Kommunernas informationssäkerhetsarbete

EN ÖVERGRIPANDE KARTLÄGGNING AV KOMMUNERNAS SYSTEMATISKA INFORMATIONSSÄKERHETSARBETE

Sveriges Kommuner och Regioner

Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

Under våren 2019 genomförde SKR en webbenkät om hur långt kommunerna[1] kommit i sitt systematiska informationssäkerhetsarbete.

Svarsfrekvensen var mycket god, hela 91% svarade:

- 242 (83%) svarade på hela enkäten
- 23 (8%) svarade på delar av enkäten
- 25 (9%) svarade inte på enkäten

Sammanfattning av resultatet:

Det finns en djup och bred förståelse av hur viktigt ett grundläggande systematiskt informationssäkerhetsarbete är för all fortsatt digitalisering. Det som fortfarande återstår på många håll är styrning, ledning, avsatta medel och resurser för arbetets planering och genomförande samt en tydlig uppföljning som är integrerad i övrig verksamhetsuppföljning.

Det återstår fortsatt arbete i införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete, inom samtliga områden vi undersökt i enkäten.

- Det finns en CISO[2] i nästan 6 av 10 kommuner, vilket är positivt för det fortsatta arbetet med informationssäkerhet.
- Färre än 3 av 10 kommunledningar informerar sig om statusen för informationssäkerhetsarbetet.
- I 2 av 10 kommuner omsätts ledningens mål i konkreta handlingsplaner.
- I strax över 5 av 10 kommuner finns en hantering av informationssäkerhetsriskerna. Detta visar att informationssäkerhet fått en tydlig roll i arbetet med riskhantering.
- Strax över 5 av 10 kommuner har ett etablerat arbetssätt för klassning av informationstillgångar.
- I 6 av 10 kommuner finns ett etablerat arbetssätt för hantering av informationssäkerhetsincidenter/-avvikelser.
- I 4 av 10 kommuner finns ett etablerat arbetssätt för planering som säkerställer verksamhetens kontinuitet.

[1] Undersökningen omfattar inte informationssäkerhet inom regioner eftersom MSB har undersökt detta och publicerat en rapport (https://www.msb.se/RibData/Filer/pdf/28722.pdf) under 2018.

[2] *CISO – Med CISO avses den som samordnar informationssäkerhetsarbetet. Vanliga benämningar är informationssäkerhetssamordnare, informationssäkerhetsstrateg eller informationssäkerhetskoordinator. I denna enkät kallar vi denna person för CISO, en förkortning efter den engelska titeln Chief Information Security Officer.*

- I 5 av 10 kommuner finns ett etablerat arbetssätt för att säkerställa medarbetarnas informationssäkerhetsmedvetande.
- I drygt 3 av 10 kommuner finns ett etablerat arbetssätt för säkerställande av att informationssäkerheten beaktas i hela upphandlingsprocessen.
- Det är bara drygt 2 av 10 kommuner som har ett etablerat arbetssätt för att följa upp tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet.

Under maj 2019 följdes webbenkäten upp med djupintervjuer för att försöka hitta gemensamma framgångsfaktorer och identifiera vilka slags hinder som kommunerna står inför.

Baserat på svaren framgår att förutsättningarna för ett lyckat införande av systematiskt informationssäkerhetsarbete verkar vara bäst där:

- det finns erfarenhet av att arbeta med sekretess,
- man genomgår en transformation mot ökad digitalisering eller
- där drivna medarbetare getts tillfälle att arbeta med frågan.

De nya utmaningar som digitaliseringen för med sig, genom att allt fler uppgifter lagras och kommuniceras via teknik, väcker frågan om informationssäkerheten kring hur tekniken används. Att ansvarsfrågan kopplas till verksamhetens informationsägare och ledningens ansvar för helheten gör att medarbetare som länge jobbat med informationssäkerhetsfrågan fått större förtroende och därmed lyckats etablera en högre medvetandegrad i hela organisationen.

På en direkt fråga till de medarbetare som har ansvar för informationssäkerhetsarbetet, om vilka svårigheter de upplever i sitt dagliga arbete, blir svaret:

- svårt att hitta metoder för att skapa insikt i organisationen kring det grundläggande behovet av informationssäkerhetsarbete
- svårt att få sändningstid och möjlighet att väcka ledningens engagemang
- Behov av tydligt uppdrag, resurser och tid för att arbeta systematiskt med informationssäkerhet
- Behov att koppla informationssäkerhetsarbetet till verksamhetsplanering och uppföljning

SKR ser sammantaget att informationssäkerhet endast ges tillräckligt med uppmärksamhet vid en incident eller när risken för en incident blir uppenbar. Detta medför att kommunens ledning inte ser behovet och nyttan av ett

proaktivt, systematiskt arbete med informationssäkerhet, vilket i sig innebär att resurser inte avsätts förrän ”olyckan redan inträffat”.

Ett lyckat införande av ett systematiskt och riskbaserat informationssäkerhetsarbete hänger ofta samman med ledningens aktiva engagemang. Enkätsvaren visar att här kan många kommuner hitta förbättringsområden. En gemensam nämnare bland de kommuner som inte skattat sitt informationssäkerhetsarbete högt är att ledningen delegerat ansvaret för uppdraget, men inte tilldelat resurser. Risken med att delegera denna styrningsfråga är att ledningen får stå till svars för incidenter och osäker hantering som man inte ens visste förekom. Det är också viktigt för både kommunens politiska och tjänstemannaledning att säkerställa att lagar och regelverk följs och ett framgångsrikt sätt att göra det är att föregå med gott exempel.

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

En framgångsrik väg framåt ser vi i de kommuner som valt att samarbeta. Både kring kompetens/resursdelning och att dela underlag, mallar och rutiner. Som i allt utvecklingsarbete är en samskapande inställning och en vilja att dela och att lära av varandra en kostnadseffektiv lösning.

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

Inledning

SKR har som målsättning att alla våra medlemmar arbetar systematiskt med sitt informationssäkerhetsarbete för att skydda individers integritet och bevara invånarnas förtroende för välfärdsleveransen.

En väsentlig del av det systematiska informationssäkerhetsarbetet är utvärdering av informationssäkerhetsarbetet och dess styrning. Genom att en kommun 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.

För att stödja kommunerna i deras arbete med utvärdering av informationssäkerhetsarbetet och dess styrning har SKR utvecklat en webbenkät.

Enkäten syftar till att följa upp det systematiska arbetet med informationssäkerhet inom kommunerna. Resultaten kan även användas för att stödja kommunerna i det systematiska arbetssättet och av kommunerna själva för uppföljning av arbetet. Resultatet presenteras för den högsta ledningen i samband med ledningens genomgång.

Frågorna i enkäten fokuserar på det övergripande systematiska informationssäkerhetsarbetet inom kommunen, den har alltså fokus på en 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[3] ansvarar för att leda och styra verksamhetens systematiska informationssäkerhetsarbete i syfte att säkerställa att det är effektivt. Ledningen ska fatta beslut om arbetets inriktning och resurser.

[3] *Med ledning avses antingen den politiska eller tjänstemannaledningen.*

Tillvägagångssätt

SKR utarbetade webbenkäten tillsammans med MSB, med stöd från statistiksektionen på avdelningen för ekonomi och styrning. Enkäten var tillgänglig för kommunerna att besvara under perioden 25 mars till den 3 maj 2019. Webbenkäten skickades till registrator eller motsvarande, det vill säga kommunens officiella e-postadress (till exempel info@kommunen.se).

Enkäten var 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.

Team informationssäkerhet vid avdelningen för digitalisering hade under perioden 23 april till 29 maj 2019 två LIA-praktikanter[4] som hade i uppdrag att följa upp enkäten med intervjuer.

- För genomförandet av intervjuerna gjordes ett urval, baserat på kommunernas egen skattning, 5 kommuner som skattat sitt eget arbete högt och 5 kommuner som lämnat ofullständiga svar eller skattat sig själva lågt.

Utgångspunkten för uppföljningen var att genomföra två intervjuer i respektive utvald kommun.

Intervjuerna för de kommuner som skattade sig högt fokuserade frågorna på framgångsfaktorer i arbetet med införandet av ett systematiskt och riskbaserat arbete med informationssäkerhet.

Intervjuerna för de kommuner som lämnat ofullständiga svar eller skattat sig själva lågt fokuserade på vilka hinder de upplevde i arbetet med införandet av ett systematiskt och riskbaserat arbete med informationssäkerhet.

[4] *Med ”LIA” menas Lärande I Arbete.*

Mognadsmodellen

För att underlätta en organisations arbete med sitt systematiska informationssäkerhetsarbete har MSB utvecklat en mognadsmodell, se bilden nedan.

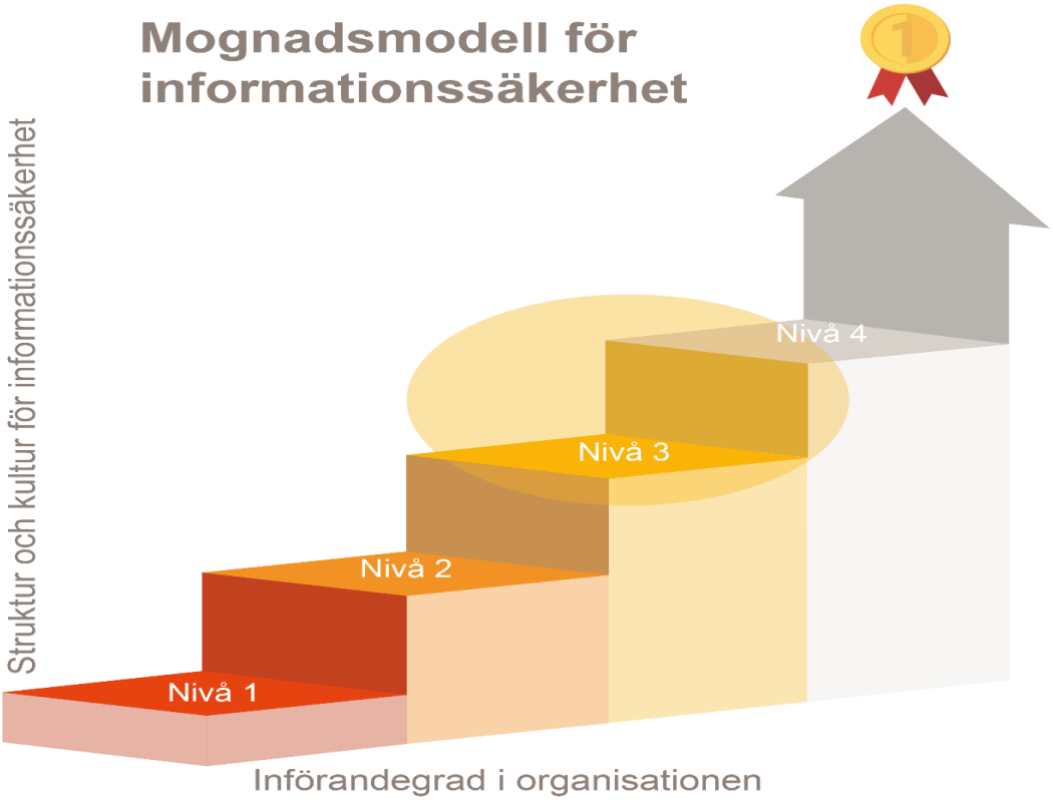

Bild 1: Mognadsmodell för det systematiska och riskbaserade informationssäkerhetsarbetet

För att en organisation ska anses ha uppnått ett systematiskt och riskbaserat informationssäkerhetsarbete bör den ha nått nivå 3, som motsvarar identifierad målnivå. Nivå 2 motsvarar lägstanivån för en tillfredsställande struktur i arbetet.

