.ex. policy, handlingsplan) får vi möjligheten att jämföra med uppföljningen från 2019.

Figur 33 Mognadsnivån för att omsätta ledningens mål till konkreta handlingsplaner, jämförelse mellan uppföljningen 2019 och 2023.



Av denna uppföljning framgår att mer än sex av tio kommuner befinner sig på nivå 2 i mognadsmodellen avseende att omsätta ledningens mål till konkreta handlingsplaner. Detta ska jämföras med att en av tio kommuner befann sig på denna nivå 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som fastställer handlingsinriktade styrdokument, har ökat från 7 (ca 15%) till 30 (ca 65%) på mognadsnivå 2, vilket motsvarar en ökning med ca 429%.

- Kommungrupp B, som fastställer handlingsinriktade styrdokument, har ökat från 14 (ca 13%) till 68 (ca 62%) på mognadsnivå 2, vilket motsvarar en ökning med ca 486%.
- Kommungrupp C, som fastställer handlingsinriktade styrdokument, har ökat från 16 (ca 12%) till 82 (ca 61%) på mognadsnivå 2, vilket motsvarar en ökning med ca 513%.

Det framgår av uppföljningen att ökningen av kommuner där ledningens mål omsätts till konkreta handlingsplaner är relativt jämförbar mellan kommungrupp A, B och C. De stora siffrorna visar på att kommunerna har kommit relativt långt i införandet av ett etablerat arbetssätt så att kommunledningens mål omsätts i konkreta handlingsplaner, kommunerna är mer mogna inom detta område än vid uppföljningen 2019.

Hantering av informationssäkerhetsrisker

Beskrivning av området

Hantering av informationssäkerhetsrisker är att betrakta som en central del i det systematiska och riskbaserade informationssäkerhetsarbetet.

Riskhantering är en process där kommunen på ett systematiskt sätt identifierar, bedömer, prioriterar, analyserar och förebygger potentiella risker för att skydda sina resurser och vidta lämpliga åtgärder för att minimera, övervaka och kontrollera sannolikheten eller inverkan kopplat till oönskade händelser.

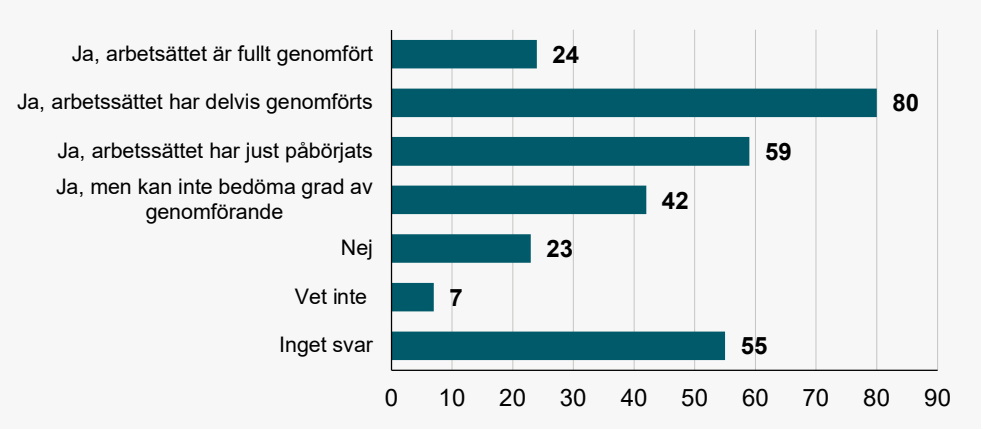
Riskanalysen (identifiera, bedöma, prioritera, analysera) syftar till att skapa ett beslutsunderlag som identifierar de väsentliga riskerna avseende informationssäkerhet. Verksamheten kan på så sätt bedöma och prioritera riskerna. Risker som inte kan accepteras behöver sedan åtgärdas på ett ändamålsenligt sätt.

För att vara effektiva ska riskanalyser ske regelbundet och/eller inför förändringar som kan tänkas påverka riskerna eller införa nya risker. Identifiering av risker behöver inkludera allt från informationsteknik, processer, till sättet att styra informationssäkerheten.

Vid riskanalyser är det centralt att säkerställa att upprepade bedömningar av informationssäkerhetsrisker genererar konsistenta, korrekta och jämförbara resultat.

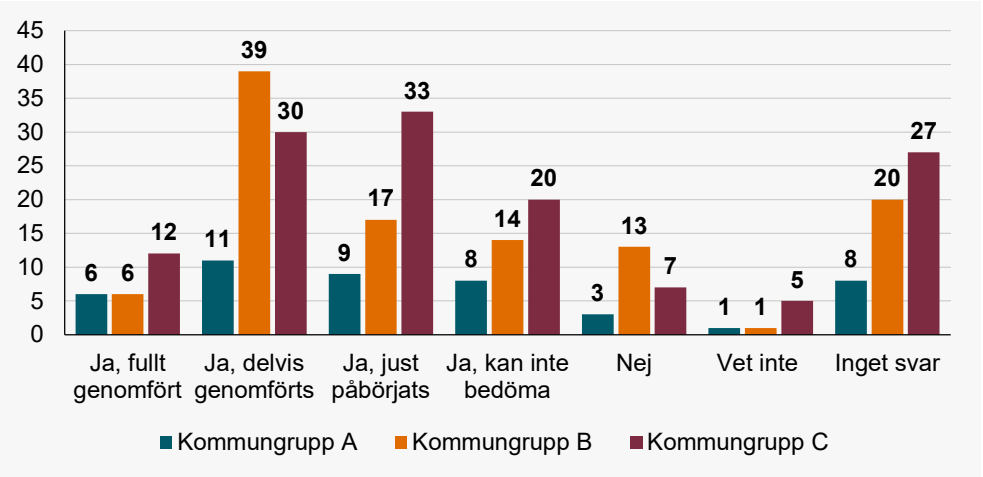
Erhållna svar

Figur 34 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsrisker hanteras?



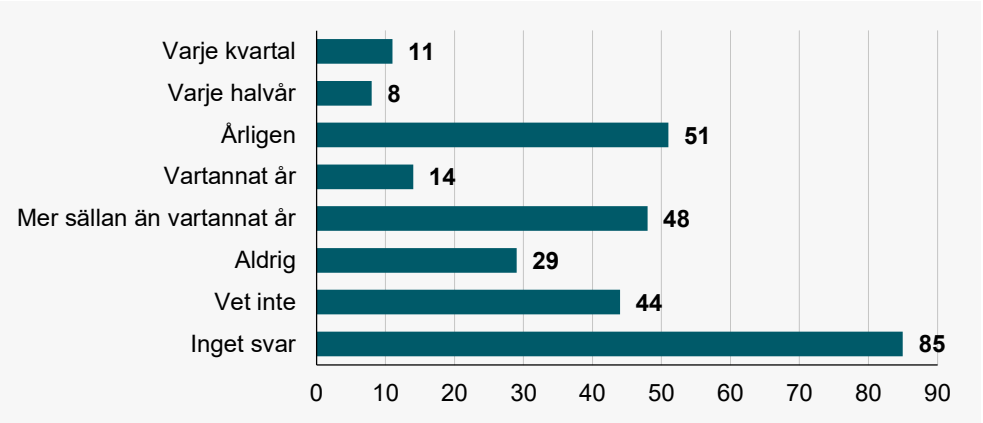
Av svaren framgår att i 24 (ca 8%) av kommunerna har ett fullt genomfört arbete så att informationssäkerhetsrisker hanteras, i 80 (ca 28%) av kommunerna har ett arbete delvis genomförts så att informationssäkerhetsrisker hanteras och i 59 (ca 20%) av kommunerna har ett arbete just påbörjats så att informationssäkerhetsrisker hanteras.

Figur 35 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsrisker hanteras, uppdelat enligt Kommungruppsindelning.



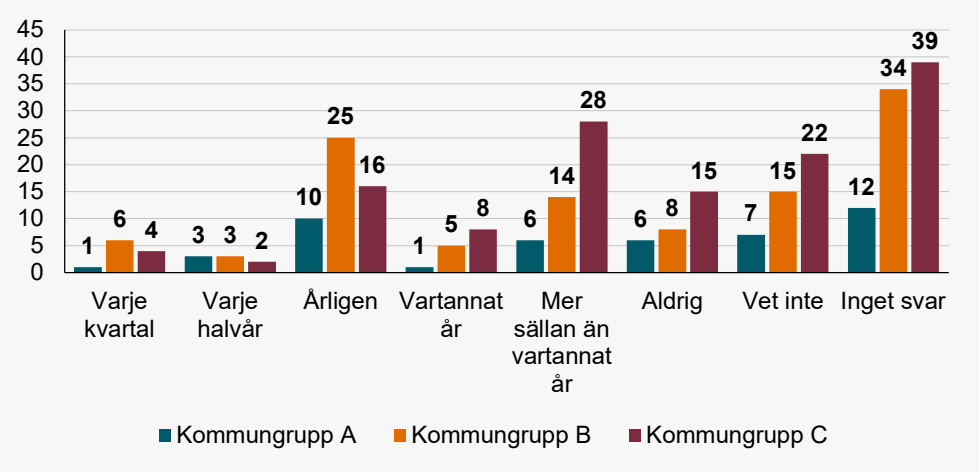
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 11 (ca 24%) av kommungrupp A och i 39 (ca 36%) av kommungrupp B har ett arbete delvis genomförts så att informationssäkerhetsrisker hanteras, medans det framgår att i 33 (ca 25%) av kommungrupp C har ett arbete just påbörjats så att informationssäkerhetsrisker hanteras.

Figur 36 Med vilken frekvens har kommunens analyser av informationssäkerhetsrisker genomförts under de senaste tre åren?



Av svaren framgår att i 11 (ca 4%) av kommunerna har informationssäkerhetsrisker analyserats varje kvartal under de 3 senaste åren, i 8 (ca 3%) av kommunerna har informationssäkerhetsrisker analyserats varje halvår under de 3 senaste åren och i 51 (ca 18%) av kommunerna har informationssäkerhetsrisker analyserats årligen under de 3 senaste åren.

Figur 37 Med vilken frekvens har kommunens analyser av informationssäkerhetsrisker genomförts under de senaste tre åren, uppdelat enligt Kommungruppsindelning.



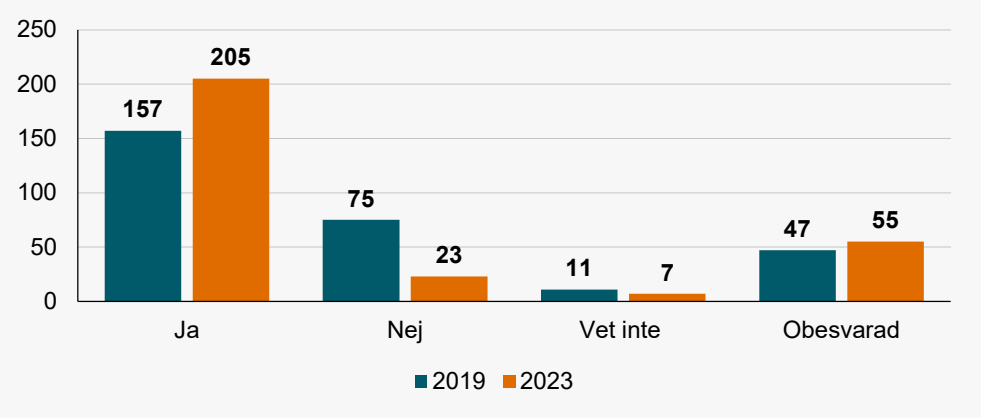
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 10 (ca 22%) av kommungrupp A och i 25 (ca 23%) av kommungrupp B har informationssäkerhetsrisker analyserats årligen under de 3 senaste åren, medans det framgår att i 28 (ca 21%) av kommungrupp C har informationssäkerhetsrisker analyserats mer sällan än vartannat år.

lakttagelser

För att kommunerna ska lyckas i sitt införande av ett systematiskt och riskbaserat informationssäkerhetsarbete är det avgörande att kommunen har en väl förankrad process för riskhantering.

Av uppföljningen framgår att 205 (ca 71%) av kommunerna har en fastställd process för hantering av informationssäkerhetsrisker, vilket kan jämföras med uppföljningen från 2019 då 157 (ca 54%) av kommunerna hade en fastställd process för hantering av informationssäkerhetsrisker.

Figur 38 Har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsrisker hanteras, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för hantering av informationssäkerhetsrisker, har ökat från 27 (ca 59%) till 34 (ca 74%), vilket motsvarar en ökning med ca 26%.
- Kommungrupp B, som har en fastställd process för hantering av informationssäkerhetsrisker, har ökat från 51 (ca 47%) till 76 (ca 69%), vilket motsvarar en ökning med ca 49%.
- Kommungrupp C, som har en fastställd process för hantering av informationssäkerhetsrisker, har ökat från 79 (ca 58%) till 95 (ca 71%), vilket motsvarar en ökning med ca 20%.

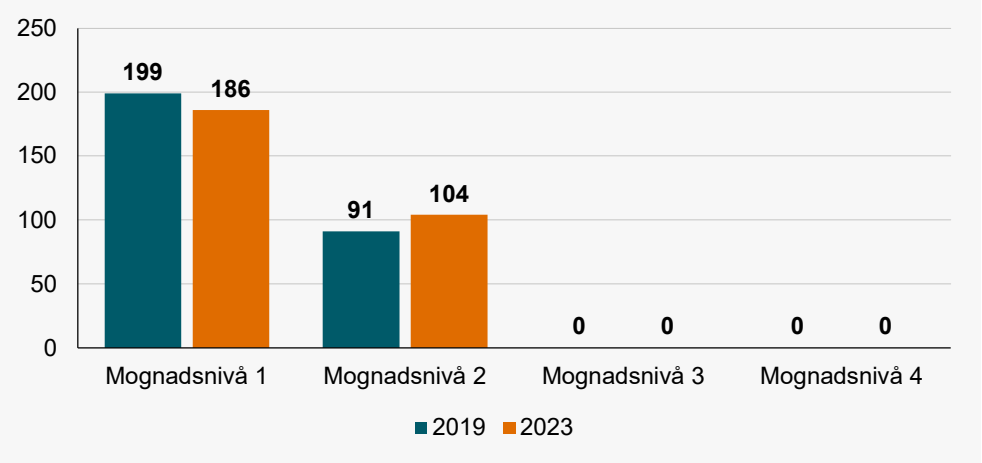
Det är positivt att mer än 7 av 10 kommuner har en process för hantering av informationssäkerhetsrisker, detta i jämförelse med uppföljningen 2019 då det var ungefär 5 av 10 kommuner som hade en process för hantering av informationssäkerhetsrisker. Det visar att riskhantering fortsatt är en central del av kommunernas systematiska informationssäkerhetsarbete.

Det framgår av uppföljningen att ökningen av kommuner som har en fastställd process för hantering av informationssäkerhetsrisker är störst för kommungrupp B, ökningen är något lägre men relativt jämförbar mellan kommungrupp A och C.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för hantering av informationssäkerhetsrisker har ökat, men när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi inte samma utveckling som inom andra områden

för denna uppföljning. Det är 104 kommuner som hamnar på mognadsnivå 2 inom riskhantering, vilket är en ökning med 13 kommuner sedan 2019.

Figur 39 Mognadsnivån för hantering av informationssäkerhetsrisker, jämförelse mellan uppföljningen 2019 och 2023.



