Myndigheten för samhällsskydd och beredskap

# Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen

## Resultatredovisning av Infosäkkollen och It-säkkollen 2023

**Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen**



Foto omslag: AdobeStock
Tryck: By Wind AB
Produktion: Advant

Publikationsnummer: MSB2333 – mars 2024
ISBN: 978-91-7927-489-4

# Förord

Jag är stolt över att Myndigheten för samhällsskydd och beredskap (MSB) bidrar till det viktiga informations- och cybersäkerhetsarbetet genom att med god evidens redogöra för nivån på det systematiska säkerhetsarbetet i offentlig förvaltning.

Jag vill särskilt tacka de kommuner, regioner och statliga myndigheter som bidragit med sina svar. Ni har tillsammans möjliggjort resultatredovisningens analyser, slutsatser och rekommendationer. Förutom alla svar på Infosäkkollen är vi också glada att se att så många svarat på It-säkkollen.

Att förstå nivån och därmed behoven i offentlig förvaltning är centralt för att ge MSB och andra myndigheter och aktörer en möjlighet att erbjuda rätt stöd eller vidareutveckla behovsanpassat stöd där så behövs. Utifrån det försämrade säkerhetspolitiska läget är det också viktigt att poängtera att nivåbedömningarna bidrar till MSB:s möjlighet att förbättra beredskapen för det civila försvaret.

Vi konstaterar dock att stora delar av den offentliga förvaltningen saknar grunderna i ett systematiskt informations- och cybersäkerhetsarbete. Resultatet visar även på bristande engagemang från organisationernas ledningar. MSB och andra aktörer bidrar med informationsdelning och behovsstyrda rekommendationer, men för att förbättra säkerhetsarbetet på riktigt efterlyser vi ett ökat engagemang av ledningen hos alla samhällsviktiga verksamheter. Omvärldsläget kräver det, vår demokrati behöver det och våra medborgare förtjänar det.

Efter Infosäkkollen 2021 efterlyste MSB en generell satsning för att stärka det systematiska säkerhetsarbetet i den offentliga förvaltningen. Samma behov identifieras återigen, nu två år senare. Arbetet är dessutom än mer angeläget idag, då samhällsviktiga verksamheter behöver hinna göra sig redo för ny EU-lagstiftning, såsom NIS2- och CER-direktiven, som snart ska implementeras i svensk rätt.

Det finns god informations- och cybersäkerhetskompetens inom många organisationer i Sverige. Samtidigt ser MSB att det finns mycket kvar att göra och med begränsade resurser behöver effektivitet premieras och här kan näringslivet bidra och lära oss mycket.

Slutligen gläder det mig att resultatredovisningen även kan vara till gagn för arbetet med den nya nationella strategin för samhällets informations- och cybersäkerhet. Jag tar också tillfället i akt för att meddela att Infosäkkollen och It-säkkollen framöver kommer att få ett nytt samlingsnamn, nämligen Cybersäkerhetskollen.

Stockholm, 2024-03-01

Åke Holmgren

Chef, Avdelningen för cybersäkerhet och säkra kommunikationer,
Myndigheten för samhällsskydd och beredskap

# Innehåll

# Sammanfattning

# Sammanfattning

Mellan 17 maj och 29 september 2023 genomfördes Infosäkkollen för andra gången. Fler än hälften av organisationerna i offentlig förvaltning deltog och bland dem var det endast 31 procent som nådde upp till någon av modellens fyra nivåer. Övriga 69 procent, av organisationerna saknar de mest grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. Motsvarande procentsiffra 2021 var dock ännu högre, nämligen 82 procent. Endast fyra av 120 statliga myndigheter[1] når det samlade resultat som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet[2]. Den första utgåvan av föreskrifterna trädde ikraft 2009.

211 organisationer har deltagit vid båda undersökningstillfällena 2021 och 2023. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en drygt 5 procentig förbättring gällande deras resultat i Infosäkkollen 2023 jämfört med 2021. Vid en jämförelse mellan de organisationer som deltagit enbart 2021 eller 2023 framkommer det dock att många organisationer med svagare resultat 2021 inte deltagit 2023 och att de organisationer som deltog 2023 hade betydligt bättre resultat än de som enbart deltog 2021. Sammantaget förklaras därför en del av det ”förbättrade” sammantagna resultatet för Infosäkkollen 2023 av att de svagare organisationerna från 2021 helt enkelt inte deltagit 2023.

Resultatet inom arbetsområdet för Ledningens styrning och kontroll visar på en avsaknad av engagemang från organisationernas ledningar. Medan ett *visst* skydd kan uppnås utan aktiv inriktning och uppföljning av ledningen är MSB:s bedömning att ett löpande engagemang från ledningshåll krävs för att bedriva ett *systematiskt* och *riskbaserat* informations- och cybersäkerhetsarbete. För att kunna arbeta systematiskt över tid måste säkerhetsarbetet prioriteras och tilldelas resurser.

I resultatredovisningen av Infosäkkollen 2021 konstaterades att ”*den mest centrala slutsatsen från MSB:s analys är att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*”[3]. Utifrån resultatet 2023 bedömer MSB också att förändringstakten inte motsvarar behovet, särskilt inte med hänsyn till rådande säkerhetspolitiska läge. Avsaknaden av väsentliga förbättringar, inom de områden som lyftes fram redan år 2021, innebär att samma rekommendationer kvarstår. Behovet av förbättring är dessutom utifrån omvärldsläget och den ekonomiska situationen allt mer angeläget idag i jämförelse med tidigare mätning, varför MSB stärker sin rekommendation ytterligare.

1. Statliga myndigheter kommer hädanefter att benämnas som myndigheter.
2. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
3. https://rib.msb.se/filer/pdf/30002.pdf

MSB bedömer att det behövs en särskild satsning gällande finansiering till organisationers informations- och cybersäkerhetsarbete baserat på deras resultat i Infosäkkollen och It-säkkollen. Detta för att tillföra de resurser som behövs för att höja organisationens nivå i den utsträckning som krävs för att kunna garantera säkerhet och tillförlitlighet i samhällsviktiga tjänster. It-incidenter är dessutom kostsamma och ur ett samhällsperspektiv torde det vara mer ekonomiskt att förekomma de incidenter som kan förebyggas.

Samtidigt bedömer MSB att säkerhetsarbetet bör kunna bedrivas mer effektivt, och att ökad effektivitet skulle kunna frigöra resurser för att arbeta bredare, och därigenom nå högre nivåer. Ett mer effektivt nyttjande av resurserna som tillhandahålls är därför en viktig komponent i en satsning mot en högre nivå. Här finns en roll för näringslivet i att utveckla och tillhandahålla verktyg, teknologi och tjänster som kan bistå den offentliga förvaltningen i det systematiska informations- och cybersäkerhetsarbetet.

I arbetet med Infosäkkollen har MSB återkommande mottagit önskemål om att organisationer ska ges bättre förutsättningar att nå längre i sitt informations- och cybersäkerhetsarbete genom att samarbeta. För att stärka samverkan på en operativ nivå mellan organisationer skulle en särskild satsning gällande informations- och cybersäkerhetsfinansiering även kunna gå till att CISO:s ges tid att utveckla samverkan med andra CISO:s. Det är också av yttersta vikt att ledningarna ger CISO det mandat som krävs för att ha den styrande och samordnande roll som arbetet kräver och de resurser som behövs för att utföra de arbetsuppgifter som ger ökad säkerhet. I större organisationer krävs att CISO får operativt stödjande personer ute i verksamheterna. Deras roll är att med sin verksamhetskunskap genomföra det operativa arbetet och ge CISO:n den strategiska, kravställande och uppföljande roll som CISO:s arbete innebär.

Kommunerna är genomgående den aktörsgrupp som har svagast resultat i Infosäkkollen 2023. Det är endast inom två arbetsområden som regionerna är svagare än kommunerna. Myndigheterna presterar genomgående bäst. Undantaget är på arbetsområdet Upphandling där regionerna har ett bättre resultat.

Resultatspridningen, det vill säga skillnaden mellan de bästa och de svagaste resultaten, är omfattande. De bäst presterande organisationerna drar kraftigt upp resultatet för sina respektive aktörsgrupper. Det är en stor skillnad i resultatet för de tio procent av organisationerna som har de bästa resultaten jämfört med de övriga 90 procenten.

267 organisationer från offentlig förvaltning deltog i It-säkkollen 2023. It-säkkollen 2023 är en självskattningsundersökning och kommer vidareutvecklas för att få samma metodologiska robusthet som Infosäkkollen inför mättillfället 2025.

Resultatet för It-säkkollen 2023 ligger på en förhållandevis god nivå, nästan motsvarande nivå 3 av 4 i modellen, vilket motsvarar ”visst skydd”. Resultatet visar på små skillnader mellan aktörsgrupperna för såväl helheten som inom varje enskilt arbetsområde. Myndigheterna presterar lite bättre än regionerna, följt av kommunerna som är marginellt svagast.

It-säkerhetsarbetet styrs och genomförs oftast av en mer avgränsad skara medarbetare än informationssäkerhetsarbetet. Arbetet leds av en it-chef som i sin tur har tillgång till eller själv medverkar i organisationens ledningsgrupp och därför har mer påverkan på att arbetet prioriteras och resurssätts. Detta kan jämföras med att långt ifrån alla organisationer har en CISO på heltid, snarare tvärtom, samt att den rollen saknar den verksamhetsmässiga tyngden en it-chef har. Vidare kan it-säkerhetsarbetet få återverkningar på hela organisationen då de flesta har en centraliserad it-miljö där all eller den mesta informationen som organisationen ansvarar för behandlas. Informationssäkerhetsarbetet å sin sida behöver genomsyra hela verksamheten. Sammantaget är det därför väntat att resultatet från Infosäkkollen 2023 påvisar att organisationerna är bättre på de arbetsområden som kan ha större betydelse för att säkra organisationens it-miljö, nämligen Analys och hantering av informationssäkerhetsrisker, Informationsklassning och Säkerhetsåtgärder och förbättringsarbete. Det förklarar också varför resultatet från It-säkkollen 2023 visar på att många av organisationerna anser sig ha goda förutsättningar för systematiskt it-säkerhetsarbete, vilket MSB noterar står i kontrast mot vad resultatet i Infosäkkollen säger om förutsättningarna att bedriva systematiskt informationssäkerhetsarbete.

Arbetsområdet Kryptering har det svagaste resultatet jämfört med övriga arbetsområden i It-säkkollen 2023. Skydd av utrustning och it-utrymmen är det arbetsområde med det klart bästa resultatet inom samtliga aktörsgrupper. Majoriteten av offentlig förvaltning uppger att de utkontrakterat en betydande andel av sin it-drift. Vidareutvecklingen av It-säkkollen behövs för att undersöka vilken typ av it-drift och om detta är en utveckling som på sikt kan bidra till en ökad leverantörskedjeproblematik

Det rapporterades in så få svar från näringslivet, särskilt NIS-leverantörer, att dessa inte kunde inkluderas i resultatsammanställningen för vare sig Infosäkkollen eller It-säkkollen. Formerna för att nå ut till näringslivet behöver ses över tillsammans med tillsynsmyndigheterna som är de aktörer som sköter kontakten gentemot NIS-leverantörerna.

# Inledning

# 1. Inledning

## 1.1 Bakgrund

Myndigheten för samhällsskydd och beredskap (MSB) fick den 19 september 2019 i uppdrag av regeringen att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen (statliga myndigheter, kommuner och regioner). Syftet kan sammanfattas som tvådelat: att ge organisationerna stöd med återkoppling om nivån på deras informationssäkerhetsarbete och förslag på förbättringar; samt att ta fram en samlad bedömning till regeringen. Uppföljningen ska genomföras regelbundet. Medverkan är frivillig. Uppdraget redovisades till regeringskansliet 22 juni 2022. Infosäkkollen lanserades för andra gången 17 maj 2023 och svarstiden löpte fram till 29 september 2023.

Regeringen gav den 23 mars 2023 i uppdrag till MSB att till Regeringskansliet (Försvarsdepartementet) även redovisa hur nivån på it-säkerheten ser ut för organisationerna. MSB ska slutredovisa (denna rapport) till Regeringskansliet senast den 1 mars 2024.

Baserat på svar från Infosäkkollen och It-säkkollen redovisar myndigheten i denna rapport en samlad bedömning av nivån på det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen 2023, och även slutsatser och rekommendationer framtagna av MSB för hur säkerhetsarbetet kan stärkas under kommande år.

## 1.2 Disposition

I kapitel 2 sammanfattas de huvudsakliga slutsatserna för såväl Infosäkkollen som It-säkkollen, samt de rekommendationer som tagits fram baserat på resultatet. Kapitel 3 ger en närmare beskrivning av Infosäkkollen och tillhörande benchmarkverktyg ur ett användarperspektiv.

Kapitel 4 ger en samlad resultatbild av Infosäkkollen för hela den offentliga förvaltningen, inklusive redogörelser på detaljnivå för kommuner, regioner och myndigheter. För statliga myndigheter ges även en indikation på efterlevnaden av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

I Kapitel 5 redogörs för den samlade resultatbilden av It-säkkollen.

## 1.3 Begreppsförklaring

Här följer en lista med begrepp som används och deras innebörd i denna rapport.

**Aktörsgrupp** används mest för jämförelse där de tre aktörsgrupperna utgörs av kommuner, regioner och myndigheter.

**Arbetsområden** är en ämnesmässig uppdelning av de frågor som ingår i Infosäkkollen och It-säkkollen utifrån olika delar av det systematiska informations- och cybersäkerhetsarbetet.

**Benchmarks** är en form av typsvar som används för att beskriva resultatet för specifika grupper. Modellens uppbyggnad gör att sammanräkningar av enbart genomsnittliga resultat inte ger en meningsfull bild av hur det gått för en grupp. Istället används benchmarks eller typsvar som visar hur en generell representant för gruppen skulle svara, baserat på hur de som är med i gruppen har svarat.

**CISO** avser den roll eller funktion som leder och samordnar informationssäkerhetsarbetet i organisationen. Andra vanliga benämningar är informationssäkerhetssamordnare, informationssäkerhetsstrateg eller informationssäkerhetskoordinator. CISO är en förkortning av den engelska titeln chief information security officer, och används som samlingsbegrepp.

**Föreskriftskrav** avser krav som ställs på ett systematiskt informations- och cybersäkerhetsarbete, som de uttrycks i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

**Infosäkkollen** är ett verktyg för uppföljning av det systematiska informations- och cybersäkerhetsarbetet i en organisation. Resultat från organisationer som genomfört Infosäkkollen ligger till grund för denna rapport.

**It-säkkollen** är en uppföljning av it-säkerhetsarbetet i en organisation. It-säkkollen utgår från MSB:s föreskrifter MSBFS 2020:7, men det krävs vidareutveckling för att It-säkkollen ska kunna ge en indikation om föreskrifternas efterlevnad.

**Nivå** beskriver hur långt en organisation kommit med sitt informations- och cybersäkerhetsarbete utifrån organisationens resultat i Infosäkkollen. Nivån betecknar normalt organisationens samlade resultat. Detta kallas ibland ”övergripande nivå”. Dessutom genereras en indikativ nivå för respektive arbetsområde i organisationens resultat. Detta kallas ibland ”nivån för arbetsområdet”.

De fyra nivåerna i Infosäkkollen är:

- Nivå 1: Grunderna i informations- och cybersäkerhetsarbetet.
- Nivå 2: Informations- och cybersäkerhetsarbetet bedrivs med viss systematik och är bättre på grunderna.
- Nivå 3: Kvalificerat innehåll i informations- och cybersäkerhetsarbetet.
- Nivå 4: Ständiga förbättringar.

**Resultattal** beskriver det samlade resultatet för en organisation på ett mer detaljerat sätt, och används för att jämföra resultat för olika organisationer. Utöver den övergripande nivån ingår också de resultat som uppnåtts för olika arbetsområden samt den poängsumma som ligger till grund för resultatberäkningen.

**Typkommunen**, **typregionen**, **typmyndigheten** och **typförvaltningen** är sammanvägda beskrivningar baserat på alla deltagande kommuners, regioners, myndigheters eller hela offentliga förvaltningens resultat. De resultat som presenteras utifrån dessa begrepp är baserade på benchmarks.

**Åtgärd** representerar något som en organisation behöver göra för att kunna svara positivt på en fråga (kryssa i en ruta och samla poäng) i Infosäkkollen.

## 1.4 Varför resultatet i Infosäkkollen är viktigt

Uppföljning av informations- och cybersäkerhetsarbetet upplevs ofta som en utmaning, samtidigt som det är en förutsättning för att en organisation ska kunna uppnå och bibehålla ett adekvat skydd.

Infosäkkollen är en modell som används inom ramen för en struktur där organisationers systematiska informations- och cybersäkerhetsarbete följs upp i två-årscykler.[4] Likt andra modeller kan Infosäkkollen enbart göra anspråk på att beskriva en approximation av hur verkligheten ser ut hos en enskild organisation. Modellens 40 frågor täcker en bred uppsättning aspekter som ingår i ett systematiskt informations- och cybersäkerhetsarbete, men de täcker inte allt. Medan Infosäkkollen alltså ger en bild, är det inte säkert att den ger en fullödig bild. Det är fullt möjligt att det finns ytterligare aspekter som hade kunnat mätas och som hade kunnat ställa enskilda organisationer i såväl bättre som sämre dager.

På motsvarande sätt kan Infosäkkollen endast göra anspråk på att beskriva en approximation av vad en organisation behöver satsa på för att utveckla sitt systematiska informations- och cybersäkerhetsarbete. Enskilda organisationer kan ha större behov av andra åtgärder än de Infosäkkollen visar att de behöver genomföra för att nå en högre nivå. Med det sagt finns det ett antal skäl till att det är viktigt för organisationer att använda Infosäkkollen för att följa upp sitt säkerhetsarbete, och att det är viktigt att nå höga nivåer i Infosäkkollen:

**Infosäkkollen omfattar noggrant utvalda områden**: Det som modellen följer upp är resultatet av 1,5 års arbete med att sammanställa en begränsad uppsättning frågor om olika delar av det systematiska informations- och cybersäkerhetsarbetet. Innehållet i modellen är framtaget med stöd av standarder och föreskrifter, diskussioner med experter och mycket annat.

4. MSB:s regleringsbrev för 2024 innefattar en aktivering av Infosäkkollen och It-säkkollen. Detta innebär att de ska genomföras även 2024. https://www.esv.se/statsliggaren/regleringsbrev/Index?rbId=23933 (hämtad 24 januari 2024).

**Infosäkkollen är konstruerad så att MSB får information som kan användas för att validera modellen**: Med stöd av inkomna svar på Infosäkkollens valideringsfrågor kommer MSB successivt att få information som kan användas för att finjustera modellen om det skulle visa sig att vissa frågor borde ersättas med andra, eller omformuleras.

**Infosäkkollen ger organisationer en standardiserad och jämförbar bild av statusen på sitt systematiska informationssäkerhetsarbete**: Organisationer får en bild av statusen på sitt systematiska informations- och cybersäkerhetsarbete, och de kan jämföra bilden de får med den bild som andra organisationer får. Det gör att de kan se om de har missat något, får bättre förutsättningar för samarbete och kan sätta mål tillsammans.

**Infosäkkollen tillämpar en naturlig ”utvecklingstrappa” vid uppföljningen av det systematiska informationssäkerhetsarbetet**: Modellens respektive övergripande nivåer motsvarar naturliga utvecklingssteg som organisationer kan följa för att successivt utveckla helheten i det systematiska informations- och cybersäkerhetsarbetet.

**Infosäkkollen betonar hela organisationens systematiska informations- och cybersäkerhetsarbete**: Modellen betonar ett antal områden som gör att hela organisationen (d.v.s. alla medarbetare, i varierande grad) blir delaktig i satsningen på att arbeta informationssäkert. Det är viktigt, för incidentrapporteringen till MSB visar att misstag och systemfel (som ofta möjliggörs av att medarbetare inte gör sådant som de borde göra) är en vanlig orsak till allvarliga incidenter.

**Infosäkkollen förutsätter att organisationen själv prioriterar åtgärder**: Organisationer har viss frihet att själva välja hur de ska avancera i Infosäkkollen. Genom att nå högre nivåer i modellen utvecklar de sitt systematiska informations- och cybersäkerhetsarbete utifrån sina egna behov.

**Infosäkkollen förutsätter att organisationen inte väljer bort något centralt område**: Genom att nå högre nivåer i Infosäkkollen kan organisationer utveckla det systematiska informations- och cybersäkerhetsarbetet utan att missa någon central del under utvecklingens gång.

När MSB framhäver vikten av att höja organisationers övergripande nivå, handlar de slutsatserna och rekommendationerna alltså om de ovanstående skälen, snarare än att goda resultat i Infosäkkollen har ett egenvärde.

## 1.5 NIS-leverantörers medverkan i undersökningarna

Sammantaget mottog MSB 13 svar till Infosäkkollen 2023 från aktörer som angav sig vara NIS-leverantörer[5]. Av dessa uppgav fyra att de var registrerade leverantörer av samhällsviktiga och digitala tjänster (bekräftade NIS-leverantörer). Motsvarande för It-säkkollen 2023 var sex svar, varav tre av dessa uppgav sig vara registrerade NIS-leverantörer.

Då aktörsgruppen NIS-leverantörer uppgår till omkring 600 organisationer är 13 inkomna svar för få för att tillåta en meningsfull statistisk analys. Dessa aktörers svar exkluderas därför från redovisningen.

Inom ramen för nuvarande NIS-reglering har MSB inte tillgång till någon förteckning över NIS-leverantörerna. Med utgångspunkt i de gällande förutsättningarna genomförde MSB i samband med lansering 17 maj 2023 ett antal insatser för att öka deltagandet från näringslivet, särskilt NIS-leverantörerna. Bland annat delades ett särskilt utskick via tillsynsmyndigheterna för NIS, NCSC[6], samt lansering nämndes vid konferenser, seminarier och särskilda frågestunder.

5. De omfattas av den reglering som implementerar det så kallade NIS-direktivet, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, det vill säga lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

6. Nationella Cybersäkerhetscentret.

# Slutsatser och rekommendationer

# 2. Slutsatser och rekommendationer

I detta kapitel presenteras slutsatser och rekommendationer för såväl Infosäkkollen som It-säkkollen 2023. Båda undersökningarna lanserades 17 maj 2023 och inrapporteringen var öppen till och med 29 september 2023.

## 2.1 Slutsatser från Infosäkkollen 2023

69 procent av alla deltagande organisationer uppnår inte grunderna i sitt systematiska informations- och cybersäkerhetsarbete. 31 procent av deltagande organisationer uppnådde nivå 1 eller bättre, drygt 10 procent uppnådde nivå 2 eller bättre, och knappt 3 procent uppnådde nivå 3 eller 4 i modellen.

211 organisationer deltog både 2021 och 2023. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en drygt 5 procentig resultatförbättring för hela Infosäkkollen för de organisationer som deltagit vid båda mättillfällena.

Vid en jämförelse mellan de organisationer som deltagit enbart 2021 eller 2023 framkommer det dock att många organisationer med svagare resultat 2021 inte deltagit 2023 och att de organisationer som deltog 2023 hade betydligt bättre resultat än de som enbart deltog 2021. De organisationer som enbart deltog 2023 hade 25,9 procent bättre resultat på hela Infosäkkollen jämfört med de som enbart deltog 2021. Sammantaget förklaras därför en del av det ”förbättrade” sammantagna resultatet för Infosäkkollen 2023 av att de svagare organisationerna från 2021 valde att inte delta 2023.

I den enkätundersökning som genomfördes bland de som rapporterade in Infosäkkollen 2023 svarade två tredjedelar av respondenterna att de inte har den personal som krävs för att fullt ut implementera förbättringsarbetet. Omkring tre femtedelar uppgav att de arbetar deltid eller mindre med informations- och cybersäkerhet.[7] Vidare uppgav nästan hälften viss eller omfattande personalomsättning under en tvåårsperiod. Samtidigt uppgav nästan två tredjedelar att organisationen besitter nödvändig kompetens.

7. Frågan var personligt ställd och organisationens respondent kan ha kollegor som arbetar med frågorna i större utsträckning än respondenten själv. Bland respondenterna från kommunerna uppgav så många som 58 procent att de arbetar med informations- och cybersäkerhet cirka 25 procent av sin arbetstid.

Vidare svarade nästan tre fjärdedelar att deras organisation saknar den budget som krävs för att förbättra informations- och cybersäkerhetsarbetet. På frågan om organisationens högsta ledning har det engagemang som krävs för att förbättra informations- och cybersäkerhetsarbetet svarade drygt hälften av respondenterna stämmer knappt eller stämmer inte.

Sammantaget är den bild som framkommer att organisationsledningarna inte engagerar sig, prioriterar eller resurssätter förbättringsarbetet i den utsträckning som krävs. Förutom brister i budgetering syns avsaknaden av resurser även i personalbristen.

Det samlade resultatet från Infosäkkollen visar att ledningens engagemang korrelerar med organisationens resultat, det vill säga att ett högre engagemang visar på ett högre resultat. Det finns också tecken i svarsmaterialet som tyder på ett orsakssamband. Dessutom angav respondenterna i enkätundersökningen i relativt stor utsträckning att relevant kompetens för förbättringsarbetet redan finns i organisationerna. Om ledningens engagemang ökar och nödvändiga resurser tillförs borde därför förbättringar kunna uppnås. Ökade resurser kan även tänkas få bieffekten att personalomsättningen minskar, vilket genom bibehållandet av institutionell kunskap även torde öka takten på förbättringsarbetet.

För att kunna arbeta systematiskt över tid måste informations- och cybersäkerhetsarbetet prioriteras och tilldelas resurser. Den stora slutsatsen från 2021 kvarstår därmed även 2023, nämligen att det behövs en generell satsning för att stärka det systematiska säkerhetsarbetet i den offentliga förvaltningen.

Övriga centrala iakttagelser och slutsatser sammanfattas i kortfattat nedan.

1. Drygt hälften av hela offentlig förvaltning deltog. Svarsfrekvensen var högst bland regionerna (86 %), följt av kommunerna (53 %) och myndigheterna (51 %).

2. Däremot rapporterades så få svar in från näringslivet, särskilt NIS-leverantörer, att dessa inte kunde inkluderas i resultatredovisningen. Ytterligare insatser behövs, bland annat i samverkan med tillsynsmyndigheterna för NIS-regleringen, så att särskilt NIS-leverantörer kan engageras framgent.

3. Knappt 3 procent av alla deltagande organisationer uppnådde nivå 3 eller 4 i modellen. Nivå 3 motsvarar MSB:s föreskriftskrav för statliga myndigheter. Fyra av 120 myndigheter når det samlade resultat som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet. Den första utgåvan av föreskrifterna trädde i kraft 2009.

4. Deltagande organisationer presterar bäst inom arbetsområdet för Säkerhetsåtgärder och förbättringsarbete, följt av Informationsklassning och därefter Analys och hantering av informationssäkerhetsrisker. Detta är i linje med fokuseringen på it-säkerhet som MSB noterade i samband med resultatredovisningen av Infosäkkollen 2021. Samtidigt bör dessa bättre resultat förstås utifrån kontexten att helhetsresultatet på Infosäkkollen 2023 visar på brister inom andra arbetsområden, varför det finns utvecklingspotential även här.

5. Deltagande organisationer är svagast inom arbetsområdet för Ledningens styrning och kontroll, följt av Uppföljning och utvärdering och därefter Incident- och kontinuitetshantering. Inom dessa arbetsområden noterar MSB viss förbättring gällande antal införda åtgärder, men att utvecklingen främst handlar om spets snarare än bredd i det systematiska informations- och cybersäkerhetsarbetet. Att utvecklas på bredden och få ihop helheten är det som premieras i Infosäkkollen.

6. Bland de organisationer som deltog vid båda mättillfällena syns störst förbättring 2023 jämfört med 2021 inom arbetsområdena för Medarbetarnas kunskaper och utbildningsverksamhet (14 %), Upprättande och utveckling av säkerhetskultur (12 %) och Uppföljning och utvärdering (10 %).

7. Bland de organisationer som deltog vid båda mättillfällena syns minst förbättring 2023 jämfört med 2021 inom arbetsområdena för Ledningens styrning och kontroll (8 %), Säkerhetsåtgärder och förbättringsarbete (7 %) och Inventering, undersökningar och omvärldsbevakning (7 %).

8. Deltagande kommuner är genomgående den aktörsgrupp som har svagast resultat. Det är endast inom två arbetsområden som regionerna är svagare än kommunerna. Myndigheterna är den aktörsgrupp som genomgående presterar bäst. Undantaget är på arbetsområdet Upphandling där regionerna är bättre.

9. En typförvaltning 2023 har genomfört nästan dubbelt så många åtgärder som typförvaltningen 2021. Skillnaden i absoluta tal är dock begränsad, vilket märks i resultattalen. Detta påvisar att bredden i det systematiska säkerhetsarbetet alltjämt saknas.

10. Resultatspridningen är omfattande. Gruppen bestående av de organisationer som hör till de tio bäst presterande procenten drar kraftigt upp resultatet för sina respektive aktörsgrupper. Det är en stor skillnad i resultatet för de tio procent av organisationerna som har de bästa resultaten jämfört med de övriga 90 procenten inom varje aktörsgrupp.

## 2.2 Slutsatser från It-säkkollen 2023

Självskattningsenkäter har inbyggda metodproblem. Respondenterna nyttjar ofta tolkningsutrymmet till att överskatta sin egen förmåga. Samtidigt kan det även finnas motiverande faktorer för att medvetet underskatta den egna förmågan. Detta påverkar i sin tur trovärdigheten och därför bör slutsatserna läsas med försiktighet och ses som indikatorer.

267 organisationer från offentlig förvaltning deltog i It-säkkollen 2023. Resultatet för It-säkkollen 2023 motsvarande nästan nivå 3 av 4 i modellen, vilket motsvarar ”visst skydd”. Resultatet i It-säkkollen visar på små skillnader mellan aktörsgrupperna för såväl helheten som inom varje enskilt arbetsområde. Myndigheterna presterar lite bättre än regionerna, följt av kommunerna som är marginellt svagast.

It-säkerhetsarbetet styrs och genomförs oftast av en mer avgränsad skara medarbetare än informationssäkerhetsarbetet. Arbetet leds av en it-chef som i sin tur har tillgång till eller själv medverkar i organisationens ledningsgrupp och därför har mer påverkan på att arbetet prioriteras och resurssätts. Detta kan jämföras med att långt ifrån alla organisationer har en CISO på heltid, samt att den rollen saknar den verksamhetsmässiga tyngden en it-chef har. Vidare kan it-säkerhetsarbetet få återverkningar på hela organisationen då de flesta har, eller hyr, en centraliserad it-miljö där all eller den mesta informationen som organisationen ansvarar för behandlas, och där brister ger omedelbara eller synliga problem. Informationssäkerhetsarbetet å sin sida behöver genomsyra hela verksamheten. Sammantaget är det därför väntat att resultatet från Infosäkkollen 2023 påvisar att organisationerna är bättre på de arbetsområden som kan ha större betydelse för att säkra organisationens it-miljö, nämligen Analys och hantering av informationssäkerhetsrisker, Informationsklassning och Säkerhetsåtgärder och förbättringsarbete. Det förklarar också varför resultatet från It-säkkollen 2023 visar på att många av organisationerna anser sig ha goda förutsättningar för systematiskt it-säkerhetsarbete, vilket MSB noterar står i kontrast mot vad resultatet i Infosäkkollen säger om förutsättningarna att bedriva systematiskt informationssäkerhetsarbete.

Arbetsområdet Kryptering visar på svagast resultat jämfört med andra arbetsområden. Skydd av utrustning och it-utrymmen är det arbetsområde med det klart bästa resultatet, oavsett aktörsgrupp.

Majoriteten av offentlig förvaltning uppger att de utkontrakterat en betydande andel av sin it-drift. Vidareutvecklingen av It-säkkollen[8] behövs för att undersöka vilken typ av it-drift och om detta är en utveckling som på sikt kan bidra till att öka leverantörskedjeproblematiken, särskilt gällande monoberoenden.[9] Exempelvis drabbades ett stort antal aktörer inom offentlig sektor av störningar till följd av det utpressningsangrepp som drabbade it-leverantören TietoEvry den 19 januari 2024.[10] Omfattningen av denna leverantörskedjeincident belyser just problematiken när många organisationers försörjning av it-stöd är beroende av en och samma tjänst.

Resultatspridningen visar på en ganska stor skillnad mellan de bästa och svagaste tio procenten, men sammantaget tyder svarsfördelningen på att arbetet har nått längre. Resultatspridningen är som förväntat minst hos de mer homogena regionerna. Den största spridningen var i aktörsgruppen myndigheter.

## 2.3 Nivån på säkerhetsarbetet kan höjas

Här delges MSB:s bedömning på hur nivån på den offentliga förvaltningens informations- och cybersäkerhet kan höjas. Ett stort antal organisationer anger, precis som i undersökningen 2021, resursbrist som det främsta hindret för att nå högre nivåer i det systematiska arbetet. Enkätundersökningen, som genomfördes

8. För information om vidareutvecklingen av It-säkkollen se 3.4.

9. En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av den tjänsten och det saknas alternativa tjänster att använda ifall den tjänst man redan använder upphör.