Övergripande kan de fyra nivåerna förklaras på följande sätt[5]:

- **Nivå 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.

[5] *En bild av landstingens informationssäkerhetsarbete 2018 - Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (Publikationsnummer: MSB1254 - oktober 2018)*

- **Nivå 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.
- **Nivå 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.
- **Nivå 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 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 nivå 3.

Enkätresultat, analys och slutsatser

Frågeområden

Undersökningen tar upp dessa frågeområden:

1. Funktion för informationssäkerhet
2. Information till ledningen
3. Handlingsplan utifrån nuläget
4. Hantering av informationssäkerhetsrisker
5. Informationsklassning
6. Incident-/avvikelsehantering
7. Kontinuitetsplanering
8. Informationssäkerhetsmedvetande inom organisationen
9. Informationssäkerhetsrelaterade krav vid upphandlingar
10. Uppföljning

Funktion för informationssäkerhet

Detta frågeområde fokuserar på huruvida det finns en person (t.ex. CISO) som har ett övergripande ansvar för att leda och samordna arbetet med informationssäkerhet inom kommunen.

Detta var en Ja/Nej-fråga, där 250 av kommunerna svarat.

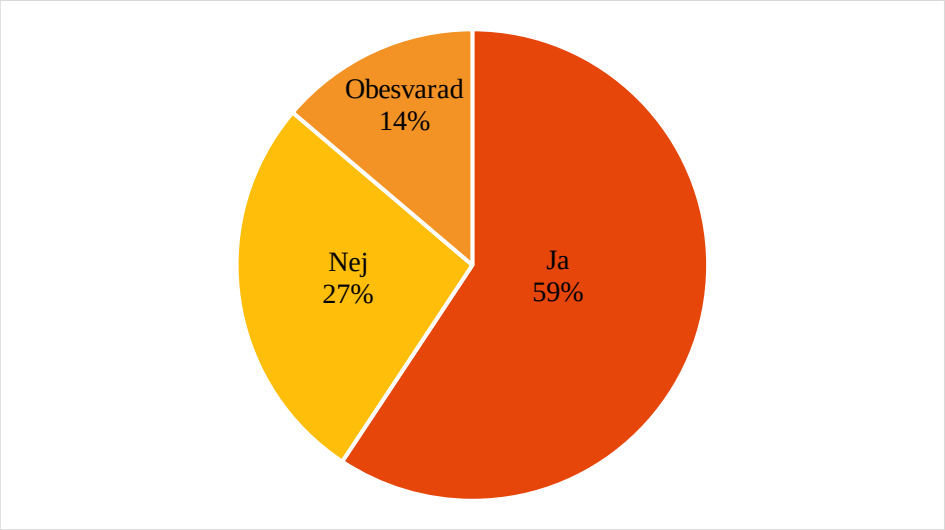

Bild 1: Har er kommun en CISO med uppdrag att samordna det övergripande informationssäkerhetsarbetet?

Det finns en CISO i nästan 6 av 10 kommuner, vilket är positivt för det fortsatta arbetet med informationssäkerhet.

De som uppgivit att det finns en CISO har fått en följdfråga, avseende uppskattad tid som denna person kan avsätta, av sin ordinarie arbetstid, till informationssäkerhetsarbete.

Detta var en flervalsfråga, där 169 av kommunerna svarat.

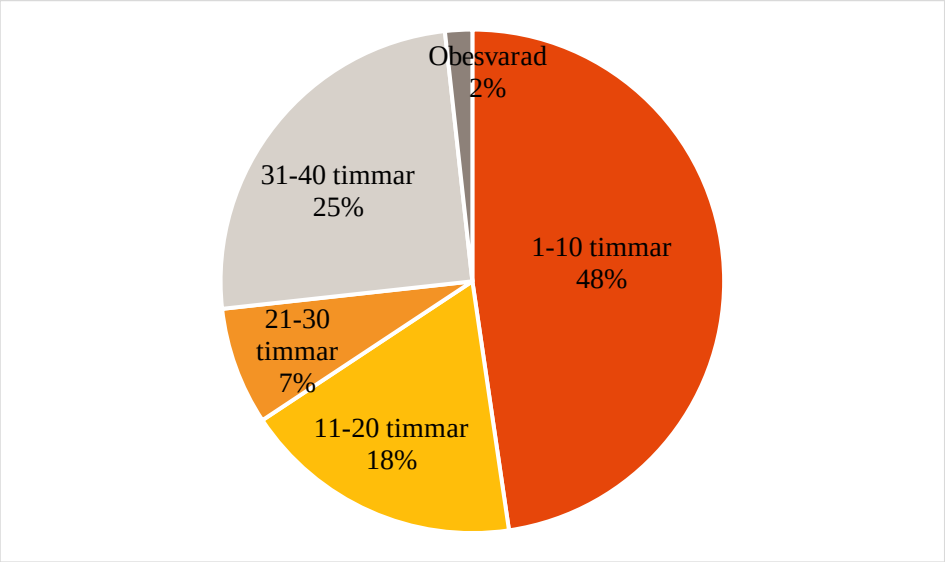

Bild 2: Hur mycket tid avsätter CISO av sin ordinarie arbetstid till informationssäkerhetsarbete?

Det är positivt att det finns en CISO i nästan två tredjedelar av kommunerna, detta innebär att det finns goda förutsättningar för införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete inom kommunerna.

Det skulle dock vara positivt om fler än en tredjedel av kommunernas CISO fick möjligheten att avsätta mer än halva sin ordinarie arbetstid till informationssäkerhetsarbetet. Det skulle snabba på arbetet med införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete, som är en viktig grundförutsättning för den fortsatta digitaliseringsresa som kommunerna har påbörjat.

Information till ledningen

Detta frågeområde fokuserar på huruvida ledningen är insatt och aktivt leder och styr informationssäkerhetsarbetet. Ett viktigt redskap för ledningen att informera sig samt leda och styra är ledningens genomgång. Vid ledningens genomgång kan till exempel riskutveckling, inträffade incidenter, vidtagna åtgärder och förslag till förbättringar lyftas.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

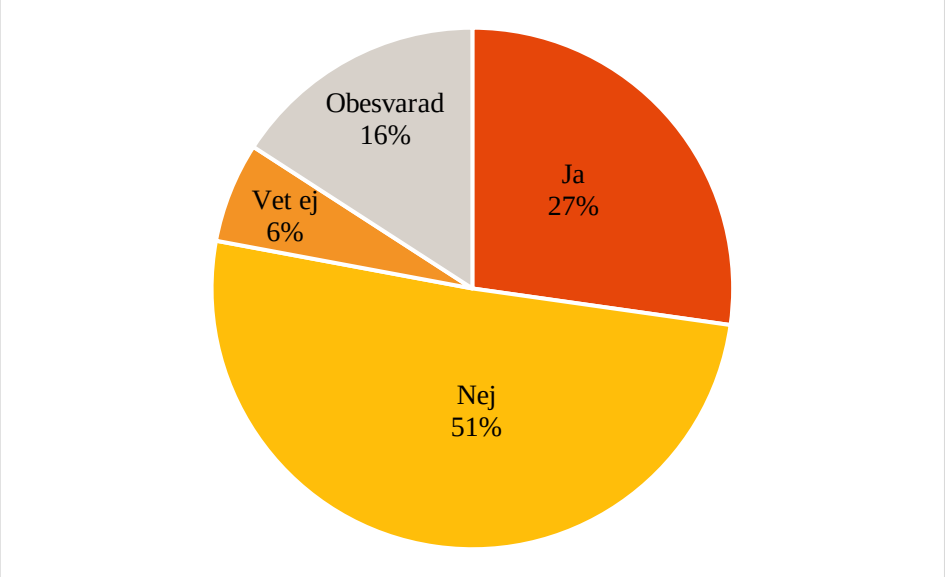

Bild 3: Har ni ett etablerat arbetssätt[6] så att ledningen regelbundet informerar sig och beslutar i informationssäkerhetsfrågor?

Det är bara 3 av 10 kommunledningar som regelbundet informerar sig om statusen för informationssäkerhetsarbetet och fattar beslut i frågan.

De som uppgivit att ledningen informerar sig och beslutar i informationssäkerhetsfrågor har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att ledningen regelbundet informerar sig.

[6] *Med ”etablerat arbetssätt” menas utarbetade och beslutade arbetssätt som används konsekvent i relevanta processer.*

Detta var en flervalsfråga, där 79 av kommunerna svarat.

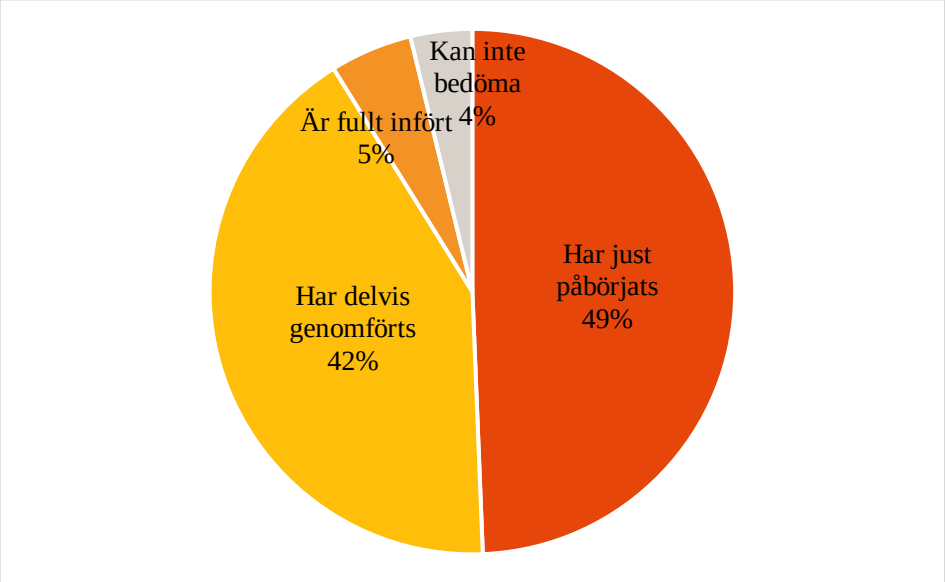

Bild 4: Till vilken grad har organisationen infört ett etablerat arbetssätt så att ledningen regelbundet informerar sig och beslutar i informationssäkerhetsfrågor?

Att bara knappt 3 av 10 kommunledningar utnyttjar sin rättighet att informera sig om statusen för informationssäkerhetsarbetet är oroväckande.

Ett systematiskt och riskbaserat informationssäkerhetsarbete är en grundförutsättning för att skapa tillit till den digitalisering som sker inom kommunerna. Det är därför av vikt att fler kommunledningar informerar sig om statusen för informationssäkerheten inom kommunen.