Mognadsnivån inom riskhantering, där mer än sex av tio kommuner befinner sig på nivå 1 gör att vi fortsatt har ett stort arbete framför oss inom detta område.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för hantering av informationssäkerhetsrisker, har minskat från 19 (ca 41%) till 17 (ca 37%) på mognadsnivå 2, vilket motsvarar en minskning med ca 11%.
- Kommungrupp B, som har en fastställd process för hantering av informationssäkerhetsrisker, har ökat från 28 (ca 26%) till 45 (ca 41%) på mognadsnivå 2, vilket motsvarar en ökning med ca 61%.
- Kommungrupp C, som har en fastställd process för hantering av informationssäkerhetsrisker, har minskat från 44 (ca 32%) till 42 (ca 31%) på mognadsnivå 2, vilket motsvarar en minskning med ca 5%.

Det blir lite blandat när vi bryter ner mognadsnivån i enlighet med Kommungruppsindelningen, det framgår av uppföljningen att antalet kommuner på mognadsnivå 2 inom både kommungrupp A och C har minskat något. Det är ökningen bland kommungrupp B som väger upp och renderar i en total ökning av

antalet kommuner på mognadsnivå 2 avseende att införa ett etablerat arbetssätt så att informationssäkerhetsrisker hanteras inom kommunerna.

Klassificering av informationstillgångar

Beskrivning av området

Informationsklassificering är en av de grundläggande aktiviteterna inom ett systematiskt och riskbaserat informationssäkerhetsarbete.
Informationsklassificering innebär att informationstillgångarna klassificeras utifrån det värde den har för de verksamheter/processer som använder informationen, samt de legala krav som informationen omfattas av. I samband med informationsklassningen tilldelas informationstillgången en skyddsnivå.

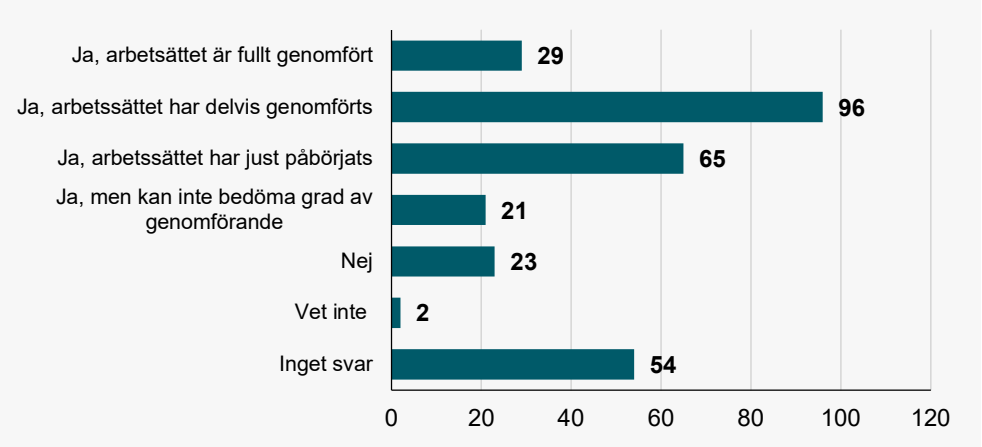
Informationsklassning syftar till att öka medvetenheten om vilka negativa konsekvenser som kan drabba kommunen om inte tillräckligt skydd av informationens konfidentialitet, riktighet eller tillgänglighet upprätthålls.

Informationsklassning behöver göras minst en gång, men man behöver regelbundet kontrollera att klassningen fortfarande är aktuell, då informationstillgångens värde kan ändras över tid. Lämpligt är därför att klassningen ses över årligen som en del av kommunens systematiska och riskbaserade informationssäkerhetsarbete.

Dessutom behöver informationsklassning genomföras vid utveckling, större förändringar eller anskaffning av nya it-system eller andra resurser som hanterar information, för att ge underlag till kravställning.

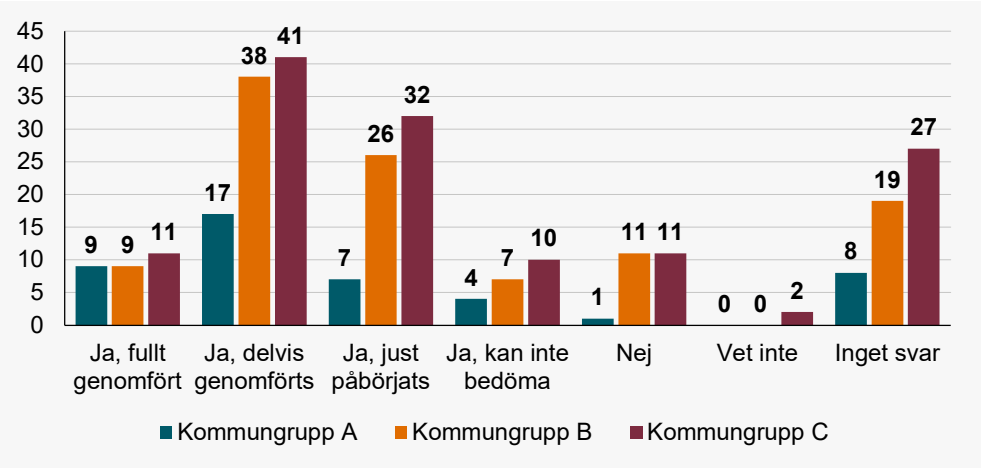
Erhållna svar

Figur 40 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationstillgångarna klassas?



Av svaren framgår att i 29 (ca 10%) av kommunerna har ett fullt etablerat arbete så att informationstillgångarna klassas, i 96 (ca 33%) av kommunerna har ett arbete delvis genomförts så att informationstillgångarna klassas. I 65 (ca 22%) av kommunerna har ett arbete påbörjats informationstillgångarna klassas.

Figur 41 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationstillgångarna klassas, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 17 (ca 37%) av kommungrupp A, i 38 (ca 35%) av kommungrupp B och i 41 (ca 31%) av

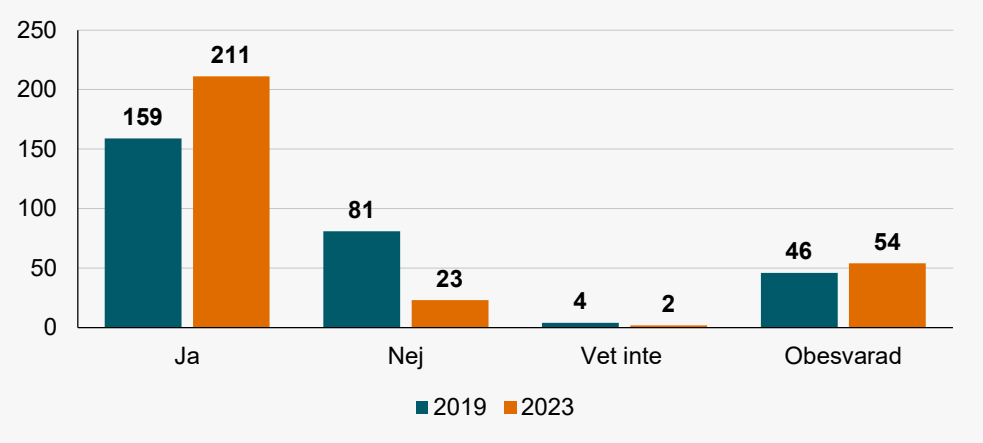
kommungrupp C har ett arbete delvis genomförts så att informationstillgångarna klassas.

Iakttagelser

För att kommunerna ska lyckas i sitt införande av ett systematiskt och riskbaserat informationssäkerhetsarbete är det avgörande att kommunen har en väl förankrad process för klassificering av informationstillgångar.

Av uppföljningen framgår att 211 (ca 73%) av kommunerna har en fastställd process för klassificering av informationstillgångar, vilket kan jämföras med uppföljningen från 2019 då 159 (ca 55%) av kommunerna hade en fastställd process för klassificering av informationstillgångar.

Figur 42 Har eller planerar er kommun att införa ett etablerat arbetssätt så att informationstillgångarna klassas, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

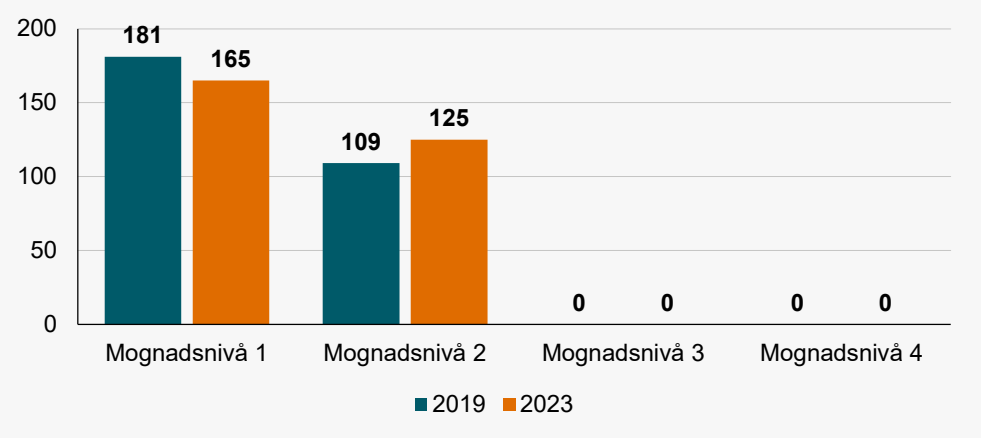
- Kommungrupp A, som har en fastställd process för klassificering av informationstillgångar, har ökat från 32 (ca 70%) till 37 (ca 80%), vilket motsvarar en ökning med ca 16%.
- Kommungrupp B, som har en fastställd process för klassificering av informationstillgångar, har ökat från 49 (ca 45%) till 80 (ca 73%), vilket motsvarar en ökning med ca 63%.
- Kommungrupp C, som har en fastställd process för klassificering av informationstillgångar, har ökat från 78 (ca 57%) till 94 (ca 70%), vilket motsvarar en ökning med ca 21%.

Det är positivt att mer än 7 av 10 kommuner har en process för klassificering av informationstillgångar, detta i jämförelse med uppföljningen 2019 då det var ungefär 5 av 10 kommuner som hade en process för klassificering av informationstillgångar. Det visar att informationsklassificering fortsatt är en viktig del av kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

Det framgår av uppföljningen att ökningen av kommuner som har en process för klassificering av informationstillgångar är störst för kommungrupp B, ökningen är något lägre men relativt jämförbar mellan kommungrupp A och C.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för klassificering av informationstillgångar har ökat, men när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi inte samma utveckling som inom andra områden för denna uppföljning. Det är 125 kommuner som hamnar på mognadsnivå 2 inom riskhantering, vilket är en ökning med 16 kommuner sedan 2019.

Figur 43 Mognadsnivån för klassificering av informationstillgångar, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för klassificering av informationstillgångar, har ökat från 24 (ca 52%) till 26 (ca 57%) på mognadsnivå 2, vilket motsvarar en ökning med ca 8%.

- Kommungrupp B, som har en fastställd process för klassificering av informationstillgångar, har ökat från 30 (ca 28%) till 47 (ca 43%) på mognadsnivå 2, vilket motsvarar en ökning med ca 57%.
- kommungrupp C, som har en fastställd process för klassificering av informationstillgångar, har minskat från 55 (ca 40%) till 52 (ca 39%) på mognadsnivå 2, vilket motsvarar en minskning med ca 6%.

Det framgår av uppföljningen att ökningen av kommuner som befinner sig på mognadsnivå 2 avseende att införa ett etablerat arbetssätt så att informationstillgångar klassificeras inom kommunerna är störst för kommungrupp B, medans ökningen för kommungrupp A är marginell. Däremot framgår det av uppföljningen att antalet kommungrupp C som befinner sig på mognadsnivå 2 avseende att införa ett etablerat arbetssätt så att informationstillgångar klassificeras inom kommunerna har minskat.

Mognadsnivån inom informationsklassificering, där nästan sex av 10 kommuner befinner sig på nivå 1 gör att vi fortsatt har ett stort arbete framför oss inom detta område.

Hantering av informationssäkerhetsincidenter

Beskrivning av området

MSB definierar incident i sitt metodstöd[4] som ”en oönskad händelse med negativa konsekvenser”. Ibland räknas även sårbarheter som ännu inte lett till negativa konsekvenser in i begreppet. Andra begrepp som används för att beskriva incidenter är till exempel problem, avvikelse, tillbud och oönskad händelse. Dessa begrepp kan också användas för att hålla isär incidenter av olika allvarlighetsgrad. En informationssäkerhetsincident är en incident som inträffar när skyddet av informationen inte är tillräckligt så att informationens konfidentialitet, riktighet eller tillgänglighet påverkas negativt.

Att organisationen har ett arbetssätt för incidenthantering är en viktig del i det systematiska och riskbaserade informationssäkerhetsarbetet. Incidenthanteringsarbetet handlar om att förbättra organisationens förmåga att minimera risken för att incidenter uppstår, minska incidenters konsekvenser, utreda

[4] https://www.informationssakerhet.se/metodstodet/

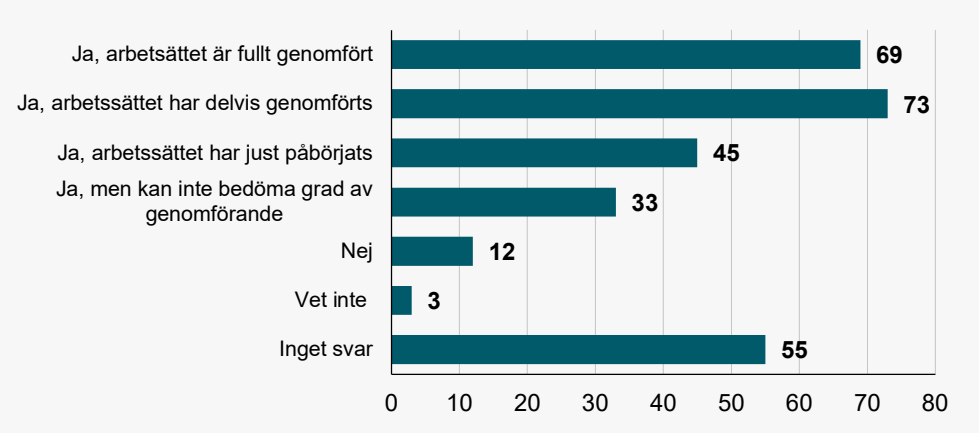
orsakerna till incidenten och därigenom förbättra skyddet så att liknande incidenter inte inträffar i framtiden.

I en del författningar finns krav på att incidenter av olika slag ska rapporteras till olika myndigheter. För att kunna rapportera behöver organisationen ha ett arbetssätt som stödjer att incidenter upptäcks, bedöms, åtgärdas och utreds samt att det framgår av arbetssättet hur rapporteringspliktiga incidenter rapporteras till rätt myndighet.

Det är värt att lägga tid på att få organisationen att arbeta så likartat som möjligt oavsett vilken typ av incident som inträffar. Det underlättar samarbetet när incidenter påverkar flera verksamheter om ni har ett liknande arbetssätt eller i alla fall ett arbetssätt som fungerar tillsammans med de andra arbetssätten.