10. https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda (hämtad 29/1 2024).

med deltagande organisationer efter inrapportering, stärker detta ytterligare och MSB instämmer i bedömningen att många organisationer, i synnerhet många kommuner, behöver mer resurser. I resultatredovisningen 2021 konstaterade MSB att ”*den mest centrala slutsatsen från MSB:s analys är att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*”[11]. Vidare bedömer MSB att förändringstakten inte motsvarar behovet, särskilt inte med det rådande säkerhetspolitiska läget. Avsaknaden av väsentliga förbättringar, inom de områden som lyftes fram redan år 2021, innebär att samma rekommendationer kvarstår. Behovet av förbättring är dessutom utifrån omvärldsläget och den ekonomiska situationen allt mer angeläget idag i jämförelse med tidigare mätning, varför MSB stärker sin rekommendation ytterligare.

MSB bedömer därför att offentlig förvaltning behöver en särskild satsning gällande finansiering till sitt informations- och cybersäkerhetsarbete. Detta för att tillföra de resurser som behövs för att höja organisationens nivå i den utsträckning som krävs för att kunna garantera säkerhet och tillförlitlighet i samhällsviktiga tjänster. It-incidenter är dessutom kostsamma och ur ett samhällsperspektiv torde det vara mer ekonomiskt att förekomma de incidenter som kan förebyggas.

Samtidigt bedömer MSB att säkerhetsarbetet bör kunna bedrivas mer effektivt, och att ökad effektivitet skulle kunna frigöra resurser för att arbeta bredare, och därigenom nå högre nivåer. Ett mer effektivt nyttjande av resurserna som tillhandahålls är därför en viktig komponent i en satsning mot en högre nivå. Här finns en roll för näringslivet i att utveckla och tillhandahålla verktyg, teknologi och tjänster som kan bistå den offentliga förvaltningen (och NIS-leverantörer) i det systematiska informations- och cybersäkerhetsarbetet.

I arbetet med Infosäkkollen har MSB återkommande mottagit önskemål om att organisationer ska ges bättre förutsättningar att nå längre i sitt informations- och cybersäkerhetsarbete genom samarbete. MSB anordnar respektive deltar sedan tidigare i olika nätverk för organisationer inom offentlig förvaltning. Nätverken har till syfte att dela kunskap och erfarenheter, och att deltagarna ska hitta kollegor som arbetar eller har arbetat med samma frågor i andra organisationer för att kunna hjälpas åt. MSB har nu också särskilt sett över frågor och ämnen där organisationer inom samma aktörsgrupp[12] (kommuner, regioner och myndigheter) bör ha möjlighet att hitta andra organisationer som de kan samarbeta med.[13] Förutsättningarna för att hitta organisationer att lära sig av är störst inom grupper där aktörerna skiljer sig mycket åt (s.k. heterogena grupper). I Infosäkkollen 2021 är kommunerna den mest heterogena gruppen, som alltså har störst potential för denna typ av samverkan, följt av myndigheterna och sist regionerna.

För att stärka samverkan på en operativ nivå mellan organisationer skulle en särskild satsning gällande informations- och cybersäkerhetsfinansiering även kunna gå till att CISO:s ges tid att utveckla samverkan med andra CISO:s. Det är också

11. https://rib.msb.se/filer/pdf/30002.pdf.

12. Vi har gjort antagandet att det är enklare, och ibland mer givande, att organisationer inom samma aktörsgrupp samarbetar.

13. Idén är (något förenklat) att om andelen ja och nej-svar är relativt jämna på en fråga, så finns det en potential för organisationer att lära av varandra när det gäller det arbete som frågan avser.

av yttersta vikt att ledningarna ger CISO det mandat som krävs för att ha den styrande och samordnande roll som arbetet kräver och de resurser som behövs för att utföra de arbetsuppgifter som ger ökad säkerhet. I större organisationer krävs att CISO får operativt stödjande personer ute i verksamheterna. Deras roll är att med sin verksamhetskunskap genomföra det operativa arbetet och ge CISO:n den strategiska, kravställande och uppföljande roll som CISO:s arbete innebär.

Utifrån analysen av Infosäkkollen 2023 gällande hur organisationer skulle kunna lära av varandra framgår också några områden där relativt få nått ett bra resultat. Här skulle särskilda stöd från MSB och andra myndigheter, såväl som näringslivet, kunna vara avgörande för att nå en förbättring. De är i synnerhet:

- uppföljning (i synnerhet uppföljning av utbildningsinsatser),
- undersökningar av medarbetarnas kunskaper,
- undersökningar av hinder och framgångsfaktorer som påverkar informations- och cybersäkerhetsarbetet,
- kontinuitetshantering (i synnerhet övningar).

## 2.4 Rekommendationer

Det säkerhetspolitiska läget i Europa är sämre än på mycket länge. Vikten av att stärka totalförsvaret och samhällets motståndskraft har återkommande lyfts. Mot den bakgrunden kan inte de begränsade framsteg i den offentliga förvaltningens strävanden efter att bedriva ett systematiskt informations- och cybersäkerhetsarbete som framkommer av resultatet från Infosäkkollen 2023 betraktas som tillräckliga. Inte heller kan förbättringstakten betraktas som tillräcklig.

69,4 procent av samtliga organisationer som har rapporterat in sina resultat i Infosäkkollen 2023 saknar de mest grundläggande delarna i ett systematiskt säkerhetsarbete. Fyra av 120 rapporterande myndigheter når det samlade resultat som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet[14] och som (i olika versioner) har funnits sedan 2009.

Rekommendationerna nedan grundar sig på brett förekommande brister som har noterats i de resultat som har skickats in till MSB. Alla svarande organisationer inom respektive aktörsgrupp (kommuner, regioner och myndigheter) har inte alla de listade bristerna, men många organisationer har många av dem.

Rekommendationerna grundar sig på slutsatserna från denna analys. Samtidigt är det viktigt att komma ihåg att alla organisationer är olika och att det systematiska informations- och cybersäkerhetsarbetet är ett hantverk som tar tid att etablera och det är centralt att bygga upp kompetens på området. MSB vill därför framförallt betona vikten av att arbeta kontinuerligt och långsiktigt med frågorna.

14. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

För att få en så relevant bild som möjligt bör organisationer också använda verktyget Infosäkkollen benchmark. Verktyget genererar en lista på åtgärder som en organisation behöver genomföra för att nå egna målsättningar, nå samma resultat som den aktörsgrupp organisationen jämför sig med, eller klara kraven i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter[15]. Verktyget hänvisar också till de delar av MSB:s metodstöd som kan vara till nytta för utvecklingsarbetet. Infosäkkollen benchmark kan laddas ned från www.msb.se/cybersakerhetskollen.

### 2.4.1 Rekommendationer till regeringen

Inom ramen för redovisningen rekommenderar MSB att regeringen överväger:

1. en särskild satsning gällande finansiering till de organisationer i offentlig förvaltning som genomfört Infosäkkollen och It-säkkollen och där brister föreligger.

2. en särskild satsning gällande finansiering för att stärka CISO-samverkan på en operativ nivå mellan organisationer.

3. om deltagandet i Infosäkkollen och It-säkkollen ska vara obligatoriskt för offentlig förvaltning och NIS-leverantörer.

4. om det bör införas nationella mål för vilka övergripande resultat i Infosäkkollen och It-säkkollen de deltagande aktörsgrupperna ska uppnå. Dessa skulle kunna kopplas till rekommendation 1.

5. mot bakgrund av det säkerhetspolitiska läget, om de särskilt påtagliga bristerna som påvisats inom Infosäkkollen avseende ledningens styrning och kontroll, uppföljning och utvärdering samt incident- och kontinuitetshantering, bör adresseras i den nya nationella informations- och cybersäkerhetsstrategin.

6. att MSB, inom ramen för Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE), ska ges medel att fördela till privata och offentliga aktörer som vill utveckla eller förbättra produkter och tjänster som adresserar sådana brister, sårbarheter och utmaningar som identifieras i Infosäkkollen och It-säkkollen.

Punkt sex ligger i linje med rekommendationerna från resultatredovisningen 2021 där MSB identifierade ett antal områden där förutsättningarna för samarbete och ömsesidigt lärande mellan organisationer i offentlig förvaltning är mer begränsade. Inom dessa områden kan därför näringslivet göra särskilt stor nytta genom att tillhandahålla tjänster och genom innovation finna nya sätt att lösa uppgifter på mer resurseffektiva sätt. MSB har fått avdelat till sig en miljon euro av EU-kommissionen att fördela från NCC-SE, men EU-bidraget förutsätter medfinansiering med motsvarande belopp från medlemsstaten.

15. Utifrån en uttolkning av vilka åtgärder i Infosäkkollen som behöver vara genomförda.

### 2.4.2 Rekommendationer till offentlig förvaltning

Inom detta stycke avhandlas de rekommendationer som gäller samtliga organisationer inom offentlig förvaltning. Då resultatet för Infosäkkollen 2023 i hög utsträckning liknar resultatet från 2021 redovisar MSB återigen de rekommendationer som myndigheten då tog fram, och som genomgående endast kan realiseras genom ledningens försorg.

1. **Prioritera det systematiska informations- och cybersäkerhetsarbetet från ledningsnivå och nedåt och tilldela mer resurser om det behövs.**

En stor andel av de svarande organisationerna anger resursbrist som den tyngst vägande faktorn bakom att man inte kommer vidare i informations- och cybersäkerhetsarbetet. Att tillföra mer resurser är inte alltid ett bra sätt att hantera ett problem, men när en betydande andel av organisationerna saknar tillräckligt med personal som dedikerat arbetar med säkerhetsarbetet förefaller mer resurser i många fall vara en nödvändig del av lösningen. I organisationer där dedikerad personal saknas förefaller det dessutom utmanande att ens veta vilka resursbehov organisationen har. Organisationer behöver ha dedikerad personal som har som minsta uppgift att leda och samordna organisationens systematiska informations- och cybersäkerhetsarbete och visa på vilka resurser som krävs för att uppnå ledningens ambitionsnivå.

2. **Dra nytta av de nya möjligheter till samarbete och samverkan som uppstår genom Infosäkkollen.**

Inom de olika aktörsgrupperna av svarande på Infosäkkollen finns det ett antal områden där det på systemnivå skulle finnas stora fördelar och relativt enkla vinster att hämta om organisationerna samarbetade i större utsträckning. Dessa områden är främst kontinuitetshantering, omvärldsbevakning, utbildning, upphandling och uppföljning. Vid sidan av enskilda samarbeten finns det också möjligheter till samverkan genom nätverken KIS, HoSIS och SNITS.

3. **Se till att spetsen inte kommer på bekostnad av bredden.**

Det finns organisationer som når ett högt resultat inom enskilda arbetsområden, men som inte har arbetat tillräckligt brett med det systematiska informations- och cybersäkerhetsarbetet för att nå ett samlat högt resultat. Att ha spetskompetens inom ett arbetsområde är inte nog för att skydda helheten. Syftet med att arbeta systematiskt och riskbaserat är att en organisation ska kunna:

- etablera, och upprätthålla, en välgrundad bild av sin egen säkerhetssituation och sina egna säkerhetsbehov,
- agera utifrån denna bild för att möta behoven och kunna följa upp om det som gjorts var ändamålsenligt och tillräckligt verksamt,
- agera igen genom att på annat sätt möta behoven om uppföljningen visar att något som gjorts inte fungerar eller inte var tillräckligt.

När en eller flera delar av arbetet med informations- och cybersäkerhet brister, brister även helheten vilket försvårar för organisationen att klara de ovanstående uppgifterna.

4. **Säkerställ en organisation som bygger på etablerade, kommunicerade och beslutade processer, rutiner och metoder istället för personberoenden.**

Bland organisationer som har fått ett lägre resultat i Infosäkkollen förefaller det ofta som att resultat har uppnåtts genom enstaka personers engagemang och inte baserat på systematik. I små organisationer kan det till viss del vara oundvikligt att en person själv agerar, efter bästa förmåga i en given situation. Vissa roller förutsätter också dedikerad personal med särskild kompetens. Trots det finns stora möjligheter att engagera fler i säkerhetsarbetet, och mycket av det som görs går att formalisera och hantera på sätt som gör att andra tar vid om någon som organisationen är beroende av skulle bli otillgänglig.

5. **Arbeta aktivt för att skapa en god säkerhetskultur där informations- och cybersäkerhet är prioriterat på alla nivåer inom organisationen.**

Statliga myndigheter och leverantörer av samhällsviktiga respektive digitala tjänster rapporterar sedan några år tillbaka it-incidenter till MSB. I sina sammanställningar ser myndigheten varje år hur misstag och systemfel som hade kunnat förhindras leder till incidenter. Det bästa sättet att minimera sådana källor till incidenter och begränsa antagonisters möjligheter att lura medarbetarna, och därigenom få tillgång till system och information som de inte är behöriga till, är att upprätta och upprätthålla en god informationssäkerhetskultur. I det ingår att ha en ledning som visar ett aktivt engagemang i frågorna och att ha kunniga och medvetna medarbetare som visas uppskattning för sina insatser till stöd för informations och cybersäkerheten. God säkerhetskultur leder till att medarbetare känner både ett starkare engagemang för att identifiera, analysera och hantera risker och ett ägandeskap och ansvar för organisationens säkerhet.

6. **Använd uppföljning som grund för löpande förbättringar i utvecklingen av informations- och cybersäkerhetsarbetet.**

Ett område som uppvisar stora brister bland alla de tre aktörsgrupperna är uppföljning och utvärdering. Det förefaller vanligt att organisationer snarare går vidare till att arbeta med något nytt än att stanna upp och se över om det som har genomförts fungerar enligt avsikt. Det leder till att organisationer över tid ackumulerar genomförda åtgärder som de inte vet är verkningsfulla och ändamålsenliga. Det kan också leda till att ineffektiva arbetssätt institutionaliseras.

I förlängningen innebär avsaknaden av uppföljning att organisationer inte arbetar systematiskt med informations- och cybersäkerhet. Detta eftersom de saknar den återkoppling som behövs för att kunna förbättra sig, eller säkerställa ändamålsenlighet. Detta är särskilt allvarligt i organisationer som har begränsade resurser, eftersom de har ett särskilt stort behov av att få ut effekt från de åtgärder som ändå kan genomföras med de resurser som finns.

Uppföljning kan ibland uppfattas som en avancerad aktivitet, som utvecklas efter att grunderna kommit på plats. Ofta kan det dock vara så att uppföljning och justeringar av det som redan har gjorts kan ge lika god effekt som att förbereda, utveckla och implementera en helt ny åtgärd. Uppföljning kan därmed vara ett viktigt verktyg i utvecklingsarbetet samtidigt som den sparar organisationen såväl tid som resurser.

7. **Stärk arbetet med kontinuitetshantering**.

Sedan pandemin har många organisationer ändrat hur de arbetar. Många har infört nya informationssystem och tjänster för att möjliggöra förändringen. Det ger många fördelar, men det kan också medföra stora problem om systemen inte fungerar som de ska. Samtidigt har många organisationer saknat ett arbetssätt för kontinuitetshantering, och bland de som har haft arbetssätt, är det få som har övat arbetssättet de senaste två åren. Det är därför angeläget att organisationer upprättar planer för vad de ska göra i sådana lägen och hur verksamhet ska kunna bedrivas under både kortare och längre avbrott. Organisationen behöver även öva sin kontinuitetshantering för att kontrollera att planerna är genomförbara och fungerar. Det gäller såväl de planer som ledningen ska följa som de som användarna av informationssystemen ska följa och de som it-driften ska arbeta utifrån för att få igång informationssystemen igen.

För att öka utvecklingen krävs ett mer aktivt engagemang från organisationsledningar. Eftersom ledningens roll är så viktig för ett framgångsrikt informations- och cybersäkerhetsarbete har MSB tagit fram specifika rekommendation för hur ledningsgruppen kan hjälpa sin organisation framåt:

1. Boka ett möte med CISO (eller motsvarande) och fråga hur ledningen bäst kan bidra till att engagera organisationen. Fråga även CISO om de resurser som behövs. Om ingen har denna roll så verka för att den tillsätts.
2. Boka in regelbundna föredragningar för ledningsgruppen (eller motsvarande) så att ledningen är informerad om allvarliga risker eller andra brister.
3. Läs publikationen *Ledningens roll inom informationssäkerhet - stöd för dig med en ledande funktion* (12 s.) som ger en översiktlig bild av vad informationssäkerhet är och hur arbetet bedrivs, samt ledningens roll.[16]
4. I samband med uppföljningsrapporter, fråga verksamheten hur de arbetar med informationssäkerhet. Ta hjälp av CISO för att analysera resultatet.
5. Verka för att din organisation genomför Infosäkkollen och It-säkkollen. Då får ni reda på hur långt ni kommit med ert systematiska informations- och cybersäkerhetsarbete. Be om en resultatredovisning.

16. https://www.msb.se/sv/publikationer/ledningens-roll-inom-informationssakerhet---stod-for-dig-med-en-ledande-funktion/

### 2.4.3 Rekommendationer till kommunerna

Även om kommunerna förbättrat sig något sedan förra mätningen 2021 så är det samma mönster som framkommer. Efter genomförd analys bedömer MSB att rekommendationerna från 2021 alltjämt är högaktuella:

1. **Stärk ledningens engagemang i det systematiska informations- och cybersäkerhetsarbetet.**

De flesta kommunledningar har någon gång satt en övergripande inriktning för arbetet och beslutat om en informationssäkerhetspolicy och andra övergripande principer för arbetet.

Men, alldeles för få av kommunerna rapporterar att deras ledning under de senaste två åren har förhört sig om statusen på organisationens systematiska informations- och cybersäkerhetsarbete. Ledningarna har därmed sällan informerat sig om vilka övergripande risker kommunen har, och därmed inte heller agerat riskägare och fattat beslut om hantering av risker som kan få stor påverkan på kommunens verksamhet och som inte kan lösas inom ramen för annat verksamhetsansvar i kommunen. Kommunernas ledningar har inte heller tagit ställning till och beslutat i frågor om att ta bort hinder eller stärka framgångsfaktorer som bidrar till att underlätta för medarbetarna att arbeta på ett informationssäkert sätt.

Den resulterande bilden är därför att kommunernas ledningar inte aktivt ser till att den inriktning som de själva satt faktiskt efterföljs, och kan därför inte heller justera inriktningen eller ändra resurstilldelning eller mandat när situationen förändras. När en fråga inte värnas av ledningen finns det alltid en risk att frågan nedprioriteras till förmån för andra saker. Den bilden stärks ytterligare av vad många organisationer själva har angett i fritext om varför de inte kommer vidare i arbetet.

2. **Etablera ett arbetssätt för analys och hantering av informationssäkerhetsrisker, och tillämpa det.**

I många fall är det bästa sättet att hantera ett problem att förebygga det innan det blir verklighet. Trots det saknar ungefär en fjärdedel av kommunerna ett arbetssätt för analys och hantering av informationssäkerhetsrisker som under den senaste tvåårsperioden antingen har:

- varit beslutat eller på annat sätt medvetet valt av organisationen,
- omfattat fördelning av roller och ansvar,
- innehållit en organisationsgemensam modell för analys av informations- och cybersäkerhetsrisker,
- varit beskrivet i stöd och vägledning för medarbetarna,
- följts upp och utvärderats minst en gång.

I brist på etablerade arbetssätt som är gemensamma för hela, eller åtminstone delar, av kommunerna får medarbetarna löpande hantera risker i den utsträckning de kan. När arbete med risker genomförs beror det på enskilda engagerade medarbetare, vilket innebär att arbetet är personberoende och inte sker på likartat sätt eller likartad grund.

När risker inte identifieras, analyseras eller åtgärdas i en gemensam ordning, får kommunen i stort leva med risker som finns men inte är kända eller inte åtgärdats på bra sätt, och som ibland realiseras utan att mildrande åtgärder finns på plats.

3. **Etablera ett arbetssätt för kontinuitetshantering och öva det.**

Under de senaste två åren har drygt hälften av kommunerna haft ett arbetssätt för kontinuitetshantering som antingen har varit:

- varit beslutat eller på annat sätt medvetet valt av organisationen,
- omfattat fördelning av roller och ansvar,
- innehållit en organisationsgemensam modell för kontinuitetshantering, inklusive scenarier som organisationen behöver öva,
- varit beskrivet i stöd och vägledning för medarbetarna,
- följts upp och utvärderats minst en gång.

Av de som har kontinuitetsplaner för sina olika verksamheter har ungefär två tredjedelar övat arbetssätten i planerna, men bland de som har övat arbetssätten har drygt 40 procent övat mindre än 50 procent av sina verksamheter. Utav den fjärdedel av de som har kontinuitetsplaner har dessa övat 0–25 procent av sina verksamheter.

Utifrån det kommunala uppdraget och de beroenden till fungerande informationssystem som finns i många verksamheter förefaller andelen övade verksamheter vara lågt.

I kombination med avsaknaden av en strukturerad riskhantering framstår en majoritet av kommunerna som dåligt förberedda om något allvarligt skulle hända.

4. **Utbilda fler och bättre.**

Typkommunen har under den senaste två-årsperioden utbildat 0–25 procent av sina medarbetare i informationssäkerhet. Efter genomförd utbildning har kommunen inte undersökt om medarbetarna vet hur de ska göra för att arbeta på ett informationssäkert sätt, eller om de tillämpar sina kunskaper om hur de kan göra det i sitt arbete. Utbildningen som har tillhandahållits har inte varit utformad utifrån:

- medarbetarnas roller, uppgifter, ansvar och behov,
- medarbetarnas kunskapsnivå,
- ledningens målsättningar för det systematiska informations- och cybersäkerhetsarbetet,
- organisationens regelverk samt olika arbetssätt och stöd för informations- och cybersäkerhetsarbetet,
- organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter.

Kommunen har inte heller undersökt medarbetarnas uppfattningar om vilka hinder och framgångsfaktorer som påverkar deras möjligheter att arbeta informationssäkert och som de möter i sin verksamhet, och saknar därför kunskap om den utbildning som tillhandahålls gör någon avgörande nytta för kommunen.

5. **Följ upp arbete och åtgärder.**

Under den senaste tvåårsperioden har typkommunen inte följt upp eller utvärderat något av sina arbetssätt för informationsklassning, analys och hantering av informationssäkerhetsrisker, hantering av informationssäkerhetsincidenter och avvikelser, kontinuitetshantering, omvärldsbevakning eller säkerställande av informationssäkerhet vid upphandling. Kommunerna har under perioden inte heller följt upp det systematiska informations- och cybersäkerhetsarbetet.

Medan typkommunen har haft ett arbetssätt för att hantera informationssäkerhetsincidenter och avvikelser, svarar ungefär en tredjedel att arbetssättet inte omfattar analys av inträffade incidenter, deras grundorsaker och hantering, samt återföra erfarenheter till det förebyggande arbetet. Eftersom mer än en fjärdedel av kommunerna saknat arbetssätt för att säkerställa informationssäkerhet vid upphandling så har det inte heller bedrivits ett systematiskt arbete enligt en på förhand beslutad struktur att följa upp om ställda krav var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

6. **Etablera ett arbetssätt för att säkerställa informationssäkerhet vid upphandling och kvalitetssäkra det.**

Mer än en fjärdedel av kommunerna har under den senaste två-årsperioden saknat ett arbetssätt för att säkerställa informationssäkerhet vid upphandling som antingen har:

- varit beslutat eller på annat sätt medvetet valt av kommunen,
- omfattat fördelning av roller och ansvar,
- innehållit en kommungemensam modell för informationssäkerhet vid upphandling,
- varit beskrivet i stöd och vägledning för medarbetarna
- följts upp och utvärderats minst en gång.

Då upphandling är centralt för att många delar av den kommunala förvaltningen ska fungera är det angeläget att kommunerna upprättar sådana arbetssätt. När de gör det bör de också säkerställa att arbetssättet omfattar att:

- klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras eller anskaffas,
- identifiera behovet av säkerhetsåtgärder utifrån resultatet av informationsklassningen och riskanalysen,

- införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv,
- ställa krav på säkerhetsåtgärder som den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat ska införa,
- följa upp om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats,
- följa upp om de ställda kraven var ändamålsenliga och tillräckliga.

### 2.4.4 Rekommendationer till regionerna

Även om regionernas deltagande glädjande ökat sedan förra mätningen 2021 så är det problematik som förekommer. Efter genomförd analys bedömer MSB att rekommendationerna från 2021 alltjämt är högaktuella:

1. **Stärk säkerhetskulturen.**

I organisationer med en stark säkerhetskultur har medarbetarna en hög medvetenhet om säkerhetsfrågorna. De bidrar aktivt till att identifiera och hantera risker samtidigt som de och ledningen samarbetar för att stärka framgångsfaktorer och ta bort hinder för att säkerställa att verksamheten bedrivs på ett säkert sätt. I sådana organisationer sker ett ständigt lärande för att möta nya säkerhetsbehov. Regionerna har, enligt sina svar, gjort en hel del för att stärka informations- och cybersäkerhetskulturen i sina organisationer, men det går att stärka den ytterligare på några områden.

Under perioden har regionerna inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder kunskaperna i sitt arbete.

Typregionen har heller inte undersökt medarbetarnas kunskaper inom:

- vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- de regler och krav som styr informationssäkerhetsarbetet inom organisationen
- vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt,
- informationssäkerhetsrelaterade hot, sårbarheter och risker,
- vad medarbetarna ska göra om en informationssäkerhetsincident inträffar.

Typregionen har vidare inte undersökt medarbetarnas uppfattningar om vilka hinder och framgångsfaktorer som påverkar deras möjligheter att arbeta informationssäkert och som de möter i sin verksamhet. Typregionens ledning har inte följt upp och vid behov beslutat om organisationens arbete med att ta bort eller reducera identifierade hinder respektive införa eller stärka framgångsfaktorer.

2. **Inventera informationsmängder och informationssystem i organisationens alla verksamheter.**

Regionerna gör som grupp generellt bra ifrån sig jämfört med de andra aktörsgrupperna. Just i fråga om att inventera sina informationsmängder och informationssystem, inklusive nätverk, har man dock under perioden gjort det i 25–50 procent av organisationens verksamheter. Det understiger klart resultaten i de andra aktörsgrupperna.

Med så pass många informationsmängder och informationssystem kvar att inventera finns det troligen i de flesta regioner ett antal tillgångar som behöver ett mer omfattande skydd än de har. Denna risk behöver hanteras.

3. **Utbilda fler.**

Typregionens arbetssätt för utbildning i informations- och cybersäkerhet innehåller flera viktiga inslag. Men, under den senaste tvåårsperioden har typregionen utbildat upp till 25 procent av sina medarbetare i informationssäkerhet. Med en snabb teknisk förändring, mer hemarbete och personalomsättning är det viktigt att bedriva en relativt omfattande utbildningsverksamhet för att säkerställa att medarbetarna är medvetna om riskerna och hur man kan arbeta säkert.

4. **Följ upp fler av säkerhetsåtgärderna och om de informationssäkerhetskrav som har ställts vid upphandling efterföljs.**

Regionerna följt upp både analys och hantering av informationssäkerhetsrisker samt hantering av informationssäkerhetsincidenter och avvikelser under de senaste två åren. Därutöver har man, i några hänseenden, följt upp resultatet av sitt systematiska informationssäkerhetsarbete.

Uppföljningen uppvisar dock vissa brister. Drygt 45 procent av regionerna har utvärderat om införda säkerhetsåtgärder har varit ändamålsenliga i mindre än 25 procent av regionens verksamheter. Mer än en femtedel har inte utfört någon utvärdering av implementerade säkerhetsåtgärder överhuvudtaget. Det har inte skett någon uppföljning av om de krav som ställdes i samband med upphandlingar var ändamålsenliga och tillräckliga, eller om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

### 2.4.5 Rekommendationer till myndigheterna

Även om myndigheterna förbättrat sig något sedan undersökningen 2021 återkommer samma problembild. MSB:s bedömning är att rekommendationerna från 2021 även fortsatt bör hörsammas:

1. **Följ MSB:s föreskrifter om statliga myndigheters informationssäkerhet.**

Myndigheter ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt (19 § förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap). Som stöd för

detta arbete har MSB sedan 2009 utfärdat föreskrifter med detaljerade krav på hur ett systematiskt informationssäkerhetsarbete ska bedrivas. Det ska omfatta all behandling av information som myndigheten ansvarar för, och integreras med myndighetens befintliga sätt att leda och styra sin organisation. Resultatet i Infosäkkollen 2023 visar att många myndigheter är ganska långt ifrån att nå upp till kraven de omfattas av.

2. **Stärk ledningens engagemang i det systematiska informations- och cybersäkerhetsarbetet.**

Det är visserligen så att en majoritet av de svarande myndigheterna anger att de i flera avseenden har en ledning som aktivt deltar i det systematiska informationssäkerhetsarbetet. Ledningens styrning och kontroll hör emellertid till ett av de arbetsområden där myndigheterna presterar svagt, och få framsteg har gjorts inom detta område sedan år 2021. De är därför av fortsatt vikt att myndighetsledningar informerar sig om statusen på organisationens systematiska säkerhetsarbete, beslutar om inriktning och nivå på informations- och cybersäkerhetsarbetet, tillsätter resurser så att beslutade åtgärder ska kunna genomföras samt aktivt tar bort hinder och stärker framgångsfaktorer för att underlätta det systematiska informations- och cybersäkerhetsarbetet.

3. **Öva kontinuitetshantering.**

Typmyndigheten har under den senaste tvåårsperioden haft ett arbetssätt för kontinuitetshantering som är beslutat eller på annat sätt medvetet valt av organisationen samt omfattar fördelning av roller och ansvar. Men övningar av kontinuitetshanteringen har enbart omfattat 0 % till mindre än 25 % av organisationens verksamheter.

Omställning till hemarbete har, i många myndigheters fall, lett till att stora mängder medarbetare nu nyttjar fjärranslutningar och nätbaserade tjänster för att kunna arbeta. Därför är det angeläget att man kontrollerar att man kan hantera såväl kortvariga som långvariga avbrott trots att stora delar av arbetsstyrkan (i synnerhet vid avbrottets början) troligen inte kommer att befinna sig på den fysiska arbetsplatsen och därmed inte kommer att kunna nyttja sådana verktyg som eventuellt finns tillgängliga där för att möjliggöra fortsatt arbete under andra former.

4. **Kvalitetssäkra arbetssätt för analys och hantering av informationssäkerhetsrisker.**

Typmyndigheten har under den senaste tvåårsperioden haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker. Arbetssättet har också tillämpats i hög grad. Arbetssätten har dessutom omfattat flera av de delar som är viktiga för en väl fungerande riskhantering. Typmyndighetens arbetssätt på området brister dock avseende värdering av riskers sannolikhet och centrala delar i en ordnad riskhanteringsprocess.

Typmyndighetens arbetssätt för analys och hantering av informationssäkerhetsrisker har under de senaste två åren inte omfattat sannolikhetsbedömningar såsom:

- när risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna,

- hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder införs,
- när risken tidigast, senast och troligast kan väntas inträffa om föreslagna säkerhetsåtgärder införs,
- hur säker man kan vara på sannolikhetsbedömningarna givet vad man vet och de antaganden man har gjort.

Följden av att inte värdera riskers sannolikheter blir att det uppstår ett överfokus på de konsekvenser som en risk anses medföra (något som implicit, i sig, är en sannolikhetsbedömning, en konsekvens räknas ju bara in om den anses trolig eller möjlig). Det kan leda till att organisationer främst fokuserar på risker som slår in mycket sällan (men som skulle ha katastrofala konsekvenser) samtidigt som man missar risker som slår in ofta, men som kanske inte leder till så allvarliga konsekvenser vid varje enskilt tillfälle som de realiseras. Den kumulativa effekten av att risker slår in frekvent kan dock vara värre än den som skulle uppstå om en mer allvarlig risk med lägre sannolikhet skulle realiseras en gång.

Typmyndighetens arbetssätt för riskhantering har de senaste två åren inte omfattat att:

- organisationen har ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka som kan accepteras utan åtgärd,
- analys av enskilda informationssäkerhetsrisker uppdateras efter att beslutade säkerhetsåtgärder har införts (det vill säga att analysen genomförs igen för att se vilken riskreducerande effekt den eller de införda säkerhetsåtgärderna har medfört),
- status för informationssäkerhetsrisker följs upp utifrån definierade intervall.

5. **Undersök medarbetarnas kunskaper och om de tillämpar sina kunskaper i sitt arbete.**

Under perioden har typmyndigheten utbildat alla sina medarbetare inom informations- och cybersäkerhet enligt sitt arbetssätt för utbildning. Under samma period har typmyndigheten också undersökt deras kunskaper om informations- och cybersäkerhet. Myndigheterna har dock inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning vet hur de ska arbeta på ett säkert sätt och inte heller om medarbetarna använder kunskaperna i sitt arbete.