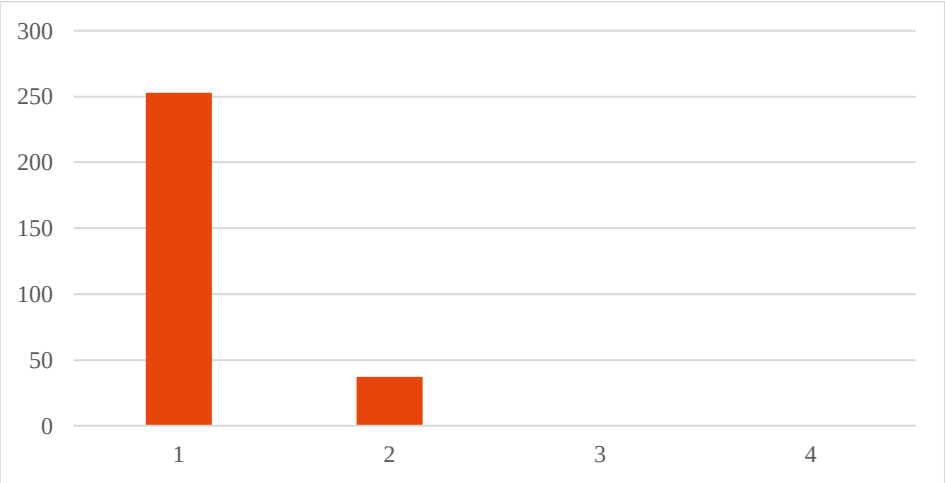

Bild 5: Mognadsnivån för ledningens engagemang.

Nästan 9 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende ledningens engagemang. Här har vi ett stort arbete framför oss, då det är ledningen som beslutar om inriktning för det fortsatta systematiska informationssäkerhetsarbetet.

Handlingsplan utifrån nuläget

Detta frågeområde fokuserar på huruvida det finns ett dokument i vilket det framgår vilka informationssäkerhetsrelaterade aktiviteter som det har tagits beslut om, för att åtgärda brister och sårbarheter. I handlingsplanen bör det finnas detaljerad information om varje aktivitet, så som ansvarig, vilka resurser som finns och tidplan för genomförandet av aktiviteten.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

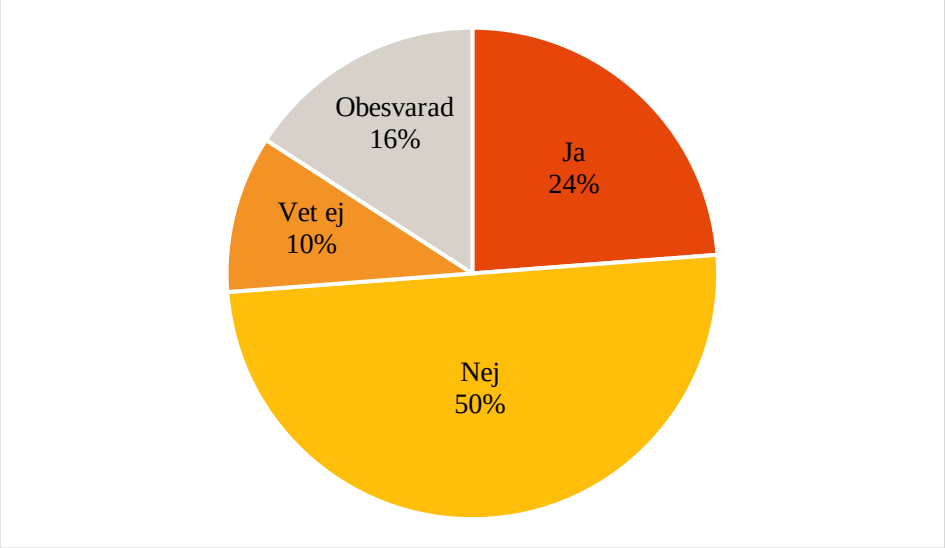

Bild 6: Har ni ett etablerat arbetssätt så att ledningens mål omsätts i konkreta handlingsplaner?

Det är bara i drygt 2 av 10 kommuner som ledningens mål omsätts i konkreta handlingsplaner. Det är viktigt för informationssäkerheten att ledningens beslut och viljeyttringar omsätts i konkreta handlingsplaner, med aktiviteter.

De som uppgivit att ledningens beslut och viljeyttringar omsätts i konkreta handlingsplaner har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att ledningens beslut och viljeyttringar omsätts i konkreta handlingsplaner.

Detta var en flervalsfråga, där 69 av kommunerna svarat.

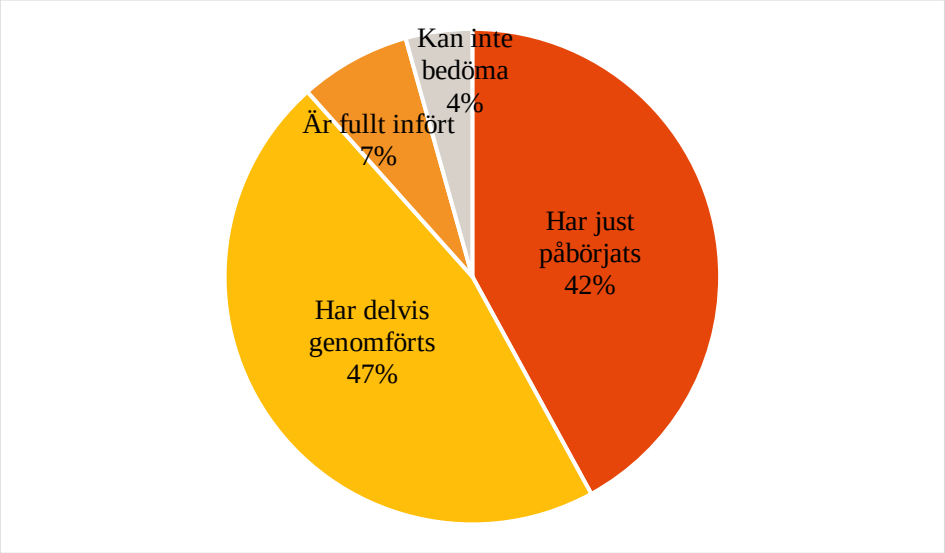

Bild 7: Till vilken grad har organisationen infört ett etablerat arbetssätt så att ledningens beslut och viljeyttringar omsätts i konkreta handlingsplaner?

Att bara drygt 2 av 10 kommuner omsätter ledningens mål till konkreta handlingsplaner är inte tillfredsställande. Det är av vikt att ledningens beslut och viljeyttring omsätts i handlingsplaner.

Om detta resultat kopplas till föregående fråga (där bara 1/3 av kommunledningarna informerar sig om statusen för informationssäkerhet) ger en ännu dystrare läsning, d.v.s. endast ca 8 % av kommunerna har en process att informera ledningen och omsätta beslut till aktiviteter.

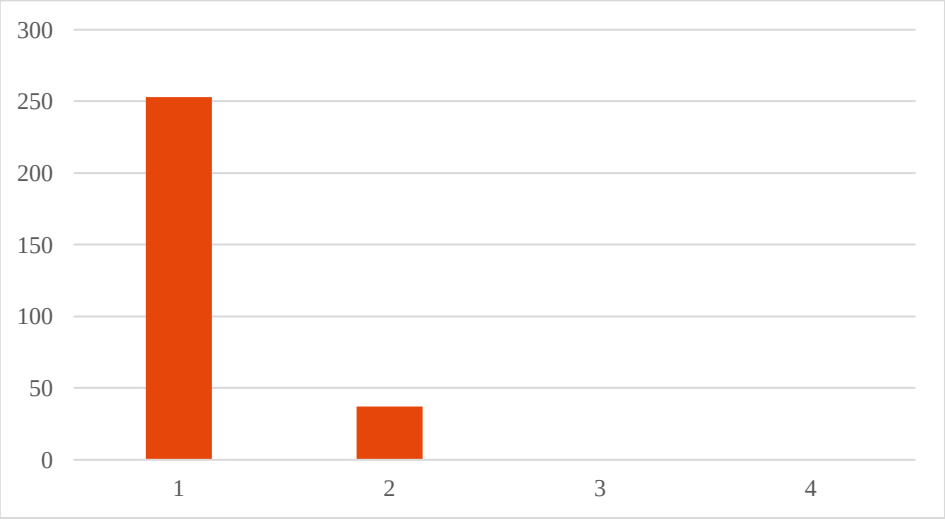

Bild 8: Mognadsnivån för kommunernas omsättning av ledningens mål i konkreta handlingsplaner.

Nästan 9 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende omsättning av ledningens mål i konkreta handlingsplaner. Här har vi ett stort arbete framför oss.

Hantering av informationssäkerhetsrisker

Detta frågeområde fokuserar på hur kommunen hanterar (genom att identifiera, prioritera, förebygga och följa upp) de risker som skulle kunna äventyra informationssäkerheten, t.ex. orsaka röjande av personuppgifter eller avbrott i verksamhetskritiska system.

Detta var en Ja/Nej-fråga, där 243 av kommunerna svarat.

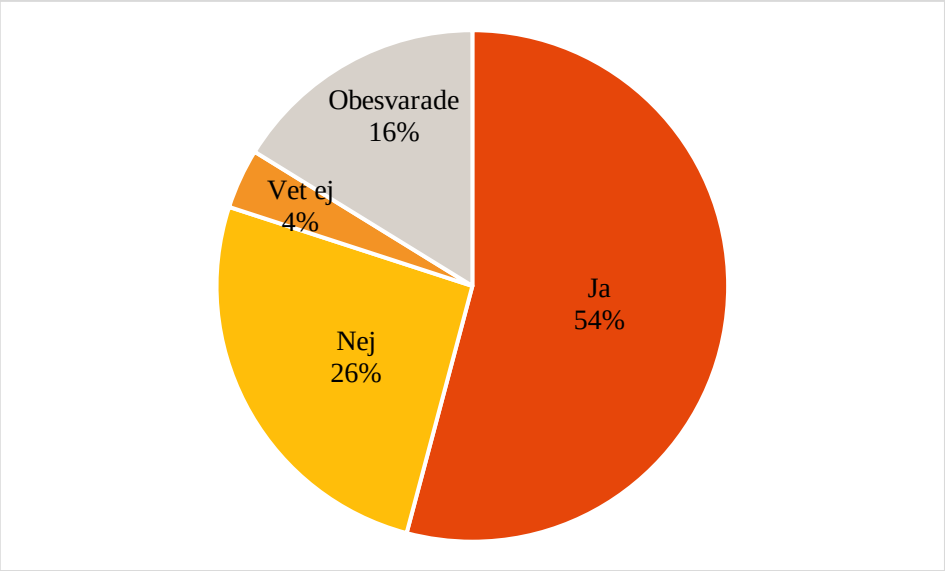

Bild 9: Har ni ett etablerat arbetssätt så att informationssäkerhetsriskerna hanteras?

I mer än 5 av 10 kommuner finns en hantering av informationssäkerhetsriskerna. Detta visar att informationssäkerhet fått en tydlig roll i arbetet med riskhantering.

De som uppgivit att det finns en hantering av informationssäkerhetsriskerna har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att informationssäkerhetsfrågorna hanteras.

Detta var en flervalsfråga, där 157 av kommunerna svarat.