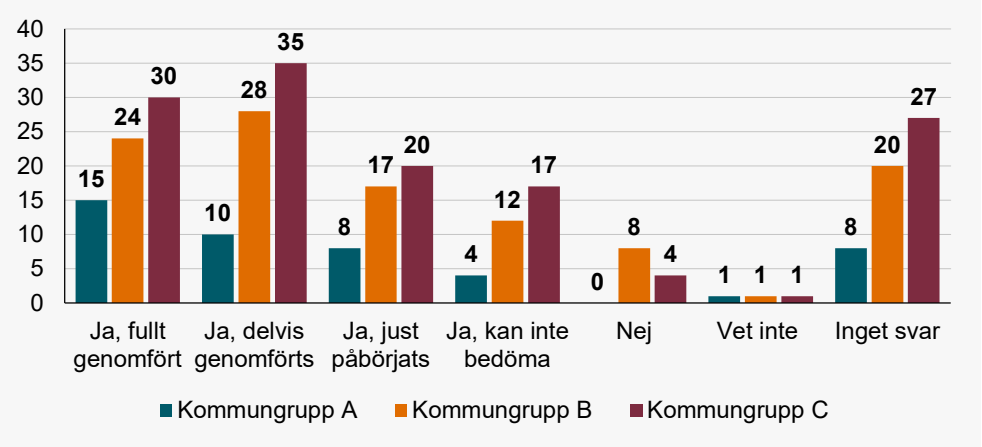
Erhållna svar

Figur 44 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsincidenter hanteras?



Av svaren framgår att i 69 (ca 24%) av kommunerna har kommunen ett fullt etablerat arbetssätt så att informationssäkerhetsincidenter hanteras, i 73 (ca 25%) av kommunerna har kommunen delvis ett etablerat arbetssätt så att informationssäkerhetsincidenter hanteras. I 45 (ca 16%) av kommunerna har ett arbete just påbörjats så att informationssäkerhetsincidenter hanteras.

Figur 45 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsincidenter hanteras, uppdelat enligt Kommungruppsindelning.



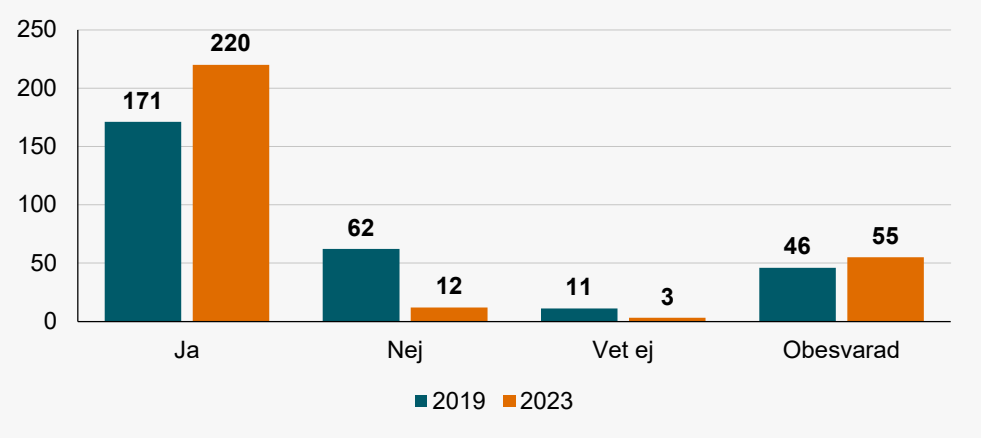
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 15 (ca 33%) av kommungrupp A har kommunen ett fullt etablerat arbetssätt så att informationssäkerhetsincidenter hanteras, medans det framgår att i 28 (ca 26%) av kommungrupp B och i 35 (ca 26%) av kommungrupp C har kommunen ett delvis genomfört arbetssätt så att informationssäkerhetsincidenter hanteras.

Iakttagelser

En väl förankrad process för hantering av informationssäkerhetsincidenter är en viktig del av kommunens systematiska och riskbaserade informationssäkerhetsarbete, en väl förankrad process för hantering av incidenter leder ofta till en minskad negativ effekt av en inträffad incident.

Av uppföljningen framgår att 220 (ca 76%) av kommunerna har en fastställd process för hantering av informationssäkerhetsincidenter, vilket kan jämföras med uppföljningen från 2019 då 171 (ca 59%) av kommunerna hade en fastställd process för hantering av informationssäkerhetsincidenter.

Figur 46 Har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetsincidenter hanteras, jämförelse mellan uppföljningen 2019 och 2023.



Det är positivt att mer än sju av tio kommuner har en process för hantering av informationssäkerhetsincidenter, jämfört med uppföljningen 2019 då det var nästan sex av tio kommuner som hade en process för hantering av informationssäkerhetsincidenter. Det visar att hantering av informationssäkerhetsincidenter fortsatt är en viktig del av kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

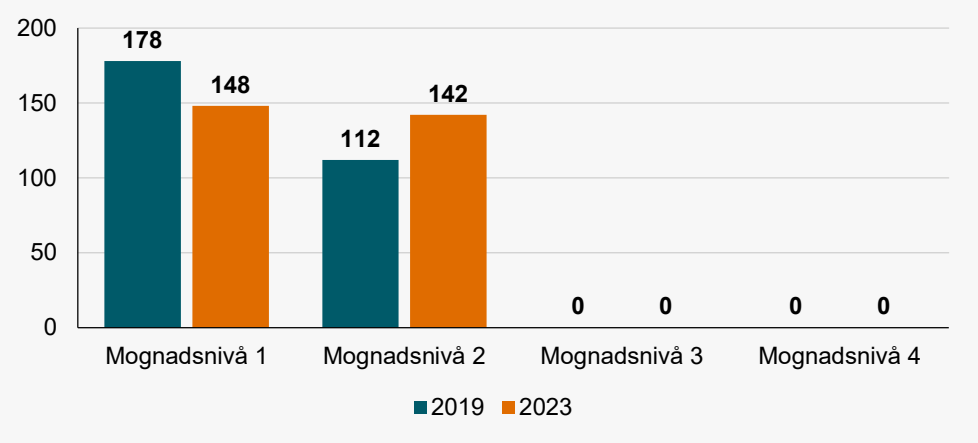
Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 27 (ca 59%) till 37 (ca 80%), vilket motsvarar en ökning med ca 37%.
- Kommungrupp B, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 59 (ca 55%) till 81 (ca 74%), vilket motsvarar en ökning med ca 37%.
- Kommungrupp C, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 85 (ca 63%) till 102 (ca 76%), vilket motsvarar en ökning med ca 20%.

När vi bryter ner siffrorna baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för hantering av informationssäkerhetsincidenter är jämförbar mellan kommungrupp A och B, medans ökningen bland kommungrupp C är något lägre.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för hantering av informationssäkerhetsincidenter har ökat, men när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi en något bättre utveckling än inom andra områden för denna uppföljning. Det är 142 kommuner som hamnar på mognadsnivå 2 inom riskhantering, vilket är en ökning med 30 kommuner sedan 2019.

Figur 47 Mognadsnivån för hantering av informationssäkerhetsincidenter, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 16 (ca 35%) till 25 (ca 54%) på mognadsnivå 2, vilket motsvarar en ökning med ca 56%.
- Kommungrupp B, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 41 (ca 38%) till 52 (ca 47%) på mognadsnivå 2, vilket motsvarar en ökning med ca 27%.
- Kommungrupp C, som har en fastställd process för hantering av informationssäkerhetsincidenter, har ökat från 55 (ca 40%) till 65 (ca 49%) på mognadsnivå 2, vilket motsvarar en ökning med ca 18%.

Av denna uppföljning framgår att nästan hälften kommunerna befinner sig på nivå två i mognadsmodellen avseende hantering av informationssäkerhetsincidenter, detta ska jämföras med att nästan fyra av tio kommuner befann sig på denna nivå 2019.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för hantering av informationssäkerhetsincidenter på mognadsnivå 2 är störst bland kommungrupp A, medans ökningen är mindre men mer jämförbar mellan kommungrupp B och C.

Med anledning av att några stora informationssäkerhetsincidenter har drabbat kommunerna de senaste åren torde nog utvecklingen ha gått något fortare.

Kontinuitetshantering

Beskrivning av området

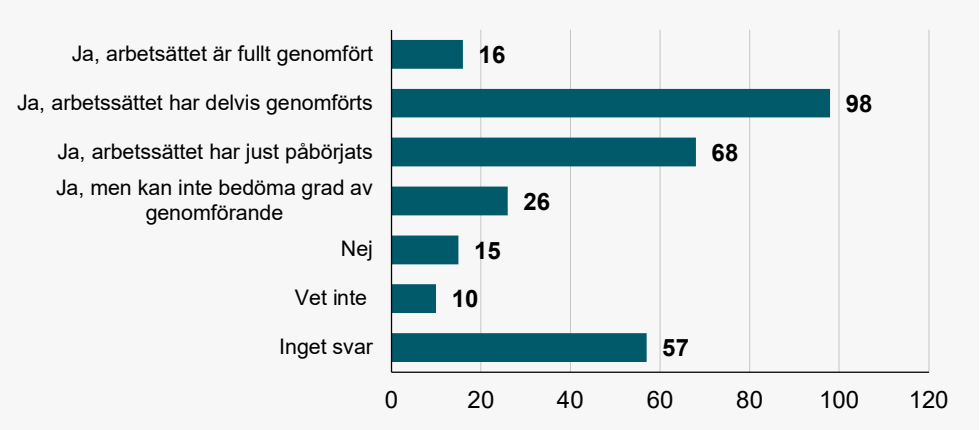
Kontinuitetshantering handlar om att planera för att upprätthålla kommunens verksamhet på en acceptabel nivå oavsett vilken störning den utsätts för. Med kontinuitetshantering kan kommuner snabbare återhämta sig från och mildra konsekvenserna av en inträffad incident (se avsnitt 5.6 Hantering av informationssäkerhetsincidenter för definition).

Det systematiska informationssäkerhetsarbetet bör vara integrerat med kommunens arbete med kontinuitetshantering.

Aktiviteter som informationsklassning, riskbedömning och bedömningar av incidenter har liksom kontinuitetshantering vissa delar gemensamt, exempelvis att göra konsekvensbedömningar. En organisation bör därför ha gemensamma, eller åtminstone kompatibla, kriterier och nivåer för bedömning av konsekvenser.

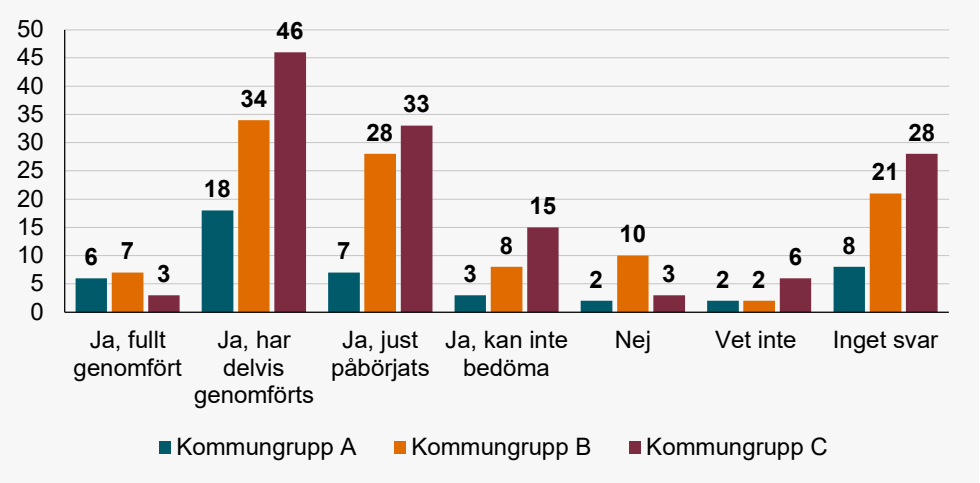
Erhållna svar

Figur 48 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs?



Av svaren framgår att i 16 (ca 6%) av kommunerna har kommunen ett fullt etablerat arbetssätt så att verksamhetens kontinuitet säkerställs, i 98 (ca 34%) av kommunerna har kommunen delvis ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs. I 68 (ca 23%) av kommunerna har ett arbete just påbörjats så att verksamhetens kontinuitet säkerställs.

Figur 49 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs, uppdelat enligt Kommungruppsindelning.



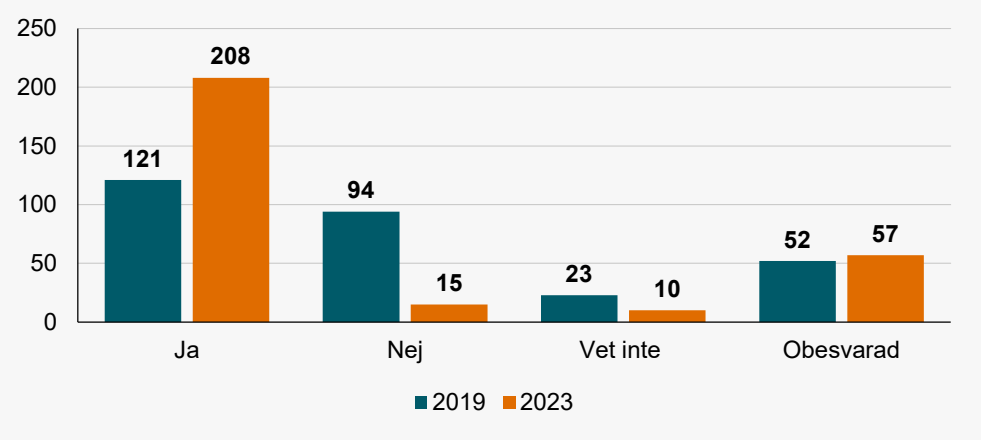
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 18 (ca 39%) av kommungrupp A, i 34 (ca 31%) av kommungrupp B och i 46 (ca 34%) av kommungrupp C har kommunen delvis ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs.

lakttagelser

En viktig del i kommunens systematiska och riskbaserade informationssäkerhetsarbete är att det finns en väl förankrad process för att säkerställa verksamhetens kontinuitet. Det behöver finnas rutiner och säkerhetsåtgärder för att förebygga och hantera avbrott i kommunens verksamhet. En kontinuitetsplan bör upprättas, införas och övas så att kritisk verksamhet kan bedrivas även vid störningar.

Av uppföljningen framgår att 208 (ca 71,7%) av kommunerna har en fastställd process för att säkerställa verksamhetens kontinuitet, vilket kan jämföras med uppföljningen från 2019 då 121 (ca 41,7%) av kommunerna hade en fastställd process för att säkerställa verksamhetens kontinuitet.

Figur 50 Har eller planerar er kommun att införa ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 21 (ca 46%) till 34 (ca 74%), vilket motsvarar en ökning med ca 62%.

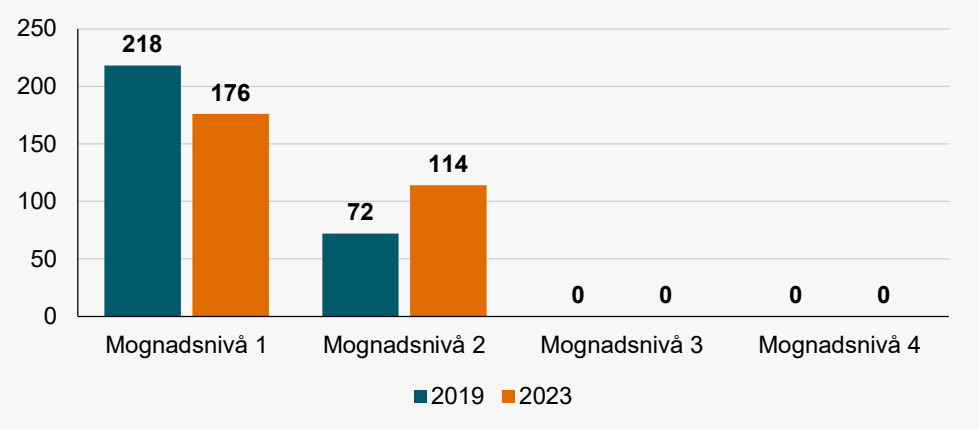
- Kommungrupp B, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 46 (ca 43%) till 77 (ca 70%), vilket motsvarar en ökning med ca 67%.
- Kommungrupp C, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 54 (ca 40%) till 97 (ca 72%), vilket motsvarar en ökning med ca 80%.