Typmyndighetens undersökning av medarbetarnas kunskaper om informationssäkerhet har under perioden inte omfattat huruvida de vet:

- vad som menas med informations- och cybersäkerhet och informations- och cybersäkerhetsarbete, samt varför det är viktigt för organisationen,
- de regler och krav som styr informations- och cybersäkerhetsarbetet inom organisationen,
- vad medarbetarna ska göra om en säkerhetsincident inträffar,

- vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt,
- informations- och cybersäkerhetsrelaterade hot, sårbarheter och risker.

6. **Följ upp arbetet och de utkontrakterade tjänsterna.**

Typmyndigheten har under perioden inte följt upp eller utvärderat arbetssätten för kontinuitetshantering, omvärldsbevakning eller säkerställande av informations- och cybersäkerhet vid upphandling.

Myndigheterna har de senaste två åren inte heller följt upp resultatet av sitt systematiska informations- och cybersäkerhetsarbete genom att sammanställa och analysera:

- skillnaden mellan införda och beslutade säkerhetsåtgärder,
- resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet.

I myndigheternas arbetssätt för att säkerställa informationssäkerhet vid upphandling har det under perioden inte ingått att följa upp om ställda krav är ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

Typmyndigheten har inte undersökt medarbetarnas uppfattningar om vilka hinder och framgångsfaktorer som påverkar deras möjligheter att arbeta informationssäkert och som de möter i sin verksamhet.

## 2.5 MSB:s satsningar

Med anledning av resultaten som redovisas i denna rapport har MSB identifierat flera områden där myndigheten kan göra ytterligare insatser för att höja nivån på den offentliga förvaltningens systematiska informationssäkerhetsarbete:

**Metodstöd**: Flera av MSB:s vägledningar kommer också att ses över i samband med att NIS2 och CER blir lag. Dessa kommer publiceras inom ramen för MSB:s metodstöd för systematiskt informations- och cybersäkerhetsarbete.

**Utbildning**: MSB har under flera år erbjudit kurser i informations- och cybersäkerhet riktade till myndighetschefer. Innehåll och utformning är särskilt anpassade för högsta ledningens perspektiv och roll för styrning och ledning av det systematiska, förebyggande arbetet. Under 2024 görs en översyn av konceptet för att eventuellt göra det tillgängligt för fler personer i ledande befattningar. NIS2 som nu ska införas ställer nya krav på ett stort antal organisationer som tidigare inte omfattats av reglering, och innebär dessutom tydligare krav på ledningen. Utifrån resultatet i Infosäkkollen 2021 och 2023 kan kursen bidra till att adressera de brister som framkommit gällande ledningens styrning och kontroll.

**Stöd till ledningar**: MSB kommer att fortsätta med kommunikationsinsatser mot ledningar i den offentliga förvaltningen. Syftet är att höja medvetenheten om vikten av informations- och cybersäkerhetsarbete i det alltmer digitaliserade samhället, och att påminna om ledningens roll för ett framgångsrikt systematiskt arbete.

**Stöd till CISO**: MSB arrangerar interaktiva webbinarier i serien *Informationssäkerhet i fokus* där tittarna får ställa frågor till de föredragande i livesändning. Myndigheten tillhandahåller nätverket Snits och deltar aktivt i KIS och HoSIS. Alla tre nätverk bidrar till vidareutveckling och samarbete. MSB:s rådgivningstjänst stödjer det förebyggande arbetet och underlättar en organisation att anpassa informations och cybersäkerhetsarbetet till den specifika verksamheten.

**Stöd till arbete med säkra kommunikationer**: MSB kommer att fortsätta arbetet med att höja förmågan inom säkra kommunikationer i den offentliga förvaltningen, till exempel genom att fortsätta att besluta om och tilldela signalskydd, samt tillhandahålla kommunikationstjänster såsom SGSI, WIS och Rakel. MSB företräder även de civila aktörerna vid utveckling av system och metoder inom ramen för säkra kommunikationer.

**Forskning**: Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) främjar samarbete mellan svenska forskningsinstitut, företag och myndigheter för utveckling av cybersäkerhetslösningar. NCC-SE erbjuder vägledning om hur man söker EU-finansiering för utveckling av nya cybersäkerhetslösningar och genomför nationella utlysningar för att stärka små och medelstora företag.

## 2.6 Samarbete och näringslivets roll

Resultatredovisningens mest centrala slutsats är att det behövs en särskild satsning på att stärka det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen. Mer behöver göras, men mer behöver också göras mer effektivt, så att de begränsade resurserna får en större effekt på det systematiska säkerhetsarbetet.

I synnerhet kommunerna, men även myndigheter och regioner, behöver stöd för att höja den övergripande nivån. MSB har identifierat ett antal områden där det finns goda förutsättningar för organisationer att lära av varandra. Inom dessa områdena kan näringslivet ha en stöttande roll. MSB har också identifierat ett antal områden där förutsättningarna för samarbete och ömsesidigt lärande är mer begränsade, främst för att få organisationer verkar ha så mycket erfarenheter att dela med sig av inom de områdena. Inom de områdena kan näringslivet göra särskilt stor nytta genom att tillhandahålla tjänster och att genom innovation finna nya sätt att lösa uppgifter på mer resurseffektiva sätt.

MSB rekommenderar kommuner, regioner och myndigheter att tillsammans se över möjligheterna att samarbeta kring nya sätt att lösa de uppgifter som ingår i det systematiska informations- och cybersäkerhetsarbetet, samt att analysera i vilka delar av säkerhetsarbetet de skulle kunna ha särskild nytta av externt stöd.

De nedanstående områdena, identifierade i analysen av inskickade svar, är områden där stöd av externa aktörer i form av kunskapsöverföring, nya tjänster och verktyg bör kunna göra särskild nytta. Inom de här områdena kan näringslivet särskilt bidra genom att tillhandahålla ett relevant utbud av tjänster och verktyg:

- uppföljning (i synnerhet uppföljning av utbildningsinsatser),
- undersökningar av medarbetarnas kunskaper,
- undersökningar av hinder och framgångsfaktorer som påverkar informations- och cybersäkerhetsarbetet,
- kontinuitetshantering (i synnerhet övningar).

### 2.6.1 Områden där kommunerna behöver stöd

Följande frågor i Infosäkkollen 2023 representerar områden där kommunerna har brister och få andra kommuner att lära från varandras erfarenheter av, och därför näringslivet kan göra en särskilt viktig insats:

- **Fråga 14**: Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 15**: Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 17**: Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 26**: Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?
- **Fråga 27**: Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30**: De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 33**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala delar?
- **Fråga 34**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat bedömning av följande centrala typer av skadeverkan och grad av skadeverkan?
- **Fråga 35**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala typer av sannolikhetsbedömning?
- **Fråga 36**: De två senaste åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat riskhantering med följande centrala delar?

- **Fråga 37**: De senaste två åren, har organisationens arbetssätt för att säkerställa informationssäkerhet vid upphandling omfattat följande centrala delar?
- **Fråga 39**: De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?
- **Fråga 40**: De senaste två åren, har organisationens ledning arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?

### 2.6.2 Områden där regionerna behöver stöd

Följande frågor i Infosäkkollen 2023 representerar områden där regionerna har brister och få andra regioner att lära från varandras erfarenheter av, och därför näringslivet kan göra en särskilt viktig insats:

- **Fråga 17**: Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 27**: Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30**: De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 39**: De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

### 2.6.3 Områden där myndigheterna behöver stöd

Följande frågor i Infosäkkollen 2023 representerar områden där myndigheterna har brister och har få andra myndigheter att lära från varandras erfarenheter av, och därför näringslivet kan göra en särskilt viktig insats:

- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 30:** De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 39:** De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

# Hur resultatet tagits fram

# 3. Hur resultatet tagits fram

## 3.1 Om Infosäkkollen

Det ena målet med Infosäkkollen är att ge den offentliga förvaltningens organisationer stöd i att följa upp sitt systematiska informations- och cybersäkerhetsarbete. Efter att organisationen svarat på frågor om sitt säkerhetsarbete ges återkoppling direkt i verktyget om vilken nivå organisationen befinner sig på och viktigare utvecklingsområden.

Det andra målet med Infosäkkollen är att MSB regelbundet ska redovisa en samlad bedömning av nivån på det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen, samt se över hur modellen och övrigt stöd på området kan utvecklas. För detta ändamål uppmuntras de organisationer som använder Infosäkkollen att rapportera in sina resultat till MSB.

Infosäkkollen har dessutom vidareutvecklats med ett återkopplingsverktyg, Infosäkkollen Benchmark, där en organisation kan jämföra sitt eget resultat med sammanställda resultat (benchmarks) från alla organisationer som rapporterat in sina svar.

Inrapporteringsmöjligheten, som gör att organisationer kan jämföra sig med varandra och att MSB kan göra en övergripande analys och samlad bedömning, kommer att återkomma vartannat år. Tvåårsintervallet är valt för att nivån på informations- och cybersäkerhetsarbetet är resultatet av arbete och val som har gjorts över tid. Då både förändringar och uppföljning tar tid att genomföra blir det inte effektivt att mäta för ofta.[17]

Uppföljningen är inriktad på det systematiska informations- och cybersäkerhetsarbetet, det vill säga att organisationen arbetar medvetet och metodiskt med att analysera, planera, genomföra samt följa upp och förbättra sin informations- och cybersäkerhet, samt att de olika delarna av arbetet kopplas ihop till en helhet.

MSB:s uppfattning om hur en organisation bör bedriva sitt systematiska informations- och cybersäkerhetsarbete framgår av myndighetens föreskrifter[18] och stöd på området, vilka bygger på standardserien ISO/IEC 27000 om ledningssystem för informationssäkerhet. Uppföljningsstrukturen har utvecklats med strävan att

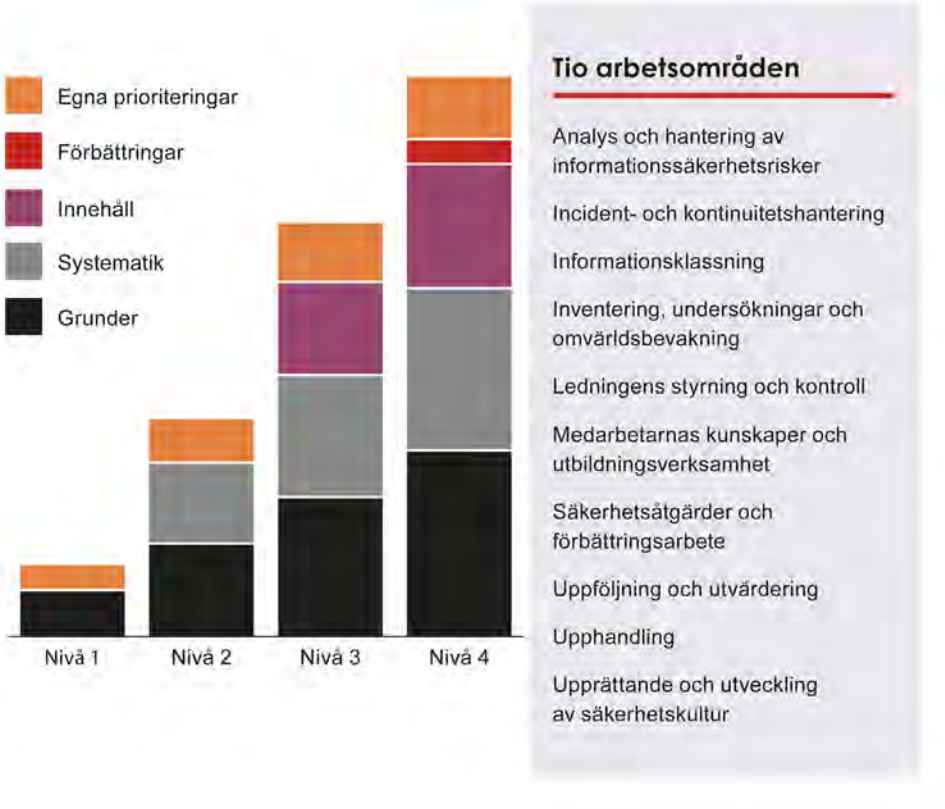
17. I MSB:s regleringsbrev för 2024 innefattar en aktivering av Infosäkkollen och it-säkkollen, dvs. att de ska genomföras även 2024. https://www.esv.se/statsliggaren/regleringsbrev/Index?rbId=23933 (hämtad 24 januari 2024).

18. Närmast föreskrifterna om informationssäkerhet för statliga myndigheter, MSBFS 2020:6.

beskriva och mäta systematiskt informationssäkerhetsarbete som det kommer till uttryck i dessa källor.

Infosäkkollen görs utifrån en modell med fyra nivåer som svarar mot ett stegvist utvecklingsarbete, och tio arbetsområden som speglar väsentliga delar i det systematiska informations- och cybersäkerhetsarbetet.

**Figur 1.** Infosäkkollens modell för uppföljning




Närmare bakgrund till och beskrivning av den modell som ligger till grund för nivåindelning och resultatberäkning finns i *fördjupningsinformationen* som återfinns Infosäkkollens webbsida[19].

## 3.2 Om analysunderlaget

Denna rapport är i huvudsak baserad på svaren som MSB fick ta del av under den andra inrapporteringsperioden av Infosäkkollen, som genomfördes från maj till september 2023. Jämförelser görs också med de svar som MSB fick inrapporterade i samband med första inrapporteringsperioden, från maj till september 2021.

Eftersom innehållet i en organisations resultat kan vara känsligt användes ett särskilt förfarande för att upprätthålla säker hantering vid överföringen. Alla inkomna svar har kontrollerats manuellt för att (i möjligaste mån) verifiera att inrapporteringen gått rätt till.

19. www.msb.se/cybersakerhetskollen

Hur verktyget använts och hur arbetet med att besvara frågorna gått till har utvärderats såväl 2021 som 2023. I enkätundersökningen 2023 svarade 174 organisationer, vilket motsvarar drygt 67 procent av svarsunderlaget. Nästan 82 procent av respondenterna ansåg Infosäkkollen värdefull för sitt säkerhetsarbete och nästan 61 procent uppgav att de genomför Infosäkkollen i egen regi årsvis eller mer frekvent än så. Mer information om enkätundersökningen återfinns i 4.1.7.

### 3.2.1 Tolkningsutrymme vid besvarande av frågorna

Under utvecklingen av Infosäkkollen lades stor vikt vid att utforma frågorna så att resultatet blir strukturerat och jämförbart, bland annat genom att fokusera på jämförbara fakta och tydlighet kring mätperiod för att begränsa utrymmet för tolkningar. Dialogen med målgrupperna genom referensgrupp och pilotomgångar bidrog i hög grad till arbetet med att successivt förtydliga frågorna och minska spridningen.

Likväl kan frågorna och svaren i viss mån uppfattas olika beroende på omständigheter kring den enskilda organisationen och den eller de som arbetar med verktyget. I underlaget finns resultat som aktualiserar möjligheten att tolkningarna skiljer sig åt, samtidigt angav en majoritet av respondenterna i enkätundersökningen efter deltagandet att de anser Infosäkkollen självförklarande. En ännu större majoritet, fler än tre fjärdedelar, angav i samma enkätundersökning att återkopplingen i Infosäkkollen var förståelig och givande, vilket är en indikation på att de förstått modellen och dess frågor.

## 3.3 Sammanställning och analys

Vid sammanställning och redovisning av de resultat som rapporterats in från deltagande organisationer finns flera aspekter som behöver beaktas. Vid en kvantitativ analys behöver hänsyn tas till uppnådda poängresultat men också till de inbördes relationerna mellan olika delar av resultatet. Vidare behövs en metod som är mer nyanserad än enbart nivåindelningen för att kunna jämföra resultat för olika organisationer. Dessutom bör det inte gå att identifiera enskilda organisationers resultat i sammanställningar och återkoppling.

För att kunna sammanställa, jämföra, analysera och presentera resultaten används därför flera specifika metoder och verktyg som beskrivs i detta avsnitt.

### 3.3.1 Benchmarks

För att beskriva resultaten för olika grupper används ”*benchmarks*”. Med benchmark för en grupp menas hur en generell representant för en grupp skulle ha svarat på Infosäkkollens frågor, givet vad medlemmarna i den gruppen som har rapporterat in sina resultat till MSB har svarat på frågorna.

De tre huvudsakliga grupperna i materialet är kommuner, regioner och myndigheter. För vardera av dessa tre grupper finns en benchmark som alltså kan likställas med typresultat baserat på svaren från alla i gruppen som finns med i underlaget; en ”typkommun”, en ”typregion” och en ”typmyndighet”.

För kommuner och myndigheter finns ytterligare en benchmark per grupp som representerar de bästa resultaten, ”30 bästa kommunerna” och ”30 bästa myndigheterna”. Antalet svar från regioner är för litet för att det ska vara meningsfullt att göra en motsvarande benchmark för denna grupp.

### 3.3.2 Resultattal

För att jämföra resultat för olika organisationer används ”*resultattal*”. Resultattalet representerar en organisations samlade resultat i Infosäkkollen och sätts samman av flera delar. I första hand jämförs den övergripande nivån. För organisationer som har samma nivå jämförs sedan i tur och ordning resultat inom arbetsområdena, uppnådd totalpoäng samt uppnått poängresultat för arbetsområdena.

### 3.3.3 Om redogörelsen för resultaten

Redogörelsen för resultaten har i huvudsak utgått från det som benchmarks visar för de olika arbetsområdena och i några fall har dessa kompletterats med klargörande detaljer från underlaget eller från enkätundersökningen.

Syftet har varit att göra resultatredovisningen tillgänglig men ändå förmedla bilden på ett relativt tydligt sätt.

## 3.4 Om It-säkkollen 2023

It-säkkollen är framtagen i enlighet med regeringsuppdraget Fö2023/00697 som uppdrogs MSB 23 mars 2023. It-säkkollen lanserades tillsammans med Infosäkkollen 17 maj 2023. It-säkkollen 2023 var en enkät med 41 frågor där respondenten självskattade sina svar utifrån ett påstående med fyra möjliga svarsalternativ: stämmer inte, stämmer knappt, stämmer väl och stämmer helt. Frågorna är baserade på MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Självskattningsenkäter är problematiska. De lämnar ett stort tolkningsutrymme hos respondenten, vilket påverkar trovärdigheten av insamlade data. Respondenter brukar särskilt överskatta sin egen förmåga. Svaren och de slutsatser som redogörs för i detta kapitel kan därför inte jämställas med trovärdigheten i svaren för Infosäkkollen. De nivåangivelser som anges är inte heller kalibrerade mot MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

It-säkkollen ska vidareutvecklas fram till 2025. Undersökningen ska ges samma metodologiska robusthet som Infosäkkollen. I detta ingår en pilot med målgrupperna för att testa modellen.

# Resultatet av Infosäkkollen 2023

# 4. Resultatet av Infosäkkollen 2023

I det här kapitlet redogörs för resultatet i Infosäkkollen 2023 för alla organisationer i offentlig förvaltning och hos de olika aktörsgrupperna, det vill säga kommuner, regioner och myndigheter.

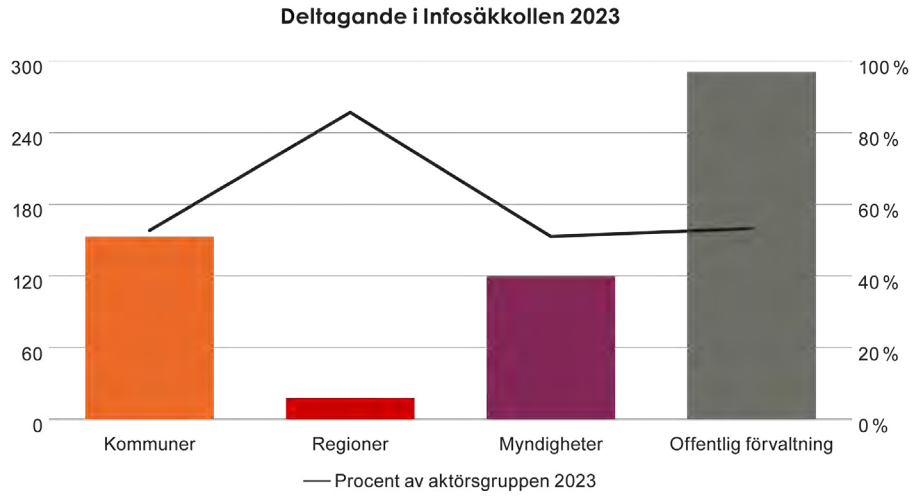
## 4.1 Övergripande bild

Den övergripande bilden redovisar resultatet för hela den samlade offentliga förvaltningen.

### 4.1.1 Deltagande

53,3 procent av organisationerna inom offentlig förvaltning deltog i Infosäkkollen 2023.[20] Deltagarfrekvensen är högst inom aktörsgruppen regioner (85,7 %), följt av kommuner (52,8 %) och till sist myndigheter (51,1 %). I samtliga fall deltog en majoritet inom varje aktörsgrupp. Svarsfrekvensen medför att resultaten med säkerhet kan extrapoleras för slutsatser och rekommendationer. Detta till trots hade MSB med fördel sett ett ännu högre deltagande. Alla samhällsviktiga verksamheter borde aktivt bidra till sitt eget förbättringsarbete genom att nyttja verktyg såsom Infosäkkollen.

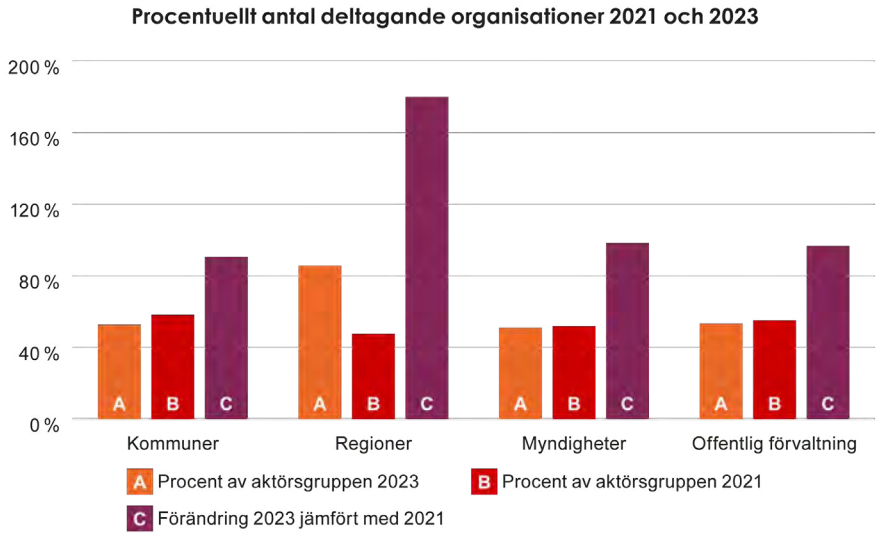
**Diagram 1.** Infosäkkollen diagram 1




20. Domstolsverket har rapporterat in ett svar för alla domstolars räkning.

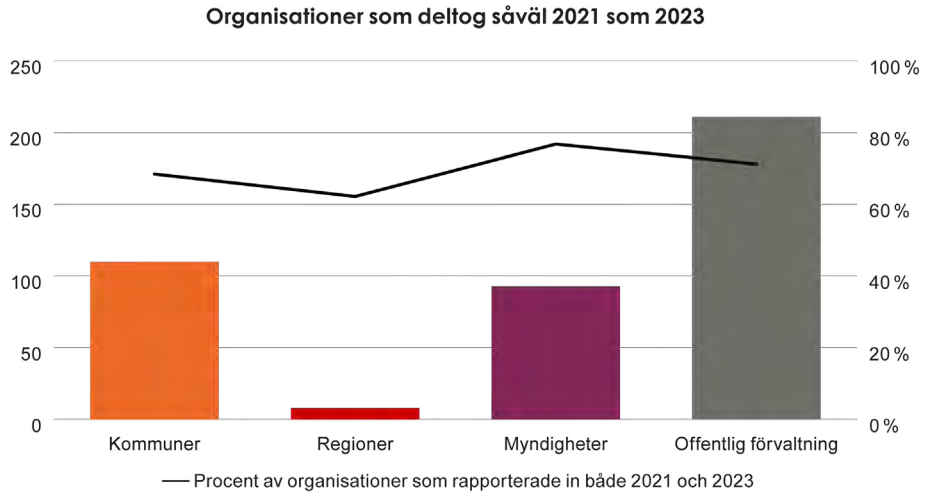
Deltagarantalet 2023 har sjunkit med 3,3 procent mellan de två mättillfällena. Även om deltagandet minskade bland kommuner (9,5 %) och myndigheter (1,6 %) så är det positivt att se nästan en fördubbling (180 %) bland regionerna.

**Diagram 2.** Infosäkkollen diagram 2




211 organisationer deltog såväl 2021 som 2023, vilket utgör 71,3 procent av alla organisationer som vid något tillfälle deltagit i Infosäkkollen. MSB ser ingen större åtskillnad gällande deltagandet mellan de olika aktörsgrupperna vid båda mättillfällena.

**Diagram 3.** Infosäkkollen diagram 3

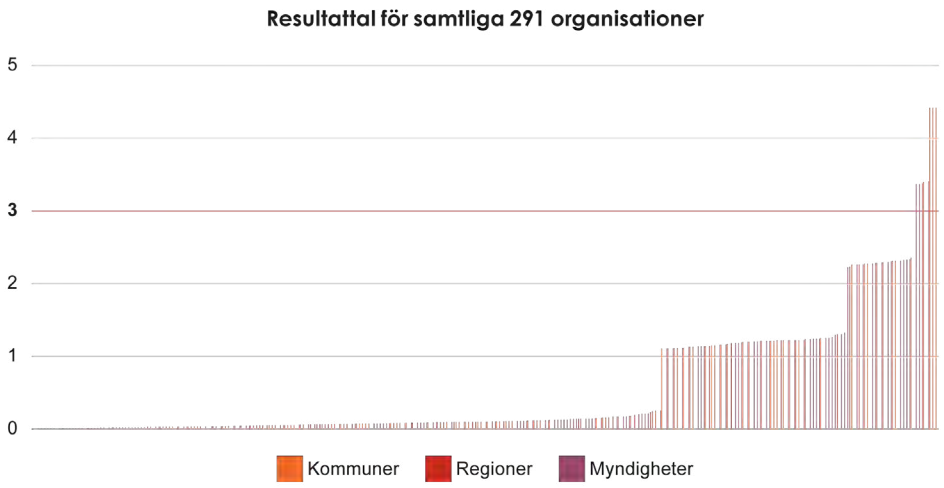


### 4.1.2 Resultattal

Resultattal beskriver det samlade resultatet för en organisation på ett mer detaljerat sätt, och används för att jämföra resultat för olika organisationer. Utöver den övergripande nivån ingår också de resultat som uppnåtts för olika arbetsområden samt den poängsumma som ligger till grund för resultatberäkningen.

89 organisationer, 30,6 procent, uppnådde nivå 1 eller högre i Infosäkkollen 2023. Nivå 1 i Infosäkkollen motsvarar att man har de grundläggande inslagen i ett systematiskt informations- och cybersäkerhetsarbete. Det betyder samtidigt att en majoritet, 69,4 procent av alla deltagande organisationer inte uppnår nivå 1 i modellen. Jämförbar siffra 2021 var 81,7 procent, vilket betyder att det sammantaget är en förbättring i utfallet. För att uppnå nivå 1 i Infosäkkollen måste organisationer ha genomfört minst en åtgärd kopplat till varje av de 15 frågorna i Infosäkkollens första avsnitt.

**Diagram 4.** Infosäkkollen diagram 4



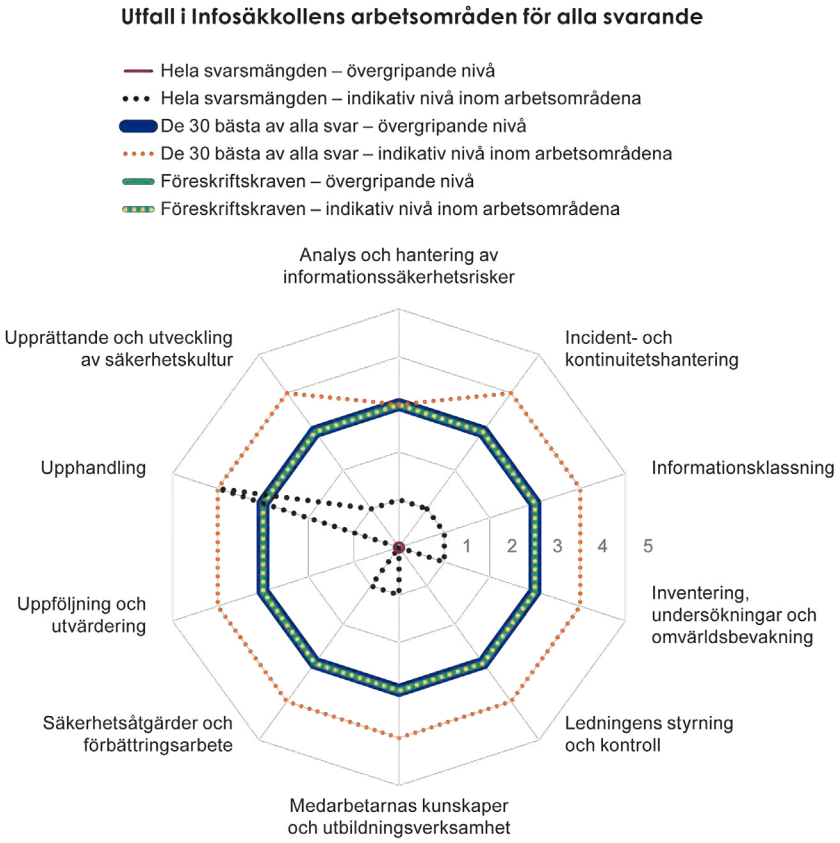

Den röda linjen i diagrammet motsvarar den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

30,6 procent av deltagande organisationer uppnådde alltså nivå 1 eller bättre, 10,3 procent uppnådde nivå 2 eller bättre, och 2,8 procent uppnådde nivå 3 eller 4 i modellen.

### 4.1.3 Utfall per arbetsområde

Benchmarken för de 30 bästa organisationerna uppnådde nivå 3 i modellen, och den gruppens indikativa nivå når nivå 4 på alla arbetsområden förutom Analys och hantering av säkerhetsrisker.

**Diagram 5.** Infosäkkollen diagram 5



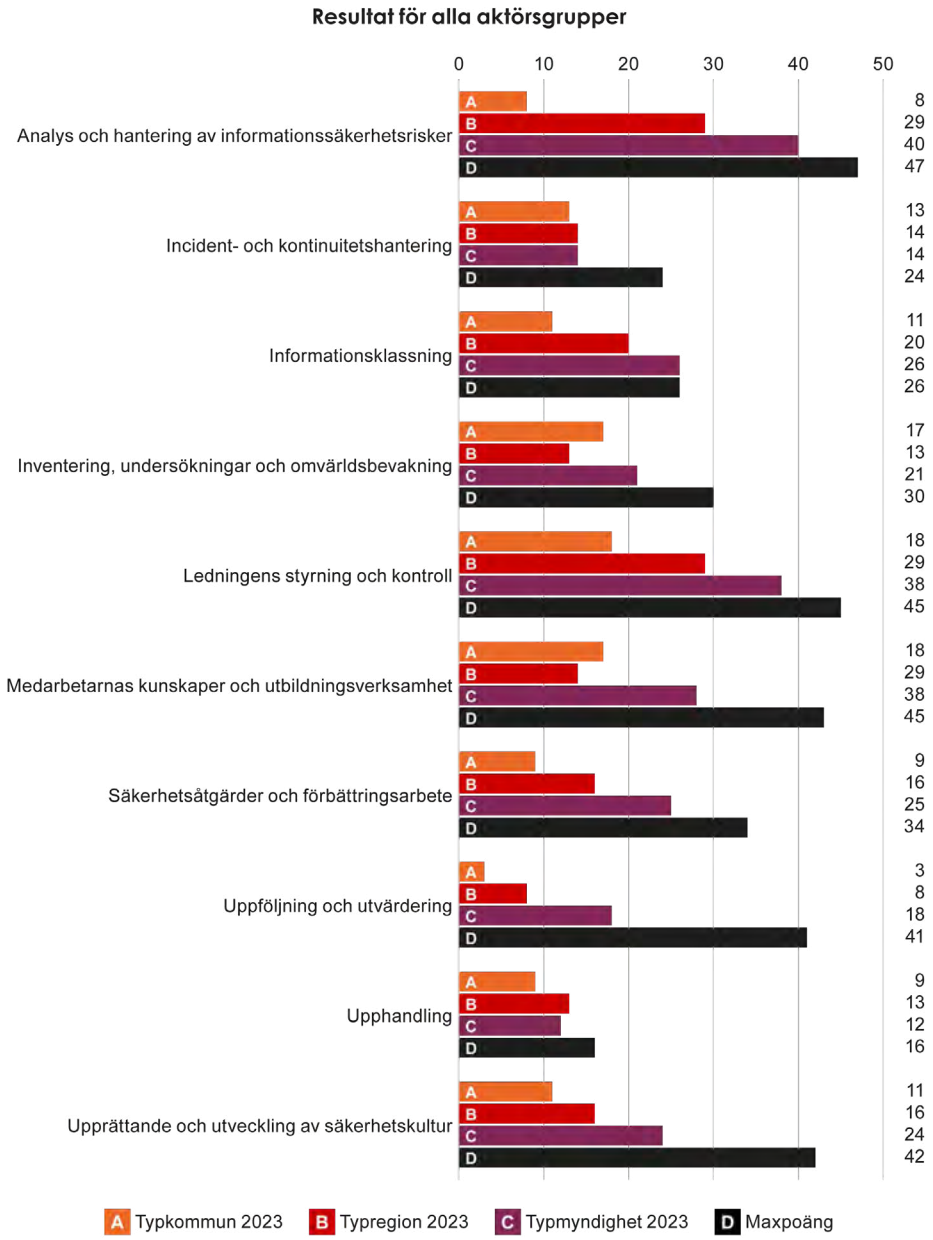

De arbetsområden där flest deltagande organisationerna uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete, följt av Informationsklassning och därefter Analys och hantering av informationssäkerhetsrisker. Medan minst antal deltagande organisationerna har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll, följt av Uppföljning och utvärdering, följt av Upprättande och utveckling av säkerhetskultur samt Incident- och kontinuitetshantering.