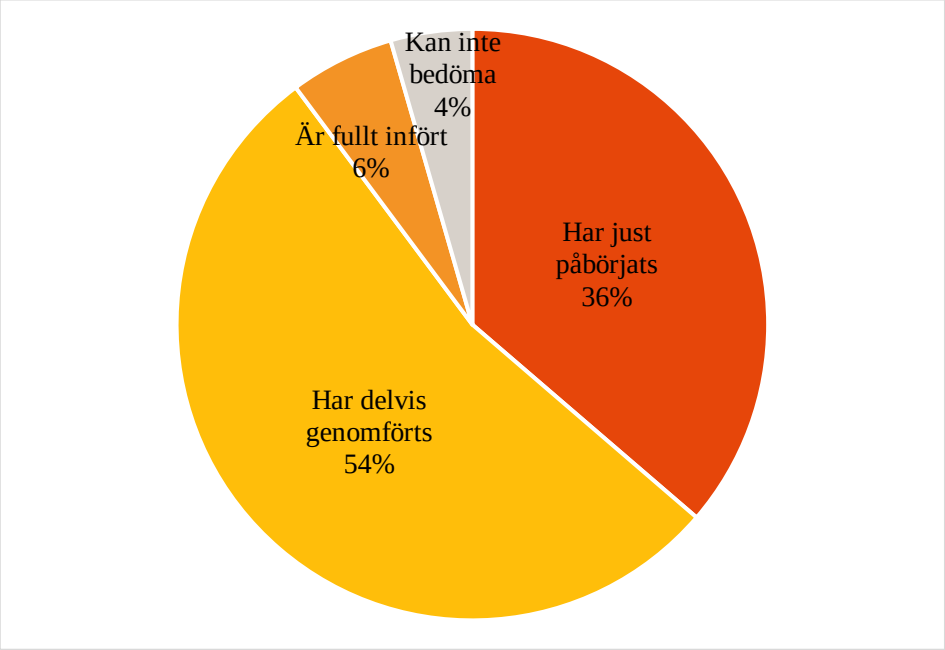

Bild 10: Till vilken grad har organisationen infört ett etablerat arbetssätt så att informationssäkerhetsriskerna hanteras?

Det är positivt att mer än 5 av 10 kommuner har en hantering av informationssäkerhetsriskerna. Riskhantering är en central del av ett systematiskt informationssäkerhetsarbete.

Det är också positivt att införandet av riskhanteringsprocessen kommit långt.

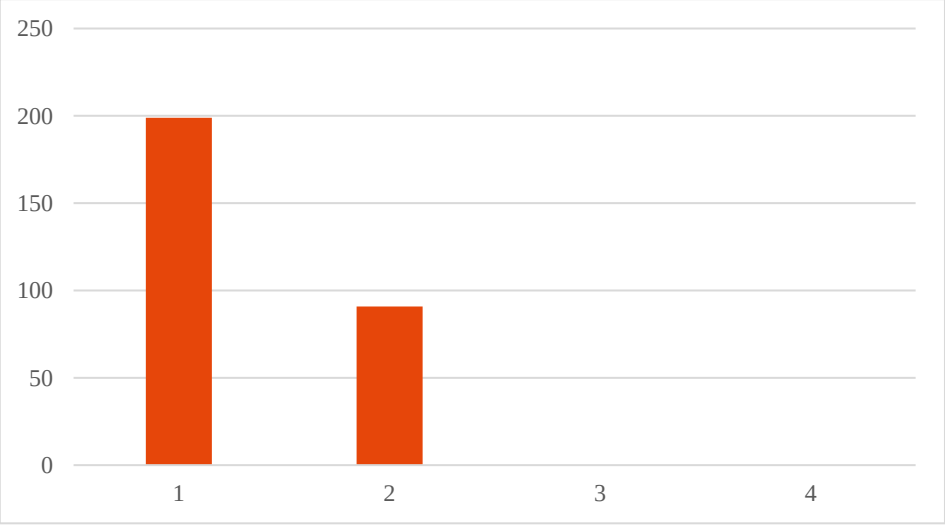

Bild 11: Mognadsnivån för kommunernas hantering av informationssäkerhetsrisker.

Nästan 7 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende hantering av informationssäkerhetsriskerna. Trots en något högre mognadsnivå har vi ett stort arbete framför oss även inom detta område.

Informationsklassning

Detta frågeområde fokuserar på huruvida det inom kommunen har identifierats vilken information som hanteras, samt att informationen klassas utifrån en beslutad modell som tar hänsyn till interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

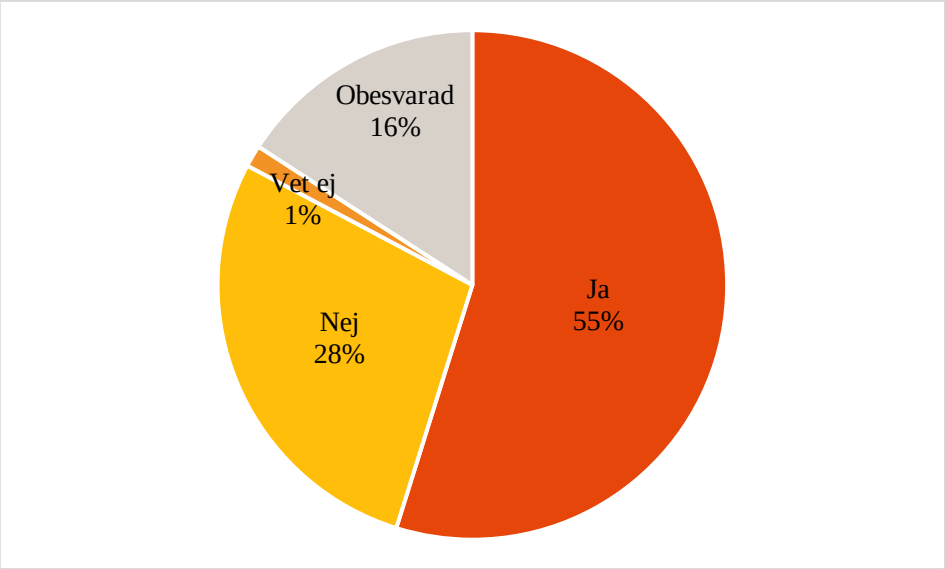

Bild 12: Har ni ett etablerat arbetssätt så att informationstillgångarna klassas?

I mer än 5 av 10 kommuner finns ett etablerat arbetssätt för klassning av informationstillgångar. Detta visar att kommunerna kommit igång med informationsklassning, och därmed kan uppnå en förmåga att säkerställa att informationen ges rätt skydd.

De som uppgivit att det finns en modell för klassning av informationstillgångar har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att informationstillgångarna klassas.

Detta var en flervalsfråga, där 159 av kommunerna svarat.

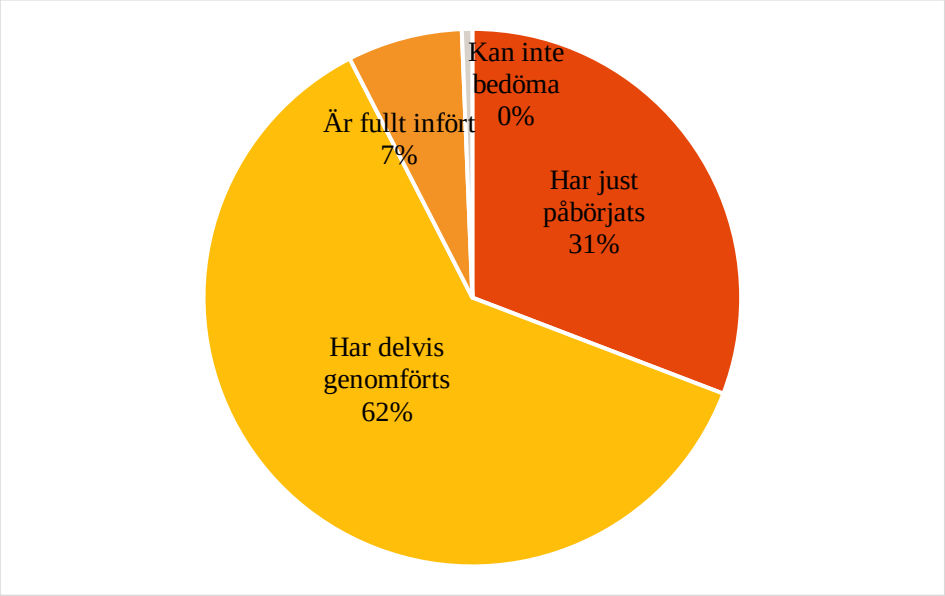

Bild 13: Till vilken grad har organisationen infört ett etablerat arbetssätt så att informationstillgångarna klassas?

Det är väldigt positivt att mer än 5 av 10 kommuner har ett etablerat arbetssätt för klassning av informationstillgångar. Informationssäkerhetsklassning är en annan central del av ett systematiskt informationssäkerhetsarbete.

Det är också väldigt positivt att införandet av klassningsprocessen kommit så långt.

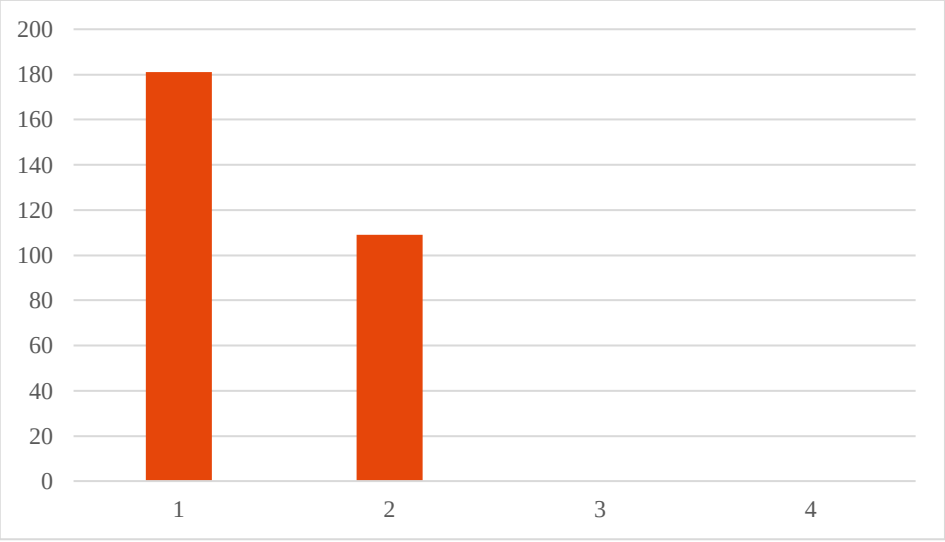

Bild 14: Mognadsnivån för kommunernas klassning av informationstillgångar.

Nästan 4 av 10 kommuner befinner sig på nivå 2 i mognadsmodellen avseende klassning av informationstillgångar. Detta område är ett av de mer mogna, men det finns fortfarande mycket jobb framåt.

Incident-/avvikelsehantering

Detta frågeområde fokuserar på huruvida incidenter och avvikelser rapporteras och åtgärdas (minimera skadan), samt hur de analyseras, utreds och förbättringar som införs och hur förbättringen följs, d.v.s. om den har fått avsedd effekt, så att problemet inte inträffar igen.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

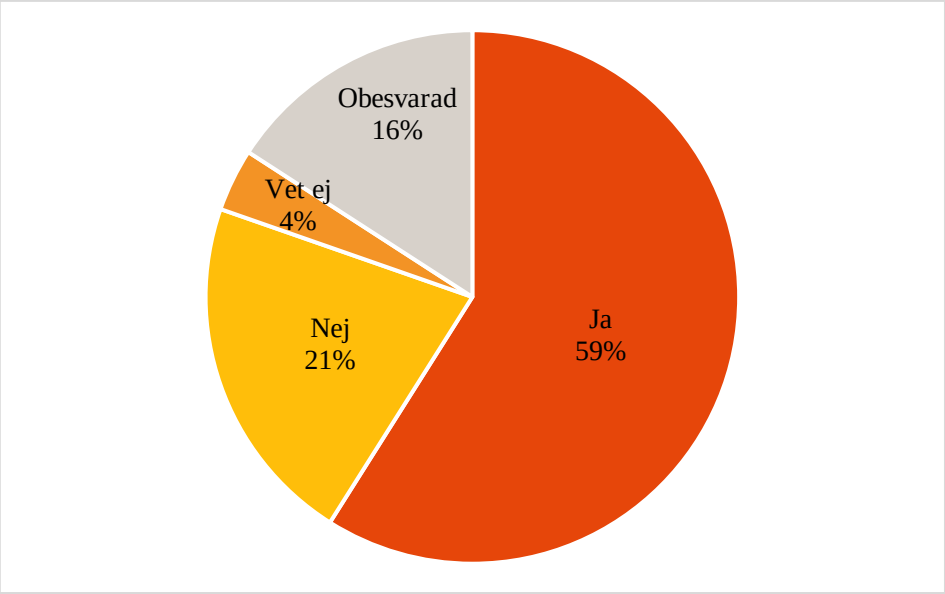

Bild 15: Har ni ett etablerat arbetssätt så att informationssäkerhetsincidenter/-avvikelser hanteras?