Det är positivt att mer än sju av tio kommuner har en process för att säkerställa verksamhetens kontinuitet, jämfört med uppföljningen 2019 då det var strax över fyra av tio kommuner som hade en process för att säkerställa verksamhetens kontinuitet. Det visar att arbetet med att säkerställa verksamhetens kontinuitet inom kommunerna har fått en större del av kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att säkerställa verksamhetens kontinuitet är jämförbar mellan kommungrupp A och B, med en något högre ökning bland kommungrupp C.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för att säkerställa verksamhetens kontinuitet har ökat, när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi en något bättre utveckling än inom andra områden för denna uppföljning. Det är 114 kommuner som hamnar på mognadsnivå 2 inom kontinuitetshantering, vilket är en ökning med 42 kommuner sedan 2019.

Figur 51 Mognadsnivån för att säkerställa verksamhetens kontinuitet, jämförelse mellan uppföljningen 2019 och 2023.



Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 12 (ca 26%) till 24 (ca 52%) på mognadsnivå 2, vilket motsvarar en ökning med ca 100%.
- Kommungrupp B, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 25 (ca 23%) till 41 (ca 37%) på mognadsnivå 2, vilket motsvarar en ökning med ca 64%.
- Kommungrupp C, som har en fastställd process för att säkerställa verksamhetens kontinuitet, har ökat från 35 (ca 26%) till 49 (ca 37%) på mognadsnivå 2, vilket motsvarar en ökning med ca 40%.

Av denna uppföljning framgår att nästan fyra av tio kommunerna befinner sig på nivå två i mognadsmodellen avseende att säkerställa verksamhetens kontinuitet. Detta ska jämföras med att strax över två av tio kommuner befann sig på denna nivå 2019.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att säkerställa verksamhetens kontinuitet på mognadsnivå 2 är störst bland kommungrupp A, där vi ser en dubblering av antalet kommuner. Ökningen är mindre hos kommungrupp B och minst bland kommungrupp C.

Med anledning av att några stora informationssäkerhetsincidenter har drabbat kommunerna de senaste åren behöver kontinuitetshantering få mer fokus i framtiden, då tillgången till information är central för att upprätthålla verksamhetens förmåga att producera och leverera oavsett vad som än händer.

Utbildning inom informationssäkerhet

Beskrivning av området

Alla i kommunen har någon form av kunskapsbehov när det gäller informationssäkerhet, från ledning ner till enskild medarbetare. Vilket kunskapsbehov man har beror på vilken roll man har. Det är med andra ord stor skillnad på kunskapsbehovet hos exempelvis en receptionist, en nätverkstekniker och en chef.

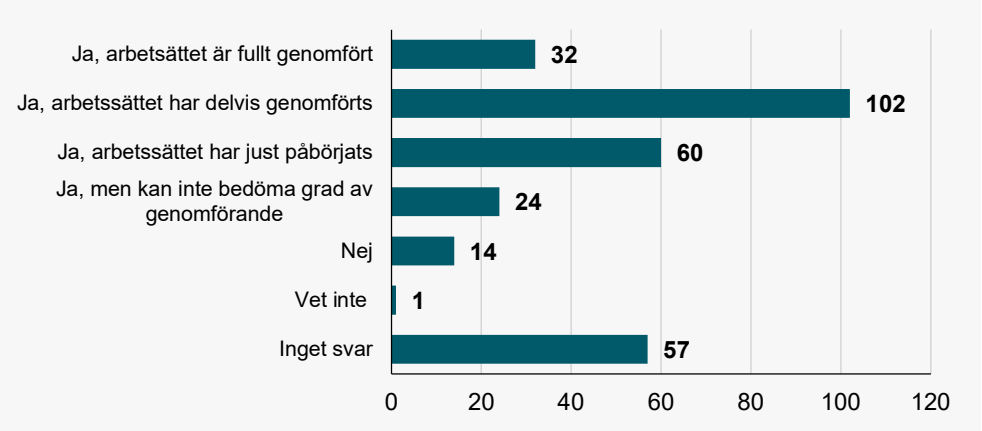
Utbildning är en väsentlig del i att upprätthålla en god nivå i informationssäkerhetsarbetet och för att bygga upp en god säkerhetskultur. Därför

ar det viktigt att anpassa utbildningen till rollernas informationssäkerhetsansvar, deras uppgifter enligt handlingsplanen, deras förväntade beteende, eller deras vilja att efterleva styrdokument.

Utbildning behöver ske, både formellt och informellt, kontinuerligt och på olika sätt och är en grundpelare i ett systematiskt och riskbaserat informationssäkerhetsarbete, utbildningen bör genomföras löpande, till och med dagligen.

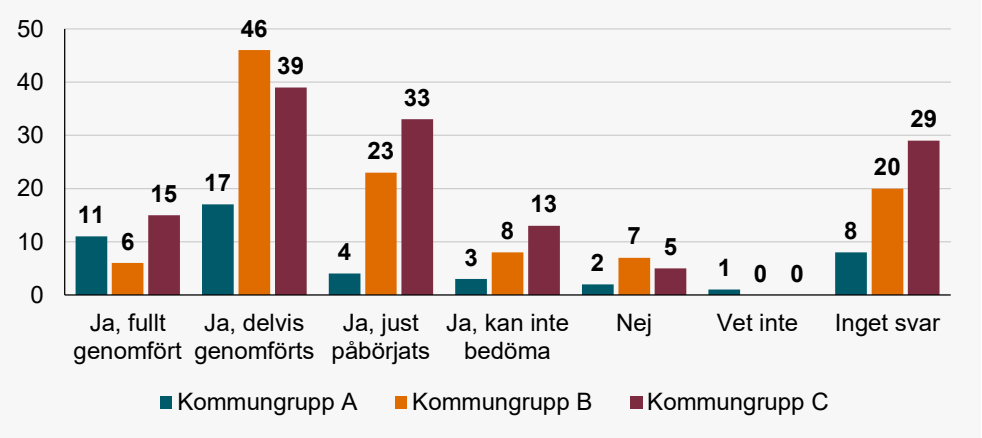
Erhållna svar

Figur 52 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs?



Av svaren framgår att i 32 (ca 11%) av kommunerna har kommunen ett fullt etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs, i 102 (ca 35%) av kommunerna har kommunen delvis ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs. I 60 (ca 21%) av kommunerna har ett arbete just påbörjats så att medarbetarnas informationssäkerhetsmedvetande säkerställs.

Figur 53 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs, uppdelat enligt Kommungruppsindelning.



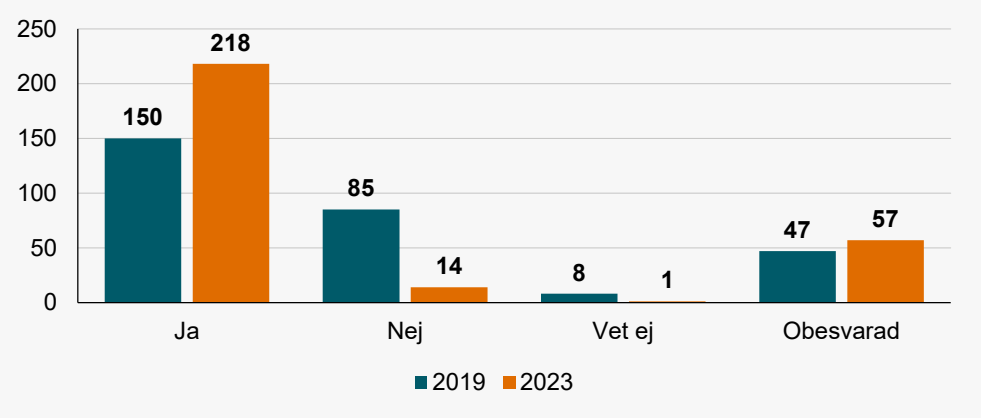
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 17 (ca 37%) av kommungrupp A, i 46 (ca 42%) av kommungrupp B och i 39 (ca 29%) av kommungrupp C har kommunen delvis ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs.

lakttagelser

En viktig del i kommunens systematiska och riskbaserade informationssäkerhetsarbete är att kommunens medarbetares informationssäkerhetsmedvetande säkerställs. Det behöver finnas en utbildningsplan (en strukturerad plan som innehåller utbildningar och olika aktiviteter). Vissa aktiviteter pågår under en begränsad tidsperiod (som en kampanj), medan andra aktiviteter är löpande (som ett nyhetsbrev).

Av uppföljningen framgår att 218 (ca 75%) av kommunerna har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, vilket kan jämföras med uppföljningen från 2019 då 150 (ca 52%) av kommunerna hade en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande.

Figur 54 Har eller planerar er kommun att införa ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs, jämförelse mellan uppföljningen 2019 och 2023.



Det är positivt att mer än tre av fyra kommuner har en process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, jämfört med uppföljningen 2019 då det var strax över hälften av kommunerna som hade en process för att säkerställa medarbetarnas informationssäkerhetsmedvetande. Det visar att arbetet med att säkerställa medarbetarnas informationssäkerhetsmedvetande inom kommunerna har blivit en viktigare del av kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

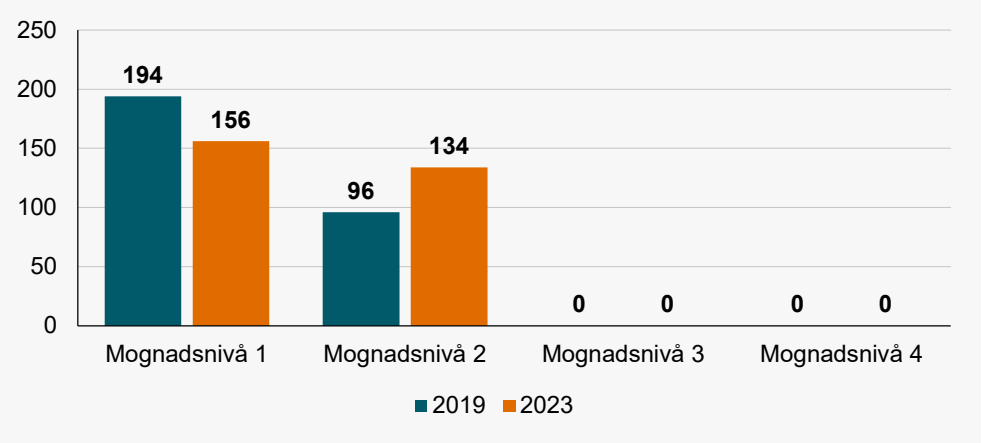
Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 21 (ca 46%) till 35 (ca 76%), vilket motsvarar en ökning med ca 67%.
- Kommungrupp B, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 51 (ca 47%) till 83 (ca 76%), vilket motsvarar en ökning med ca 63%.
- Kommungrupp C, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 78 (ca 57%) till 100 (ca 75%), vilket motsvarar en ökning med ca 28%.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande är jämförbar mellan kommungrupp A och B, med en lägre ökning bland kommungrupp C.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för att säkerställa medarbetarnas informationssäkerhetsmedvetande har ökat, när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi en något bättre utveckling än inom andra områden för denna uppföljning. Det är 134 kommuner som hamnar på mognadsnivå 2 inom kontinuitetshantering, vilket är en ökning med 38 kommuner sedan 2019.

Figur 55 Mognadsnivån för att säkerställa medarbetarnas informationssäkerhetsmedvetande, jämförelse mellan uppföljningen 2019 och 2023.



Av denna uppföljning framgår att nästan hälften av kommunerna befinner sig på nivå två i mognadsmodellen avseende att säkerställa medarbetarnas informationssäkerhetsmedvetande. Detta ska jämföras med att strax över tre av tio kommuner befann sig på denna nivå 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 15 (ca 33%) till 28 (ca 61%) på mognadsnivå 2, vilket motsvarar en ökning med ca 87%.
- Kommungrupp B, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 37 (ca 34%) till 52 (ca 47%) på mognadsnivå 2, vilket motsvarar en ökning med ca 41%.

- Kommungrupp C, som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande, har ökat från 44 (ca 32%) till 54 (ca 40%) på mognadsnivå 2, vilket motsvarar en ökning med ca 23%.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att säkerställa medarbetarnas informationssäkerhetsmedvetande på mognadsnivå 2 är störst bland kommungrupp A, medans ökning är mindre hos kommungrupp B och minst bland kommungrupp C.

Att sprida kunskap om informationssäkerhet är ett ständigt pågående arbete som är nödvändigt för att kunna skapa ett systematiskt och riskbaserat informationssäkerhetsarbete. En hög nivå av informationssäkerhetsmedvetande hos kommunens medarbetare förbättrar verksamhetens kvalitet och effektivitet samt ofta är en förutsättning för många nödvändiga företeelser, som exempelvis digitalisering och mobilitet.

Informationssäkerhetsrelaterade krav vid upphandlingar

Beskrivning av området

I dagens digitaliserade samhälle ställs allt högre krav på att hantera information säkert. Det är inte ovanligt att hela eller delar av en verksamhet och dess information hanteras av en extern leverantör genom varor eller tjänster. Det medför i första hand ett behov av upprättande och användande av informationssäkerhetsrelaterade krav, som behöver inkluderas vid upphandling och utveckling, samt att kunna verifiera att ställda informationssäkerhetskrav är uppfyllda (för att varan eller tjänsten bibehåller skyddet).

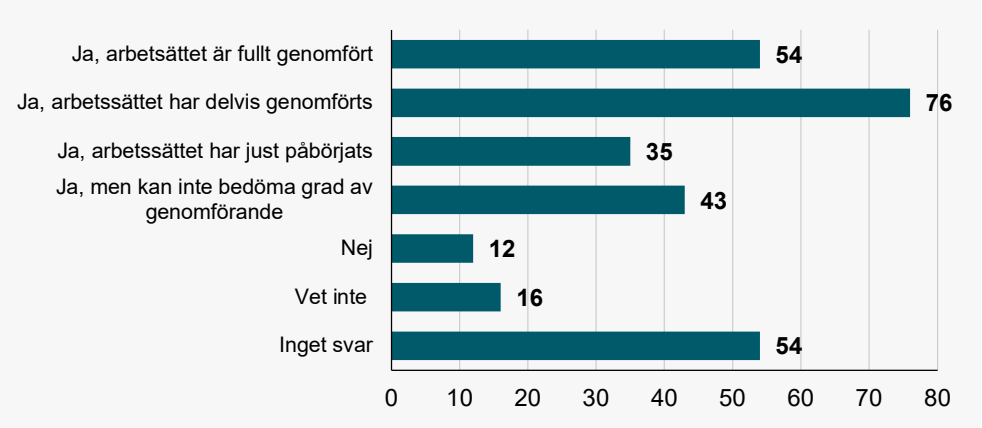
Genom att kommunerna arbetar systematiskt med informationsklassning och riskbedömningar identifieras vilket värde informationen har för kommunen och vilka risker som måste hanteras under upphandlingen och avtalsperioden.

Har kommunen processer för upphandling och kravställning vid upphandling bör arbetet med att få in informationssäkerhet i upphandlingen integreras med dessa processer.

Kommuner kan få stöd med informationsklassning och kravställning av KLASSA[5], ett verktyg som SKR utvecklat.