Noterbart är att den indikativa nivån för samtliga deltagande organisationer uppnår Nivå 4 på arbetsområdet Upphandling.

### 4.1.4 Generella resultat

Med generella resultat avses uträkningar utifrån en aktörsgrupp och dess resultat.

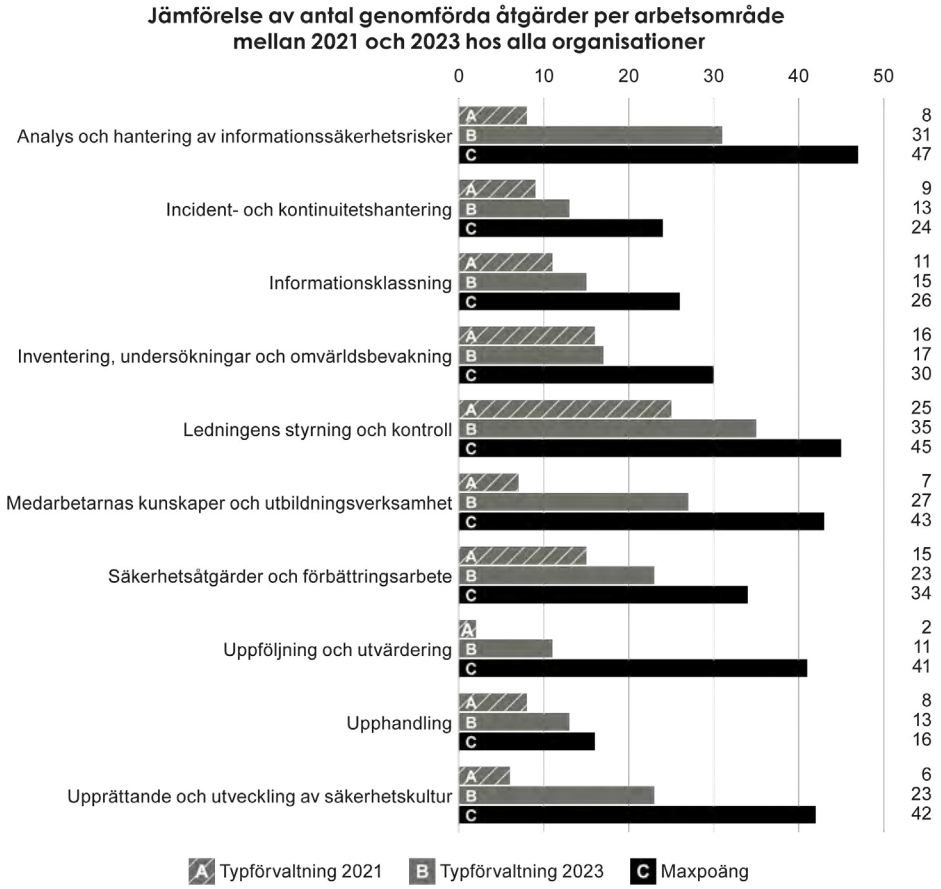
**Diagram 6.** Infosäkkollen diagram 6




Deltagande kommuner är genomgående den aktörsgrupp med svagast resultat, det är endast i två arbetsområden där någon annan aktörsgrupp (regionerna) är svagare än kommunerna. Myndigheterna är bäst på allt förutom Upphandling där regionerna är bättre.

En typmyndighet presterar relativt bra på de flesta arbetsområden, med två stora undantag vilket gäller arbetsområdena för Uppföljning och utvärdering och Upprättande och utveckling av säkerhetskultur.

**Diagram 7.** Infosäkkollen diagram 7




Ovan diagram är baserat på benchmarks för en typförvaltning. Vissa resultat kan antyda att en högre nivå i modellen borde uppnåtts. Det förklaras av att arbetssätt kan finns på plats i större utsträckning, samt innehålla ändamålsenliga inslag, men endast tillämpas i begränsad utsträckning. Detta tar modellen vid nivåbedömningen höjd för.

I de flesta arbetsområden syns en omfattande förbättring från 2021 jämfört med 2023. Detta antyder att de organisationer som deltog 2021, men fick ett väldigt svagt resultat då, inte deltagit 2023, alternativt att dessa förbättrat sig avsevärt, vilket vi kommer återkomma till i 2.6 nedan.

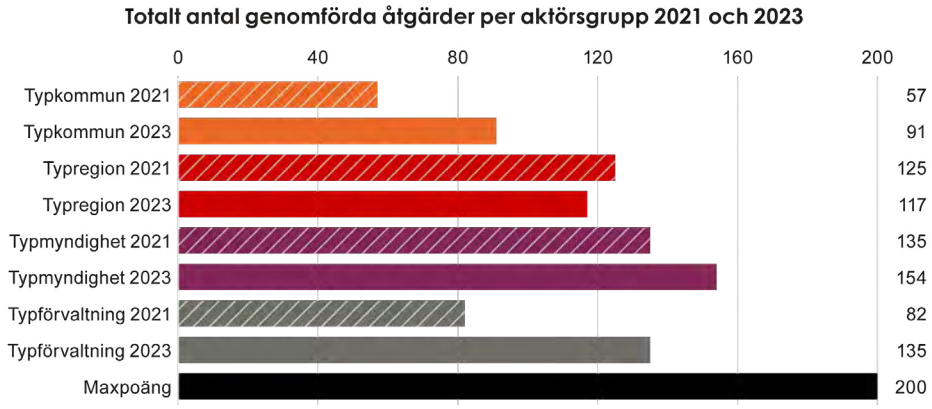
Diagram 3 påvisade att 71,3 procent av alla organisationer som deltog 2021 även deltog 2023. Då detta utgör mer än två tredjedelar är ändå utvecklingen positiv.

Störst förbättring från 2021 till 2023 ses för arbetsområdena för Analys och hantering av informationssäkerhetsrisker, Medarbetarnas kunskaper och utbildningsverksamhet, samt Upprättande och utveckling av säkerhetskultur. Resultatet gällande arbetsområdet Analys och hantering av informationssäkerhetsrisker är ett bra exempel på hur ovan diagram ska utläsas, nämligen att arbetssätt i större utsträckning finns på plats 2023 jämfört med 2021, men alltjämt tillämpas endast i begränsad utsträckning, då typförvaltningen 2023 fortfarande inte klarar åtgärderna som undersöks på nivå 2 i modellen.

Minst förbättring från 2021 till 2023 gäller för arbetsområdena för Inventering, undersökningar och omvärldsbevakning, samt Informationsklassning och Incident- och kontinuitetshantering.

Gällande Ledningen styrning och kontroll har förvisso fler åtgärder genomförts 2023 jämfört med 2021, men nivåresultatet påverkas inte i samma utsträckning då resultatet avseende organisationens uppföljning av sitt eget arbete brister.

**Diagram 8.** Infosäkkollen diagram 8




En deltagande typförvaltning 2023 har genomfört 64,6 procent fler åtgärder än en typförvaltning 2021.

Den aktörsgrupp som förbättrats mest är kommunerna, som höjt sig med 59,6 procent. Ungefär en tredjedel av de deltagande kommunerna genomför Infosäkkollen för första gången och deltog alltså inte 2021, vilket vi kommer se nedan påverkat resultatet.

Den positiva trenden bryts dock av regionerna där typregionen 2023 har ett 6,4 procent sämre resultat jämfört med 2021. Det förklaras av att deltagandet inom den aktörsgruppen nästan fördubblats mellan mättillfällena och det är de regioner som inte deltog 2021, men som deltog 2023 dragit ner det generella resultatet.

**Diagram 9.** Infosäkkollen diagram 9

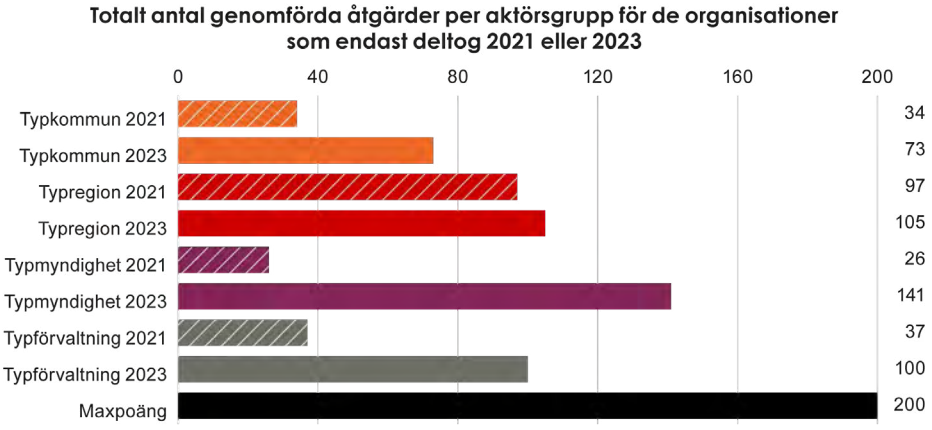


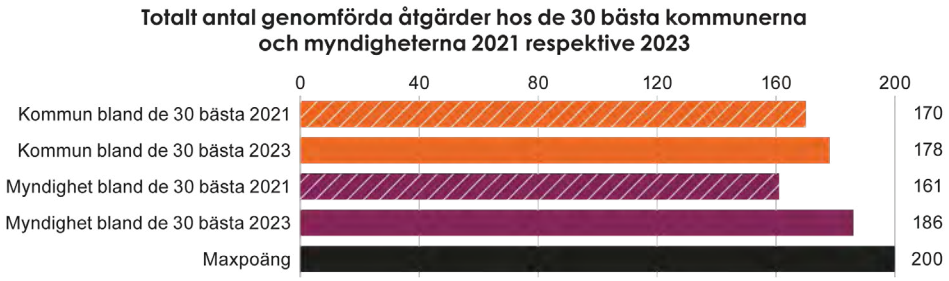

Diagram 9 jämfört med diagram 8 visar ett mycket intressant mönster. Samtliga organisationer som deltog 2021, men stod över 2023, hade 2021 färre antal införda åtgärder än typförvaltningen inom samtliga aktörsgrupper samma år. Med andra ord hade de organisationer som endast deltog 2021 svagare resultat

än andra organisationer i sina aktörsgrupper. Det är möjligt att de inte utvecklats så mycket sedan 2021 och därför inte såg det värdefullt att delta även 2023.

Samma mönster framträder för de organisationer som endast deltagit 2023, de hade färre antal införda åtgärder än typförvaltningen inom samtliga aktörsgrupper som deltagit både 2021 och 2023. De kan ha gjort bedömningen att de inte var mogna nog att delta 2021. Det skulle även förklara varför de som bara deltagit 2023 har så mycket bättre resultat än de som enbart deltog 2021.

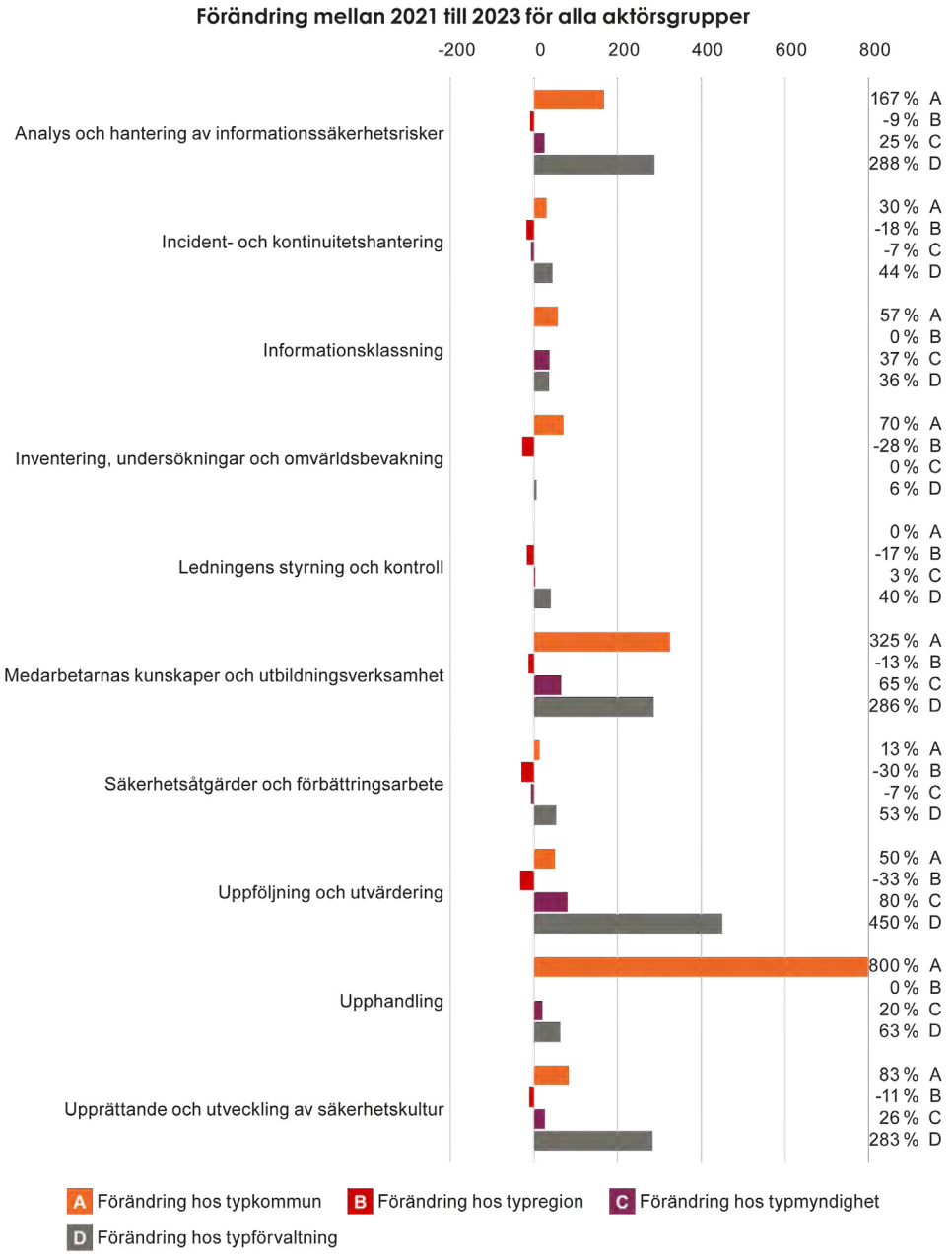
Sammantaget visar diagrammet att både de organisationer som endast deltagit 2021 och 2023 har dragit ner resultatet för alla aktörsgrupper, men att de som endast deltog 2021 gjorde det i större utsträckning en de som endast deltog 2023. 89 organisationer deltog enbart 2021, och 80 organisationer enbart 2023, vilket är relativt likvärdigt och därför inte torde påverka utfallet.

**Diagram 10.** Infosäkkollen diagram 10




I diagram 8 ovan påtalade MSB att den generella nivån har höjts avsevärt bland kommunerna, men här syns att även högstanivån har förbättrats med 4,7 procent. En ännu större förbättring, 15,5 procent, ses hos myndigheterna.

**Diagram 11.** Infosäkkollen diagram 11




Ovan diagram ska utläsas med försiktighet. Stora procentuella förbättringar beror på ett särdeles svagt resultat 2021 och framstår som ännu större inom de arbetsområden som har relativt få mätbara åtgärder. Typexemplet är den 800 procentiga förbättringen hos en typkommun gällande upphandling, där en typkommun gått från en genomförd åtgärd 2021 till nio genomförda åtgärder 2023. Vidare motsvarar 9 utav 16 genomförda åtgärder på arbetsområdet ett resultat på 56,3 procent, och typkommunen har inte heller genomfört sådana åtgärder som behövs inom ramen för nivå 1 gällande Upphandling 2023.

Typregionens resultat har försämrats på alla utom två arbetsområden mellan mättillfällena. Som tidigare nämnt förklaras detta av att deltagandet inom den aktörsgruppen nästan fördubblats mellan mättillfällena och de regioner som inte deltog 2021, men som deltagit 2023, har dragit ner det generella resultatet.

Den största procentuella förbättringen syns hos typkommunen, särskilt kopplat till Upphandling samt Medarbetarnas kunskaper och utbildningsverksamhet. Ökningen är dock utifrån ytterst få genomförda åtgärder 2021.

Noterbart är en 80 procentig förbättring bland myndigheter gällande antalet genomförda åtgärder på arbetsområdet för Uppföljning och utvärdering.

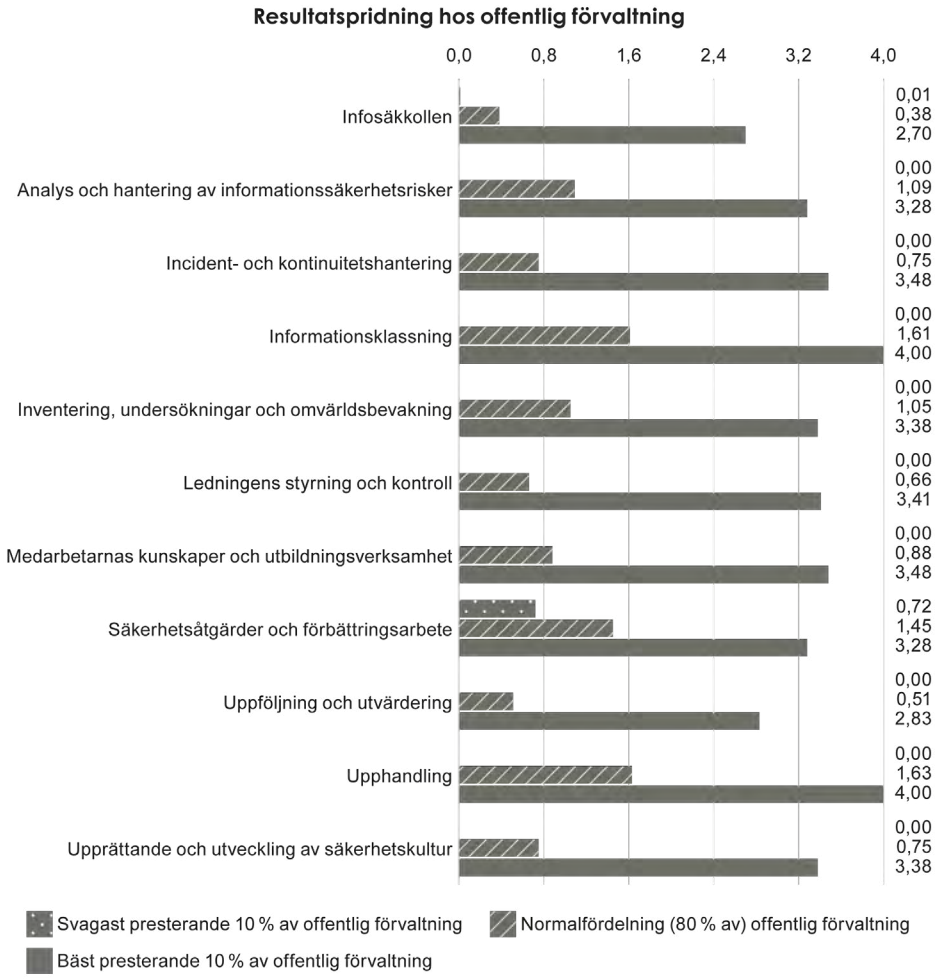
De arbetsområden där minst skillnad mellan mättillfällena syns, Informationsklassning, Ledningens styrning och kontroll, samt Incident- och kontinuitetshantering, antyder att dessa arbetsområden har haft lägst prioritet i förbättringsarbetet.

Uppföljning och utvärdering är det arbetsområde där flest nya antal åtgärder genomförts mellan mättillfällena, vilket får ses som positivt särskilt som det arbetsområdet var ett av de två arbetsområden där resultaten var svagast 2021.

### 4.1.5 Resultatspridning

Här återges det samlade resultatet för en organisation på ett sätt som möjliggör att jämföra resultatspridningen mellan organisationer. Här ingår också de resultat som uppnåtts för olika arbetsområden, samt den poängsumma som ligger till grund för resultatberäkningen.

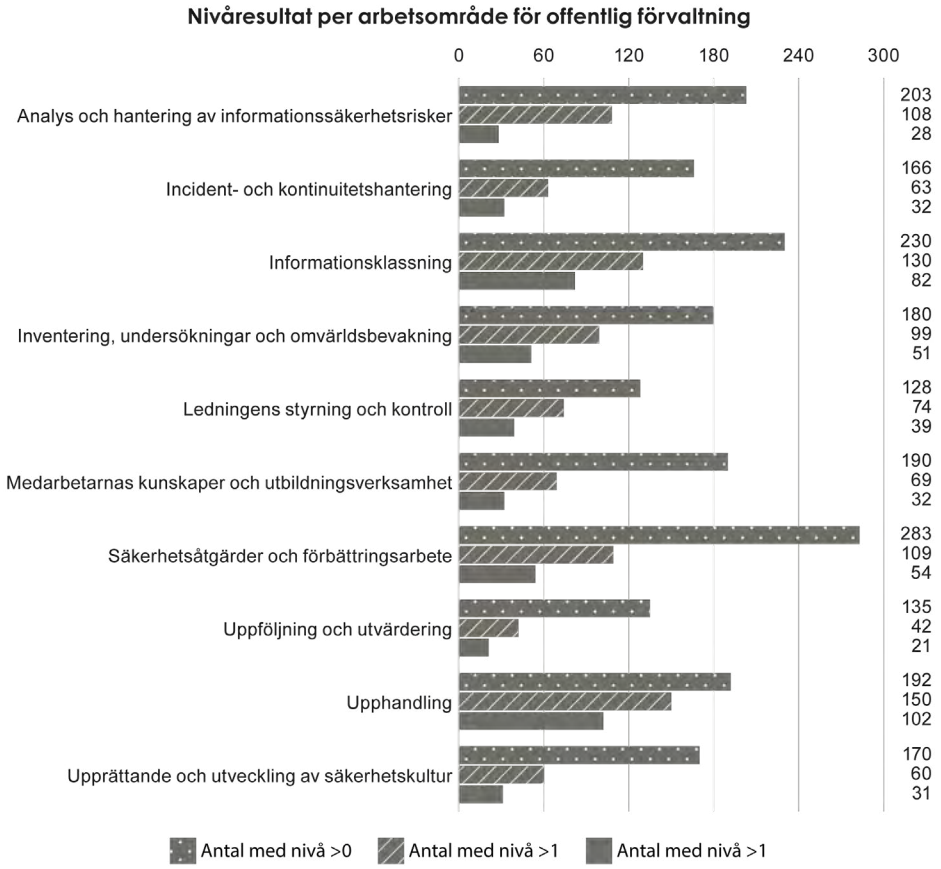
**Diagram 12.** Infosäkkollen diagram 12




Diagrammet tydliggör hur mycket de 10 procent bäst presenterande organisationerna drar upp resultatet för en organisationen inom sin aktörsgrupp. Det är en kraftig skillnad mellan resultatet för de 10 procent bästa visavi de 80 procent som här återges som normalfördelning.

Det enda arbetsområdet där de svagaste 10 procenten av offentlig förvaltning ens uppnått ett egentligt resultat är inom Säkerhetsåtgärder och förbättringsarbete. Mer information om potentiella förklaringar för att just det arbetsområdet har ett relativt bra resultat återfinns i kapitel 5 om It-säkkollen.

**Diagram 13.** Infosäkkollen diagram 13




I diagrammet här visas hur många organisationer som uppnått Infosäkkollens fyra nivåer. Arbetsområdet Säkerhetsåtgärder och förbättringsarbete är där offentlig förvaltning lyckats bäst. Inom detta arbetsområde har hela 283 organisationer, motsvarande 97,3 procent av helheten, klarat modellens krav för att uppnå nivå 1.

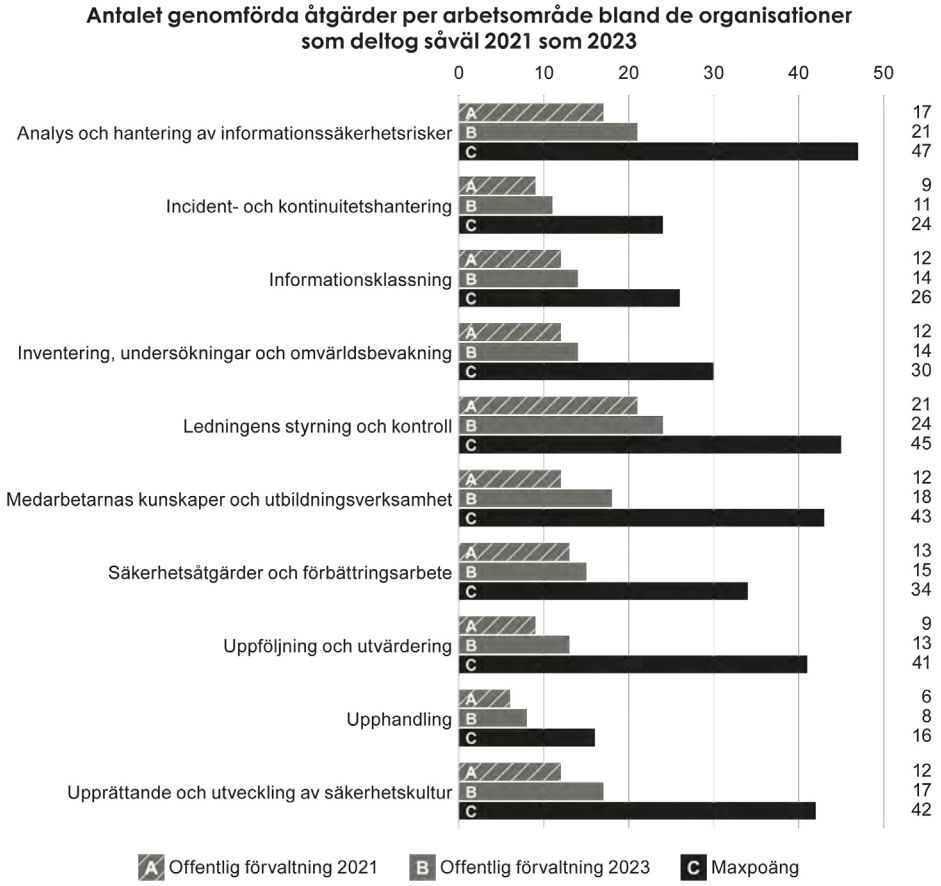
Det svagaste resultatet finns inom arbetsområdet för Ledningens styrning och kontroll där 128 organisationer, eller 43,9 procent av helheten, har klarat av nivå 1. Arbetsområdet för Uppföljning och utvärdering är där minst antal organisationer uppnått nivå 2 eller högre, samt nivå 3 eller 4. Brist på uppföljning och utvärdering riskerar att innebära att implementerade åtgärder inte uppnår förväntad effekt.

Upphandling är det arbetsområde där flest organisationer uppnår bra resultat på modellens högre nivåer. Detta trots att bara knappt två tredjedelar av organisationerna når nivå 1. Sammantaget tyder detta på att detta är ett arbetsområde som antingen inte prioriteras särskilt mycket alls, eller prioriteras mest av alla arbetsområden hela vägen i kedjan. 102 organisationer, 51,1 procent, når nivå 3 eller 4 i modellen för arbetsområdet Upphandling.

### 4.1.6 Förändring i resultatet från 2021 till 2023

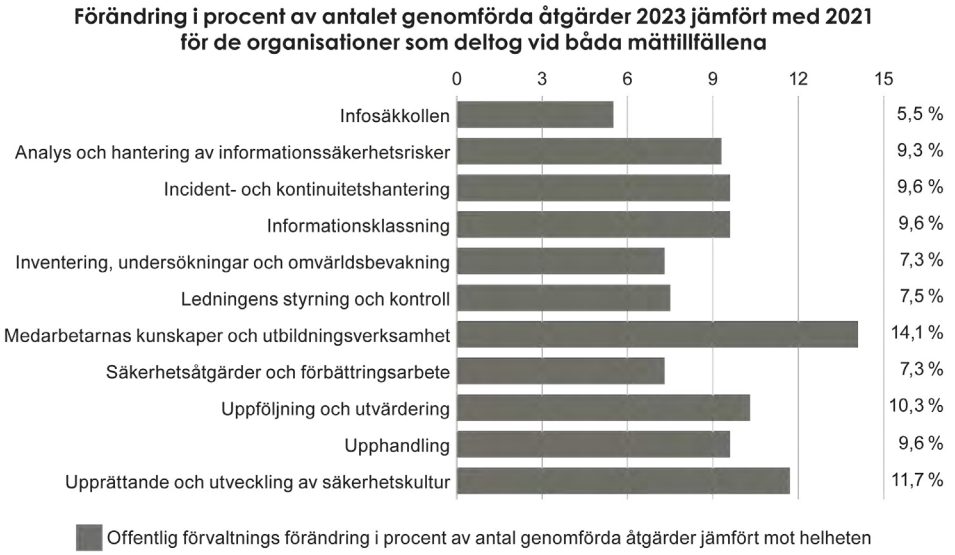
211 organisationer deltog såväl 2021 som 2023. 89 organisationer deltog enbart 2021, och motsvarande antal för 2023 var 80 organisationer. Dessa är särskilt intressanta att studera för att se resultatförändring mellan de två mättillfällena.

**Diagram 14.** Infosäkkollen diagram 14




Ett genomsnitt av resultatet för genomförda åtgärder för samtliga organisationer som deltagit vid båda mättillfällena visar på en tydlig förbättring inom samtliga arbetsområden.

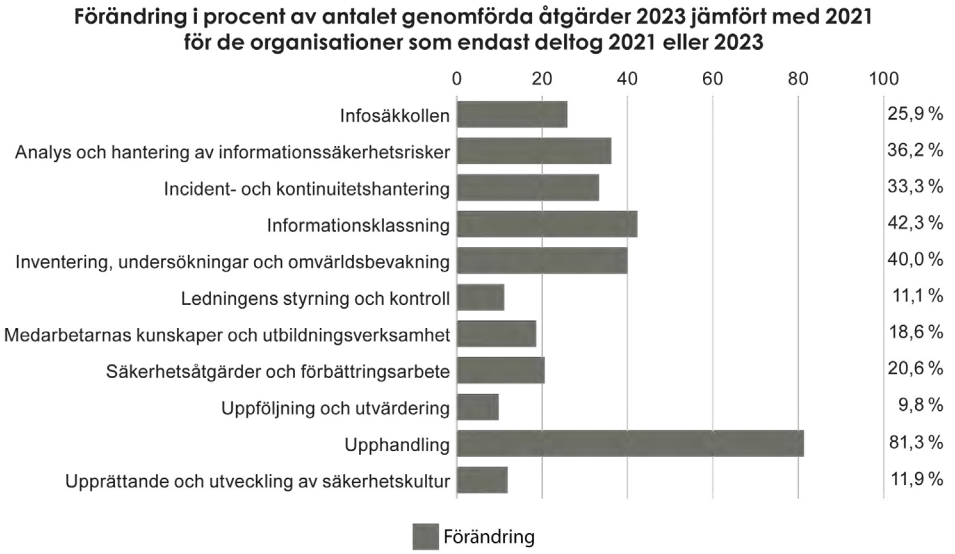
**Diagram 15.** Infosäkkollen diagram 15




Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 5,5 procentig resultatförbättring av hela Infosäkkollen. Den genomsnittliga förändringen per arbetsområde är 9,6 procent. Sammantaget berättar detta att störst förbättring uppnåtts inom de arbetsområden där minst antal åtgärder mäts.

Utav de 211 organisationer som deltog både 2021 och 2023 har den genomsnittliga totalpoängen ökat från 77,8 år 2021 till 96,8 år 2023. Det motsvarar en förbättring på 24,4 procent. Detta har bidragit till en resultatförbättring för hela Infosäkkollen.