I 6 av 10 kommuner finns ett etablerat arbetssätt för hantering av informationssäkerhetsincidenter/-avvikelser.

De som uppgivit att det finns ett etablerat arbetssätt för hantering av informationssäkerhetsincidenter/-avvikelser har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att informationssäkerhetsincidenter/-avvikelser hanteras.

Detta var en flervalsfråga, där 171 av kommunerna svarat.

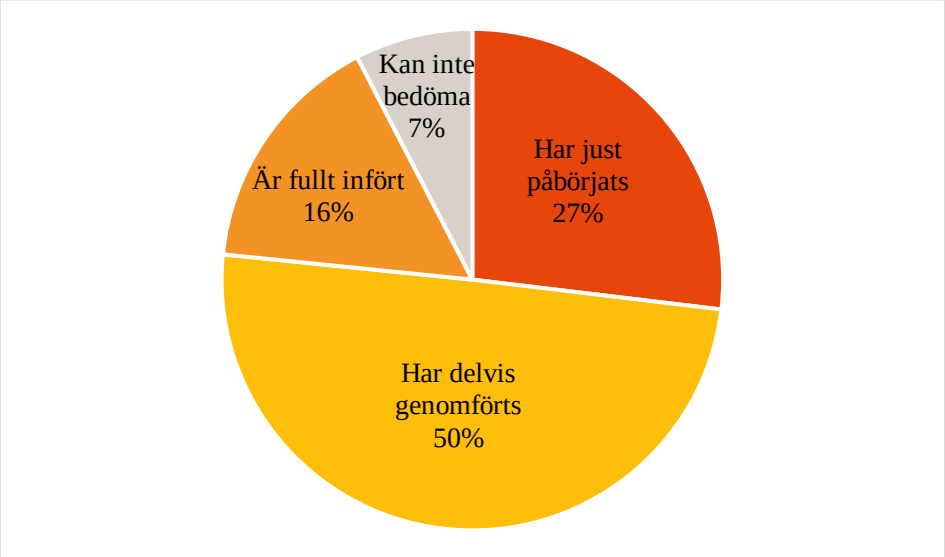

Bild 16: Till vilken grad har organisationen infört ett etablerat arbetssätt så att informationssäkerhetsincidenter/-avvikelser hanteras?

Det är positivt att 6 av 10 kommunerna har ett etablerat arbetssätt för hantering av informationssäkerhetsincidenter/-avvikelser. Incidenthantering är också en central del av ett systematiskt informationssäkerhetsarbete, där det handlar om att lära sig av de incidenter/avvikelser som sker inom kommunen.

Det är också positivt att införandet av riskhanteringsprocessen kommit så långt, detta visar att kommunerna har haft ett bra fokus på arbetet med hantering av informationssäkerhetsincidenter/-avvikelser, här har säkert GDPR och NIS-direktivet haft en positiv inverkan.

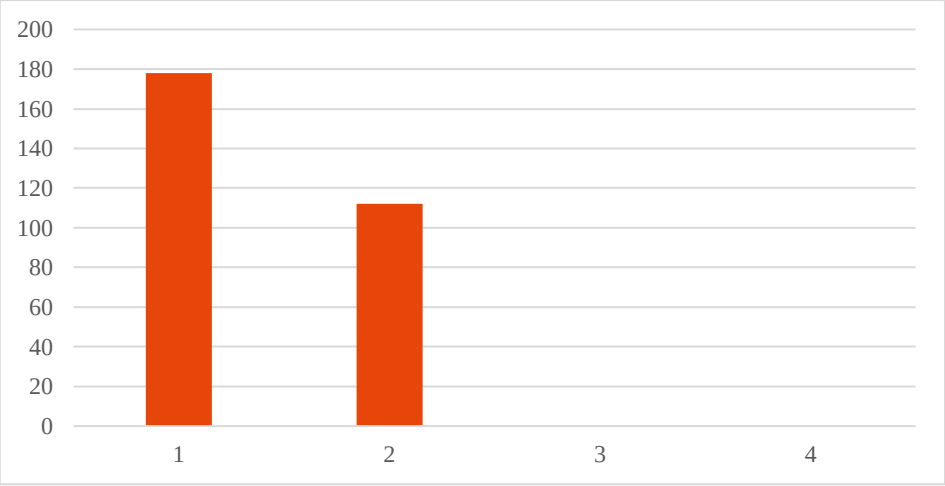

Bild 17: Mognadsnivån för kommunernas hantering av informationssäkerhetsincidenter/-avvikelser.

Nästan 4 av 10 kommuner befinner sig på nivå 2 i mognadsmodellen avseende hantering av informationssäkerhetsincidenter/-avvikelser. Detta är också ett av de mer mogna områdena, men det är viktigt att ha fokus då hantering av incidenter/avvikelser ger verksamheten värdefull information kring den fortsatta utvecklingen.

Kontinuitetsplanering

Detta frågeområde fokuserar på 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.

Detta var en Ja/Nej-fråga, där 238 av kommunerna svarat.

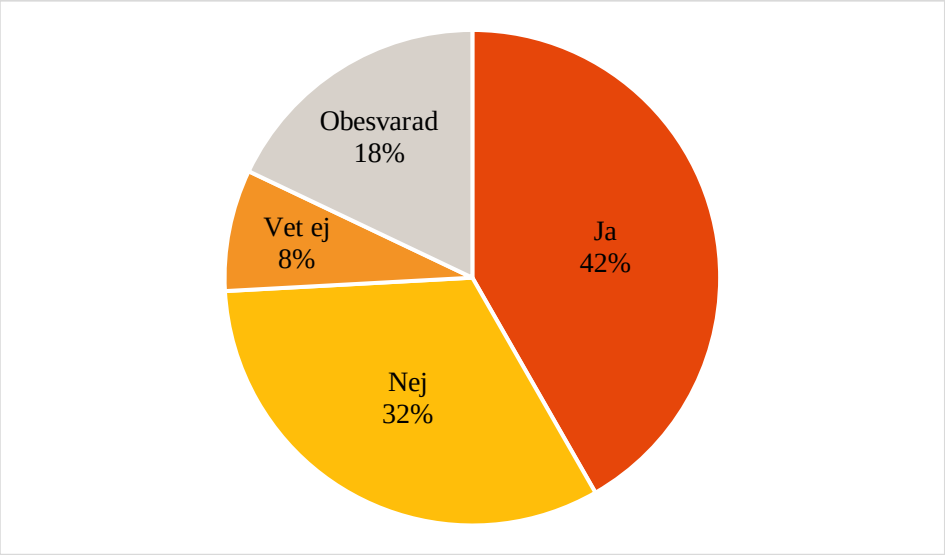

Bild 18: Har ni ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs?

I 4 av 10 kommuner finns ett etablerat arbetssätt för planering som säkerställer verksamhetens kontinuitet. Detta är inte en tillfredsställande nivå.

De som uppgivit att det finns ett etablerat arbetssätt för planering som säkerställer verksamhetens kontinuitet har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs.

Detta var en flervalsfråga, där 121 av kommunerna svarat.

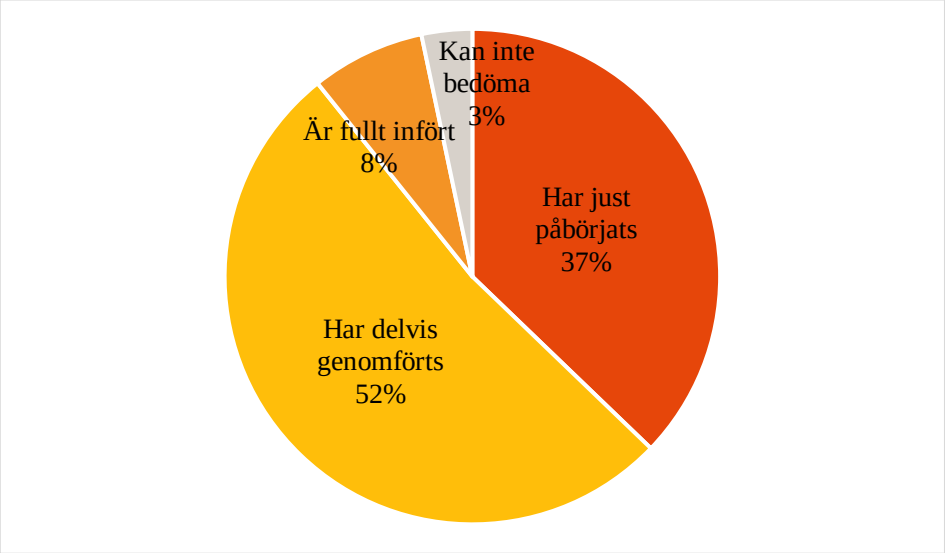

Bild 19: Till vilken grad har organisationen infört ett etablerat arbetssätt så att verksamhetens kontinuitet säkerställs?

Att det i mindre än hälften av kommunerna finns en planering som säkerställer verksamhetens kontinuitet är en siffra som borde vara mycket högre, en planeringsprocess för kontinuiteten borde vara en naturlig del inom kommunerna.

I denna planeringsprocess är det viktigt att inte missa informationssäkerheten (d.v.s. tillgängligheten till information i samband med t.ex. avbrott).

Det positiva är att de kommuner som har en planeringsprocess för kontinuiteten har kommit igång bra med införandet.

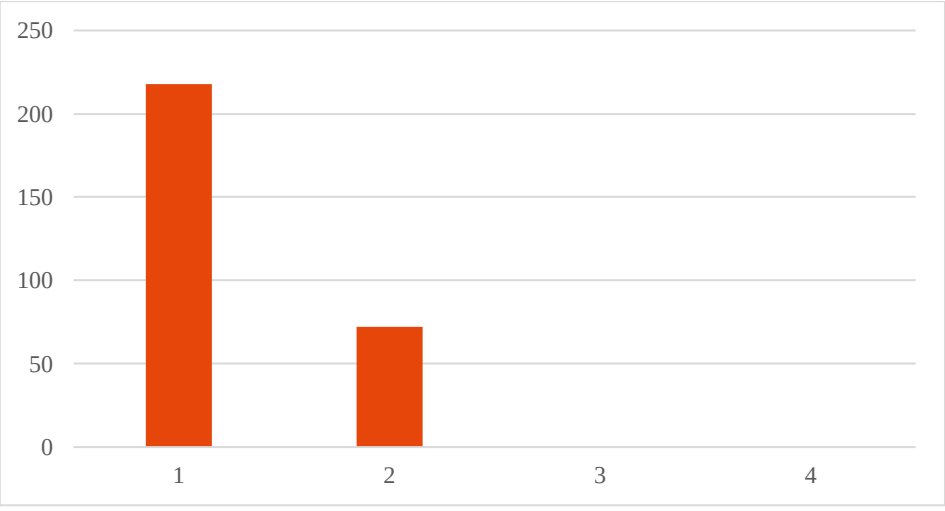

Bild 20: Mognadsnivån för kommunernas kontinuitetsplanering.