Erhållna svar

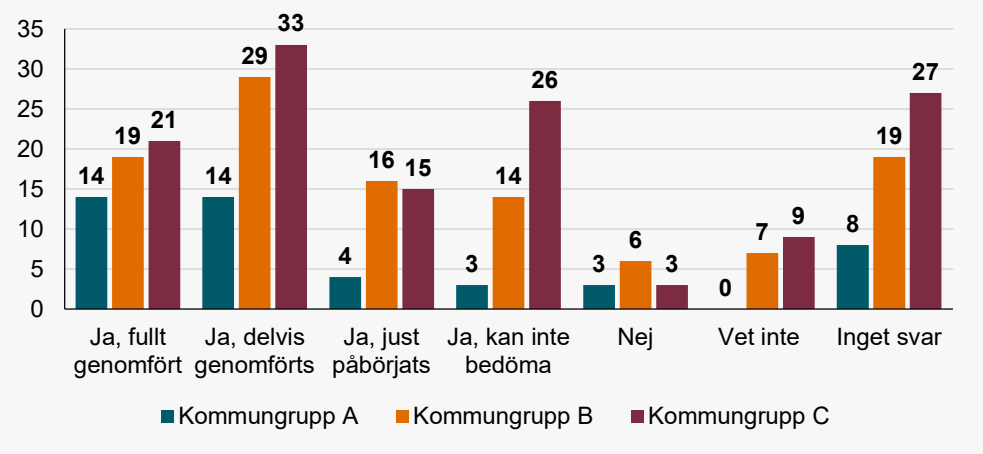
Figur 56 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar?



Av svaren framgår att i 54 (ca 19%) av kommunerna har kommunen ett fullt etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar, i 76 (ca 26%) av kommunerna har kommunen delvis ett etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar. I 35 (ca 12%) av kommunerna har ett arbete just påbörjats så att informationssäkerhetskrav ställs i relevanta upphandlingar.

[5] För mer information om KLASSA se https://klassa.skr.se/

Figur 57 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar, uppdelat enligt Kommungruppsindelning.



När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i kommungrupp A är det 14 (ca 30%) kommuner som har ett fullt etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar och 14 (ca 30%) kommuner som har ett delvis genomfört arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar, medans det framgår att i 29 (ca 26%) av kommungrupp B och i 33 (ca 25%) av kommungrupp C har kommunen ett delvis genomfört arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar.

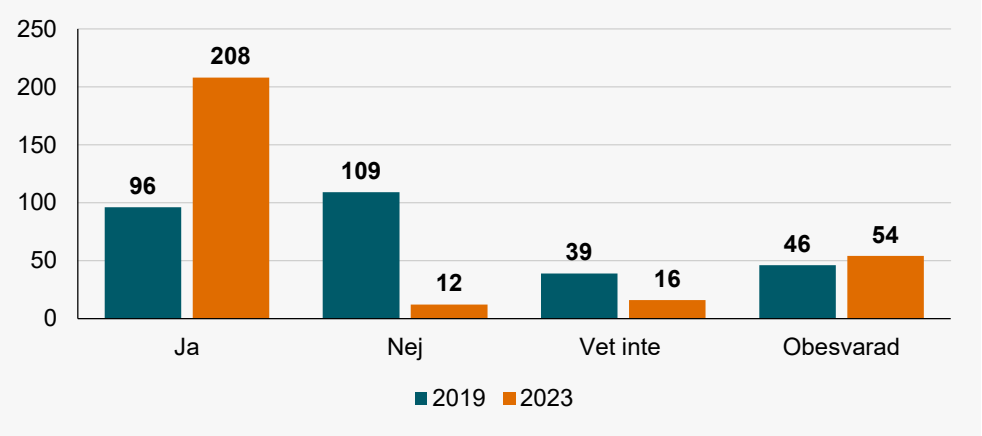
Iakttagelser

För att säkerställa att kommunens information skyddas är det viktigt att kommunen har en väl förankrade processer för upphandlingar, och att informationssäkerhet är en naturlig del i dessa processer.

Att ta med informationssäkerhetsrelaterade krav redan innan upphandlingen medför generellt sätt en högre nivå av säkerhet och är ett mer kostnadseffektivt tillvägagångsätt än att lägga på säkerheten efteråt.

Av uppföljningen framgår att 208 (ca 72%) av kommunerna har en fastställd process för att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar, vilket kan jämföras med uppföljningen från 2019 då 96 (ca 33%) av kommunerna hade en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar.

Figur 58 Har eller planerar er kommun att införa ett etablerat arbetssätt så att informationssäkerhetskrav ställs i relevanta upphandlingar, jämförelse mellan uppföljningen 2019 och 2023.



Det är positivt att nästan tre av fyra kommuner har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, jämfört med uppföljningen 2019 då det var strax över tre av tio kommuner som hade en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar. Det visar att arbetet med att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar inom kommunerna har blivit en viktigare del av kommunernas systematiska och riskbaserade informationssäkerhetsarbete.

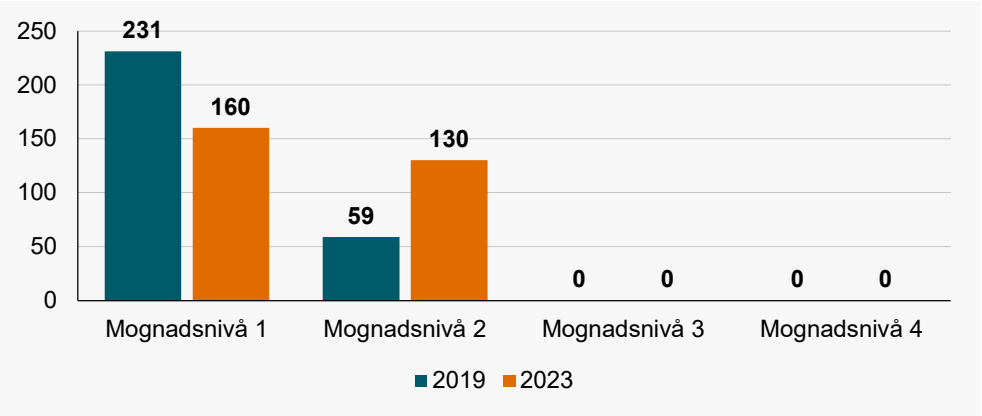
Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 17 (ca 37%) till 35 (ca 76%), vilket motsvarar en ökning med ca 106%.
- Kommungrupp B, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 30 (ca 28%) till 78 (ca 71%), vilket motsvarar en ökning med ca 160%.
- Kommungrupp C, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 49 (ca 36%) till 95 (ca 71%), vilket motsvarar en ökning med ca 94%.

När vi bryter ner siffrorna baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar är störst hos kommungrupp B, mer än en dubblering av antalet kommuner. Ökningen bland kommungrupp A och C är något lägre, men fortfarande runt en dubblering.

Vi kan se, av uppföljningen, att antalet kommuner som har en process för att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar har ökat, när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi en bättre utveckling än inom andra områden för denna uppföljning. Det är 130 kommuner som hamnar på mognadsnivå 2 inom kontinuitetshantering, vilket är en ökning med 71 kommuner sedan 2019.

Figur 59 Mognadsnivån för att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar, jämförelse mellan uppföljningen 2019 och 2023.



Av denna uppföljning framgår att nästan hälften av kommunerna befinner sig på nivå två i mognadsmodellen avseende att säkerställa att informationssäkerhetskrav ställs i relevanta upphandlingar. Detta ska jämföras med att två av tio kommuner befann sig på denna nivå 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 10 (ca 22%) till 28 (ca 61%) på mognadsnivå 2, vilket motsvarar en ökning med ca 180%.

- Kommungrupp B, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 24 (ca 22%) till 48 (ca 44%) på mognadsnivå 2, vilket motsvarar en ökning med ca 100%.
- Kommungrupp C, som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar, har ökat från 25 (ca 18%) till 54 (ca 40%) på mognadsnivå 2, vilket motsvarar en ökning med ca 160%.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process för att informationssäkerhetskrav ställs i relevanta upphandlingar på mognadsnivå 2 är störst bland kommungrupp A och C, medans ökning är mindre hos kommungrupp B, men fortfarande en dubblering.

Förmågan att kunna ställa och verifiera uppfyllnad av informationssäkerhetskrav är en nödvändig förmåga i kommunernas systematiska och riskbaserade informationssäkerhetsarbete, då de lösningar som upphandlas ofta har långa livscykler och kommunen därmed kan få leva länge med dåliga lösningar.

Uppföljning

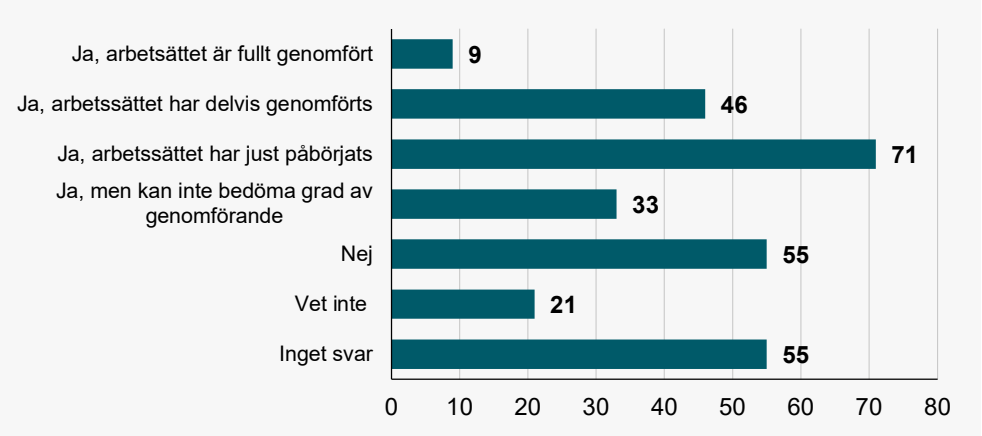
Beskrivning av området

En viktig del i kommunens systematiska och riskbaserade informationssäkerhetsarbete är att genom löpande utvärdering (övervakning, mätning och måluppföljning) säkerställa att informationssäkerheten i stort är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande.

Resultatet från utvärderingen ligger till grund för ledningens genomgång, samt ingångsvärde till eventuella förbättringar och förändringar i kommunens systematiska och riskbaserade informationssäkerhetsarbetet.

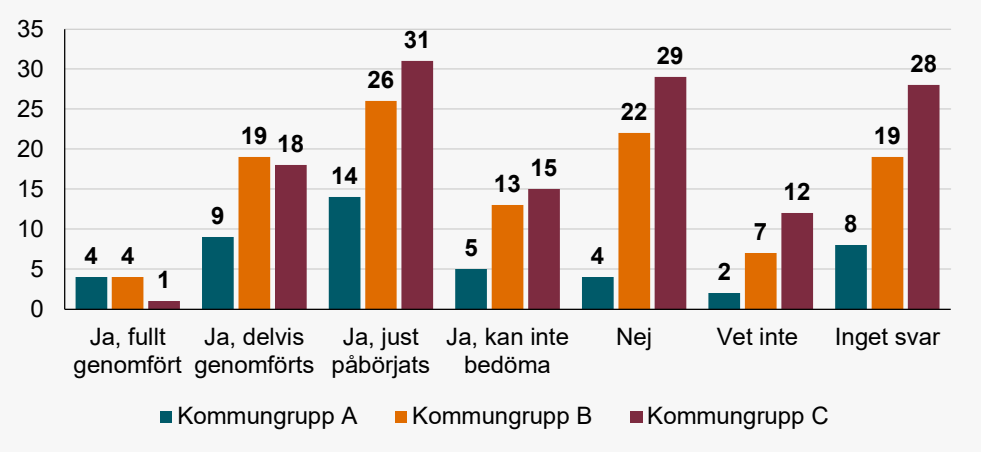
Erhållna svar

Figur 60 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (t.ex. egenkontroll, leverantörsuppföljning) följs upp?



Av svaren framgår att i 9 (ca 3%) av kommunerna har kommunen ett fullt etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, i 46 (ca 16%) av kommunerna har kommunen delvis ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp. I 71 (ca 25%) av kommunerna har ett arbete just påbörjats så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp.

Figur 61 Inom följande områden, har eller planerar er kommun att införa ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (t.ex. egenkontroll, leverantörsuppföljning) följs upp, uppdelat enligt Kommungruppsindelning.



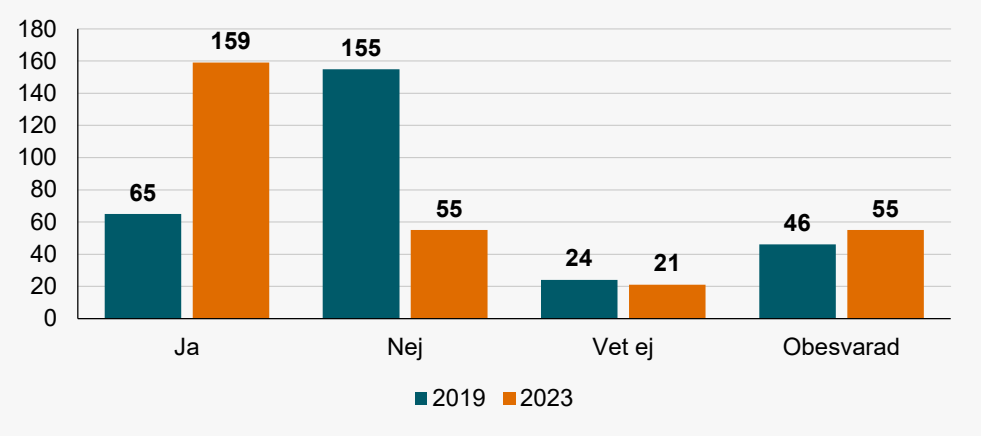
När vi bryter ner svaren utifrån kommungruppsindelningen framgår att i 14 (ca 30%) av kommungrupp A, i 26 (ca 24%) av kommungrupp B och i 31 (ca 23%) av kommungrupp C har kommunerna just påbörjat ett arbete så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp.

Iakttagelser

Utvärdering av kommunens informationssäkerhetsarbete och styrning, särskilt avseende lämplighet, tillräcklighet och verkan är en väldigt central del av kommunens systematiska och riskbaserade informationssäkerhetsarbete.

Av uppföljningen framgår att 159 (ca 55%) av kommunerna har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, vilket kan jämföras med uppföljningen från 2019 då 65 (ca 22%) av kommunerna hade en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp.

Figur 62 Har eller planerar er kommun att införa ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (t.ex. egenkontroll, leverantörsuppföljning) följs upp, jämförelse mellan uppföljningen 2019 och 2023.



Det är positivt att mer än hälften av kommunerna har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, jämfört med uppföljningen 2019 då det var strax över två av tio kommuner som hade en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp. Det visar att arbetet med att följa upp att kommunens systematiska och riskbaserade informationssäkerhetsarbete har avsedd lämplighet, tillräcklighet och verkan har blivit viktigare.

Utifrån kommungruppsindelningen framgår att:

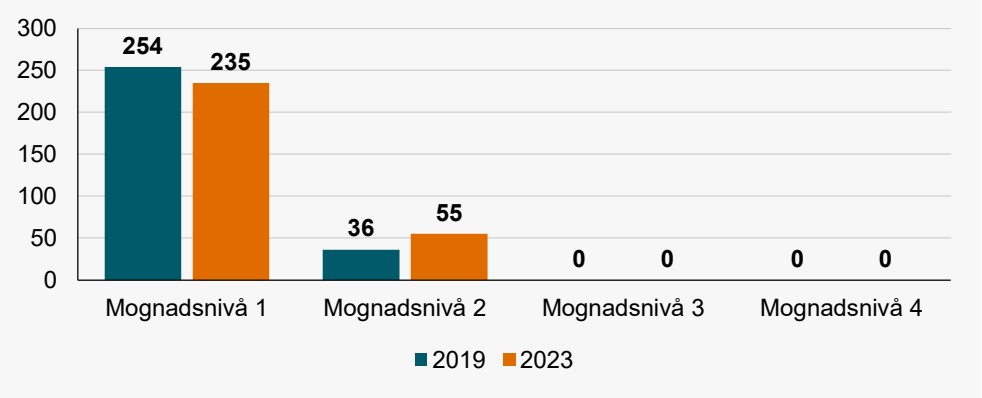
- Kommungrupp A, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 12 (ca 26%) till 32 (ca 70%), vilket motsvarar en ökning med ca 167%.
- Kommungrupp B, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 26 (ca 24%) till 62 (ca 56%), vilket motsvarar en ökning med ca 139%.
- Kommungrupp C, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 27 (ca 10%) till 65 (ca 49%), vilket motsvarar en ökning med ca 141%.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp är störst bland kommungrupp A, med en något lägre och jämförbar ökning hos kommungrupp B och C.