**Diagram 16.** Infosäkkollen diagram 16




Här jämförs de organisationer som enbart deltog 2021 respektive 2023 och mätt i antalet genomförda åtgärder motsvarar utvecklingen en 26 procentig resultatförbättring av hela Infosäkkollen. Långt mer än de 5,5 procent som noterades för organisationer som deltagit vid båda mättillfällena. Den genomsnittliga förändringen per arbetsområden är 30,5 procent.

Utav de 89 respektive 80 organisationer som enbart deltog 2021 eller 2023 har den genomsnittliga totalpoängen ökat från 48,3 år 2021 till 80,0 år 2023. Det motsvarar en förbättring på 65,6 procent. Detta har bidragit till en resultatförbättring för hela Infosäkkollen.

Tidigare redovisades att en deltagande typförvaltning 2023 har genomfört 64,6 procent fler åtgärder än en typförvaltning 2021. Kombinerat med föregående stycke kan MSB konstatera att stora delar av förändringen i den sammantagna ökningen beror på den dryga tredjedelen av organisationer som skiljer sig mellan mättillfällena. Det vill säga att de svagaste organisationerna från 2021 inte deltagit 2023, och att de organisationer som deltagit 2023 är bättre än motsvarande grupp 2021.

### 4.1.7 Enkätundersökning

Under perioden 15-28 november 2023 genomförde MSB en enkätundersökning som syftade till att öka MSB:s förståelse av organisationernas behov och myndighetens vidareutvecklingsarbete kopplat till Infosäkkollen, samt viss fördjupning kopplat till resultatet från undersökningen. Enkäten skickades till de organisationer som inrapporterade Infosäkkollen 2023.[21] Undersökningen var frivillig och frågorna tog ungefär tio minuter att besvara. Ingen fråga var obligatorisk att besvara, varför svarsfrekvensen per fråga varierar. Svaren var anonyma och presenteras på aggregerad nivå nedan.

Totalt svarade 174 organisationer, vilket motsvarar drygt 67 procent av svarsunderlaget. 81 kommuner (47 %), nio regioner (5 %) och 84 myndigheter (48 %) besvarade enkätundersökningen. De som besvarade hade uppgivit att de deltagit aktivt i organisationens genomförande av Infosäkkollen och respondenterna arbetar i roller såsom CISO, it-strateg, it-chef, säkerhetsskyddschef och så vidare.

På frågan om Infosäkkollen är värdefull för organisationens informations- och cybersäkerhetsarbete mottogs 160 svar. 29,4 procent svarade att det *stämmer helt*, 52,5 procent angav *stämmer väl*, 18,1 procent fyllde i *stämmer knappt*, medan ingen svarade *stämmer inte*. Att nästan 82 procent av respondenterna anser Infosäkkollen värdefull i sitt arbete får ses som ett gott betyg för modellen.

MSB frågade hur många organisationer som använder Infosäkkollen i sitt löpande informations- och cybersäkerhetsarbete och mottog 150 svar. 52 procent svarade *ja, varje år*, sex procent *ja, varje halvår*, två procent *ja, varje kvartal*, 0,7 procent *ja, tertialt*, medan 39,3 procent uppgav *nej*. MSB har fått återkoppling i olika sammanhang av många organisationer att de använder Infosäkkollen oftare än i samband med genomförandet vartannat år, och det är slående att nästan 61 procent genomför Infosäkkollen i egen regi årsvis eller mer frekvent än så.

21. De organisationer som, enligt anvisad rutin, inrapporterade Infosäkkollen via MSB:s e-tjänsteportal fick enkätundersökningen utskickad. Vissa organisationer inkom med svaret på andra sätt och de exkluderades från undersökningen av GDPR-skäl.

På frågan om organisationen använder Infosäkkollen för att planera kommande åtgärder bevarades av 149 respondenter. 13,4 procent uppgav *stämmer helt*, 42,3 procent *stämmer väl*, 32,2 procent *stämmer knappt* och 12,1 procent *stämmer inte*. Att nästan två tredjedelar anger att de använder Infosäkkollen är ett gott betyg för verktyget.

Gällande i vilken utsträckning de arbetar med informations- och cybersäkerhet mottogs 162 svar där 36,4 procent uppgav heltid, 4,3 procent angav cirka 75 procent, 14,2 procent svarade halvtid och 45,1 procent angav cirka 25 procent. Bland kommunerna uppgav så många som 57,5 procent att de arbetar med informations- och cybersäkerhet cirka 25 procent av sin arbetstid. Det är viktigt i sammanhanget att påpeka att frågan var personligt ställd och organisationens respondent kan ha kollegor som arbetar med frågorna i större utsträckning än respondenten. Det är dock en indikator på hur prioriterat arbetet är, särskilt som den stora majoriteten av respondenter har roller som direkt kopplar mot informations- och cybersäkerhet.

MSB undersökte om samma kollegor var ansvariga för organisationens informations- och cybersäkerhetsarbete som för två år sedan. Totalt mottogs 150 svar, där 22 procent angav *ja, alla medarbetare är kvar*, 32,7 procent *ja, de flesta medarbetare har varit densamma*, 29,3 procent *nej, vi har haft viss personalomsättning*, och 16 procent *nej, vi har haft omfattande personalomsättning*. Myndigheterna har haft mindre personalomsättning än kommuner och regioner. Svaren är svårtolkade då MSB saknar data på ”normal” personalomsättning inom branschen och tidsspannet, men att drygt 45 procent anger viss eller omfattande personalomsättning under en tvåårsperiod är noterbart.

Respondenterna fick ta ställning till om deras organisation har den personal som krävs för att förbättra informations- och cybersäkerhetsarbetet. De 147 svaren fördelades på så vis att 3,4 procent uppgav *stämmer helt*, 28,6 procent *stämmer väl*, 47,6 procent *stämmer knappt*, och 20,4 procent *stämmer inte*. Det förekommer viss resultatspridning mellan aktörsgrupperna, exempelvis anger kommuner i mindre utsträckning än regioner och myndigheter att de saknar personal. På det hela taget anger således två tredjedelar (68 %) av respondenterna stämmer knappt eller stämmer inte.

MSB undersökte om respondenten ansåg att organisation har den kompetens som krävs för att förbättra informations- och cybersäkerhetsarbetet. Av de 148 svaren angav 10,1 procent *stämmer helt*, 55,4 procent *stämmer väl*, 27,7 procent *stämmer knappt* och 6,8 procent *stämmer inte*. Myndigheter och kommuners svar var relativt lika, men bland regionerna svarade hela 75 procent antingen stämmer knappt eller stämmer inte. Sammantaget uppgav 65,5 procent, nästan två tredjedelar, att organisationen besitter nödvändig kompetens.

139 respondenterna svarade på huruvida deras organisation har den budget som krävs för att förbättra informations- och cybersäkerhetsarbetet. 2,1 procent angav *stämmer helt*, 24,5 procent *stämmer väl*, 45,3 procent *stämmer knappt*, medan 28,1 procent svarade *stämmer inte*. Att nästan tre fjärdedelar uppger stämmer knappt eller stämmer inte är nedslående. Att så många som en dryg fjärdedel (28,1 %) svarar stämmer inte är ännu mer bekymrande. Faktum är att 41,3 procent av kommunerna svarade stämmer inte, vilket kan jämföras med 16,7 respektive 17,1 procent hos regioner och myndigheter.

På frågan om Infosäkkollens resultat presenterats för organisationens högsta ledning svarade 149 respondenter. 48,3 procent uppgav *ja*, 38,3 procent *nej* och 13,4 procent *vet ej*. MSB rekommenderar samtliga organisationer att föredra resultatet för ledningen före inrapportering. Att knappt hälften av respondenterna kan svara jakande på frågeställningen indikerar att ledningen antingen inte velat informera sig om resultatet, alternativt att de som arbetat med Infosäkkollen bedömt att ledningen inte skulle vara intresserad av en föredragning.

MSB frågade om respondenten anser att organisationens högsta ledning har det engagemang som krävs för att förbättra informations- och cybersäkerhetsarbetet. Totalt mottogs 143 svar, där 15,4 procent angav *stämmer helt*, 34,3 procent *stämmer väl*, 41,2 procent *stämmer knappt* och 9,1 procent *stämmer inte*. Resultatspridningen mellan aktörsgrupperna var dock stor. Enligt respondenterna visar myndighetsledningarna betydligt mer engagemang, där 62,5 procent svarade stämmer helt eller stämmer väl. Bland regionerna uppgav 85,7 procent stämmer knappt eller stämmer inte. För kommunerna svarade 60,9 procent stämmer knappt eller stämmer inte. På det hela taget är det noterbart att drygt hälften av respondenterna (50,3 %) angett stämmer knappt eller stämmer inte.

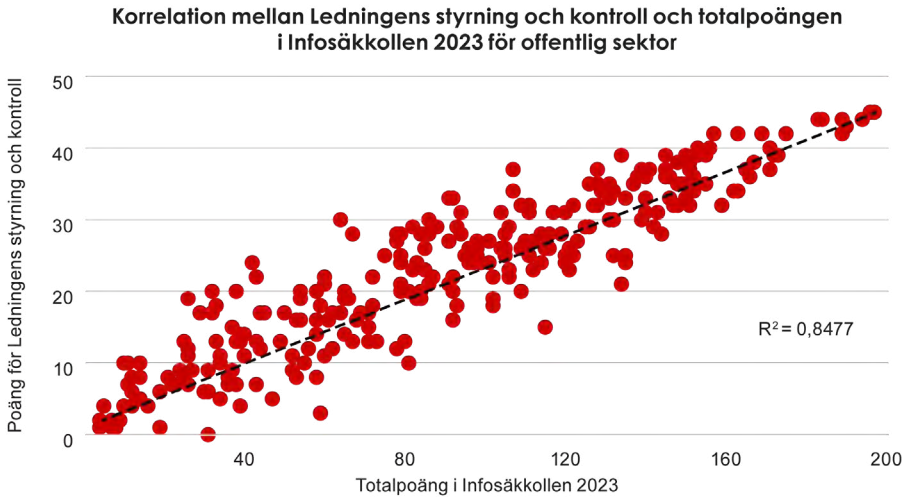
MSB undersökte i enkätundersökningen vad de huvudsakliga hindren för förbättringsarbetet består av. De flesta respondenterna uppgav resursbrist och avsaknad av engagemang från ledningen som de huvudsakliga orsakerna. En respondent svarade ”*att bygga ett systematiskt informationssäkerhetsarbete är omfattande och kräver långsiktighet och tid, samt förändringsledning från ledningen, vilket det behövs mer kompetens och medvetenhet kring.*”

Slutligen ställde MSB två frågor kring metodstödet. På frågan om organisationen använder MSB:s metodstöd som stöd för sitt säkerhetsarbete mottogs 143 svar där 16,8 procent uppgav *stämmer helt*, 48,9 procent *stämmer väl*, 23,8 procent *stämmer knappt* och 10,5 procent *stämmer inte*. För frågan om huruvida organisationen har de resurser som behövs för att tillgodogöra sig MSB:s metodstöd inkom 145 svar. Där uppgav 8,3 procent *stämmer helt*, 41,4 procent *stämmer väl*, 37,2 procent *stämmer knappt* och 13,1 procent *stämmer inte*. Nästa två tredjedelar svarade således att de nyttjar metodstödet, medan ungefär hälften svarar samtidigt att de har resurserna för att tillgodogöra sig detsamma. Sammantaget tyder det på att metodstödet uppskattas och hade använts mer förutsatt att organisationerna hade haft möjlighet att använda sig mer av metodstödet.

### 4.1.8 Ledningens styrning och kontroll

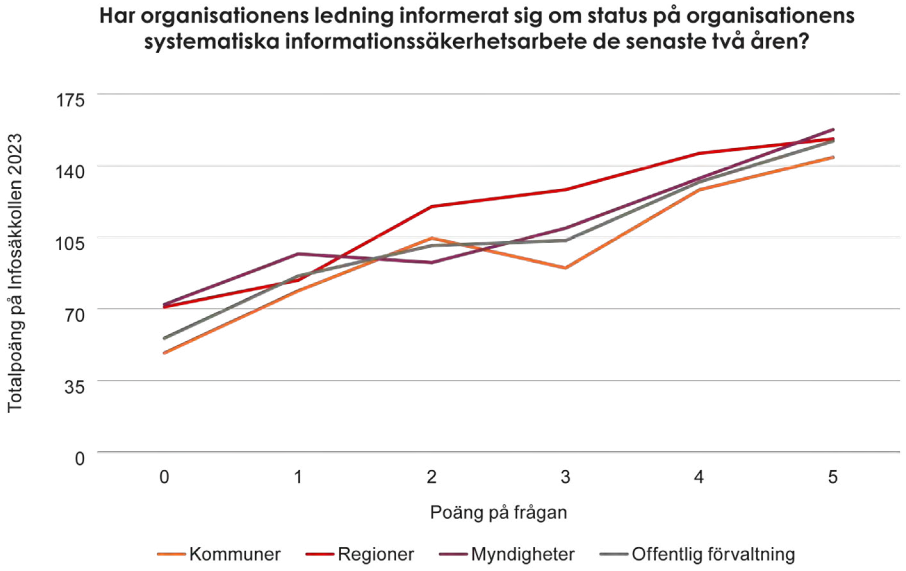
Infosäkkollen mäter resultatet på tio arbetsområden. Ett särdeles viktigt och likaledes det arbetsområde där minst antal organisationer klarade nivå 1 i undersökningen 2023 är Ledningens styrning och kontroll. Ett lyckosamt informations- och cybersäkerhetsarbete bedrivs systematiskt och riskbaserat utifrån allriskperspektivet. Organisationsledningen behöver sätta tydliga mål och förväntningar för säkerhetsarbetet, regelbundet informera sig om förbättringsarbetet, samt kommunicera vikten av säkerhetsarbetet.

**Diagram 17.** Infosäkkollen diagram 17




Diagrammet ovan påvisar en stark korrelation mellan ett bra resultat för arbetsområdet Ledningens styrning och kontroll och ett bra resultat för hela Infosäkkollen 2023.[22] Även om korrelation inte är samma sak som kausalitet kan det i sammanhanget vara rimligt att anta att ett ökat engagemang från organisationsledningar, och därmed ett bättre resultat inom arbetsområdet, även kan antas leda till positiva effekter på andra arbetsområden. Med andra ord, en engagerad organisationsledning kan göra stor skillnad för informations- och cybersäkerhetsarbetet.

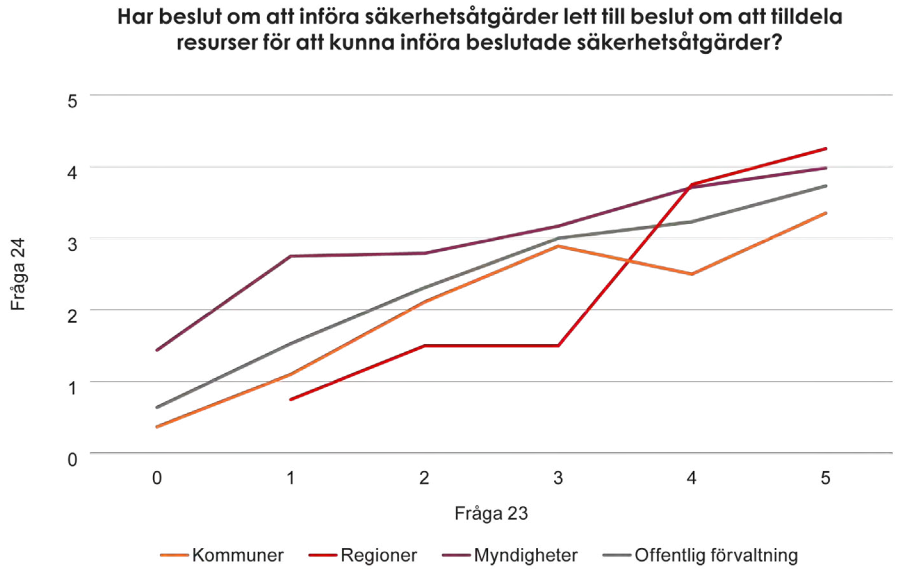
**Diagram 18.** Infosäkkollen diagram 18




Fråga 15 i Infosäkkollen handlar om huruvida organisationsledningen informerat sig om säkerhetsarbetet och poängfördelning sker utefter hur många åtgärder som genomförts för att informera sig. I diagrammet syns en tydlig koppling mellan att organisationsledningen informerat sig och det totala antalet poäng för hela Infosäkkollen.

22. Korrelationskoefficienten ($R^2$) har ett värde mellan 1 och -1. 1 anger maximalt positivt samband och -1 anger maximalt negativt samband. Små variationer noterades även mellan aktörsgrupperna (kommuner $R^2 = 0,8263$, regioner $R^2 = 0,8791$ och myndigheter $R^2 = 0,8371$).

**Diagram 19.** Infosäkkollen diagram 19




Fråga 23 behandlar om organisationen, under de senaste två åren, fattat beslut om att införa, eller att inte införa, säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker. Fråga 24 undersöker om organisationen, under de senaste två åren, har beslutat om att tilldela resurser för att kunna införa beslutade säkerhetsåtgärder. När de jämförs med varandra framträder en bild av att det finns en kausalitet, nämligen att de organisationer vars beslutsfattare engagerat sig med informations- och cybersäkerhetsfrågor och beslutat om införande av säkerhetsåtgärder, där har också resurser tillförts för dess implementering.

I enkätundersökningen som genomfördes med de som rapporterade in Infosäkkollen 2023 svarade två tredjedelar att de inte har den personal som krävs för att fullt ut implementera förbättringsarbetet. Omkring tre femtedelar uppgav att de arbetar deltid eller mindre med informations- och cybersäkerhet.[23] Vidare uppgav nästan hälften viss eller omfattande personalomsättning under en tvåårsperiod. Samtidigt uppgav nästan två tredjedelar att organisationen besitter nödvändig kompetens.

Att ungefär hälften av respondenterna haft en föredragning om resultatet från Infosäkkollen 2023 till sin organisationsledning indikerar att det är svårt att få gehör för frågorna. Ungefär hälften av respondenterna svarade också att högsta ledningen saknar det engagemang som krävs för att förbättra informations- och cybersäkerhetsarbetet.[24] Nästan tre fjärdedelar svarade att deras organisation inte har den budget som krävs för att förbättra informations- och cybersäkerhetsarbetet.

Sammantaget är den bild som framkommer att organisationsledningarna inte engagerar sig, prioriterar eller resurssätter förbättringsarbetet i den utsträckning som krävs. Förutom brister i budgetering syns avsaknaden av resurser även

23. Frågan var personligt ställd och organisationens respondent kan ha kollegor som arbetar med frågorna i större utsträckning än respondenten själv. Bland respondenterna från kommunerna uppgav så många som 58 procent att de arbetar med informations- och cybersäkerhet cirka 25 procent av sin arbetstid.

24. Bland regionerna uppgav 85 procent stämmer knappt eller stämmer inte på frågan om ledningens engagemang. För kommunerna svarade 61 procent stämmer knappt eller stämmer inte.

i personalbristen. Det positiva är att diagram 17, 18 och 19 påvisar att ledningens engagemang korrelerar med bättre resultat i Infosäkkollen, samt antyder ett orsakssamband mellan engagemang och ett bättre resultat. Dessutom angav respondenterna i enkätundersökningen i relativt stor utsträckning att relevant kompetens för förbättringsarbetet redan finns i organisationerna. Så om ledningens engagemang ökar och nödvändiga resurser tillförs borde förbättringar kunna uppnås. Ökade resurser kan även tänkas få bieffekten att det minskar personalomsättningen, vilket genom bibehållandet av institutionell kunskap även torde öka takten på förbättringsarbetet.

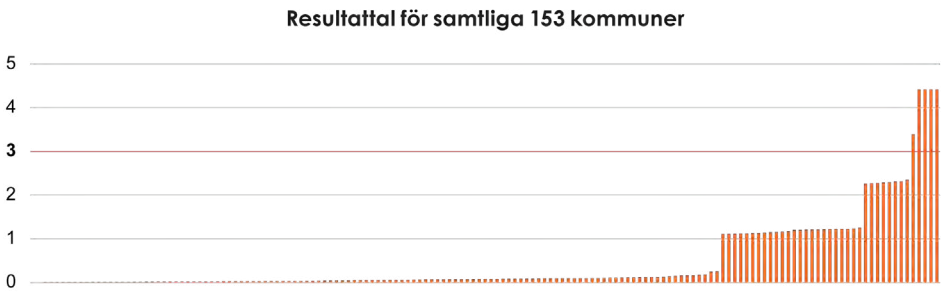
## 4.2 Kommuner

I det här avsnittet presenteras den bild som framkommit genom sammanställning av 153 inrapporterande kommuners resultat. Först redovisas en övergripande bild av läget bland kommunerna och därefter följer en mer detaljerad redogörelse för resultaten inom de tio olika arbetsområdena. Den detaljerade redogörelsen presenterar huvudsakligen vad benchmarken för alla de svarande kommunerna visar.

### 4.2.1 Resultattal

36 av alla deltagande kommuner uppnådde nivå 1 i modellen. En majoritet, 76,5 procent, uppnår inte nivå 1. Nivå 1 motsvarar de grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. För att uppnå nivå 1 i Infosäkkollen måste organisationer ha genomfört minst en åtgärd kopplat till varje av de 15 frågorna i Infosäkkollens första avsnitt.

**Diagram 20.** Infosäkkollen diagram 20



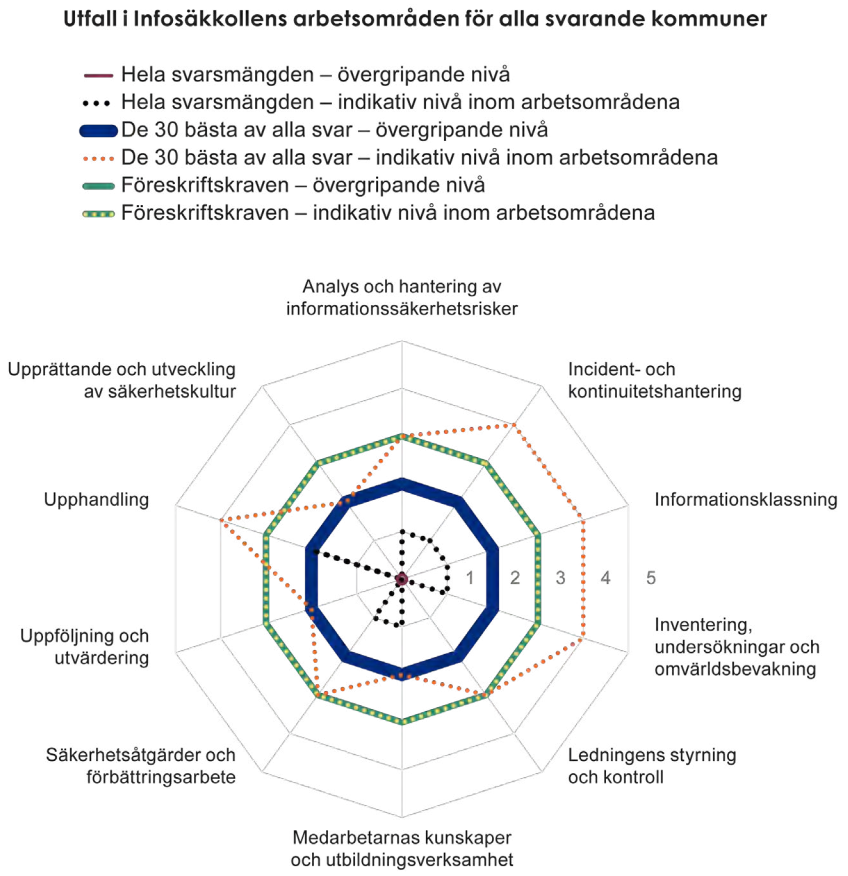

Den röda linjen i diagrammet motsvarar den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

23,5 procent av deltagande kommuner uppnådde nivå 1 eller mer, 7,8 procent uppnådde nivå 2 eller mer, och 2,6 procent uppnådde nivå 3 eller 4 i modellen.

### 4.2.2 Utfall per arbetsområde

Gruppen med de 30 bästa kommunerna uppnår modellens nivå 2, och den indikativa nivån når nivå 3 eller bättre i sju arbetsområden. Gruppen med alla svarande kommuner klarar inte att nå nivå 1, men når dock nivå 1 eller bättre på indikativ nivå inom sju arbetsområden.

**Diagram 21.** Infosäkkollen diagram 21

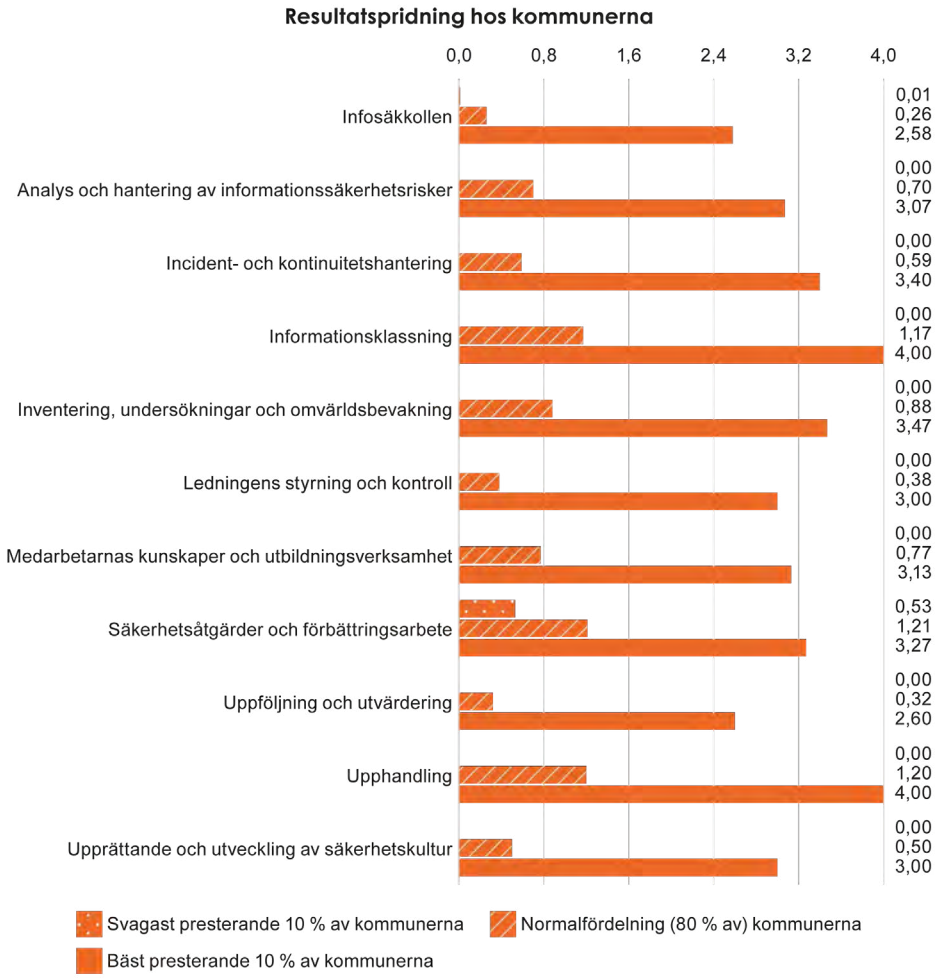



De arbetsområden där flest deltagande kommuner uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete, följt av Informationsklassning och därefter Medarbetarnas kunskaper och utbildningsverksamhet. Minst antal deltagande kommuner har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll, följt av Uppföljning och utvärdering samt Upprättande och utveckling av säkerhetskultur.

### 4.2.3 Resultatspridning

Diagrammet nedan tydliggör hur mycket de 10 procent bästa kommunerna drar upp resultatet för en typkommun i de redovisade diagrammen i kapitel 2. Det är en omfattande skillnad mellan resultatet för de 10 procent bästa kommunerna visavi de 80 procent av kommunerna som här motsvarar normalfördelningen.

**Diagram 22.** Infosäkkollen diagram 22



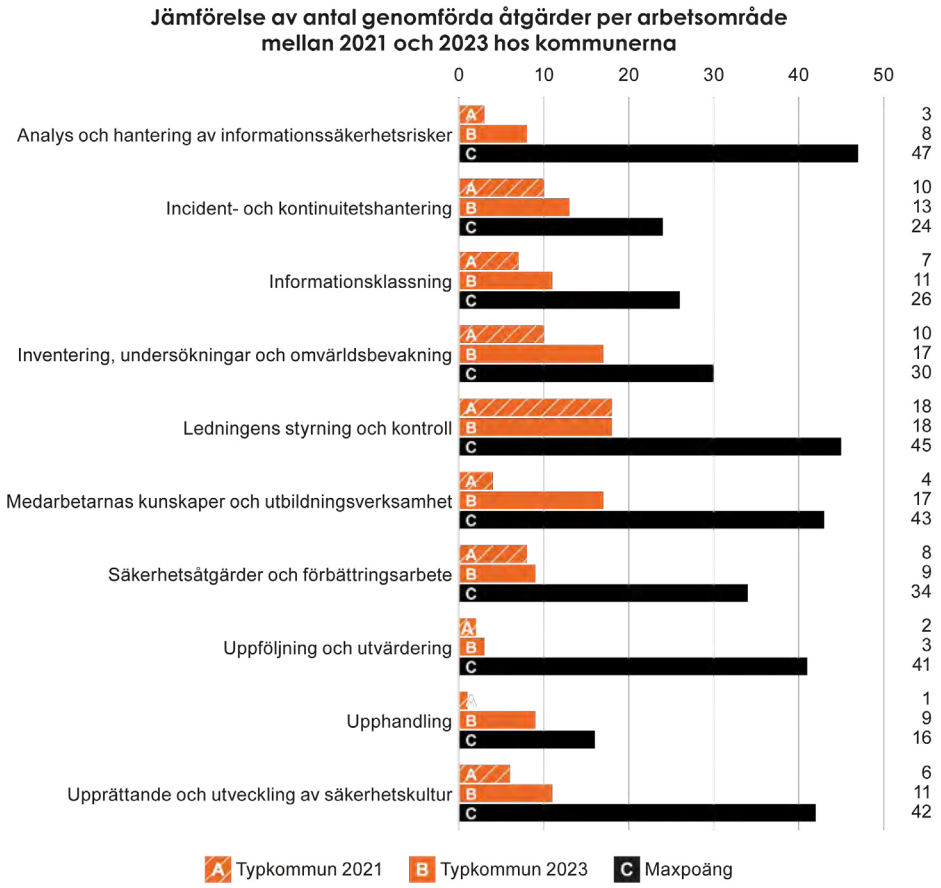

Det enda arbetsområdet där de svagaste 10 procenten av kommunerna ens uppnått ett egentligt resultat är inom Säkerhetsåtgärder och förbättringsarbete. De 10 bästa procenten av kommunerna har uppnått maxresultat i modellens arbetsområden för Informationsklassning och Upphandling.

För de 80 procent av kommunerna som återfinns i normalfördelningen är resultaten genomgående nedslående. På Infosäkkollen som helhet är inte denna grupp ens i närheten att nå nivå 1 (0,26). Inom de olika arbetsområden ser det ungefär lika dystert ut, med undantag av arbetsområdena för Informationsklassning, Säkerhetsåtgärder och förbättringsarbete, samt Upphandling där den normalfördelande gruppen når upp till nivå 1.

### 4.2.4 Resultatförändring mellan mättillfällena

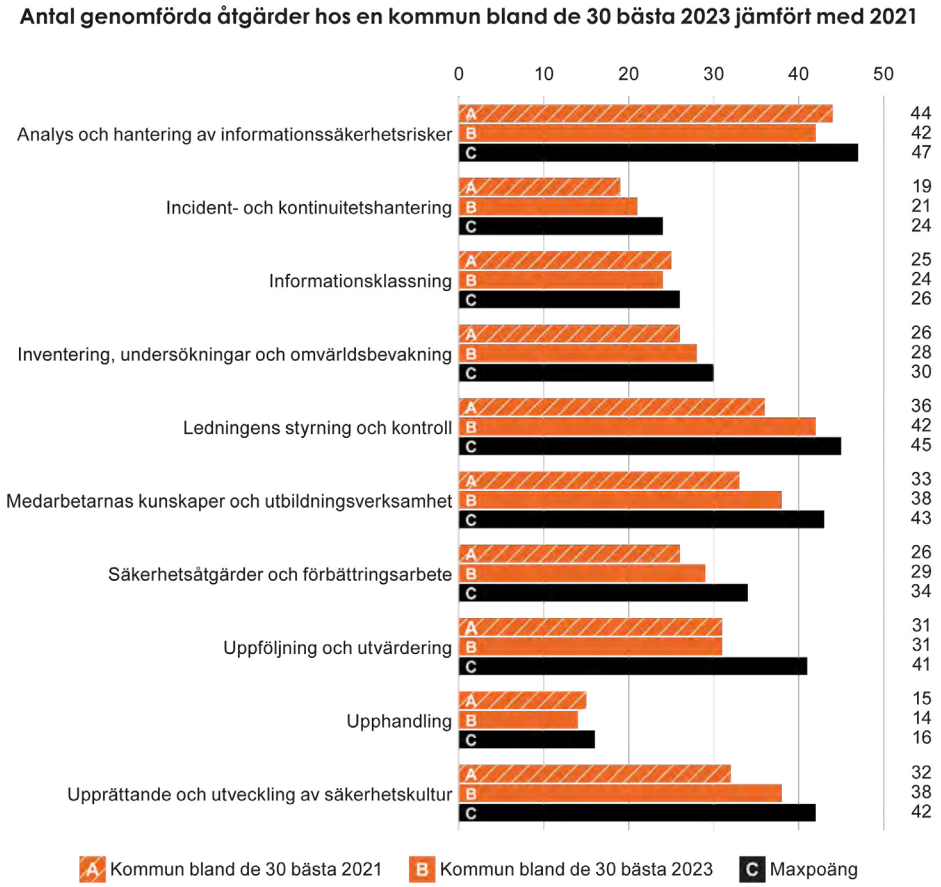
I detta avsnitt kommer resultatförändringen mellan 2021 och 2023 att redogöras. Vad det anbelangar kommunerna så har typkommunen tagit ett kliv framåt 2023 jämfört med resultatet 2021.