Mer än 7 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende planering som säkerställer verksamhetens kontinuitet. Detta område behöver 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.

Informationssäkerhetsmedvetande inom organisationen

Detta frågeområde fokuserar på hur kommunen arbetar för att höja informationssäkerhetsmedvetandet inom organisationen, samt ger stöd till chefer och medarbetare så att de kan arbeta enligt verksamhetens informationssäkerhetskrav. Detta kan till exempel ske genom utbildning samt genom vägledningar och annan kommunikation.

Detta var en Ja/Nej-fråga, där 243 av kommunerna svarat.

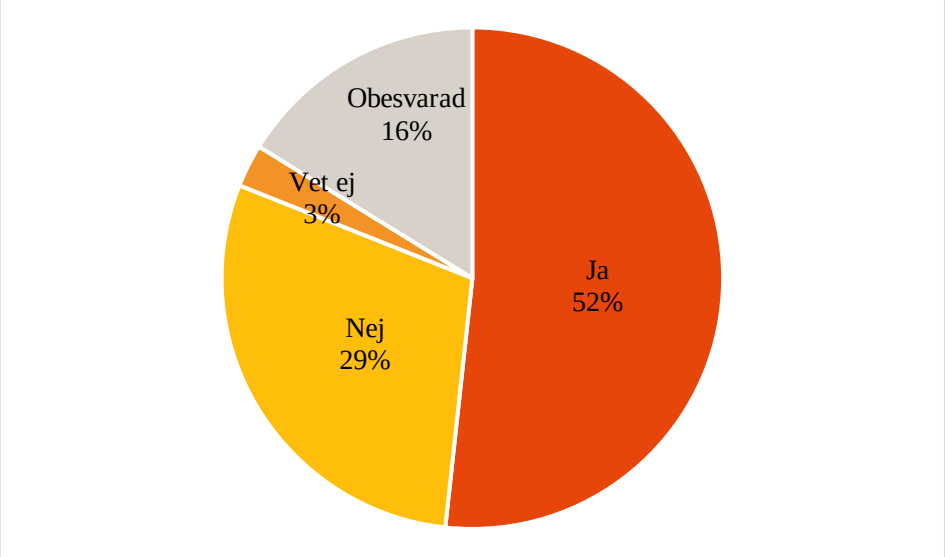

Bild 21: Har ni ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs?

I 5 av 10 kommuner finns ett etablerat arbetssätt för att säkerställa medarbetarnas informationssäkerhetsmedvetande, vilket är en ganska bra siffra. Detta visar på att kommunerna har börjat se till att kommunens medarbetare har tillfredsställande kompetensnivå inom informationssäkerhetsområdet.

De som uppgivit att det finns ett etablerat arbetssätt för att medarbetarnas informationssäkerhetsmedvetande säkerställs har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs.

Detta var en flervalsfråga, där 149 av kommunerna svarat.

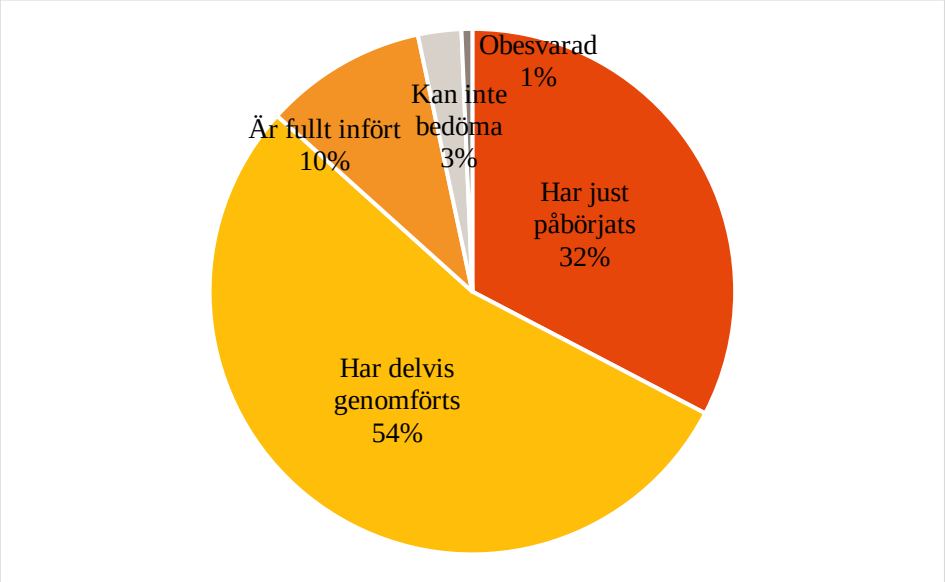

Bild 22: Till vilken grad har organisationen infört ett etablerat arbetssätt så att medarbetarnas informationssäkerhetsmedvetande säkerställs?

Det är positivt att konstatera att det i 5 av 10 kommuner finns ett etablerat arbetssätt för att säkerställa medarbetarnas informationssäkerhetsmedvetande.

Detta visar på att kommunerna lägger vikt vid kompetensperspektivet och arbetar med att utbilda medarbetarna inom informationssäkerhetsområdet.

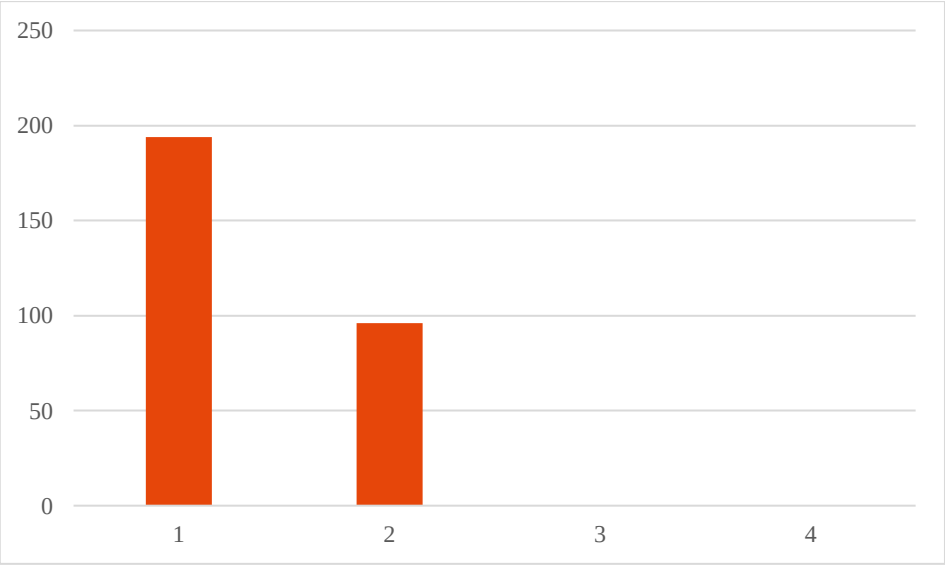

Bild 23: Mognadsnivån för kommunernas säkerställa av medarbetarnas informationssäkerhetsmedvetande.

Nästan 7 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende medarbetarnas informationssäkerhetsmedvetande. Detta område behöver få mer fokus i framtiden, då medarbetarnas informationssäkerhetsmedvetande är väsentligt för att skapa förutsättningar för efterlevnad av styrdokument.

Informationssäkerhetsrelaterade krav vid upphandlingar

Detta frågeområde fokuserar på huruvida kommunen har förmåga att fånga upp informationssäkerhetsrelaterade krav i hela upphandlingsprocessen, från behovsfångst, kravställning, tilldelning och avtal.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

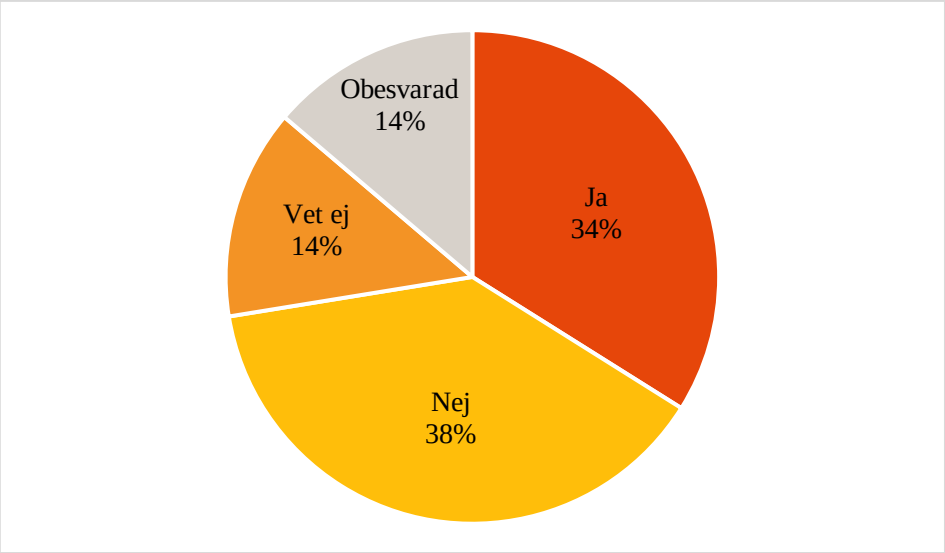

Bild 24: Har ni ett etablerat arbetssätt så att beaktningen av informationssäkerhet i hela upphandlingsprocessen säkerställs?

I drygt 3 av 10 kommuner finns ett etablerat arbetssätt för säkerställande av att informationssäkerheten beaktas i hela upphandlingsprocessen.

De som uppgivit att det finns ett etablerat arbetssätt för att säkerställa att informationssäkerheten beaktas i hela upphandlingsprocessen har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att beaktningen av informationssäkerhet i hela upphandlingsprocessen säkerställs.

Detta var en flervalsfråga, där 96 av kommunerna svarat.

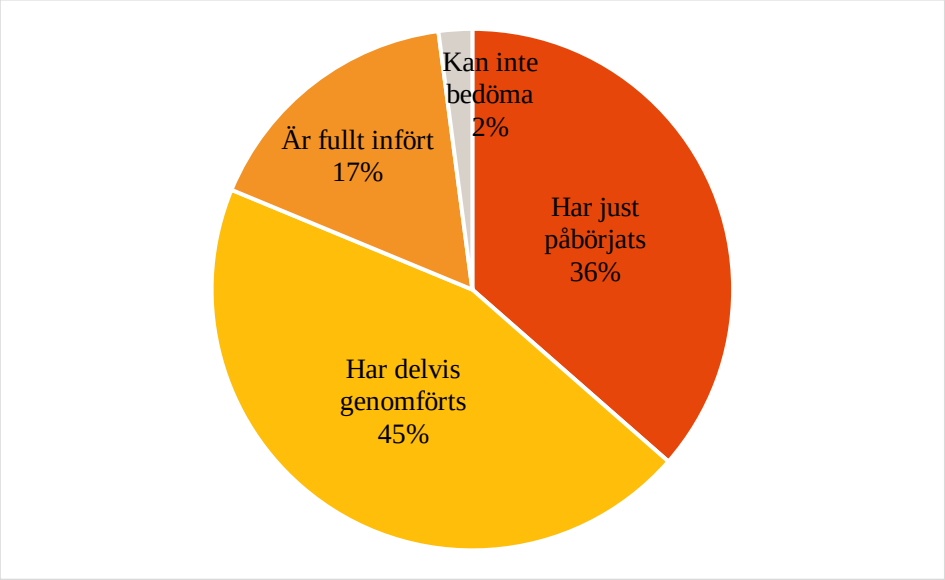

Bild 25: Till vilken grad har organisationen infört ett etablerat arbetssätt så att beaktningen av informationssäkerhet i hela upphandlingsprocessen säkerställs?