Utvecklingen inom detta område följer utvecklingen för ledningens genomgång (se avsnitt 5.2 Information till ledningen). Detta visar tydligt hur viktigt ledningens engagemang är kopplat till kommunens systematiska och riskbaserade informationssäkerhetsarbete.

Vi kan se, av uppföljningen, att antalet kommuner som har en process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp har ökat, när vi tittar på hur väl genomfört arbetet är i kommunerna så ser vi inte samma utveckling som inom andra områden för denna uppföljning. Det är 55 kommuner som hamnar på mognadsnivå 2 inom uppföljning av informationssäkerhetsarbetet, vilket är en ökning med 19 kommuner sedan 2019.

Figur 63 Mognadsnivån för att säkerställa att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, jämförelse mellan uppföljningen 2019 och 2023.



Av denna uppföljning framgår att nästan två av tio kommuner befinner sig på nivå två i mognadsmodellen avseende att följa upp att kommunens systematiska och riskbaserade informationssäkerhetsarbete. Detta ska jämföras med att strax över en av tio kommuner befann sig på denna nivå 2019.

Utifrån kommungruppsindelningen framgår att:

- Kommungrupp A, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 6 (ca 13%) till 13 (ca 28%) på mognadsnivå 2, vilket motsvarar en ökning med ca 117%.
- Kommungrupp B, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 14 (ca 13%) till 23 (ca 21%) på mognadsnivå 2, vilket motsvarar en ökning med ca 64%.
- Kommungrupp A, som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp, har ökat från 16 (ca 12%) till 19 (ca 14%) på mognadsnivå 2, vilket motsvarar en ökning med ca 19%.

När siffrorna bryts ner baserat på Kommungruppsindelningen framgår att ökningen av kommuner som har en fastställd process så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet följs upp på mognadsnivå 2 är störst bland kommungrupp A, mer än en dubblering av antalet kommuner når upp till nivå 2. Ökningen är något mindre hos kommungrupp B och lägst bland kommungrupp C.

Precis som för uppföljningsområde information till ledningen är kommunerna på väg i rätt riktning, men har fortsatt mycket arbete framför sig.

Rekommendationer

SKR ser att ett systematiskt informationssäkerhetsarbete är en nödvändig del för en framgångsrik digitalisering och bedömer att området kräver ett ökat fokus i samband med enskilda digitaliseringslösningar. SKR bedömer även att ett stärkt informationssäkerhetsarbete behövs för att öka kommunernas förmåga att stå emot hot och kunna säkerställa tillit från medborgarna.

Ett lyckat införande av ett systematiskt och riskbaserat informationssäkerhetsarbete hänger ofta samman med ledningens aktiva engagemang.

Ett bristande informationssäkerhetsarbete kan också innebära att kommunen riskerar att drabbas av sanktioner från olika tillsynsmyndigheter, t.ex. IMY, Energimyndigheten och Inspektionen för vård och omsorg.

Det är flera nya regelverk på gång, som exempel kommer Sverige att införa EU:s NIS2-direktiv i svensk lag under 2024. Denna nya reglering kommer innebära att kommunerna behöver snabba på införandet av ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete.

Vad kommunerna behöver göra

Kommunerna behöver fortsätta, men också snabba på, det arbete som pågår med att säkerställa att det systematiskt och riskbaserat informations- och cybersäkerhetsarbete är lämpligt, tillräckligt, effektivt och leder till en förbättring av informations- och cybersäkerheten i kommunerna.

- **Utse en informationssäkerhetssamordnare**
  För att kommunerna ska lyckas med sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete är det viktigt att det finns en utpekad funktion med uppdrag att samordna eller leda det övergripande informationssäkerhetsarbetet inom kommunen. Kommunerna behöver också säkerställa att den utpekade funktionen använder så mycket som möjligt av sin disponibla arbetstid åt informations- och cybersäkerhet.
  Det finns stora ekonomiska fördelar med att samarbeta och samverka, att kommuner går samman och gemensamt rekryterat en informationssäkerhetssamordnare ökar förutsättningarna för att

informationssäkerhetssamordnaren kan arbeta med uppgiften på heltid.

- **Genomför ledningens genomgång**
  För att kommunerna ska lyckas med sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete är det viktigt att ledningen tar en aktiv roll för att säkerställa att kommunens LIS är lämpligt, tillräckligt, effektivt och leder till en förbättring av informations- och cybersäkerheten. Genom införandet av NIS2-direktivet i svensk lag ökar kraven på kommunernas ledningar, t.ex. ska ledningen godkänna riskhanteringsåtgärder och genomgå utbildning i informations- och cybersäkerhet.
  Det krävs en god relation och kommunikation mellan ledning och informationssäkerhetssamordnare, för att hitta formerna för att göra ledningens genomgång till en konstruktiv dialog.

- **Omsätt ledningens mål i konkreta handlingsplaner**
  För att kommunerna ska lyckas med sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete är det viktigt att ledningens mål och beslut, från ledningens genomgång, omsätts i konkreta handlingsplaner, med aktiviteter. Detta är viktigt för att kommunens systematiska och riskbaserade informations- och cybersäkerhetsarbete ska få en djup förankring i verksamheten och utförs på ett strukturerat sätt.

- **Förankra riskhanteringsprocessen i hela kommunens verksamhet**
  Många kommuner har en fastställd process för hantering av informations- och cybersäkerhetsrisker, men den har inte förankrats i kommunernas verksamheter. Brister i ett förankrat arbetssätt för hantering av informations- och cybersäkerhetsrisker gör att kommunernas medarbetarna löpande tvingas hantera risker (det blir mer släcka bränder än ett strukturerat arbetssätt).
  Genom införandet av NIS2-direktivet i svensk lag ökar kraven på

kommunerna att arbete mer strukturerat med hanteringen av informations- och cybersäkerhetsrisker, det innebär att riskåtgärder ska godkännas och att deras genomförande övervakas men också att effekten av riskåtgärderna ska utvärderas.

- **Förankra klassificeringsprocessen i hela kommunens verksamhet**
  Flertalet kommuner har en fastställd process för klassificering av informationstillgångar, men brister i ett förankrat arbetssätt för att klassificera kommunens informationstillgångar leder till att informationstillgångarna saknar adekvata säkerhetsåtgärder.

- **Förankra incidenthanteringsprocessen i hela kommunens verksamhet**
  Många kommuner har en fastställd process för hantering av informations- och cybersäkerhetsincidenter, men brister i ett förankrat arbetssätt för att hantera incidenter i hela kommunens verksamhet leder till onödiga ledtider innan incidenter identifieras och hanteras, vilket gör att kommunens verksamhet drabbas längre än nödvändigt av inträffade incidenter.

- **Säkerställ verksamhetens tillgång till information**
  En viktig del i kommunens systematiska och riskbaserade informations- och cybersäkerhetsarbete är att det finns en väl förankrad process för att säkerställa verksamhetens kontinuitet. Kommunerna behöver säkerställa att det finns rutiner och säkerhetsåtgärder för att förebygga och hantera avbrott i kommunernas verksamhet, så att kritisk verksamhet kan bedrivas även vid störningar.

- **Utbilda samtliga medarbetare i informationssäkerhet**
  Utbildning är en väsentlig del i att bygga upp och upprätthålla en hög nivå i informations- och cybersäkerhetsarbetet och en god

informationssäkerhetskultur. När kommunerna utbildar sina medarbetare i informations- och cybersäkerhet leder det till att medarbetare känner ett starkare engagemang för att efterleva styrande dokument och därigenom minimeras t.ex. orsaker till incidenter (t.ex. misstag och systemfel) och verksamhetens kontinuitet upprätthålls.

- **Ställ informationssäkerhetskrav vid samtliga relevanta upphandlingar**
  För att säkerställa att kommunens information skyddas är det viktigt att kommunen har väl förankrade processer för upphandlingar, och att informationssäkerhet är en naturlig del i dessa processer. Förmågan att kunna ställa och verifiera uppfyllnad av informations- och cybersäkerhetskrav är en nödvändig förmåga i kommunernas systematiska och riskbaserade informations- och cybersäkerhetsarbete, då de lösningar som upphandlas ofta har långa livscykler och kommunen därmed kan få leva länge med dåliga lösningar.

- **Följ upp kommunens informationssäkerhetsarbete**
  Det är viktigt att kommunerna löpande följer upp arbetet med kommunens informations- och cybersäkerhetsarbete, brister i ett förankrat arbetssätt för att följa upp kommunens informations- och cybersäkerhetsarbete gör att informationen till ledningens brister och följden på det blir att ledningen riskerar att fatta felaktiga beslut rörande det framtida informationssäkerhetsarbetet i kommunen.

Vad SKR ska göra

- **KLASSA**
  SKR har utvecklat och tillhandahållit verktyget KLASSA sedan 2014. KLASSA utgör ett stöd i kommunernas systematiska och riskbaserade informationssäkerhetsarbete inom t.ex. informationsklassning, informationssäkerhetskrav vid upphandlingar och uppföljning av levererad tjänst eller system.
  KLASSA kommer under de kommande två åren att utvecklas med

funktionalitet inom t.ex. riskhantering, processorienterad informationskartläggning och mognadsmätning. KLASSA kommer också att finnas i en on-premversion.

- **Kompetensgemenskap informationssäkerhet**
  SKR har skapat Kompetensgemenskap informationssäkerhet (bestående av 8-12 representanter från kommuner och regioner). Kompetensgemenskap informationssäkerhet kommer ta fram stödmaterial avseende införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete i kommunerna. Kompetensgemenskapen kommer också utveckla exempeldokument inom ramen för det systematiska och riskbaserade informationssäkerhetsarbetet, det handlar t.ex. om incidenthantering, kontinuitetsplanering, utbildning i informationssäkerhet och uppföljning.

- **Kompetensgemenskap cybersäkerhet**
  SKR har även skapat en kompetensgemenskap för cybersäkerhet, som i nära samarbete med kompetensgemenskapen för informationssäkerhet syftar till att stödja kommunerna med vägledning, erfarenhetsspridning och förslag på åtgärder inom cybersäkerhetsområdet.

Jämförelsetal

Nedan redovisas en sammanställning av resultatet, baserat på mognadsnivån inom respektive uppföljningsområde, i form av olika spindeldiagram.

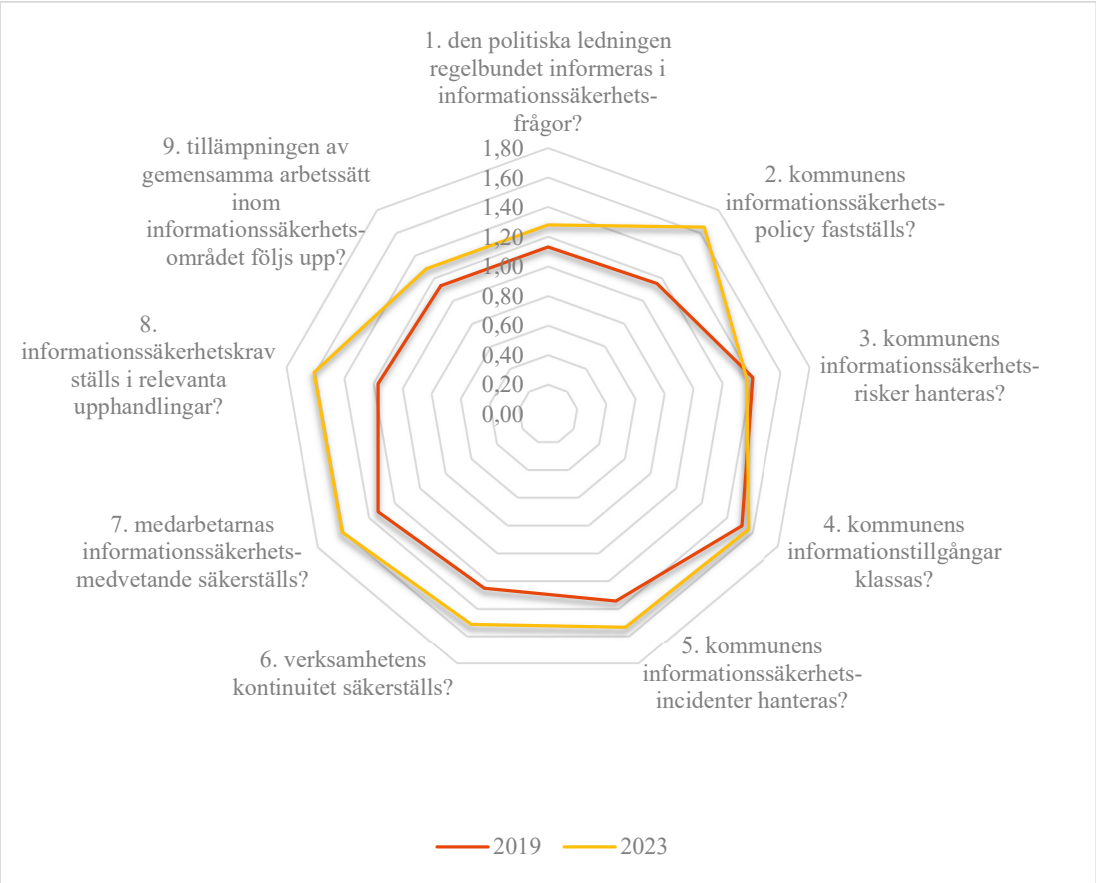
Dessa är:

- Kommungrupp A
- Kommungrupp B
- Kommungrupp C
- Nationellt

Syftet med detta avsnitt är att erbjuda kommunerna möjligheten att jämföra sitt resultat mellan undersökningen 2019 och 2023, men också mot andra kommuner i sin grupp (enligt kommungruppsindelningen) och nationellt.

Kommungrupp A

Figur 64 Mognadsnivån för kommungrupp A, jämförelse mellan uppföljningen 2019 och 2023.