**Diagram 23.** Infosäkkollen diagram 23




En typkommun 2021 hade genomfört 69 åtgärder, medan samma typkommun 2023 hade genomfört 116 åtgärder. Detta utgör således en sammantagen ökning med 68,1 procent. Faktum är att samtliga arbetsområden utom ett har förbättrats, nämligen Ledningens styrning och kontroll, där resultatet är detsamma som 2021. Det är dock viktigt att betänka att en typkommun 2021 hade genomfört 69 av 348 (19,8 %) möjliga åtgärder, så det fanns god förbättringspotential.

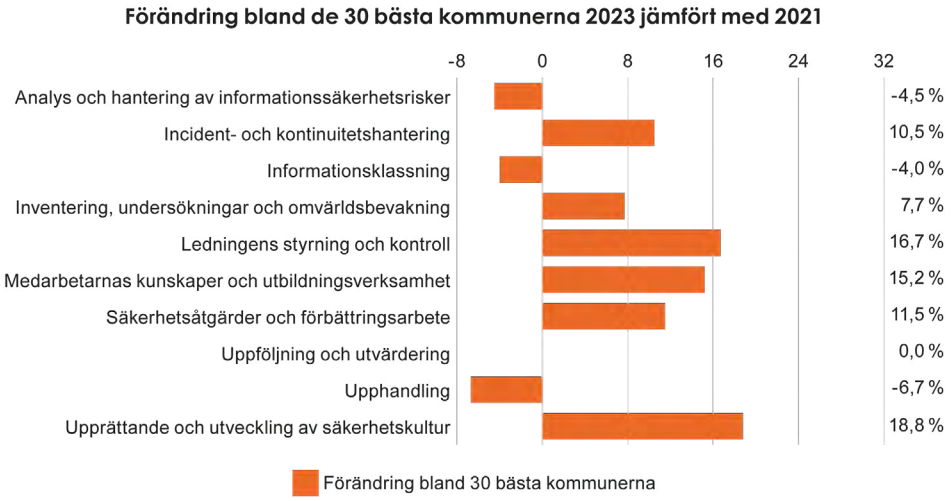
**Diagram 24.** Infosäkkollen diagram 24




En typkommun av de 30 bästa 2021 hade genomfört 287 åtgärder, medan samma aktör 2023 hade genomfört 307 åtgärder, en förbättring med 7 procent.

Sex arbetsområden visar på förbättring, tre på en försämring och Uppföljning och utvärdering får samma resultat.

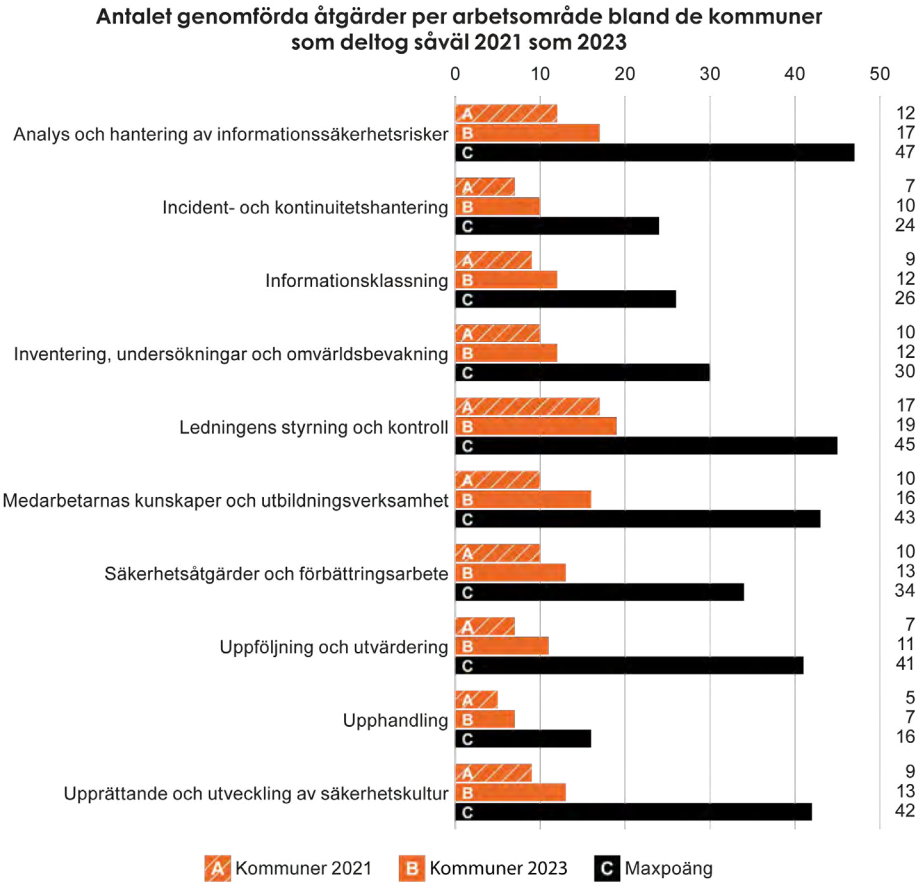
**Diagram 25.** Infosäkkollen diagram 25



Fem arbetsområden visar på en positiv förbättring på över tio procent, medan tre visar på en negativ utveckling. Även om Upphandling minskar 6,7 procent så är det faktiskt bara en åtgärds skillnad. Att det får så pass stor effekt beror på att Upphandling är det arbetsområdet där minst antal åtgärder mäts.

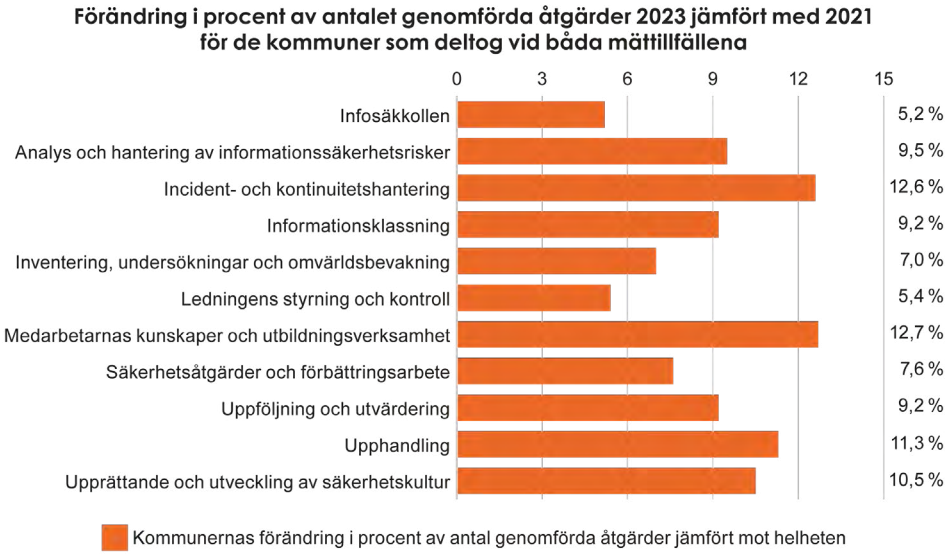
110 kommuner deltog såväl 2021 som 2023. Ett genomsnitt av resultatet för genomförda åtgärder för de kommuner som deltagit vid båda mättillfällena visar på en tydlig förbättring inom samtliga arbetsområden.

**Diagram 26.** Infosäkkollen diagram 26



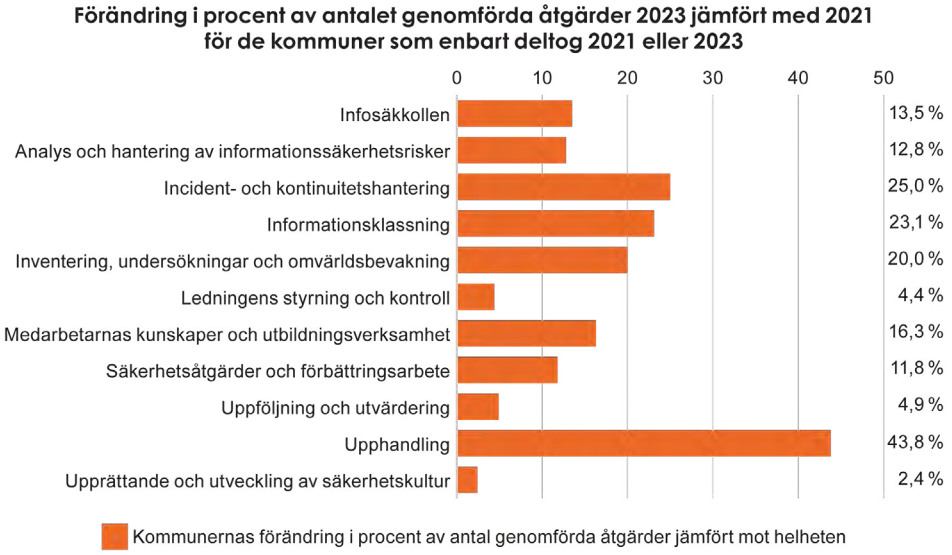

Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 5,2 procentig resultatförbättring av hela Infosäkkollen.

**Diagram 27.** Infosäkkollen diagram 27




Den genomsnittliga förändringen för alla arbetsområden är 9,5 procent. Det gör att kommunerna, om än marginellt, är den aktörsgrupp som har haft svagast förbättringsutveckling.

**Diagram 28.** Infosäkkollen diagram 28




Den genomsnittliga förändringen för alla arbetsområden är 16,4 procent mellan de som enbart deltog 2023 jämfört med de som enbart deltog 2021. Detta påvisar att många av de kommunerna med svagast resultat 2021 inte deltagit igen 2023, medan de som enbart deltagit 2023 fått bättre resultat visavi de som deltog 2021. Sammantaget har hela aktörsgruppens övergripande resultat påverkats positivt, även om informations- och cybersäkerhetsarbetet för hela aktörsgruppen kanske inte utvecklats i motsvarande takt.

### 4.2.5 Förutsättningar för samarbeten

De frågor där det finns en övervägande majoritet som inte fått några poäng finns det anledning för centrala myndigheter och andra stöttande organisationer på alla nivåer i samhället att se över sitt stöd. Detta rör främst fråga 14, 15, 17, 18, 26, 27, 30, 33, 34, 35, 36, 37, 39 och 40.[25]

- **Fråga 14**: Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 15**: Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 17**: Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 26**: Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?
- **Fråga 27**: Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30**: De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 33**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala delar?
- **Fråga 34**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat bedömning av följande centrala typer av skadeverkan och grad av skadeverkan?
- **Fråga 35**: De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala typer av sannolikhetsbedömning?
- **Fråga 36**: De två senaste åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat riskhantering med följande centrala delar?
- **Fråga 37**: De senaste två åren, har organisationens arbetssätt för att säkerställa informationssäkerhet vid upphandling omfattat följande centrala delar?
- **Fråga 39**: De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?
- **Fråga 40**: De senaste två åren, har organisationens ledning arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?

25. Jämfört med Infosäkkollen 2021 är det samma frågor med ett undantag. På fråga 31 har ett visst framsteg gjorts. Fråga 31: De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?

Det är dock viktigt att poängtera att det ytterst är varje organisation som är ansvarig för sitt informations- och cybersäkerhetsarbete, att det håller en adekvat nivå och följer de krav som ställs.

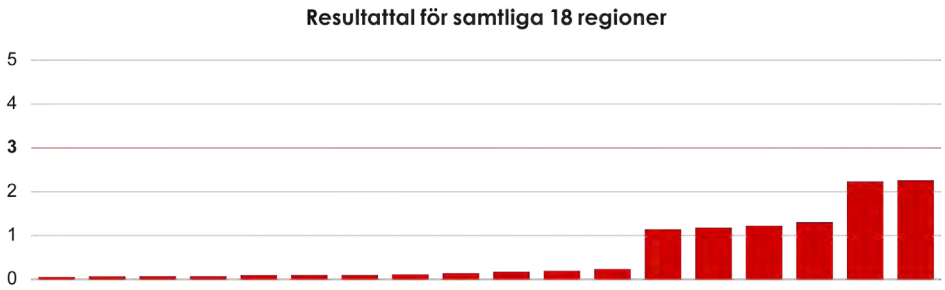
## 4.3 Regioner

I avsnittet nedan framförs sammanställningen av de 18 inrapporterande regionernas resultat. Det inleds med en övergripande bild av läget och därefter följer en mer detaljerad redogörelse för resultaten inom de tio olika arbetsområdena. Den detaljerade redogörelsen baseras i huvudsak på vad benchmarken för de svarande regionerna visar.

### 4.3.1 Resultattal

Sex regioner uppnår nivå 1 eller högre i modellen. 66,7 procent av alla deltagande regioner uppnår inte nivå 1 i modellen, vilket motsvarar de grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. För att uppnå nivå 1 i Infosäkkollen måste organisationer ha genomfört minst en åtgärd kopplat till varje av de 15 frågorna i Infosäkkollens första avsnitt.

**Diagram 29.** Infosäkkollen diagram 29



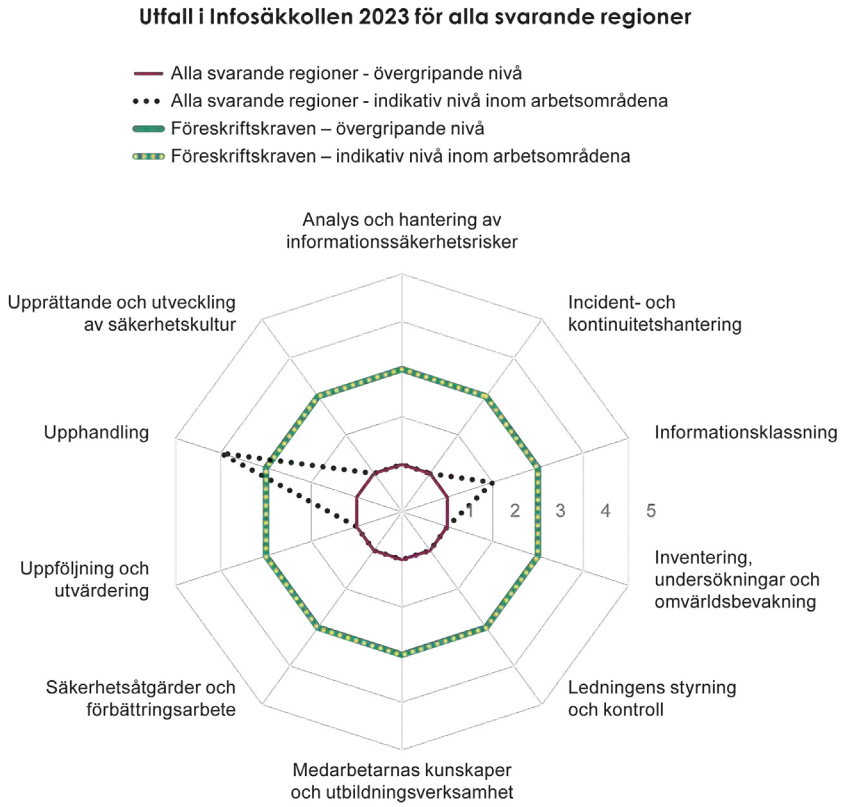

Den röda linjen i diagrammet motsvarar den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

33,3 procent av deltagande regioner uppnådde nivå 1 eller mer, 11,1 procent uppnådde nivå 2 eller mer, och ingen region uppnådde nivå 3 eller 4 i modellen.

### 4.3.2 Utfall per arbetsområde

Bland regionerna nås ett övergripande resultat på nivå 1. Inom arbetsområdet för Upphandling når den indikativa nivån maxresultatet på nivå 4.

**Diagram 30.** Infosäkkollen diagram 30



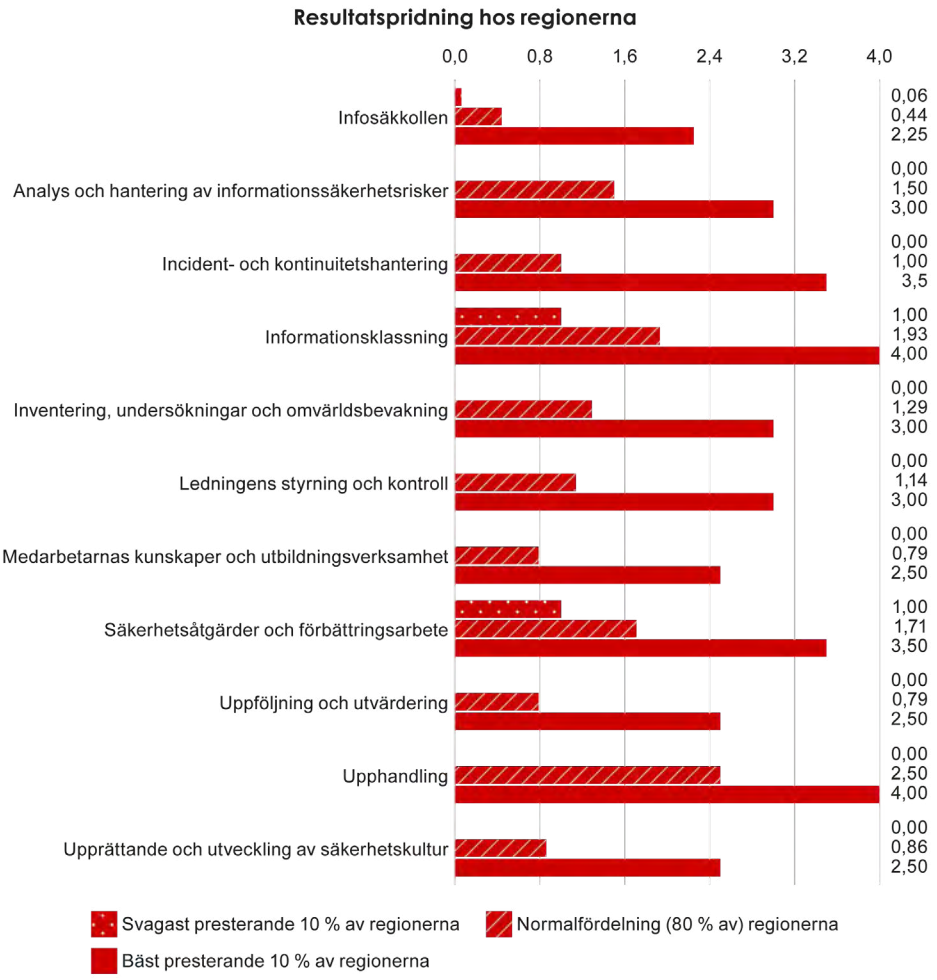

Bland samtliga deltagande regioner har nivå 1 uppnåtts inom arbetsområdena för Säkerhetsåtgärder och förbättringsarbete samt Informationsklassning. Regionerna presterar även bra inom Analys och hantering av informationssäkerhetsrisker och Upphandling.

Minst antal deltagande regioner har nått nivå 1 inom arbetsområdet för Incident- och kontinuitetshantering samt Inventering, undersökningar och omvärldsbevakning.

### 4.3.3 Resultatspridning

Diagrammet nedan förtydligar hur mycket de 10 procent bästa regionerna drar upp resultatet för typregionen i de redovisade diagrammen i kapitel 2. Det är en omfattande skillnad mellan resultatet för de 10 procent bästa regionerna jämfört med de 80 procent som här motsvarar normalfördelningen. Sammantaget är dock resultatspridningen hos regionerna mindre än hos kommunerna.

**Diagram 31.** Infosäkkollen diagram 31



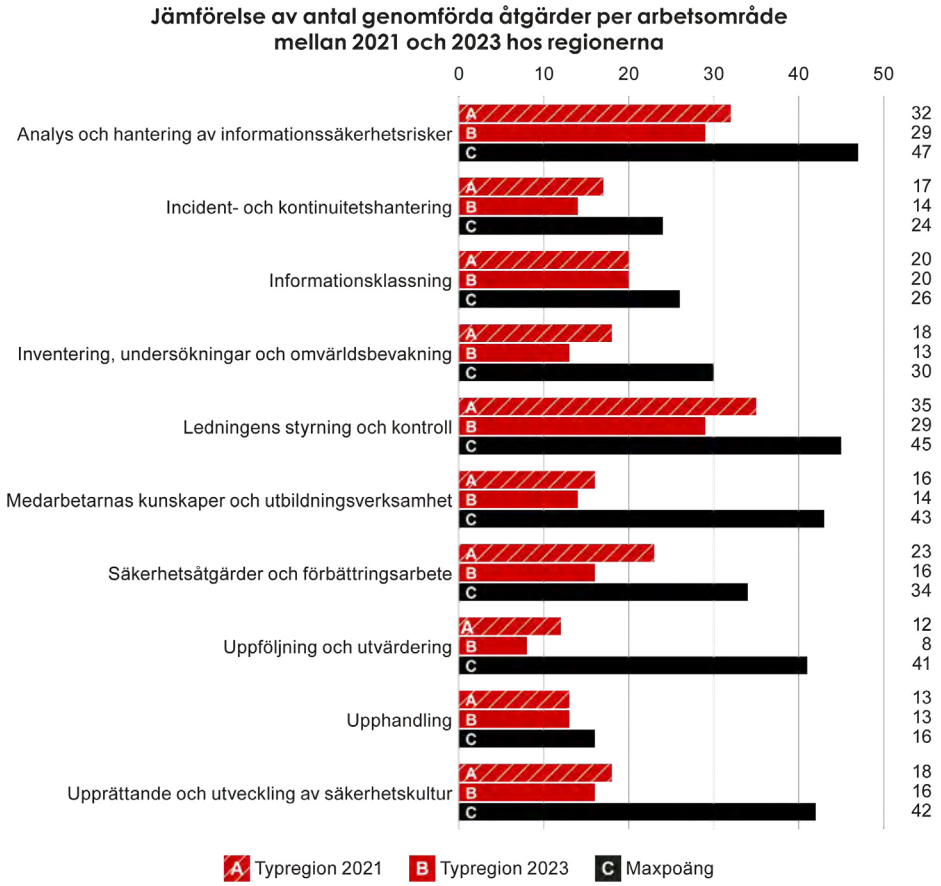

Det svagaste 10 procenten av regionerna har bara uppnått ett egentligt resultat inom två arbetsområden. De 10 procent bästa regionerna har uppnått maxresultat i modellens arbetsområden för Informationsklassning och Upphandling.

Av de 80 procent av regionerna som utgör normalfördelningen är resultaten varierande. På Infosäkkollen som helhet är inte denna grupp nära att nå nivå 1 utan får ett resultat på 0,44. Samtidigt har denna grupp uppnått nivå 1 eller bättre i åtta av modellens tio arbetsområden.

### 4.3.4 Resultatförändring mellan mättillfällena

I detta avsnitt redogörs för resultatförändringen mellan 2021 och 2023.
Hos regionerna har typregionen regredierat 2023 jämfört med resultatet 2021.

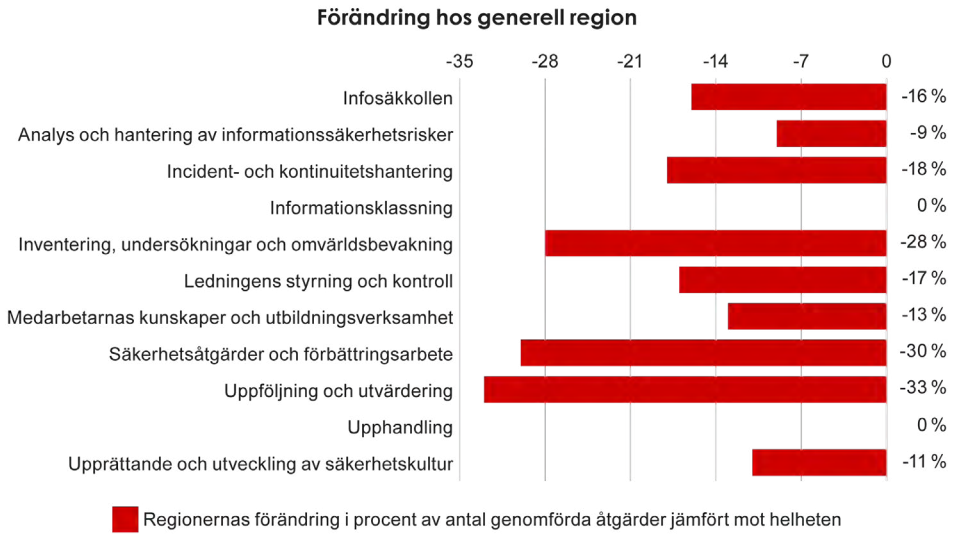
**Diagram 32.** Infosäkkollen diagram 32




En typregion hade genomfört 204 av 348 (58,6 %) möjliga åtgärder år 2021, medan samma typregion hade genomfört 172 åtgärder (49,4 %) år 2023. Det motsvarar en minskning med 18,6 procent.

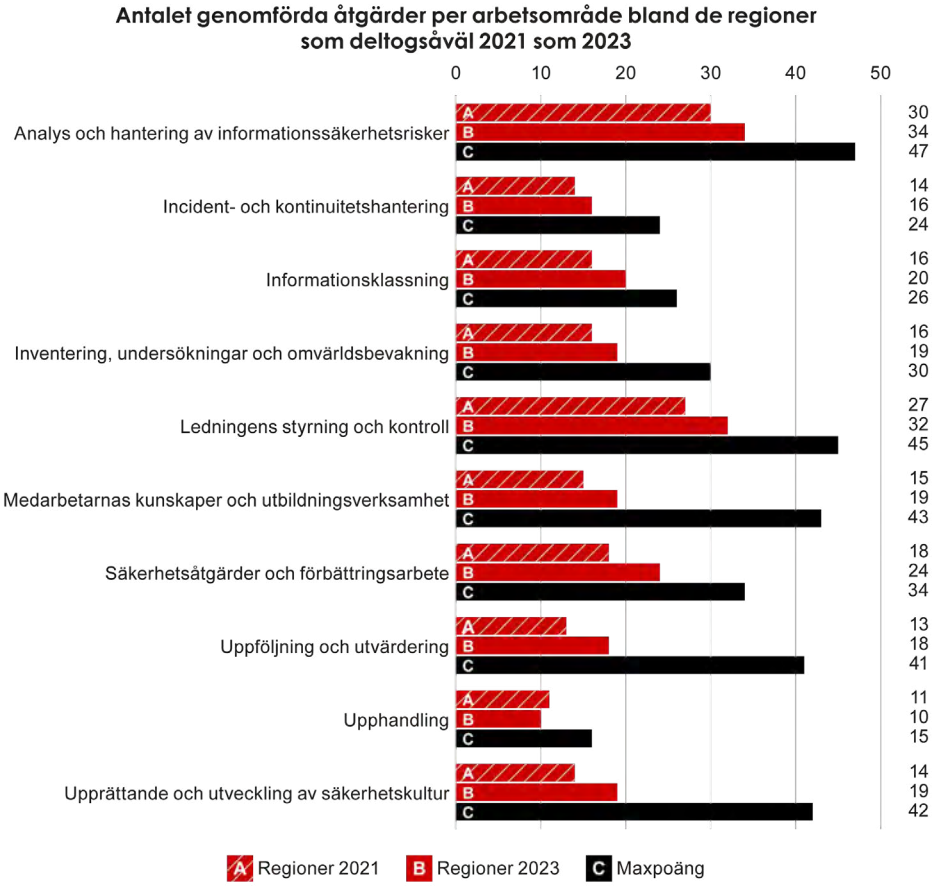
Samtliga arbetsområden utom två har försämrats, och där är resultaten likadana som 2021. Förändringen redogörs för i procent i diagrammet nedan.

**Diagram 33.** Infosäkkollen diagram 33



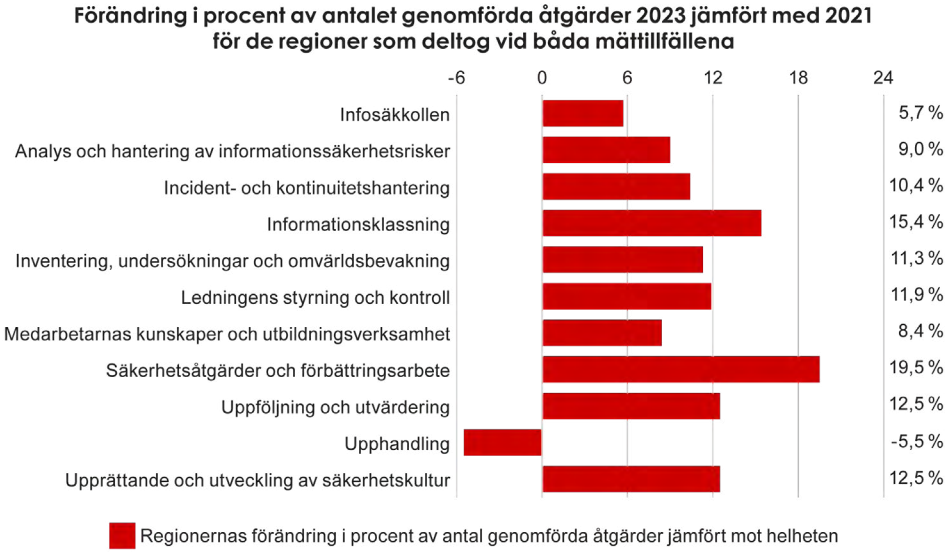

Åtta regioner deltog såväl 2021 som 2023. Ett genomsnitt av resultatet för genomförda åtgärder för de regioner som deltagit vid båda mättillfällena visar på förbättring inom alla utom ett arbetsområde.

**Diagram 34.** Infosäkkollen diagram 34



Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 5,7 procentig resultatförbättring av hela Infosäkkollen.

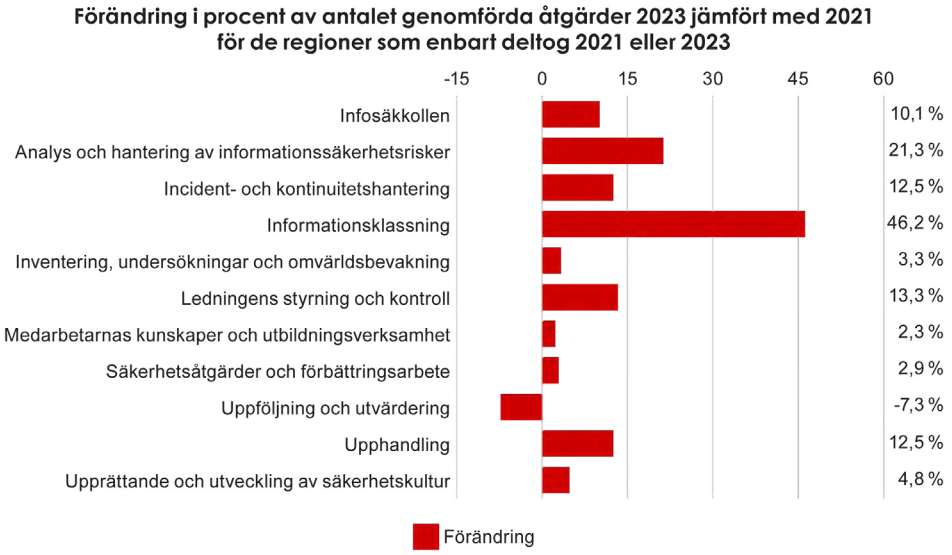
**Diagram 35.** Infosäkkollen diagram 35




Den genomsnittliga förändringen per arbetsområden är 10,5 procent. Det gör att regionerna, om än marginellt, är den aktörsgrupp som har haft bäst förbättringsutveckling.