Att det endast i drygt 3 av 10 kommuner finns ett etablerat arbetssätt för säkerställande av att informationssäkerheten beaktas i hela upphandlings-processen är ingen tillfredsställande nivå.

Det är dock positivt att se att införandet, i de kommuner som har informations-säkerhet med i upphandlingar, är långt gången. Detta är positivt inför framtida digitaliseringssatsningar, där säkerhet och integritet måste finnas med i upphandlingsunderlagen.

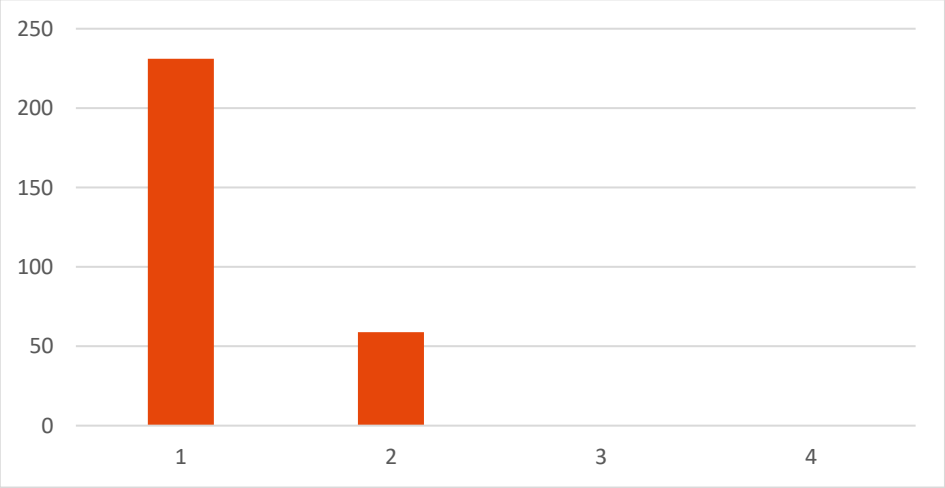

Bild 26: Mognadsnivån för kommunernas säkerställande av att informationssäkerheten beaktas i hela upphandlingsprocessen.

Nästan 8 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende att informationssäkerheten beaktas i hela upphandlingsprocessen. Detta område behöver få mer fokus i framtiden, då de lösningar som upphandlas ofta har en lång livscykel och verksamheten därmed får leva länge med dåliga lösningar.

Uppföljning

Detta frågeområde fokuserar på huruvida kommunen genomför uppföljningar i syfte att säkerställa att organisationen och leverantörer efterlever regler, styrdokument och villkor.

Detta var en Ja/Nej-fråga, där 244 av kommunerna svarat.

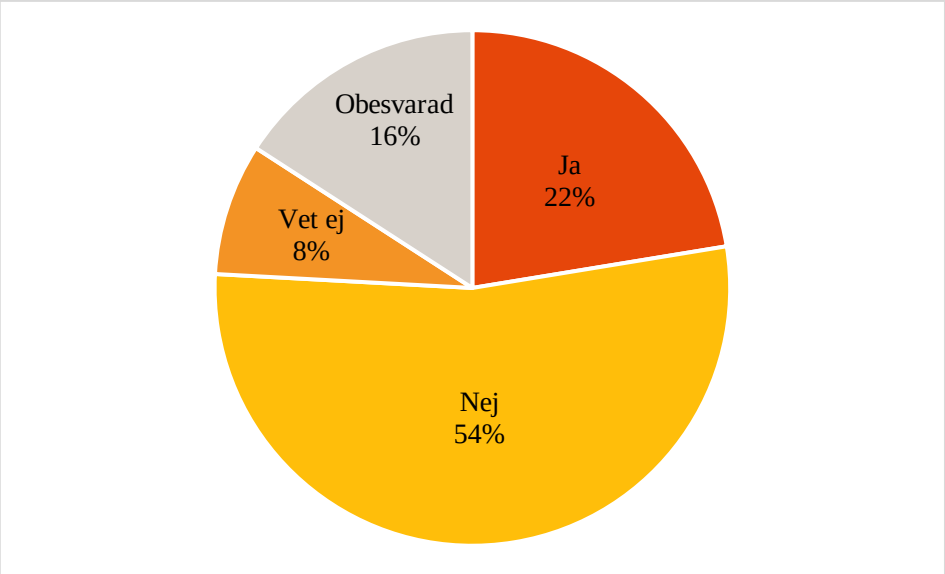

Bild 27: Har ni ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (till exempel. egenkontroll, leverantörsuppföljning, revisioner) följs upp?

Det är bara drygt 2 av 10 kommuner som har ett etablerat arbetssätt för att följa upp tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet.

De som uppgivit att det finns ett etablerat arbetssätt för att följa upp tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet har fått en följdfråga, avseende till vilken grad kommunen infört ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (till exempel egenkontroll, leverantörsuppföljning, revisioner.) följs upp.

Detta var en flervalsfråga, där 65 av kommunerna svarat.

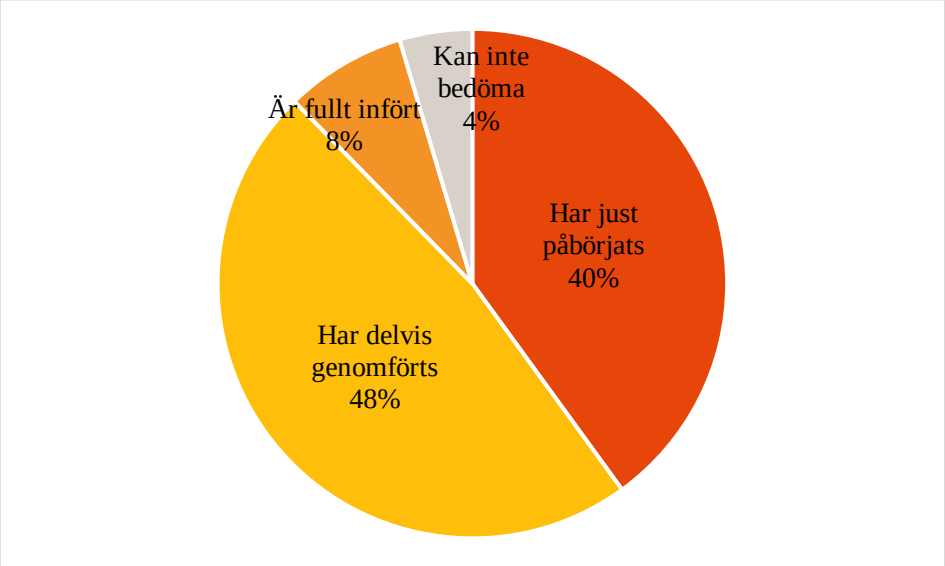

Bild 28: Till vilken grad har organisationen infört ett etablerat arbetssätt så att tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet (till exempel. egenkontroll, leverantörsuppföljning, revisioner) följs upp?

Det är bara drygt 2 av 10 kommuner som har ett etablerat arbetssätt för att följa upp tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet, detta är inte en tillfredsställande nivå.

Att följa upp statusen inom informationssäkerheten inom kommunen är ett viktigt redskap för att säkerställa den fortsatta lämpligheten, tillräckligheten och verkan av det systematiska och riskbaserade informationssäkerhetsarbetet. Uppföljningen är också en viktig pusselbit för informationen till kommunledningen.

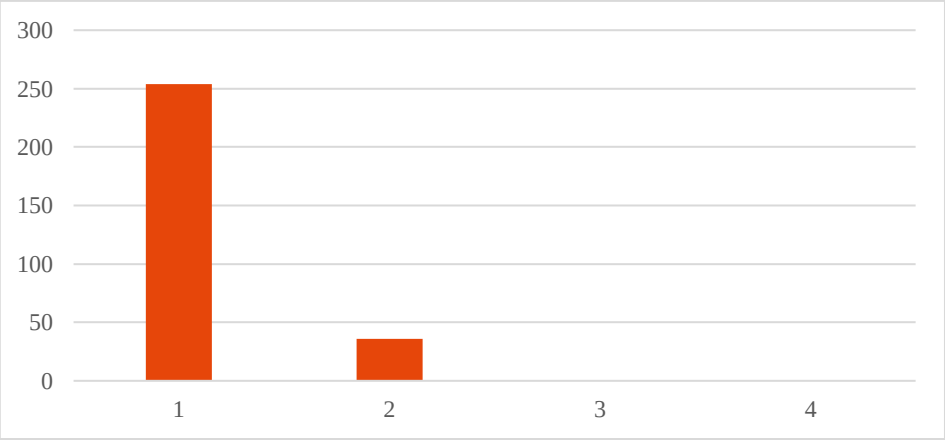

Bild 26: Mognadsnivån för kommunernas uppföljning av tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet.

Nästan 9 av 10 kommuner befinner sig på nivå 1 i mognadsmodellen avseende att följa upp tillämpningen av gemensamma arbetssätt inom informationssäkerhetsområdet. Detta område behöver verkligen få mer fokus i framtiden då det hänger mycket ihop med ledningens förmåga att följa upp och informera sig om aktuellt status för informationssäkerheten inom organisationen.

Djupintervjuer, analys och slutsatser

Framgångsfaktorer

Under intervjuerna har framgångsfaktorer efterfrågats hos de kommuner som skattat att de kommit långt i sitt arbete gällande informationssäkerhet. De har bland annat nämnt vikten av central stöttning med en medveten ledningsgrupp.

> *”Klartecken från ledningsgruppen på arbetet och att de är med på vad arbetet innebär, samt att informationssäkerhetsarbetet ligger högt på agendan. Det gäller både för den politiska ledningen som på tjänstemannanivå.”*

En kommun framhåller sitt systematiska arbete där man arbetat med enkla metoder som är lätta att förstå och snabbt ger resultat.

> *”En enkel metod som alla förstår.”*

Eldsjälar i organisationen är också en framgångsfaktor. Ett par kommuner uppger att incidenter gjort att frågan om säkerhet aktualiserats, vilket gjorde att informationssäkerhet lyftes högre upp på prioriteringslistan. Även ökade krav från allmänheten ses som en faktor för framgång.

Hinder

Kommunerna som inte kommit igång med informationssäkerhet har själva fått ange vilka hinder de upplever försvårar.

> *”En liten kommun får fördela ett stort antal uppgifter med stor variation på ett fåtal personer.”*

Flera svarade brist på resurser, brist på kompetens och brist på insikt om vikten att skydda information.

> *”[Ett hinder vi överkom var] När åtgärder börjar kosta pengar, alltså prioriteringar mellan olika investeringar. Överkom många av dessa genom att söka nollkostnadslösningar som att flytta skyddsvärda objekt till redan befintliga lokaler med högre skalskydd.”*

De menar även på att det är en utmaning att få ut kunskap och engagemang i hela verksamheten, än mer när man inte har stöd från den politiska ledningen och/eller kommunledning.