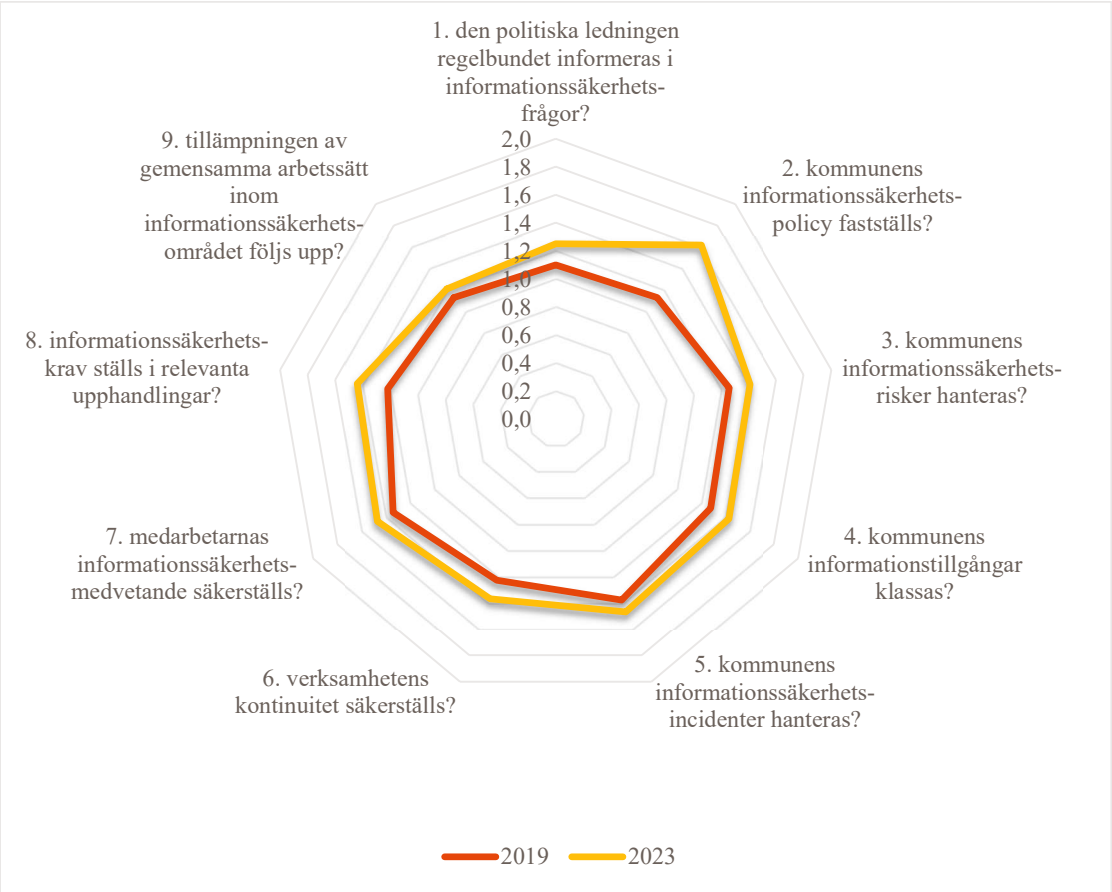
<u>Notera:</u> samtliga område inleds med ”Har ni ett etablerat arbetssätt så att…”

I tabellen nedan framgår mognadsnivåerna för kommungrupp A, avseende uppföljningarna från 2019 och 2023.

	1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**
2019	1,13	1,15	1,41	1,52	1,35	1,26	1,33	1,17	1,13
2023	1,28	1,65	1,37	1,57	1,54	1,52	1,61	1,61	1,28

Kommungrupp B

Figur 65 Mognadsnivån för kommungrupp B, jämförelse mellan uppföljningen 2019 och 2023.



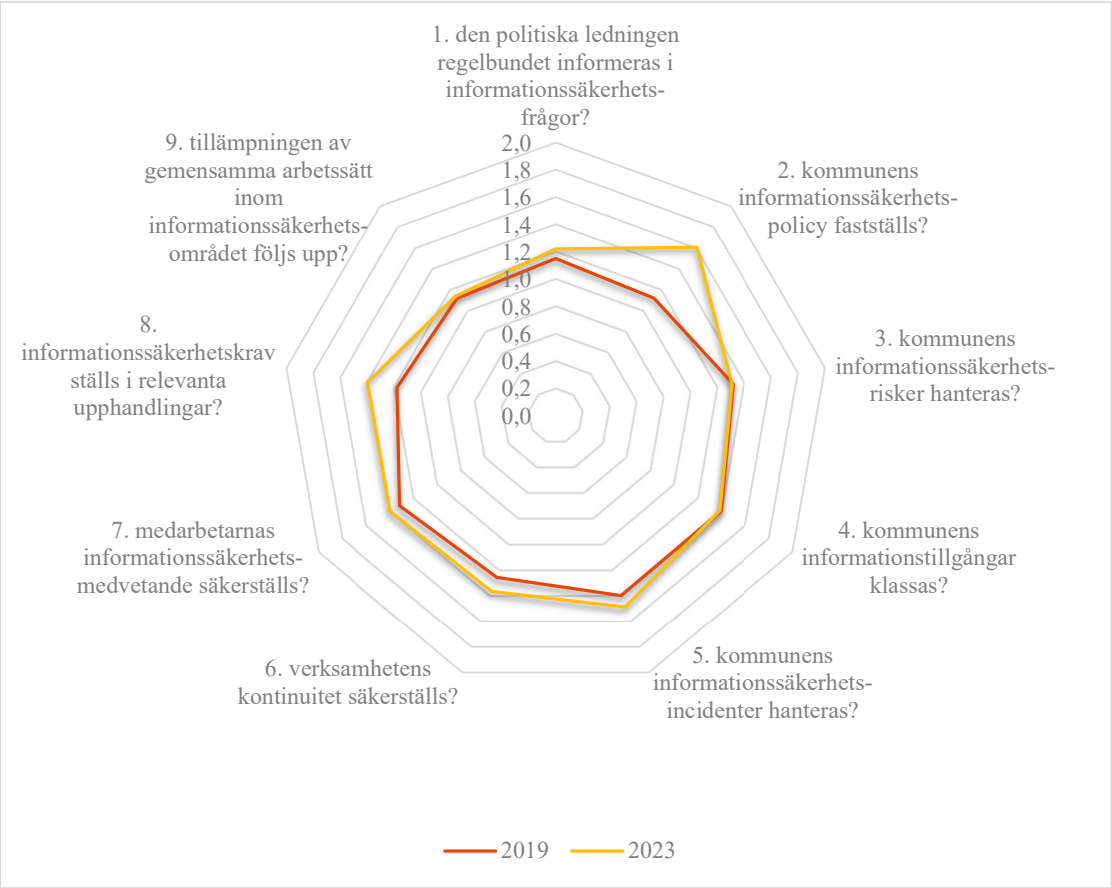
<u>Notera:</u> samtliga område inleds med ”Har ni ett etablerat arbetssätt så att…”

I tabellen nedan framgår mognadsnivåerna för kommungrupp B, avseende uppföljningarna från 2019 och 2023.

	1.	2.	3.	4.	5.	6.	7.	8.	9.
2019	1,10	1,13	1,26	1,28	1,38	1,23	1,34	1,22	1,13
2023	1,25	1,62	1,41	1,43	1,47	1,37	1,47	1,44	1,21

Kommungrupp C

Figur 66 Mognadsnivån för kommungrupp C, jämförelse mellan uppföljningen 2019 och 2023.



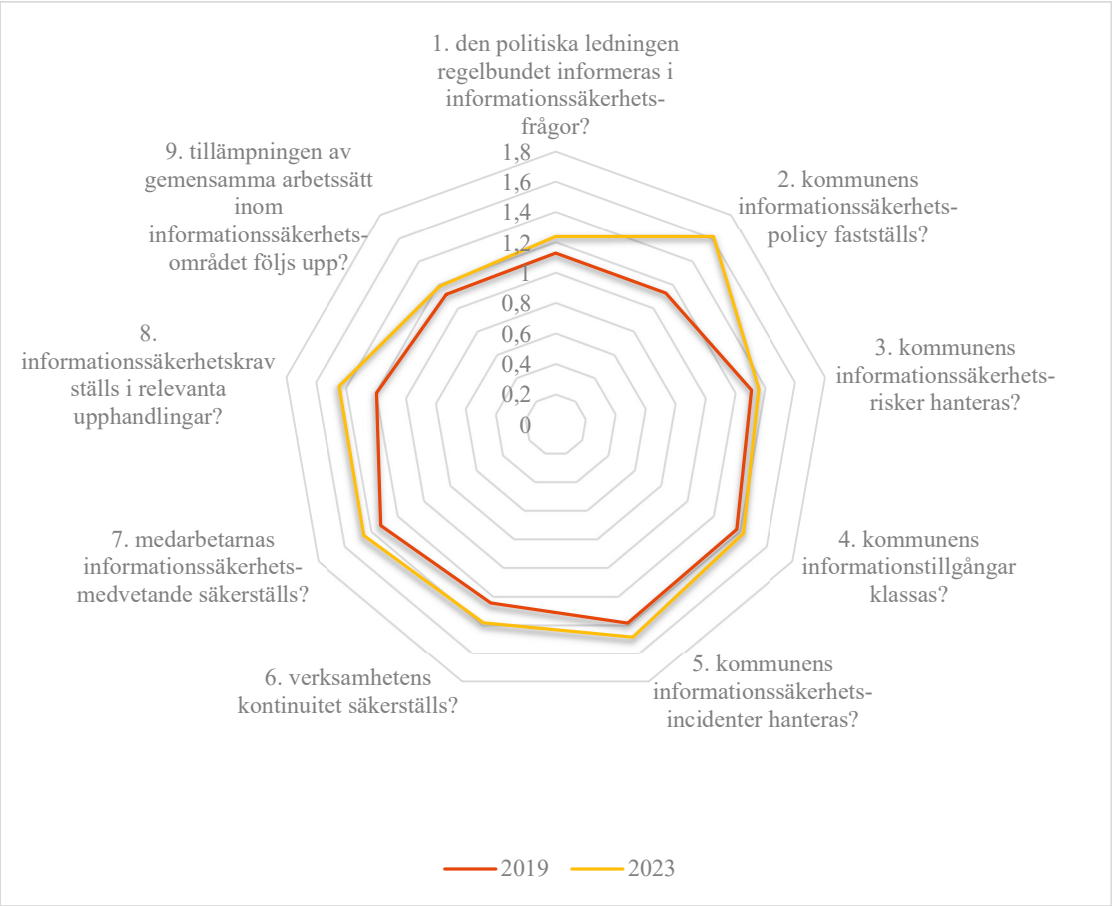
<u>Notera:</u> samtliga område inleds med ”Har ni ett etablerat arbetssätt så att…”

I tabellen nedan framgår mognadsnivåerna för kommungrupp C, avseende uppföljningarna från 2019 och 2023.

	1.	2.	3.	4.	5.	6.	7.	8.	9.
2019	1,15	1,12	1,32	1,40	1,40	1,26	1,32	1,18	1,12
2023	1,22	1,61	1,31	1,39	1,49	1,37	1,40	1,40	1,14

Nationellt

Figur 67 Mognadsnivån för Sveriges samtliga kommuner, jämförelse mellan uppföljningen 2019 och 2023.



<u>Notera:</u> samtliga område inleds med ”Har ni ett etablerat arbetssätt så att…”

I tabellen nedan framgår mognadsnivåerna för Sveriges samtliga kommuner, avseende uppföljningarna från 2019 och 2023.

	1.	2.	3.	4.	5.	6.	7.	8.	9.
2019	1,13	1,13	1,31	1,38	1,39	1,25	1,33	1,20	1,12
2023	1,24	1,62	1,36	1,43	1,49	1,39	1,46	1,45	1,19

Uppföljningens omfattning

Bakgrund

Informations- och cybersäkerhet har fått ökad aktualitet både genom utvecklingen mot ett allt mer digitaliserat samhälle och nya former av hot och risker. Inte minst har det efter Rysslands invasion av Ukraina blivit tydligt att Sveriges förmåga att stå emot hot och angrepp behöver stärkas.

Även om det är en nationell angelägenhet att säkerställa Sveriges samlade förmåga inom informations- och cybersäkerhet, vilar ett stort ansvar på varje kommun, region, privat utförare, statlig myndighet och företag att vidareutveckla och stärka sitt systematiska och riskbaserade informationssäkerhetsarbete.

Sveriges Kommuner och Regioner (SKR) har som ambition att stötta alla sina medlemmar till att arbeta systematiskt och riskbaserat med informationssäkerhet, för att skydda individers integritet och bevara invånarnas förtroende för välfärdsleveransen.

En väsentlig del av ett systematiskt och riskbaserat informationssäkerhetsarbetet är utvärdering av informationssäkerhetsarbetet och dess styrning. Genom att en organisation använder sig av en strukturerad övervakning och mätning ges förutsättningar för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder är implementerade och fungerar tillfredsställande.

Som ett led både i att utveckla SKR:s stöd inom området och att skapa bättre förutsättningar för samarbete och erfarenhetsutbyte mellan landets kommuner, samt utvärdering av informationssäkerhetsarbetet och dess styrning har SKR utvecklat en webbenkät.

Resultaten av enkäten kan ge kommunens ledning information om förbättringsområden och organisationens mognad inom informationssäkerhetsområdet, samt för att identifiera behov som kan mötas med gemensamma insatser.

Frågorna i enkäten fokuserar på det övergripande informationssäkerhetsarbetet inom kommunen, den ska alltså besvaras på kommunövergripande nivå, och inte för en viss förvaltning/del av verksamhet.

Informationssäkerhet förbättrar organisationens kvalitet och effektivitet samt är ofta en förutsättning för genomförandet av t.ex. upphandling, digitalisering och mobilitet.

Kommunens ledning ansvarar för att leda och styra verksamhetens systematiska och riskbaserade informationssäkerhetsarbete i syfte att säkerställa att det är effektivt. Ledningen ska fatta beslut om arbetets inriktning och resurser.

Ingångsvärde

Ett viktigt ingångsvärde i skapandet av denna uppföljning har varit SKR:s webbenkät som skickades till kommunerna under 2019 och SKR:s webbenkät som skickades till regionerna under 2021, dessutom har frågeställningarna som Myndigheten för samhällsskydd och beredskap (MSB) använder sig av i Infosäkkollen[6] utgjort ett underlag.

Tillvägagångssätt

SKR har utarbetat webbenkäten i samarbete med forskare verksamma vid Högskolan Väst och Göteborgs universitet. Forskarna genomför en forskningsstudie om cybersäkerhet finansierad av Vetenskapsrådet (2021-06310), studiens övergripande syfte är att genom en jämförande ansats öka vår kunskap om cybersäkerhet i svenska kommuner. Forskarna kommer använda webbenkätens data som underlag för vetenskapliga artiklar, informationsmöten och forskningspresentationer för kommunsektorn.

Under arbetet med webbenkäten har också stöd inhämtats från ES Data och analys på avdelningen för ekonomi och styrning på SKR.

Webbenkäten är utformad för att kartlägga om resurser avsatts för att driva informationssäkerhetsarbetet, om grundläggande åtgärder vidtagits och vilken mognadsgrad den svarande kommunen själv skattade att den nått.

Webbenkäten var tillgänglig för kommunerna att besvara under perioden 28 februari till den 8 maj 2023. Webbenkäten skickades till registrator eller motsvarande, d.v.s. kommunens officiella e-postadress (t.ex. info@kommunen.se).

[6] Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter, (https://www.msb.se/infosakkollen)

Varje kommun fick en enkät, vilken var frivillig för kommunen att besvara och enkäten besvarades av nästan 82% av kommunerna.

Uppföljningen ger en bild av hur kommunerna själva uppfattar sitt systematiska och riskbaserade informationssäkerhetsarbete. Det handlar med andra ord om en uppföljning baserat på självskattning, vilket kan vara värt att ha i beaktande.

Uppföljningsområdena baseras på SKR:s rapport från 2019 där vissa förändringar gjorts genom att vissa frågor har tillkommit.