Regionerna är den enda aktörsgrupp som haft en negativ utveckling inom ett arbetsområde, vilket förklaras av att deltagandet nästan fördubblats och de organisationer som enbart deltagit 2023 påverkat utfallet. Arbetsområdet för Upphandling är dock det arbetsområde där minsta minst antal åtgärder, 16 stycken, mäts, vilket gör att den procentuella förändringen ser större ut jämfört med andra arbetsområden. Det är förvisso en försämring, men endast med en åtgärd.

**Diagram 36.** Infosäkkollen diagram 36



Den genomsnittliga förändringen för alla arbetsområden är 11,2 procent mellan de regioner som enbart deltog 2023 jämfört med de som enbart deltog 2021. Detta påvisar att de regioner som hade ett svagare resultat 2021 inte deltog igen 2023, medan de som enbart deltagit 2023 fått bättre resultat visavi de som deltog 2021. Sammantaget har hela aktörsgruppens övergripande resultat påverkats positivt, även om informations- och cybersäkerhetsarbetet för hela aktörsgruppen kanske inte utvecklats i motsvarande takt.

### 4.3.5 Förutsättningar för samarbeten

De frågor där det finns en övervägande majoritet som inte fått några poäng finns det anledning för centrala myndigheter och andra stöttande organisationer på alla nivåer i samhället att se över sitt stöd. Detta rör främst fråga 17, 18, 27, 30 och 39.

- **Fråga 17**: Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 27**: Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30**: De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 39**: De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

Det är dock viktigt att poängtera att det ytterst är varje organisation som är ansvarig för sitt informations- och cybersäkerhetsarbete, att det håller en adekvat nivå och följer de krav som ställs.

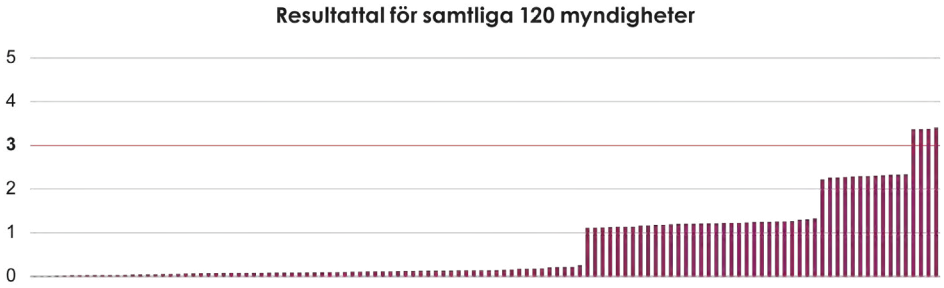
## 4.4 Myndigheter

I det här kapitlet redogörs för sammanställningen av resultatet för 120 inrapporterande myndigheter. Likt tidigare kapitel inleds det med en övergripande bild av läget och sedan följer en detaljerad redogörelse för resultaten utifrån de tio arbetsområdena. Den mer detaljerade redogörelsen baseras främst på vad benchmarken för de svarande myndigheterna visar.

### 4.4.1 Resultattal

47 myndigheter uppnår nivå 1 eller högre i Infosäkkollen 2023. 60,8 procent av alla deltagande myndigheter uppnår inte nivå 1 i modellen. Nivå 1 motsvarar de grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. För att uppnå nivå 1 i Infosäkkollen måste organisationer ha genomfört minst en åtgärd kopplat till varje av de 15 frågorna i Infosäkkollens första avsnitt.

**Diagram 37.** Infosäkkollen diagram 37



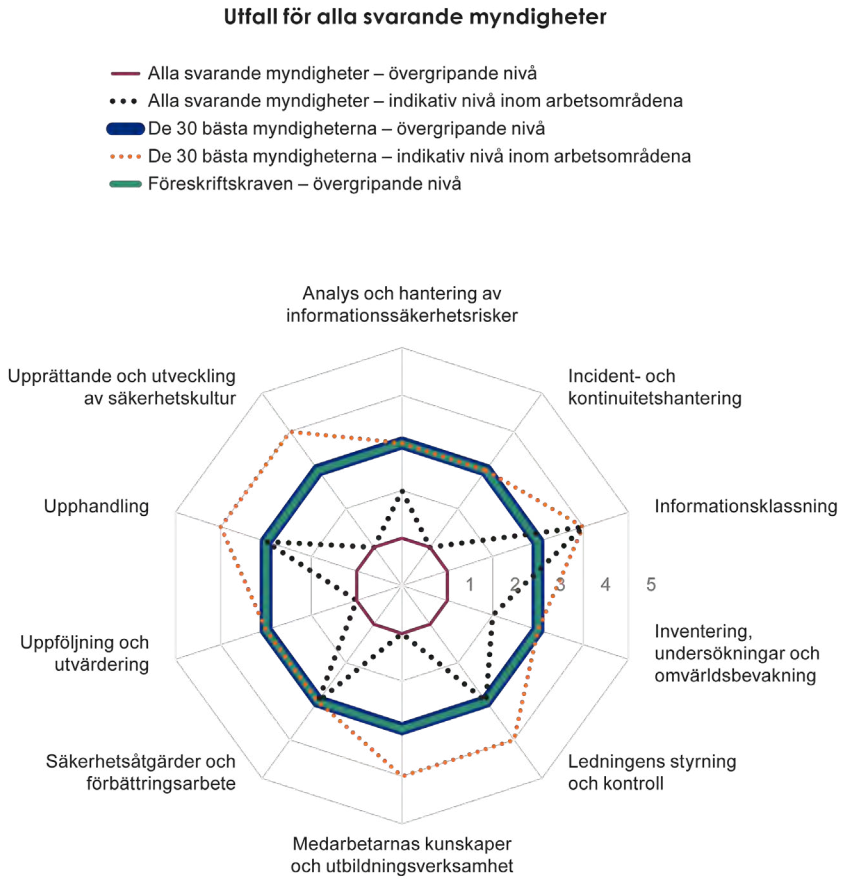

Den röda linjen i diagrammet motsvarar den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

39,2 procent av deltagande myndigheter uppnådde nivå 1 eller mer, 13,3 procent uppnådde nivå 2 eller mer, och 3,3 procent uppnådde nivå 3 eller 4 i modellen.

### 4.4.2 Utfall per arbetsområde

Myndigheterna uppnår samlat nivå 1 i modellen. På den indikativa nivån för myndigheterna så uppnås MSB:s föreskriftskrav inom fyra arbetsområden. De 30 bästa myndigheterna uppnår nivå 3, och därmed även MSB:s föreskriftskrav.

**Diagram 38.** Infosäkkollen diagram 38



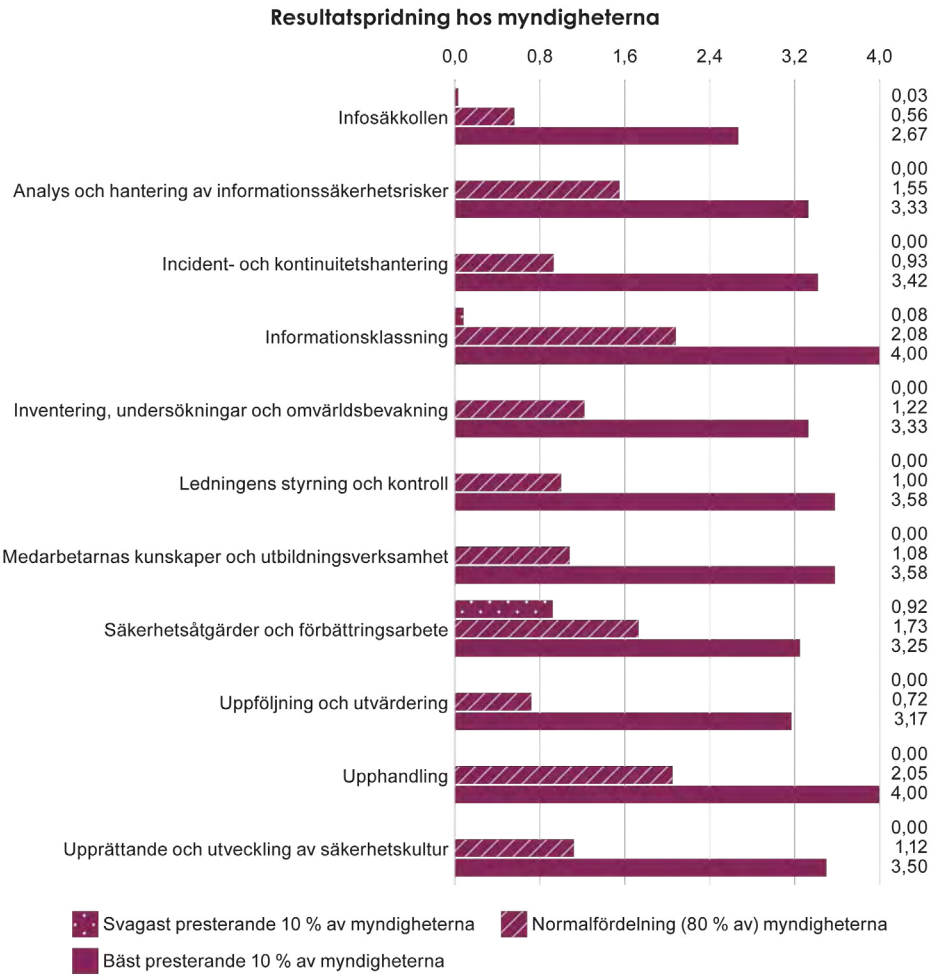

De arbetsområden där flest deltagande myndigheter uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete, följt av Informationsklassning och därefter Analys och hantering av informationssäkerhetsrisker.

Minst antal deltagande myndigheter har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll, följt av Uppföljning och utvärdering. Tredje svagaste arbetsområdet delas av Medarbetarnas kunskaper och utbildningsverksamhet samt Incident- och kontinuitetshantering.

### 4.4.3 Resultatspridning

Diagrammet nedan påvisar, precis som med kommunerna och regionerna tidigare, hur mycket de 10 procent bästa myndigheterna drar upp resultatet för en typmyndighet i de redovisade diagrammen i kapitel 2. Det är återigen en kraftig skillnad mellan resultaten för de 10 procent bästa myndigheterna jämfört med de 80 procent som utgör normalfördelningen. Sammantaget är resultatspridningen hos myndigheterna mindre än hos kommunerna, men påminner desto mer om samma diagram för regionerna.

**Diagram 39.** Infosäkkollen diagram 39



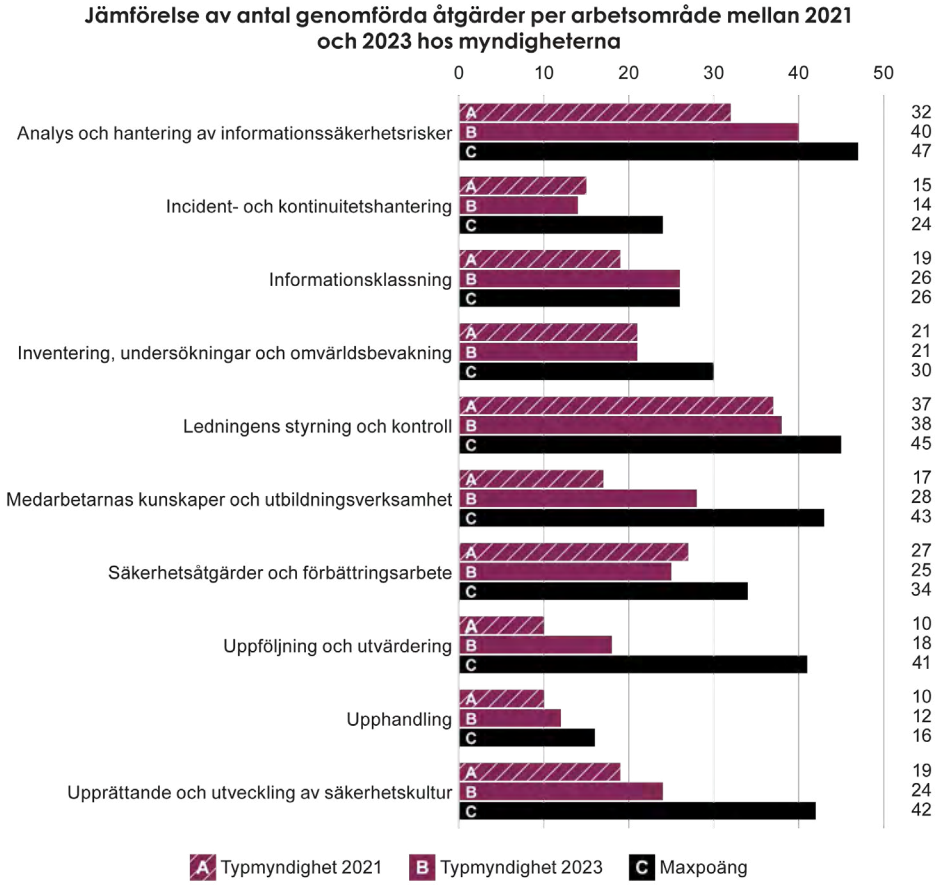

Det svagaste tio procenten av myndigheterna har enbart uppnått ett egentligt påvisbart resultat inom ett arbetsområde. De tio procent bästa myndigheterna har däremot uppnått maxresultat i modellens arbetsområden för Informationsklassning och Upphandling, samma resultat som för de bästa tio procenten av kommunerna och regionerna.

Av de 80 procent av myndigheterna som utgör normalfördelningen är resultatspridningen relativt stor. På Infosäkkollen som helhet är inte heller denna grupp nära att nå nivå 1 (0,56), även om det är bättre jämfört med regionerna (0,44) och kommunerna (0,26). Normalfördelningsgruppen har, precis som motsvarande grupp bland regionerna, uppnått nivå 1 eller bättre i åtta av modellens tio arbetsområden. Detta inkluderar två arbetsområden där gruppen nått över nivå 2, vilket indikerar att dessa organisationer bedriver sitt informations- och cybersäkerhetsarbete med en viss systematik.

### 4.4.4 Resultatförändring mellan mättillfällena

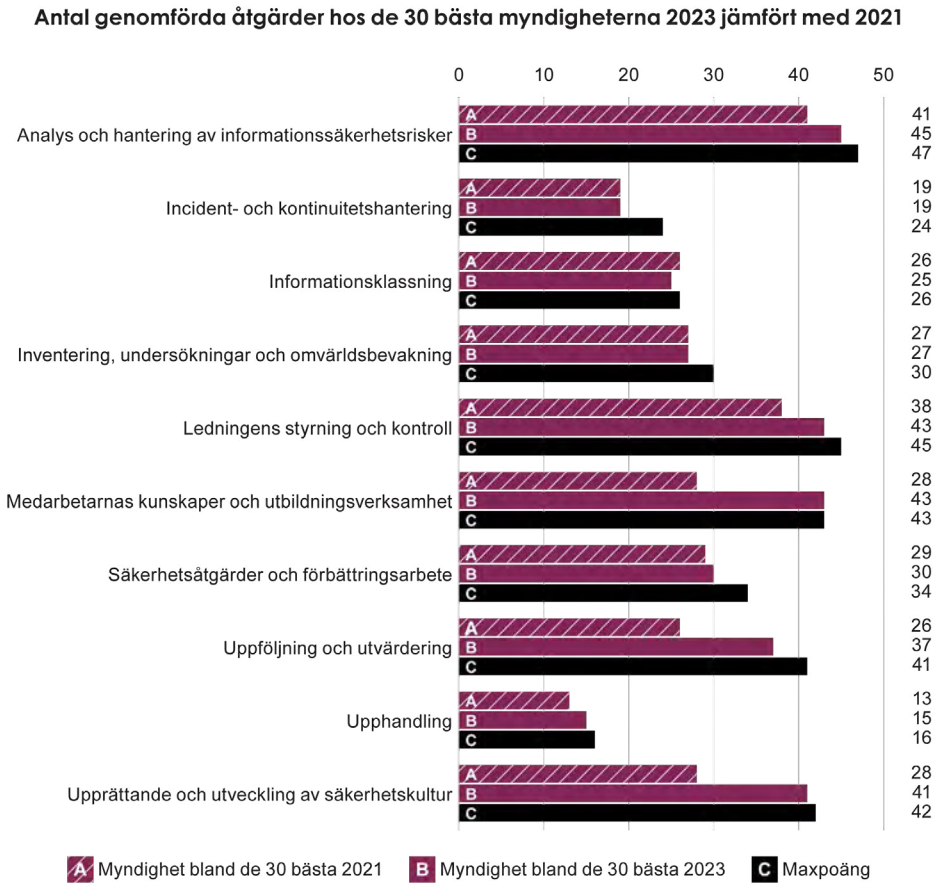
Inom ramen för detta avsnitt kommer resultatförändringen hos myndigheter mellan 2021 och 2023 presenteras. Typmyndigheten har förbättrat sitt resultat 2023 jämfört med 2021.

**Diagram 40.** Infosäkkollen diagram 40




En typmyndighet hade genomfört 207 av 348 (59,5 %) möjliga åtgärder år 2021, medan samma typmyndighet hade genomfört 246 åtgärder (70,7 %) år 2023. Det motsvarar en ökning med 18,8 procent. Resultatet har förbättrats inom sju arbetsområden, är detsamma som 2021 inom ett arbetsområde och i två arbetsområden ses en försämring.

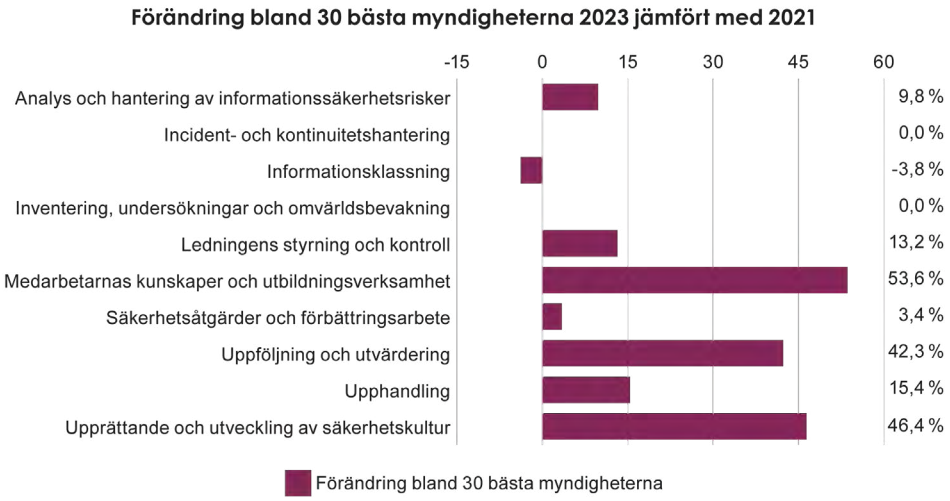
**Diagram 41.** Infosäkkollen diagram 41




En typmyndighet av de 30 bästa 2021 hade genomfört 275 åtgärder, medan samma aktör 2023 hade genomfört 325 åtgärder, en ökning med 18,2 procent. Det är samma mönster, även om ökningen är lite kraftigare, som sågs i 3.4 hos typkommunen av de 30 bästa kommunerna.

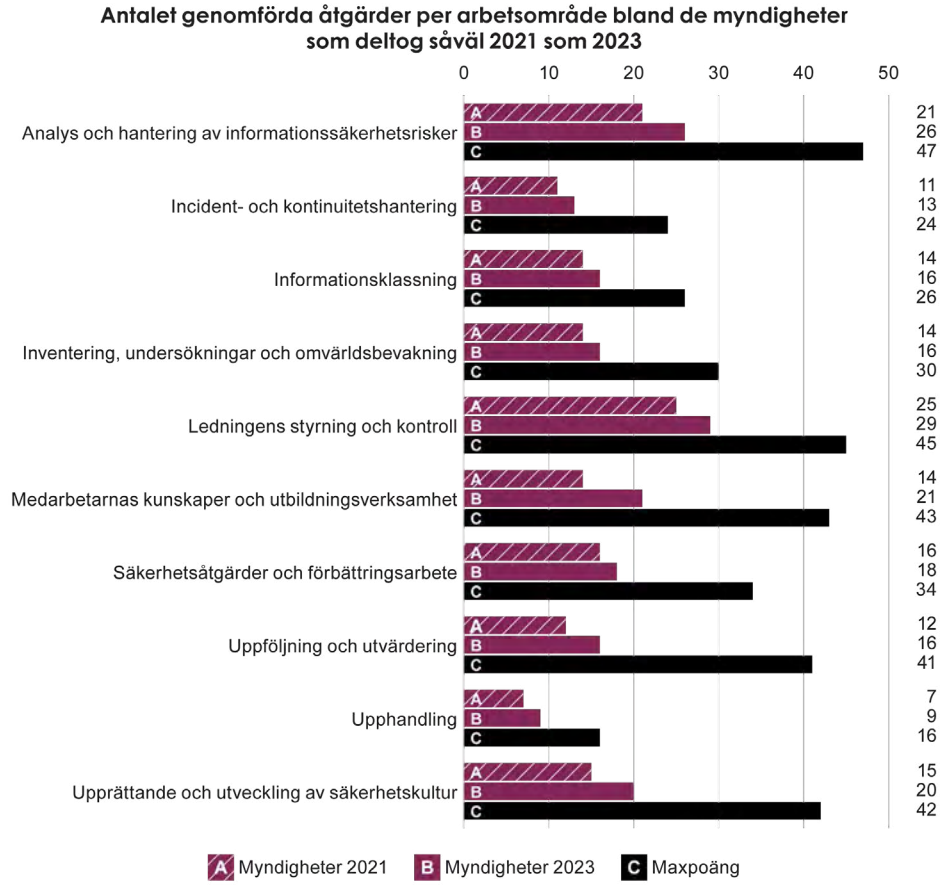
Sju arbetsområden visar på en förbättring, varav Medarbetarnas kunskaper och utbildningsverksamhet, Upprättande och utveckling av säkerhetskultur och Uppföljning och utvärdering visar på särskilt omfattande förbättring i denna grupp. Resultatet redogörs för i procent i diagrammet nedan.

**Diagram 42.** Infosäkkollen diagram 42




93 myndigheter deltog såväl 2021 som 2023. Ett genomsnitt av resultatet för genomförda åtgärder för de myndigheter som deltagit vid båda mättillfällena visar på förbättring inom alla arbetsområden.

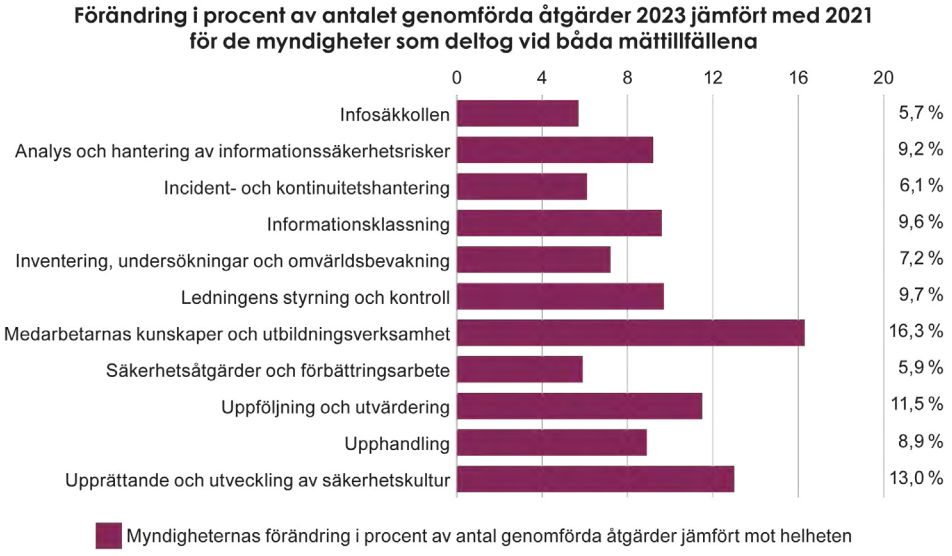
**Diagram 43.** Infosäkkollen diagram 43




Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 5,7 procentig resultatförbättring av hela Infosäkkollen, vilket var detsamma som för regionerna.

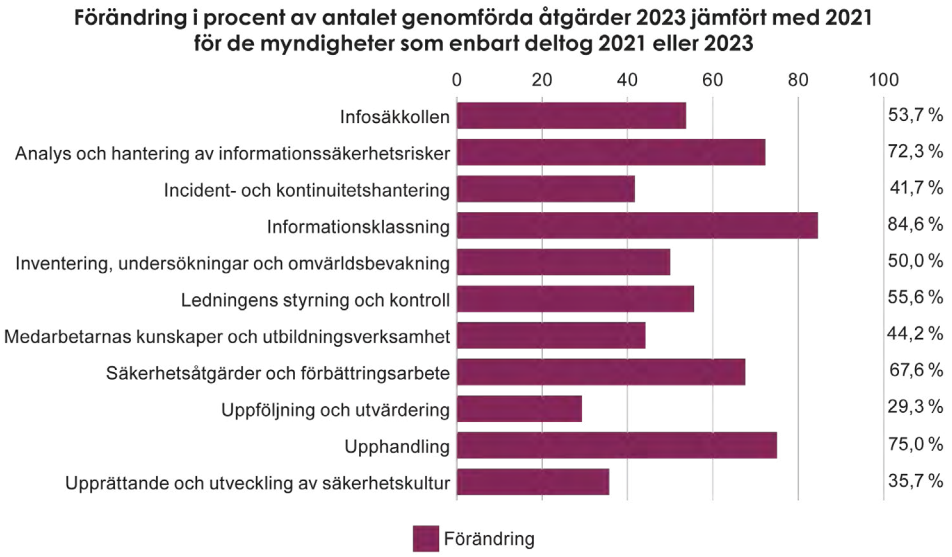
Myndigheterna var den aktörsgrupp som hade bäst resultat 2021, och kunde kanske därför förväntas ha mindre faktisk förbättring än andra aktörsgrupper.

**Diagram 44.** Infosäkkollen diagram 44




Den genomsnittliga förändringen per arbetsområde är 9,7 procent. För tre arbetsområden är förbättringen mer än tio procent.

**Diagram 45.** Infosäkkollen diagram 45




Den genomsnittliga förändringen för alla arbetsområden är hela 55,6 procent mellan de myndigheter som enbart deltog 2023 jämfört med de som enbart deltog 2021. Detta påvisar att många av de myndigheter med svagast resultat 2021 inte deltagit igen 2023, medan de som enbart deltagit 2023 fått bättre resultat visavi de som deltog 2021. Typmyndigheten bland förstagångsdeltagarna 2023 uppnår faktiskt nivå 1 i modellen och på sex arbetsområden nivå 2 eller högre i modellen, vilket tyder på att relativt bra organisationer som inte deltog 2021 tillkommit till 2023.

Således har hela aktörsgruppens övergripande resultat påverkats positivt, även om informations- och cybersäkerhetsarbetet för hela aktörsgruppen kanske inte utvecklats i motsvarande takt.

### 4.4.5 MSB:s föreskrifter om statliga myndigheters informationssäkerhet

Som analysen av resultattalen från myndigheter visar kan det konstateras att en tydlig majoritet av myndigheterna uppvisar ett resultat som indikerar att de kommer att behöva vidta en rad åtgärder innan de uppfyller kraven i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Myndigheternas resultat spänner över ett spektrum där några endast har haft enstaka åtgärder på plats under perioden. 14 myndigheter har fått mindre än 50 poäng, av Infosäkkollens totalt 200 poäng, och ingen av dem har uppnått någon övergripande nivå. Några har fått goda resultat, 72 myndigheter har fått mer än 100 poäng, dock har 30 av dem ändå inte uppnått någon nivå då de har saknat bredden i arbetet, huvudsakligen på grund av brister avseende uppföljning, utbildning och omvärldsbevakning. Bland de myndigheter som har nått höga poäng i Infosäkkollen är det alltså en klar majoritet som har genomfört stora delar av de åtgärder som föreskrifterna kräver, men som samtidigt uppvisar brister inom något eller några arbetsområden. Av alla deltagande 120 myndigheter är det fyra som når det samlade resultat som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

Även om MSB:s föreskrifter med krav på statliga myndigheters informationssäkerhetsarbete har uppdaterats och förtydligats i några omgångar sedan de först trädde i kraft 2009 bör det ändå noteras att myndigheterna har omfattats av författningskrav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i tolv år. Under den tiden har några nya myndigheter skapats och det kan vara så att dessa inte har haft tid att bygga upp det systematiska informationssäkerhetsarbetet fullt ut. Den faktorn är dock inte tillräcklig för att förklara resultatet.

MSB har inte i uppgift att utöva tillsyn över hur enskilda myndigheter efterlever föreskrifterna om statliga myndigheters informationssäkerhet. Myndigheten har därför inte någon djupare insyn än den som ges genom Infosäkkollen, incidentrapportering och informella kontakter. Trots det blir den övergripande slutsatsen ändå att arbetet med att efterleva föreskrifterna är eftersatt hos majoriteten av myndigheterna.

### 4.4.6 Förutsättningar för samarbeten

De frågor där det finns en övervägande majoritet som inte fått några poäng finns det anledning för centrala myndigheter och andra stöttande organisationer på alla nivåer i samhället att se över sitt stöd. Detta rör främst fråga 18, 30, och 39.[26]

- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 30:** De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 39:** De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

Det är dock viktigt att poängtera att det ytterst är varje organisation som är ansvarig för sitt informations- och cybersäkerhetsarbete, att det håller en adekvat nivå och följer de krav som ställs.

26. Jämfört med utfallet från Infosäkkollen 2021 har fråga 17 och 27 kunnat avföras. Fråga 17: Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt? Fråga 27: Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?

# Resultatet av It-säkkollen 2023

# 5. Resultatet av It-säkkollen 2023

I det här kapitlet redogörs för resultatet i It-säkkollen 2023 för alla organisationer i offentlig förvaltning. It-säkkollen 2023 består av 41 frågor där respondenten skattar sitt svar utifrån ett påstående med fyra möjliga svarsalternativ. Frågorna är baserade på MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Självskattningsenkäter är problematiska. De lämnar ett stort tolkningsutrymme hos respondenten, vilket påverkar trovärdigheten av insamlade data. Respondenter brukar särskilt överskatta sin egen förmåga. Redogörelsen av resultatet för It-säkkollen kan inte jämställas med trovärdigheten i svaren för Infosäkkollen. De nivåangivelser som anges är inte heller kalibrerade mot MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).[27]

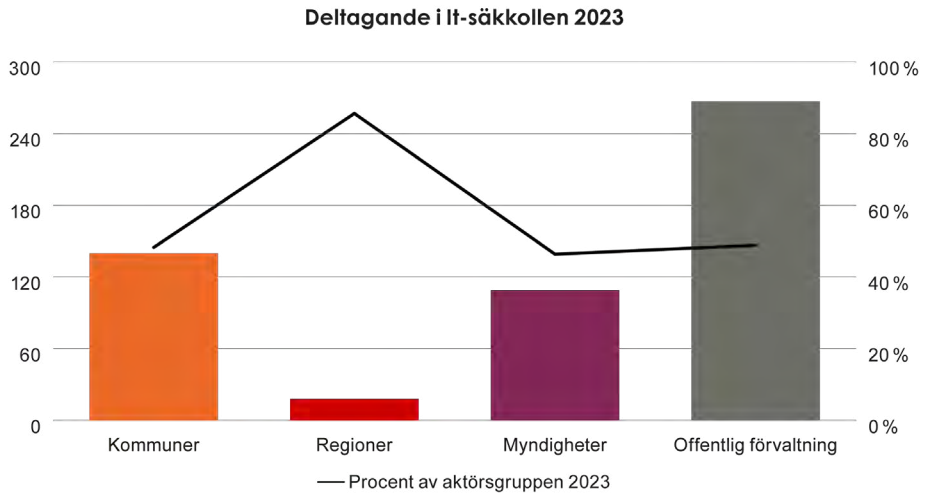
## 5.1 Övergripande bild

### 5.1.1 Deltagande

Totalt deltog 267 organisationer från offentlig förvaltning i It-säkkollen 2023. Av dessa var 140 kommuner, 18 regioner och 109 myndigheter. 91,8 procent av alla som deltog i Infosäkkollen 2023 deltog också i It-säkkollen 2023. 48,9 procent av offentlig förvaltning deltog i It-säkkollen.