> *”Upplever att det kommer in en generation på arbetsmarknaden som inte varit med under kalla kriget och som saknar erfarenhet av att tänka kring säkerhet.”*

Relevanta processer/politisk ledning/kommunledning

Huvuddelen av kommunerna har inlett arbetet med informationssäkerhet inom främst socialförvaltning, vård och omsorg samt skola. Då de verksamheterna har tydliga lagkrav på sig har inte arbetet initierats utifrån informationssäkerhet utan av gällande lagkrav, till exempel GDPR och Offentlighets- och sekretesslagen. Flertalet av de chefer som intervjuats säger att de är medvetna om att informationssäkerhet behöver implementeras i alla delar i organisationen men att de har svårt att få de ekonomiska förutsättningarna som behövs för att accelerera arbetet. De uppger dock att de inte aktivt arbetar med för att få den politiska ledningen att avsätta ekonomiska medel, då den politiska ledningen har andra frågor i fokus såsom expandering av bostäder och förskolor och därför förlitar sig på andra.

> *”Vi litar på att de större leverantörerna typ Visma och Procapita har koll på vår information.”*

I väldigt få av de kommuner som intervjuats har den politiska ledningen påvisat ett intresse för just informationssäkerhet. Det som lyfts i intervjuerna är att det är först när brister påvisats i revision eller nya lagkrav såsom GDPR där eventuella ekonomiska påföljder kan komma att bli direkt märkbara för kommunen som möjligheten att få upp informationssäkerhet på agendan varit möjlig.

> *"När något händer hamnar frågan högst upp på politiska agendan."*

Majoriteten av cheferna uppger att arbetet som utförs görs i största mån av enskilda engagerade medarbetare som förstår vikten av informationssäkerhet. Kommunledningen har gett uppdraget att arbeta med informationssäkerhet till enskilda medarbetare och därefter släppt frågan. I en kommun visade en förstudie om informationssäkerhet att de borde anställa en informationssäkerhetsamordnare då kompetens saknades och behovet var stort. Resultatet av förstudien har dock inte hörsammats utan det har satts på vänt då det varit en för stor utmaning att behöva äska medel för att få in en resurs med kompetens i frågan.

Målsättning/hur arbetet lagts upp

Majoriteten av de kommunchefer som intervjuats har sagt att informationssäkerhet bör ha en hög prioritet. Men det är bara en kommun vars kommunledning har gett ett klart uppdrag med en konkret målsättning. Den målsättningen uppkom i samband med att regionen erbjöd utbildning i informationssäkerhet. Kommunledningen satte då som mål att allt administrativt, såsom policys och rutiner, skulle vara upprättat och redo för implementering inom ett år, ett mål som de verkställande i kommunen klarade av.

> *”Det saknas i stort målsättning för informationssäkerhetsarbetet.”*

Upprättandet av policys och rutiner gjordes i samarbete med flera andra kommuner vilka träffades en gång i veckan under ett års tid. De tog då hjälp av varandra med att upprätta dokument men som var anpassade till respektive

kommun. Två av kommunerna har färdig informationssäkerhetspolicy, som inom kort ska tas upp i Kommunfullmäktige.

Resurser/organisatoriskt/ nätverk

Hur man har lagt upp arbete gällande informationssäkerhet ser väldigt olika ut i de kommuner som intervjuats. I flertalet intervjuer har kommunchefen uppgett att arbetet utförs av eldsjälar som aktivt tar ett stort ansvar då individen inser vikten av att säkra skyddsvärda informationstillgångar.

> *”Kommunen har egentligen inte avsatt några resurser för informationssäkerhet, utan de två som just nu tagit ansvar för det, gör det inom sin ordinarie arbetstid utan att andra uppgifter tas bort.”*

En av kommunerna försöker i nuläget att ersättningsrekrytera en informationssäkerhetssamordnare på heltid, en tjänst som funnits en längre tid. En kommun har fördelat arbetet på sex personer på få procent av sin arbetstid. Någon kommun har en informationssäkerhetssamordnare som delar sin tjänst på sex kommuner. En kommunchef tycker att de har en bra täckning på resurser gällande informationssäkerhet då de anställt en extra kommunjurist samt har flertalet kommunikatörer som sköter all information internt och externt. De som har någon form av informationssäkerhetssamordnare har denna tjänst antingen under säkerhetschefen på tekniska förvaltningen eller under IT-chefen som befinner sig i staben direkt under kommunchefen. En kommun har en central funktion direkt under kommunchef, ett team som jobbar med all sorts säkerhet där de har en informationssäkerhetssamordnare på heltid.

> *”I början var alla kommuner i regionen med i ett översiktsarbete om informationssäkerhet. Det vara bara vår kommun som valde att arbeta vidare med de brister som uppmärksammades.”*

Det är inte alla kommuner som är med i externa nätverk. En kommun har försökt få till ett nätverk med närliggande kommuner utan framgång. Några regioner har skapat nätverk gällande digitalisering där informationssäkerhet ibland är en del av agendan. En kommun har ett nätverk via Länsstyrelsen, men de upplever att det varit tyst därifrån en längre tid. Ett par av kommunerna är med i nätverk för dataskyddsombud med närliggande kommuner. Även där är det så att informationssäkerhet kommer upp som en punkt på agendan då och då. Det är enbart den kommun vars region erbjöd utbildning i informationssäkerhet som har ett nätverk där informationssäkerhet är huvudsaken.

Något alla som blivit intervjuade är överens om är att nätverkande med informationssäkerhet i fokus är av stort intresse, under förutsättning att det finns möjlighet att avsätta resurser till nätverkandet och att det ger något tillbaka till verksamheten relativt snabbt.

Rekommendationer

Slutsatser

Kommunerna verkar ofta i sin egen kontext och med sina unika förutsättningar. Därför finns det inga gemensamma nämnare som de intervjuade kommunerna lyfter fram som framgångsfaktorer eller hinder.

Att uppmärksamma GDPR verkar vara en motiverande faktor för kommunernas informationssäkerhetsarbete. Lite överraskande är det dock att få uppger nya säkerhetsskyddslagen eller NIS-direktivet som en faktor till att informationssäkerhet hamnat högre på prioriteringsordningen.

Något som flera kommuner fört fram som positivt för att medvetandegörande, är när flera kommuner samarbetar, eller en extern part tar ett initiativ och bjuder in till gemensamma insatser. Det kan gälla såväl utbildning som analyser av nuläget. En återkommande reflektion har varit att medarbetare har haft svårt att få gehör för sina nya insikter i den egna organisationen. Det verkar också som om många kommuner, även de framgångsrika, är själva i att ta fram sina arbetsmetoder.

Ett lyckat införande av ett systematiskt och riskbaserat informationssäkerhetsarbete beror ofta på ledningens aktiva engagemang, här uppvisar många kommuner brister. Snarare förefaller ledningen delegera ned även styrningen av arbetet i organisationen. Vissa av de kommuner som själva skattat sitt arbete högt verkar ha kommit så långt tack vare intresserade och motiverade medarbetare som givits utrymme att utforma informationssäkerhetsarbetet. Risken med personberoende är att medarbetaren tar med sig såväl drivet, som den generella kompetensen och rutinerna för det upparbetade arbetssättet, om den lämnar organisationen.

En gemensam nämnare bland de kommuner som inte skattat sitt arbete högt är att ledningen delegerat ansvaret för uppdraget, men inte tilldelat resurser. Att engagera ledningen verkar vara kopplat till frågan om medvetenhet. Det förefaller ofta saknas tillräcklig kunskap om den egna organisationens behov av informationssäkerhet hos såväl den politiska- som tjänstemannaledningen.

Den ökade graden av digitalisering och högre krav från allmänheten att få ta del av information verkar driva arbetet med informationssäkerhet. De som lyckats med sitt arbete förefaller ha tagit ett enhetligt grepp om frågan och arbetat aktivt med att förenkla sina arbetssätt och anpassar dem efter lokala förhållanden. Det är troligt att detta kräver en större arbetsinsats initialt, när anpassningen sker och metoden fastställs. Däremot är det troligt att det i det längre loppet sparar resurser, eftersom andra medarbetare inom organisationen kan dra nytta av detta arbete. Omvänt verkar avsaknaden av ett systematiskt angreppssätt verka begränsande på kommunens arbete, även där medarbetare uppmärksammat behovet av informationssäkerhet. Här verkar det vanligare med *ad hoc*-insatser med situationsanpassade lösningar, som troligtvis kostar större resurser men inte nödvändigtvis med högre kvalitet.

Nuläget i kommunerna

Informationssäkerhet hör hemma på agendan för kommunens högsta ledning, det är inte en IT-fråga. Nuläget skiljer sig en hel del mellan kommunerna:

- I någon kommun genomför just nu en obligatorisk e-utbildning om informationssäkerhet för samtliga medarbetare.
- En annan kommun arbetar intensivt vidare med digitalisering och automatisering.
- Några av kommunerna ska komma igång med klassificering av informationstillgångar.
- En del av kommuner vill strukturera upp sin organisation och införa ledningssystem för informationssäkerhet (LIS).
- I flera av kommunerna uttrycker vilja att synliggöra och medvetengöra vikten av att arbeta med informationssäkerhet, både hos den politiska ledningen och hos kommunledningen.
- En av kommunerna ska tydliggöra systemförvaltarskapet.
- Penetrationstester ska genomföras hos ett fåtal av kommunerna, både att testa sitt IT-skydd och att testa sin fysiska säkerhet i form av access in i lokalerna.

Kommunernas nästa steg i arbetet med informationssäkerhet ser helt olika ut.

> *”Nästa steg behöver vara att få upp frågan om informationssäkerhet på agendan för politiken.”*

Det fortsatta arbetet

Det fortsatta arbetet med införandet av ett systematiskt och riskbaserat informationssäkerhetsarbete bör fokusera på att etablera tydliga och effektiva arbetssätt, som ska tillämpas i kommunens hela verksamhet.

Detta gäller samtliga viktiga områden inom informationssäkerhet, men framför allt:

1. Hur ledningen ska leda och styra
2. Riskhantering
3. Informationsklassning
4. Incident-/avvikelsehantering
5. Kontinuitetsplanering
6. Utbildning och medvetandehöjande insatser
7. Upphandlingar
8. Uppföljning

Och som i allt utvecklingsarbete lär av varandra, det går mycket bra att samarbeta inom informationssäkerhetsområdet. Utnyttja möjligheten till samarbete över kommungränserna. Gör införandet av det systematiska och riskbaserade informationssäkerhetsarbetet till ett gemensamt arbete i kommunen.

Kommunernas informationssäkerhetsarbete

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

Under våren 2019 genomförde SKR en webbenkät om hur långt kommunerna kommit i sitt systematiska informationssäkerhetsarbete.

Det finns en djup och bred förståelse av hur viktigt ett grundläggande systematiskt informationssäkerhetsarbete är för all fortsatt digitalisering. Det som fortfarande återstår på många håll är styrning, ledning, avsatta medel och resurser för arbetets planering och genomförande samt en tydlig uppföljning som är integrerad i övrig verksamhetsuppföljning.

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

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

ISBN/Beställningsnummer: Ange nummer
Text: Jonas Nilsson

ISBN XXX-XX-XXXX-XXX-X
Beställ eller ladda ner på webbutik.skr.se
Post: 118 82 Stockholm | **Besök:** Hornsgatan 20
Telefon: 08-452 70 00 | www.skr.se