Mognadsmodellen

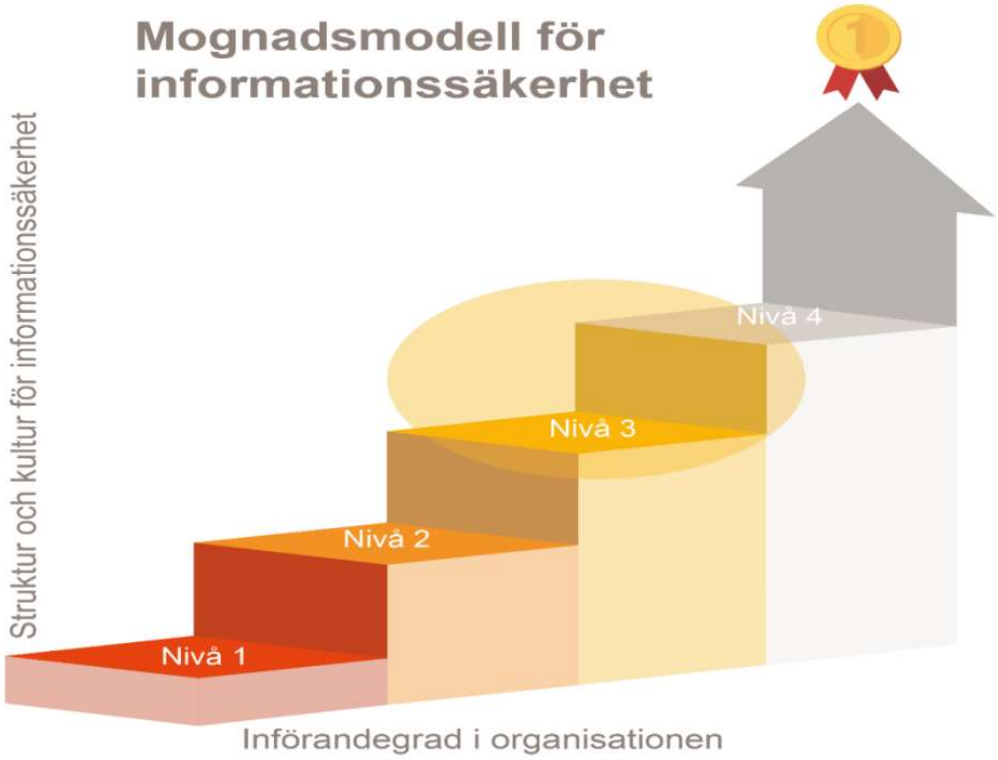
MSB presenterade en rapport[7] 2018 över landstingens informationssäkerhetsarbete inom hälso- och sjukvården, i samband med den rapporten presenterade MSB samtidigt en mognadsmodell.

Denna mognadsmodell låg också till grund för de bedömningar som gjordes under SKR:s uppföljning över kommunernas systematiska och riskbaserade informationssäkerhetsarbete 2019.

Mognadsmodellen har senare vidareutvecklats av MSB, men för spårbarhet och jämförelse mellan 2019 och 2023 väljer SKR, i denna uppföljning, att behålla den mognadsmodell som användes vid uppföljningen 2019.

[7] En bild av landstingens informationssäkerhetsarbete 2018 : kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (https://www.msb.se/sv/publikationer/en-bild-av-landstingens-informationssakerhetsarbete-2018--kartlaggning-och-analys-av-landstingens-informationssakerhetsarbete-inom-halso--och-sjukvardsverksamheten/)

Figur 68 Mognadsmodell för det systematiska och riskbaserade informationssäkerhetsarbetet



För att en organisation ska anses ha uppnått ett systematiskt och riskbaserat informationssäkerhetsarbete bör den ha nått mognadsnivå 3, som motsvarar identifierad målnivå. Mognadsnivå 2 motsvarar lägstanivån för en tillfredsställande struktur i arbetet. Övergripande kan de fyra mognadsnivåerna förklaras på följande sätt:

- **Mognadsnivå 1** kännetecknas av att organisationen är reaktiv och händelsestyrd. Betydelsen av informationssäkerhet har inte uppmärksammats och ett systematiskt arbetssätt saknas. Det systematiska informationssäkerhetsarbetet är personberoende.
- **Mognadsnivå 2** kännetecknas av att organisationen har insikt och medvetenhet om brister relaterade till informationssäkerhet. Organisationen har fokus på att utarbeta arbetssätt, prövar dem och energin går till att införa arbetssätten. Visst gehör finns men också motstånd mot förändringarna. Organisationen gör planer och använder dessa till viss del.

- **Mognadsnivå 3** kännetecknas av ett högt driv och en tydligare viljeinriktning. Organisationen börjar belöna proaktivitet och förbättringar av etablerade arbetssätt. Det finns god samverkan mellan arbetssätten och de är integrerade i verksamhetens processer. Organisationen följer till del arbetssätt och vissa uppvisar goda resultat.
- **Mognadsnivå 4** kännetecknas av ett väl fungerande, effektivt och väl anpassat riskbaserat och systematiskt informationssäkerhetsarbete där organisationen över tid har utvecklat tydliga och medvetna arbetssätt. Organisationen har en stark drivkraft och förmåga att ständigt förbättra arbetssätten. Organisationen fångar effektivt upp trender, problem och utmaningar tidigt och kan agera proaktivt samt vet vilka resultat arbetssätten ger. Organisationen skapar höga resultat och uppvisar positiva trender.

Det är av vikt att understryka att inget arbete har gjorts för att rangordna kommunerna sinsemellan då målsättningen med uppdraget varit att stödja kommunerna i deras arbete med utvärdering av informationssäkerhetsarbetet och dess styrning, samt att se vilka områden inom det systematiska och riskbaserade informationssäkerhetsarbetet som generellt behöver mest stöd och fokus.

Vid denna analys finns en osäkerhetsfaktor eftersom resultatet bygger på kommunernas självskattning, d.v.s. SKR har inte genomfört någon verifiering av svaren.

Det är också värt att notera att denna webbenkät endast har haft som syfte att mäta mot de två lägre nivåerna i mognadsmodellen, det går således inte att utläsa huruvida det finns någon av kommunerna som ligger på mognadsnivåerna 3 eller 4.

Om kommunerna

Kommunernas åtaganden

Kommunerna ansvarar för en stor del av den samhällsservice som finns där vi bor. Bland de viktigaste uppgifterna är förskola, skola, socialtjänst och äldreomsorg.

Kommunerna är skyldiga att ha vissa verksamheter enligt lag. Andra verksamheter är frivilliga och beslutas av lokalpolitikerna.

De obligatoriska åtaganden är:

- Social omsorg (äldre- och handikappomsorg samt individ- och familjeomsorg)
- För-, grund- och gymnasieskola samt kommunal vuxenutbildning (komvux)
- Plan och byggfrågor
- Miljö- och hälsoskydd
- Renhållning och avfallshantering
- Vatten och avlopp
- Räddningstjänst
- Krisberedskap och civilt försvar
- Biblioteksverksamhet
- Bostäder

De frivilliga åtaganden är:

- Fritid och kultur
- Energi
- Sysselsättning
- Näringslivsutveckling

Antalet anställda i kommunerna uppgick i november 2022 till nästan 900 000.

Kommungruppsindelning

För att underlätta analyser och jämförelser ur ett regionalt perspektiv har SKR sedan 1980-talet utarbetat en gruppering av landets kommuner.

SKR:s kommungruppsindelning[8] syftar till att gruppera kommuner efter deras förutsättningar ur ett perspektiv sett till befolkningsstorlek, geografiskt täthet och närhet till större städer eller tätorter.

Kommunerna är indelade i tre huvudgrupper:

- Storstäder och storstadsnära kommuner
  - Storstäder, 3 kommuner
  - Pendlingskommun nära storstad, 43 kommuner
- Större städer och kommuner nära större stad
  - Större stad, 23 kommuner
  - Pendlingskommun nära större stad, 63 kommuner
  - Lågpendlingskommun nära större stad, 24 kommuner
- Mindre städer/tätorter och landsbygdskommuner
  - Mindre stad/tätort, 27 kommuner
  - Pendlingskommun nära mindre stad/tätort, 51 kommuner
  - Landsbygdskommun, 35 kommuner
  - Landsbygdskommun med besöksnäring, 21 kommuner

I tabellen nedan framgår en förteckning över kommungruppsindelningen, listan är sorterad enligt Bilaga 1 i Kommungruppsindelning.

Gruppkod	Kommun
A	Stockholm, Malmö, Göteborg, Upplands Väsby, Vallentuna, Österåker, Värmdö, Järfälla, Ekerö, Huddinge, Botkyrka, Salem, Haninge, Tyresö, Upplands-Bro, Täby, Danderyd, Sollentuna, Nacka, Sundbyberg, Solna, Lidingö, Vaxholm, Sigtuna, Nynäshamn, Håbo, Staffanstorp, Burlöv, Vellinge, Kävlinge, Lomma, Svedala, Skurup, Trelleborg, Kungsbacka, Härryda, Partille, Öckerö, Stenungsund, Ale, Lerum, Bollebygd, Lilla Edet, Mölndal, Kungälv, Alingsås
B	Södertälje, Uppsala, Eskilstuna, Linköping, Norrköping, Jönköping, Växjö, Kalmar, Lund, Helsingborg, Kristianstad, Halmstad, Trollhättan, Borås, Karlstad, Örebro, Västerås, Borlänge, Gävle, Sundsvall, Östersund, Umeå, Luleå, Nykvarn, Älvkarleby, Knivsta, Heby, Tierp, Enköping, Gnesta, Strängnäs, Trosa, Kinda, Åtvidaberg, Valdemarsvik, Söderköping, Mjölby, Aneby, Mullsjö, Habo, Vaggeryd, Lessebo, Alvesta, Torsås, Mörbylånga, Sölvesborg, Svalöv, Östra Göinge, Örkelljunga, Bjuv, Sjöbo, Hörby, Bromölla, Perstorp, Klippan, Åstorp, Landskrona, Höganäs, Eslöv, Ängelholm, Laholm, Grästorp, Mark, Svenljunga, Herrljunga, Vänersborg, Kil,

[8] Kommungruppsindelning (https://skr.se/download/18.ef4ba7d1849a2f55db2898a/1669978414789/Kommungruppsindelning-2023.pdf)

	Hammarö, Forshaga, Grums, Lekeberg, Hallsberg, Kumla, Nora, Surahammar, Hallstahammar, Sala, Gagnef, Säter, Ockelbo, Timrå, Krokom, Nordmaling, Bjurholm, Robertsfors, Vännäs, Östhammar, Finspång, Motala, Nässjö, Uppvidinge, Tingsryd, Nybro, Hässleholm, Hylte, Tranemo, Uddevalla, Ulricehamn, Munkfors, Kristinehamn, Laxå, Askersund, Lindesberg, Köping, Sandviken, Bräcke, Berg, Vindeln, Älvsbyn, Boden
C	Norrtälje, Nyköping, Katrineholm, Värnamo, Ljungby, Oskarshamn, Västervik, Gotland, Karlskrona, Karlshamn, Ystad, Falkenberg, Varberg, Mariestad, Lidköping, Skövde, Falköping, Karlskoga, Falun, Avesta, Ludvika, Hudiksvall, Härnösand, Örnsköldsvik, Skellefteå, Piteå, Kiruna, Vingåker, Oxelösund, Flen, Ödeshög, Ydre, Boxholm, Vadstena, Gnosjö, Sävsjö, Eksjö, Älmhult, Markaryd, Högsby, Hultsfred, Mönsterås, Emmaboda, Olofström, Ronneby, Höör, Tomelilla, Osby, Tjörn, Orust, Munkedal, Dals-Ed, Färgelanda, Vårgårda, Essunga, Karlsborg, Gullspång, Mellerud, Vara, Götene, Tibro, Töreboda, Åmål, Skara, Hjo, Tidaholm, Storfors, Degerfors, Ljusnarsberg, Skinnskatteberg, Kungsör, Norberg, Fagersta, Arboga, Smedjebacken, Hedemora, Hofors, Nordanstig, Gislaved, Vetlanda, Tranås, Vimmerby, Bengtsfors, Lysekil, Torsby, Sunne, Filipstad, Hagfors, Arvika, Säffle, Hällefors, Vansbro, Ovanåker, Ljusdal, Söderhamn, Bollnäs, Kramfors, Sollefteå, Ragunda, Strömsund, Norsjö, Malå, Dorotea, Vilhelmina, Åsele, Lycksele, Arvidsjaur, Överkalix, Kalix, Övertorneå, Pajala, Haparanda, Borgholm, Båstad, Simrishamn, Sotenäs, Tanum, Strömstad, Eda, Årjäng, Malung-Sälen, Leksand, Rättvik, Orsa, Älvdalen, Mora, Åre, Härjedalen, Storuman, Sorsele, Arjeplog, Jokkmokk, Gällivare

Så styrs kommunerna

Sverige är indelat i 21 regioner och 290 kommuner. Kommuner och regioner är självstyrande och styrs av regionalt och lokalt folkvalda politiker. Självstyret är grundlagsstadgat.

Kommunerna styrs av politiker som valts direkt av medborgarna, vilket betyder att medborgarna har stora möjligheter att påverka och kontrollera hur kommuner utför sina uppdrag.

Kommunerna styrs genom direktvalda politiska församlingar, så kallade kommunfullmäktige. Dessutom finns det politiska uppdrag inom kommunstyrelser, i olika nämnder och utskott. Det finns drygt 38 000 förtroendevalda i landets 290 kommuner. Merparten, 97 procent, är fritidspolitiker och sköter därmed sina uppdrag vid sidan av arbete eller studier.

Kommunfullmäktige är kommunens högsta beslutande organ. Kommunfullmäktige representerar folket i kommunen och tar beslut i kommunens viktigaste frågor.

Kommunfullmäktige:

- tar beslut om kommunens inriktning, verksamhet och ekonomi. De tar t.ex. beslut om budget, skattesats och avgifter för kommunal service.
- tar beslut om den kommunala förvaltningens organisation och verksamhetsformer.
- väljer ledamöter och ersättare till kommunstyrelsen och nämnderna.
- väljer revisorer som granskar kommunens verksamhet.
- utser Kommunstyrelsen

Kommunstyrelsen:

- leder och samordnar allt arbete inom kommunen.
- ansvarar för kommunens ekonomi.

Kommunfullmäktige beslutar vilka nämnder som ska finnas och väljer ledamöter. Varje nämnd ansvarar för ett visst område, exempel på nämnder som finns i många kommuner är miljönämnd, socialnämnd och kulturnämnd. Eftersom kommunerna själva bestämmer vilka nämnder de vill ha ser det olika ut runt om i Sverige. Alla frågor som kommer till fullmäktige förbereds i någon av nämnderna. I mindre frågor kan nämnderna besluta direkt.

Nämnderna:

- ansvarar för den löpande verksamheten inom kommunen.
- förbereder ärenden som ska beslutas av fullmäktige.
- genomför beslut som fattas i fullmäktige.

I praktiken är det tjänstemän som sköter själva genomförandet av kommuners verksamheter, men de förtroendevalda har alltid det yttersta ansvaret. Arbetsuppgifterna kan vara att ge byggnadslov, bevilja ekonomiskt bistånd eller att organisera äldreomsorgen.

Kommunernas informationssäkerhetsarbete

SKR ser att ett systematiskt och riskbaserat informationssäkerhetsarbete är en nödvändig del i en framgångsrik digitalisering för kommunerna och bedömer att området kräver ett ökat fokus.

Under våren 2023 genomförde SKR en uppföljning av hur långt kommunerna kommit i sitt systematiska informationssäkerhetsarbete. Kommunerna har sedan förra uppföljningen (2019) genomfört ett gediget arbete med det systematiska och riskbaserade informationssäkerhetsarbetet och det framgår en tydlig förbättring inom flera områden.

Det är nya regelverk på gång, t.ex. EU:s NIS2-direktiv, som kommer ställa tydligare och mer omfattande krav på kommunerna att arbete systematiskt och riskbaserat med sin informations- och cybersäkerhet.

Denna publikation vänder sig till både ledning och CISO i kommunerna.

Upplysningar om innehållet
Jonas Nilsson, jonas.nilsson@skr.se

© Sveriges Kommuner och Regioner, 2022
ISBN: 978-91-8047-222-7
Text: Jonas Nilsson
www.skr.se