27. För information om It-säkkollens utformning och planerade vidareutveckling, se kapitel 3.

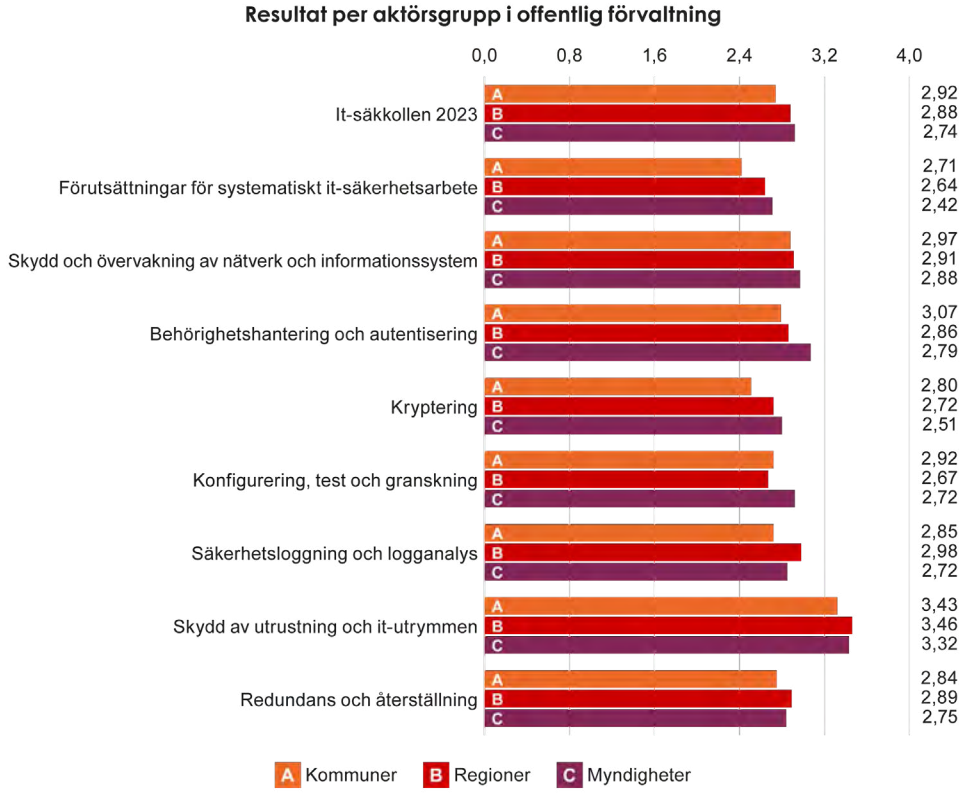
**Diagram 46.** It-säkkollen diagram 1




## 5.1.2 Utfall per arbetsområde

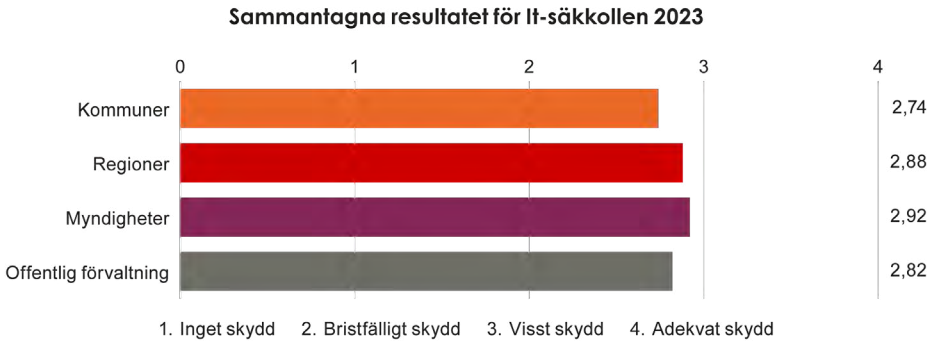
Resultatet i It-säkkollen visar på väldigt små skillnader mellan aktörsgrupperna för såväl helheten som inom varje enskilt arbetsområde. Myndigheterna presterar lite bättre än regionerna, följt av kommunerna som är marginellt svagast.

**Diagram 47.** It-säkkollen diagram 2



Resultatet för It-säkkollen 2023 når nästan upp till nivå 3 vilket betecknas som ”visst skydd”. Skillnaderna mellan aktörsgrupperna är små. Till följd av föreskriftskraven fanns en förväntan att myndigheterna skulle prestera bättre, men skillnaden är marginell.

**Diagram 48.** It-säkkollen diagram 3

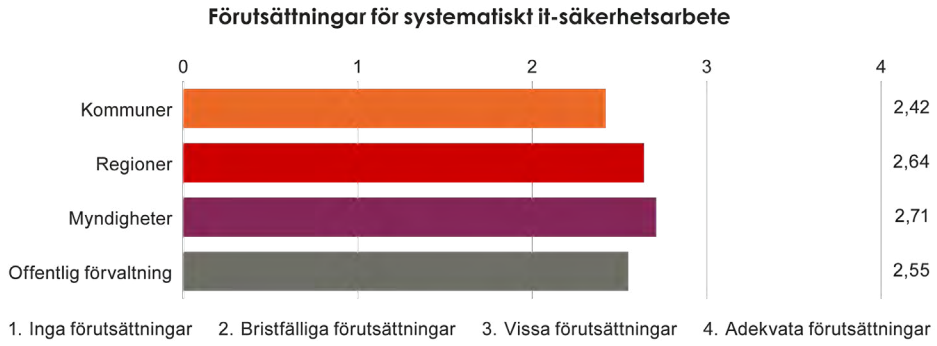



It-säkerhetsarbetet styrs och genomförs oftast av en mer avgränsad skara medarbetare än informationssäkerhetsarbetet. Arbetet leds av en it-chef som i sin tur har tillgång till eller själv medverkar i organisationens ledningsgrupp och därför har mer påverkan på att arbetet prioriteras och resurssätts. Detta kan jämföras med att långt ifrån alla organisationer har en CISO på heltid, samt att den rollen saknar den verksamhetsmässiga tyngden en it-chef har. Vidare kan it-säkerhetsarbetet få återverkningar på hela organisationen då de flesta har en centraliserad it-miljö där all eller den mesta informationen som organisationen ansvarar för behandlas. Informationssäkerhetsarbetet å sin sida behöver genomsyra hela verksamheten. Sammantaget är det därför väntat att resultatet från Infosäkkollen 2023 påvisar att organisationerna är bättre på de arbetsområden som behandlar it-säkerhet, nämligen Analys och hantering av informationssäkerhetsrisker, Informationsklassning och Säkerhetsåtgärder och förbättringsarbete. Det förklarar också varför resultatet från It-säkkollen 2023 visar på att många av organisationerna anser sig ha goda förutsättningar för systematiskt it-säkerhetsarbete, vilket MSB noterar står i kontrast mot vad resultatet i Infosäkkollen säger om förutsättningarna att bedriva systematiskt informationssäkerhetsarbete.

Det är viktigt att särskilja modellerna. Infosäkkollen undersöker faktiskt genomförda åtgärder, med svarsalternativ utifrån ”ja” och ”nej”. För att kunna avancera i de övergripande nivåerna i Infosäkkollen krävs också dokumentation och annan evidens för de svar som anges. It-säkkollen är som ovan påtalat en självskattningsenkät om den grad i vilken en organisation bedömer att den har genomfört åtgärder. Därför är det problematiskt att jämföra mellan undersökningarnas resultat.

I diagrammet nedan är det notabelt att organisationerna anser sig ha så pass goda förutsättningar för systematiskt it-säkerhetsarbete. Analysen av redogörelserna för de rapporterande organisationernas förutsättningar att bedriva systematiskt informationssäkerhetsarbete från 2021 visade ett jämförelsevis betydligt sämre läge.

**Diagram 49.** It-säkkollen diagram 4




Det är återigen en liten skillnad mellan aktörsgrupperna. Det kan kanske förklaras av att alla organisationer kan förväntas ha en IT-chef och att denne dessutom ofta har en arbetsgrupp och dedikerade resurser. Detta i motsats till att många aktörer på informationssäkerhetsområdet har en CISO på deltid eller mindre, samt att den rollen är placerad längre ner i hierarkin med mindre resurser. En annan möjlig förklaring är att när it-driften är utkontrakterad så förutsätter organisationen att leverantören tar betalt för att bedriva ett ändamålsenligt it-säkerhetsarbete.

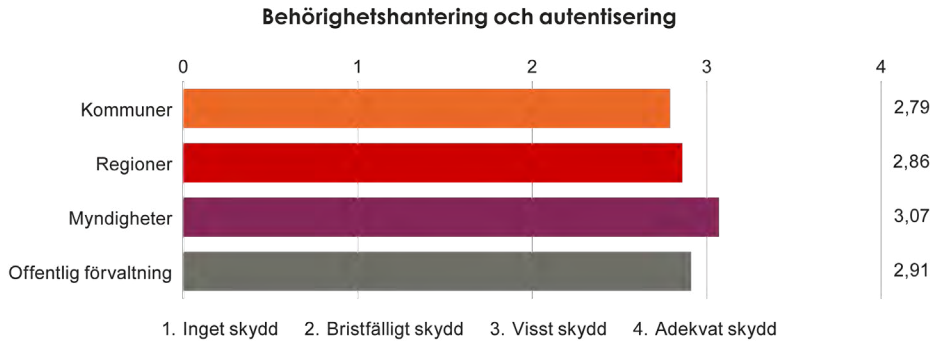
Vidare kan, om än något förenklat, till exempel system och behörigheter ställas in av en administratör och gälla hela verksamheten, till skillnad från informationssäkerhetsarbete som måste utföras av hela verksamheten.

Gällande Skydd och övervakning av nätverk och informationssystem syns återigen knappt någon skillnad i nivån mellan aktörsgrupperna. Alla aktörsgrupper når nästan upp till nivå 3, vilket motsvarar ”visst skydd”.

**Diagram 50.** It-säkkollen diagram 5

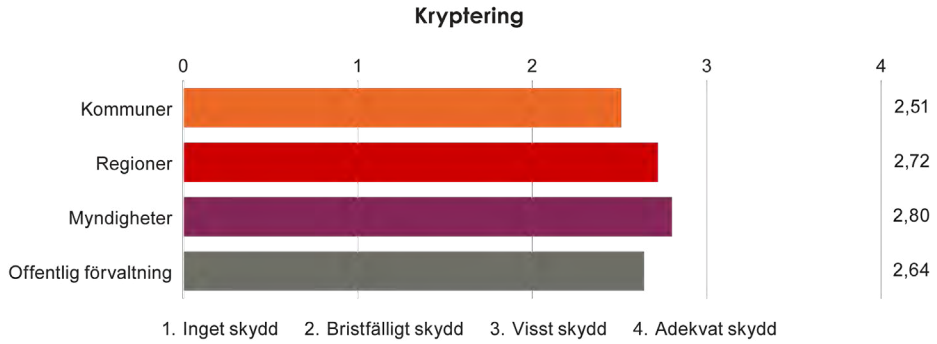

Behörighetshantering och autentisering är grundläggande och förhållandevis enkelt jämfört med andra it-säkerhetsåtgärder.

**Diagram 51.** It-säkkollen diagram 6



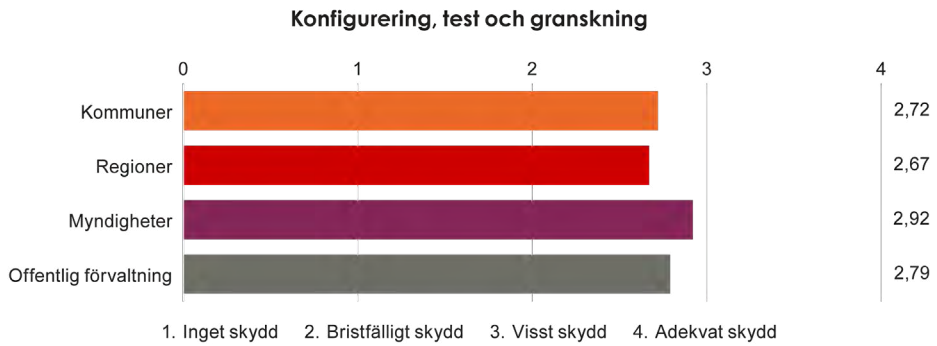

Resultatet för arbetsområdet Kryptering är svagt jämfört med andra arbetsområden. Mer analys behövs för att eventuellt utröna om det är någon särskild fråga som påverkar helheten, eller andra brister.

**Diagram 52.** It-säkkollen diagram 7



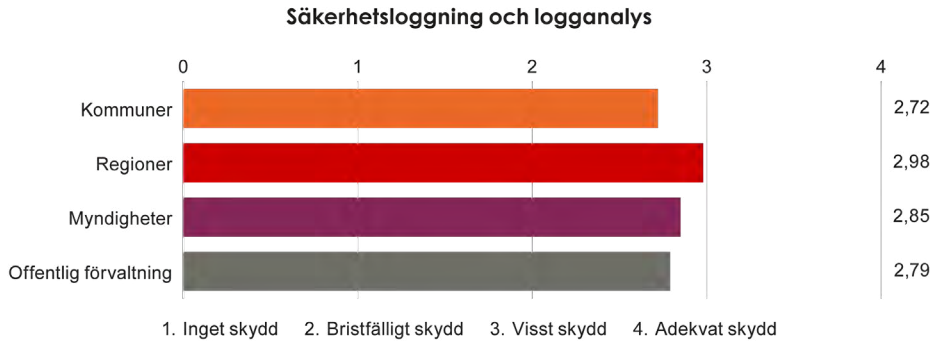

Att organisationerna skulle prestera sämre på Konfigurering, test och granskning var delvis förväntat. Dessa åtgärder ligger ofta i slutet av arbetsflödet och brukar ibland prioriteras ner. Svaren på Infosäkkollen för arbetsområdet för Uppföljning och utvärdering påvisar samma mönster.

**Diagram 53.** It-säkkollen diagram 8



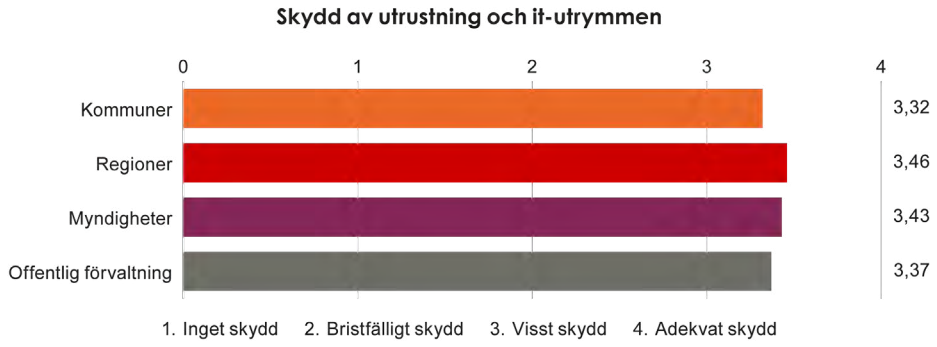

Det kan vara svårt, tidsödande eller resurskrävande att göra fullgoda logganalyser. Frågornas detaljnivå säger dock inget om den kompetens som krävs för att bedriva kvalitet i detta arbete, därför kan mer detaljerade frågor förändra resultatet till 2025.

**Diagram 54.** It-säkkollen diagram 9



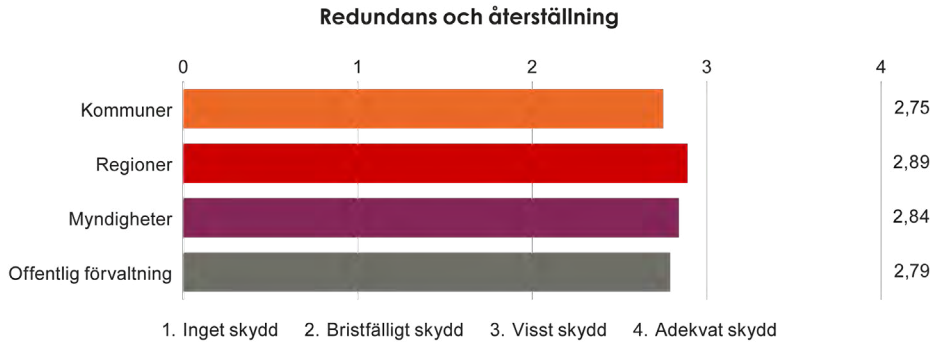

Skydd av utrustning och it-utrymmen är det arbetsområde med det klart bästa resultatet, oavsett aktörsgrupp. Det var även förväntat att resultatet skulle utfalla så. Det är det minst abstrakta arbetsområdet och kanske därför lättare att förstå vikten av, samt genomföra åtgärder för.

**Diagram 55.** It-säkkollen diagram 10



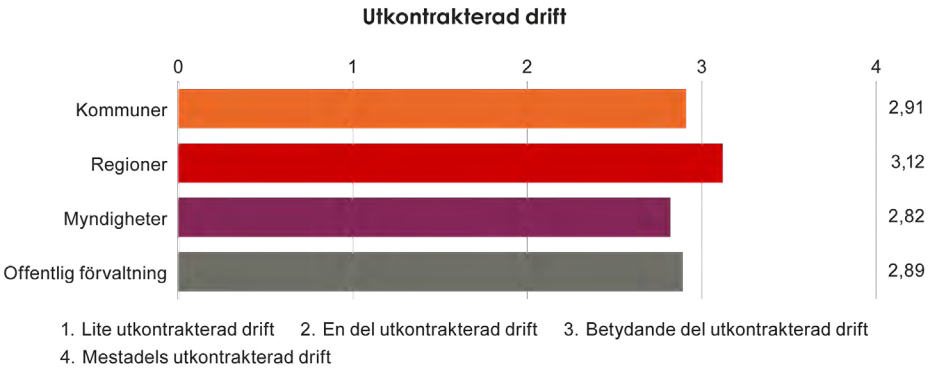

Arbetsområdet för Redundans och återställning påvisar ett bättre resultat än MSB förväntat. Det är den typen av arbete som ibland prioriteras ner, eftersom det ofta hanterar eventuellt framtida risker.

**Diagram 56.** It-säkkollen diagram 11



Det är slående hur stor andel av offentlig förvaltning som uppger att de utkontrakterat sin it-drift. Det är möjligt att denna fråga lämnar ett visst tolkningsutrymme och att bättre metodologi kommer påverka utfallet till nästa mättillfälle. Även om regionerna uppger att de utkontrakterat i högre utsträckning än andra aktörsgrupper motsvarar de flesta svar en nivå av ”Betydande andel utkontrakterad drift”.

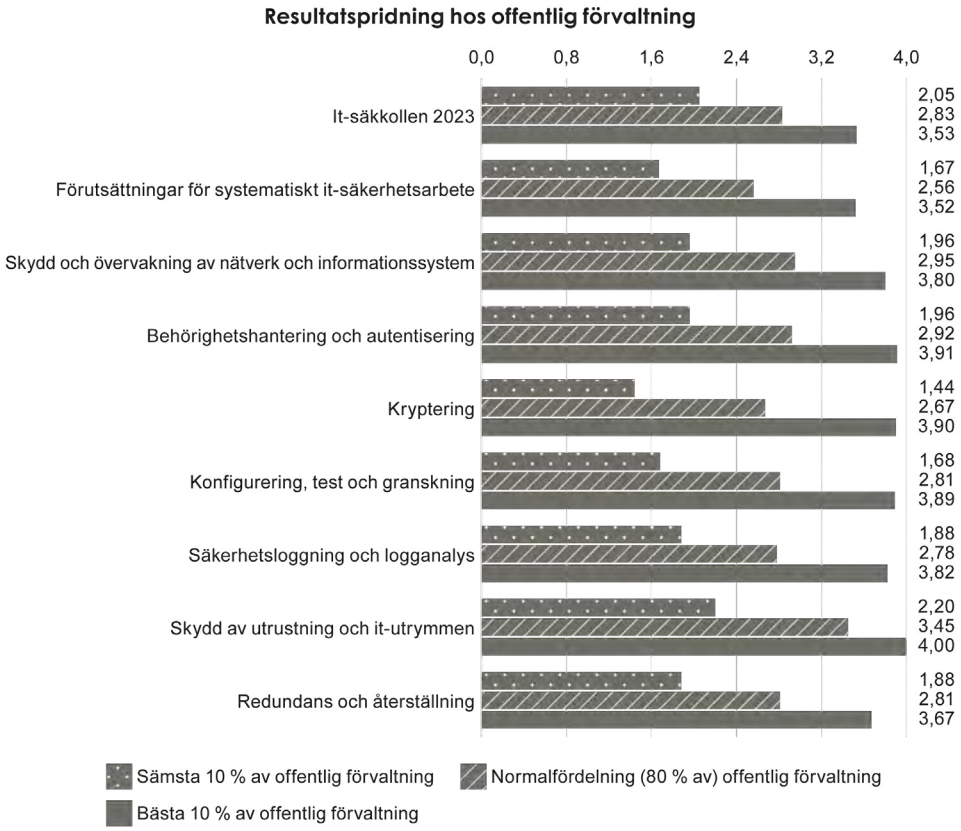
**Diagram 57.** It-säkkollen diagram 12




## 5.1.3 Resultatspridning

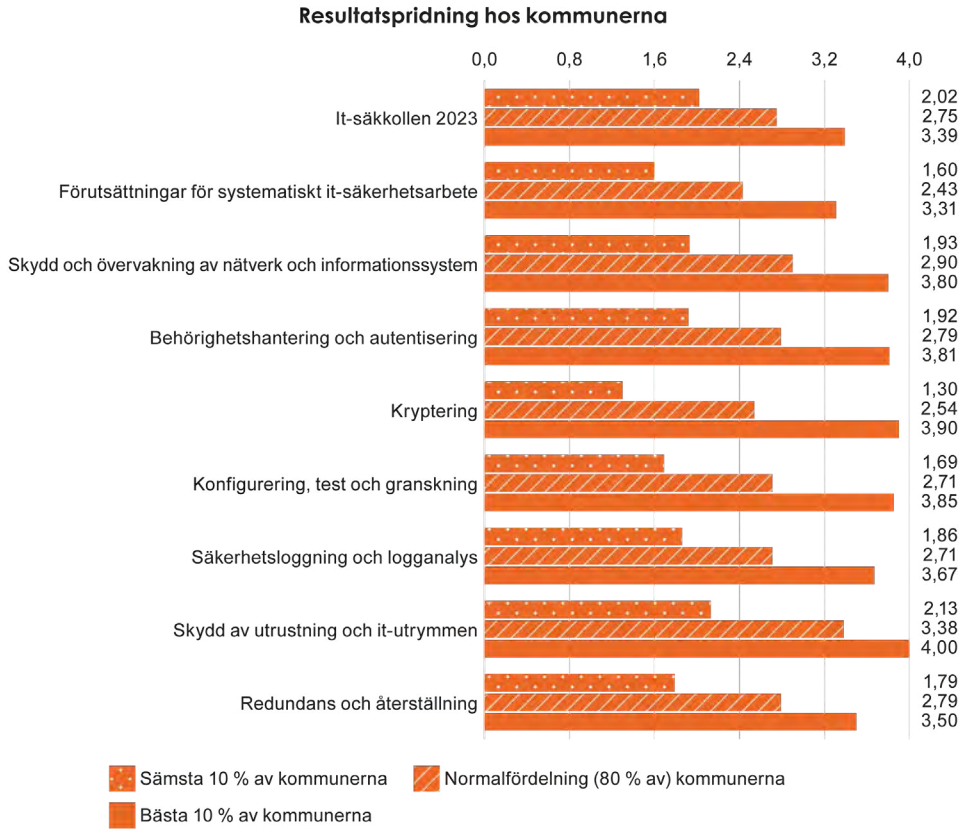
Här återges det samlade resultatet för en organisation på ett sätt som möjliggör att jämföra resultatspridningen mellan organisationer.

**Diagram 58.** It-säkkollen diagram 13



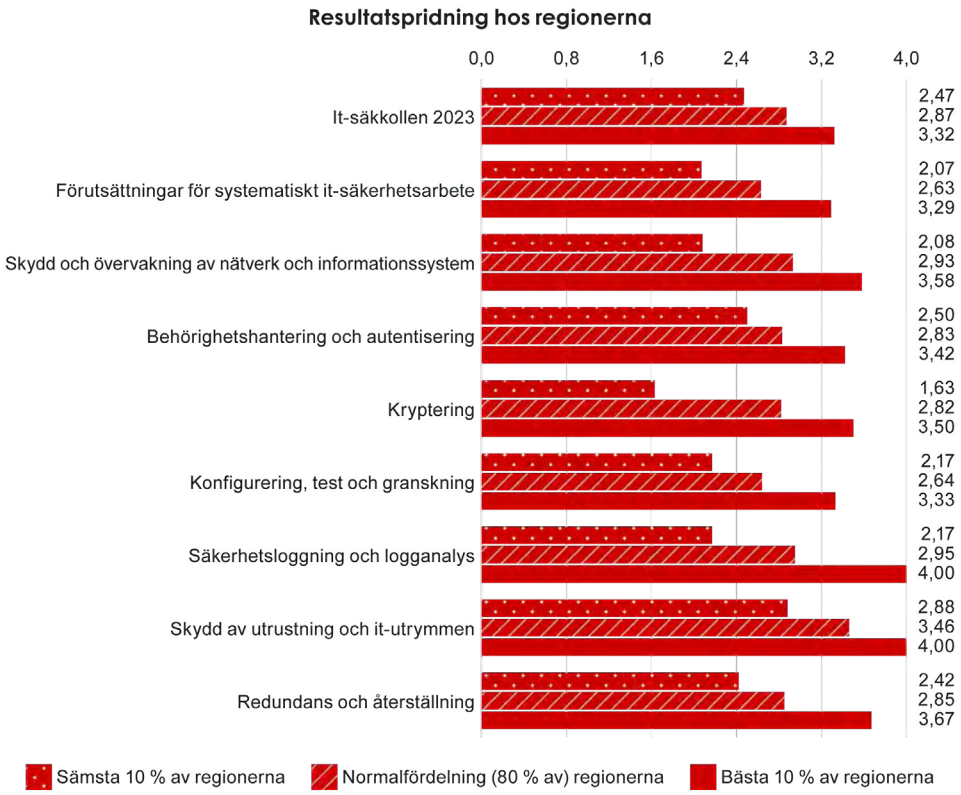
Då det är första gången It-säkkollen genomförs går inte resultatspridningen att jämföra mot motsvarande tidigare undersökning, men hos den samlade mängden respondenter är spridningen relativt liten jämfört med den spridning som denna resultatredovisning påvisat för Infosäkkollen. Det är förvisso en ganska stor skillnad på de bästa och svagaste tio procenten, men sammantaget tyder svarsfördelningen på att arbetet har nått längre.

**Diagram 59.** It-säkkollen diagram 14



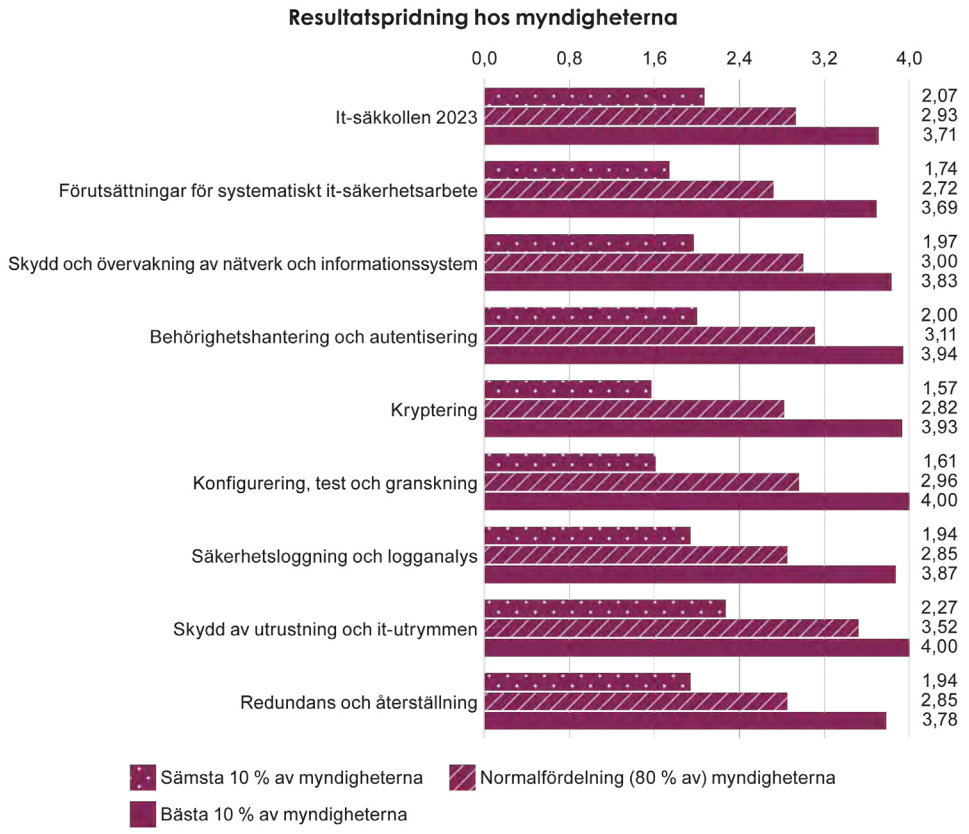

Resultatspridningen hos kommunerna är mindre än för myndigheterna, men större än för regionerna. Det är relativt väl fördelat mellan arbetsområdena, men i Skydd av utrustning och it-utrymmen är skillnaden mellan normalfördelningen och de bästa tio procenten som minst. Motsatsen hittas inom Kryptering där de tio procent bästa kommunerna presterar mycket bättre än normalfördelningen.

**Diagram 60.** It-säkkollen diagram 15




Hos regionerna syns den minsta spridningen mellan organisationerna. Det kan sannolikt förklaras av att det är den minsta aktörsgruppen, samt den mest homogena. En förklaringsmodell som stärks ytterligare av hur väl de svagaste tio procenten bland regionerna presterar jämfört med de svagaste tio procenten av kommuner och myndigheter. Det är endast inom arbetsområdet för Kryptering som de svagaste tio procenten av regionerna inte når motsvarande nivå 2.

**Diagram 61.** It-säkkollen diagram 16




Myndigheterna är den aktörsgrupp med störst spridning. Det är också den aktörsgrupp där de bästa tio procenten presterar bäst jämfört med motsvarande grupp hos kommunerna och regionerna. De svagaste tio procenten av myndigheterna klarar bara att nå upp till nivå 2, bristfälligt skydd, inom två av arbetsområdena, och når endast just över nivå 2 (2,07) på helheten.

# Utvecklingen framåt

# 6. Utvecklingen framåt

Huvudsyftet med Infosäkkollen och It-säkkollen är att stödja uppföljning och därmed utveckling av organisationers systematiska och riskbaserade informations- och cybersäkerhetsarbete och i förlängningen därigenom bidra till ett stärkt totalförsvar genom ett säkrare och robustare samhälle.

Inrapportering av Infosäkkollen och It-säkkollen bidrar till en förbättrad och mer heltäckande bild av arbetet med informations- och cybersäkerhet i Sverige, och baserat på detta och andra informationskällor kan MSB göra en bedömning av cybersäkerheten inom det civila försvaret. Förutom en nationell lägesbild ger också deltagandet i undersökningarna MSB möjlighet att ge direkt återkoppling och anpassat stöd till organisationer gällande vidareutvecklingen av säkerhetsarbetet.

För att MSB fullt ut ska kunna bedöma cyberförmågan utifrån ett totalförsvarsperspektiv är det centralt att NIS-leverantörer deltar i undersökningarna. En stor del av våra samhällsviktiga tjänster, produkter och infrastruktur bedrivs och tillhandahålls av privat sektor. Därför är det centralt att MSB får en bild av NIS-leverantörers informations- och cybersäkerhet.

Resonemanget ovan ställs på sin spets av it-incidenten som TietoEvry erfarit i relativ närtid, och där ett drygt hundratal organisationer i sin tur drabbats.[28] MSB har i tidigare rapporter påtalat risken för leverantörskedjeincidenter[29], och i årsrapporten för 2022 lyfte MSB att myndigheten vill få i uppdrag att undersöka leverantörskedjorna hos samhällsviktiga verksamheter för att identifiera och hantera monoberoenden[30]. En förståelse kring nivån på informations- och cybersäkerhetsarbete hos NIS-leverantörer genom genomförandet av Infosäkkollen och It-säkkollen skulle bidra till MSB:s riskbedömningar och lägesbilder.

Ny EU-reglering, särskilt NIS2- och CER-direktiven, ställer långtgående krav på samhällsviktiga verksamheters säkerhetsarbete. Kraven som kommer att ställas utifrån dessa regleringar gör inte skillnad på om en organisation tillhör offentlig eller privat sektor. Att genomföra Infosäkkollen och It-säkkollen ger en organisation en förståelse kring hur de klarar av lagkraven, men också stöd för deras förbättringsarbete. Baserat på detta hoppas MSB på ett större deltagande i framtida undersökningar.

28. https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda (hämtad 29/1 2024).

29. https://rib.msb.se/filer/pdf/29829.pdf.

30. https://rib.msb.se/filer/pdf/30339.pdf.

It-säkkollen är i nuläget en självskattningsenkät. Det medför metodologiska svagheter som MSB avser adressera under 2024. It-säkkollen ska arbetas om för att efterlikna Infosäkkollen, detta i huvudsak genom att gå från självskattning till att respondenten istället anger införda säkerhetsåtgärder. Det minskar risken för tolkning och ger samtidigt detaljer som gagnar det analytiska arbetet. Modellen kommer genomgå pilot med målgrupperna innan lansering i ny form under 2025.


Myndigheten för
samhällsskydd
och beredskap


651 81 Karlstad  Tel 0771-240 240  **www.msb.se**
Publ.nr MSB2333 – mars 2024  ISBN 978-91-7927-489-4