Myndigheten för samhällsskydd och beredskap

Resultatredovisning av Cybersäkerhetskollen 2024

Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen

Resultatredovisning av Cybersäkerhetskollen 2024
– Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen

Foto: MSB:s bildbank (Johnér)
Tryck: Åtta45 Tryckeri
Produktion: Advant

Publikationsnummer: MSB2545 – januari 2025
ISBN-nummer: 978-91-7927-599-0

Förord

För tredje gången har MSB genomfört Cybersäkerhetskollen. Varje mätning fördjupar kunskapen kring nivån på cybersäkerhetsarbetet hos samhällsviktiga verksamheter. Jag vill passa på att tacka de kommuner, regioner och statliga myndigheter som bidragit med sina svar. Tillsammans har ni möjliggjort denna resultatredovisning. Samtidigt konstaterar jag att svarsfrekvensen för varje år är vikande och att deltagande från privat sektor är fortsatt påtagligt lågt.

Årets mätning visar att stora delar av den offentliga förvaltningen alltjämt saknar grunderna i ett systematiskt cybersäkerhetsarbete. Vi ser ett fortsatt bristande engagemang från organisationsledningar.

Utifrån det försämrade säkerhetspolitiska läget måste det också poängteras att en samlad och detaljerad av bild av våra sårbarheter är en helt central förutsättning för regeringens och myndigheternas vidareutveckling av beredskapen inom det civila försvaret. Omvärldsläget gör det tydligt att motståndskraften på kort tid behöver stärkas betydligt.

Cybersäkerhetskollen och incidentrapporteringen utgör centrala informationskällor i arbetet med att inrikta och designa såväl reglering som investeringar och stöd på informations- och cybersäkerhetsområdet. Betydelsen av Cybersäkerhetskollen i det arbetet understryks även av att regeringen i budgetpropositionen inför 2025 har aviserat särskilda satsningar på såväl Cybersäkerhetskollens utveckling, som på en särskild undersökning av kommuners och små och medelstora aktörers tekniska cybersäkerhetsförmåga. Sådana satsningar kan generera stort värde för statens fortsatta arbete med att höja nivån på organisationers cybersäkerhetsarbete, men en central förutsättning för att det ska fungera är att alla berörda organisationer deltar.

Sverige har nu testat en modell med frivilligt deltagande i Cybersäkerhetskollen. Det arbetssättet har inte lett till tillräckligt högt deltagande. När Sverige nu får en ny cybersäkerhetslag kan användning av Cybersäkerhetskollen göras obligatorisk. Cybersäkerhetskollen kan utgöra kärnan i såväl tillsyn som samordning mellan tillsynsmyndigheterna. Fler organisationer skulle ha ett bättre underlag för planering, staten skulle ha ett bättre underlag för sitt arbete med reglering och stöd, och tillsynen bli mer harmoniserad mellan sektorerna.

Nivån på det systematiska säkerhetsarbetet i den offentliga förvaltningen måste höjas. Det är hög tid.

Stockholm, 2024-01-31

Åke Holmgren
Avdelningschef

Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer
Myndigheten för samhällsskydd och beredskap

Innehåll

Sammanfattning

Sammanfattning

Mellan 3 april och 13 september 2024 genomfördes Infosäkkollen, som tillsammans med It-säkkollen utgör Cybersäkerhetskollen, för tredje gången. Knappt hälften av organisationerna i offentlig förvaltning deltog och bland dem var det endast lite fler än fyra utav tio organisationer som nådde upp till någon av modellens fyra nivåer. Övriga 58,6 procent av organisationerna saknar de mest grundläggande delarna i ett systematiskt cybersäkerhetsarbete.

Vid första anblick kan resultatet för 2024 se bättre ut jämfört med tidigare mätningar än vad det faktiskt är. Detta beror på att antalet deltagande kommuner, den aktörsgrupp som presterar svagast, har minskat samtidigt som antalet myndigheter, den aktörsgrupp som presterar starkast, har ökat relativt mot hela underlaget.

Resultatet är förvisso en förbättring jämfört med tidigare mätningar av Infosäkkollen, men endast marginellt. Enbart 5,2 procent uppnår nivå 3 eller 4 i modellen. MSB bedömer att förbättringstakten, utifrån det säkerhetspolitiska läget, underskrider behovet.

Endast 8 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[1]. Den första utgåvan av föreskrifterna trädde ikraft 2009.

193 organisationer deltog i Infosäkkollen både 2023 och 2024. Mätt i antalet genomförda åtgärder motsvarar resultatet en 12,4 procentig förbättring mellan mätningarna. Gruppen som deltog i båda mätningarna har genomfört i snitt 12,3 fler åtgärder 2024 jämfört med 2023.

För Infosäkkollen var det 98 organisationer som deltog enbart 2023 och 75 organisationer som deltog enbart 2024. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 3,6 procentig resultatförbättring för de organisationer som endast deltog 2024 jämfört med de som endast deltog 2023. Förbättringen i antalet genomförda åtgärder är 2,8 fler 2024 jämfört med 2023.

De organisationer som deltog i Infosäkkollen både 2023 och 2024 har i genomsnitt genomfört 111,1 åtgärder. De organisationer som deltog endast 2024 har i jämförelse genomfört i genomsnitt 82 åtgärder. Resultatjämförelsen mellan de

Not 1. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

organisationer som deltar i Cybersäkerhetskollen varje år visavi de som deltar sporadiskt är en indikator på att de organisationer som arbetar systematiskt över tid också är de organisationer som utvecklas såväl bäst som snabbast.

Infosäkkollens arbetsområde för Ledningens styrning och kontroll är det arbetsområde där minst antal organisationer klarar nivå 1. Sammantaget är den bild som framkommer att organisationsledningarna inte engagerar sig, prioriterar eller tillför de resurser till förbättringsarbetet i den utsträckning som krävs. Medan ett *visst* skydd kan uppnås utan aktiv inriktning och uppföljning av ledningen så är MSB:s bedömning att förutsättningarna för att bedriva ett *systematiskt och riskbaserat* cybersäkerhetsarbete saknas utan ledningens löpande engagemang.

Resultatredovisningarna av Infosäkkollen 2021 och 2023 konstaterade 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”*. Resultatet 2024 befäster återigen samma centrala slutsats. Dock justeras rekommendationen något, och MSB förespråkar en särskild satsning avseende finansiering till stöd för små och medelstora företag. De som avses är de som har genomfört Cybersäkerhetskollen eller som utvecklar tjänster som adresserar bristerna som redovisningen av Cybersäkerhetskollen lyfter. En sådan satsning skulle komplettera den satsning som nu görs på offentliga aktörer inom det civila försvaret.

Det är ledningens ansvar att tillse att tillräckliga resurser tilldelas säkerhetsarbetet för att de säkerhetseffekter som krävs ska kunna uppnås. Samtidigt kan MSB konstatera att Cybersäkerhetskollen via Infosäkkollen återkommande har visat att tilldelningen av resurser ligger på en relativt konstant nivå, och att organisationerna själva anger att de inte har tillräckligt med resurser för att kunna bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete. Det är helt enkelt omöjligt att omhänderta stöd från MSB och andra organisationer för att höja nivån. Mot den bakgrunden ser MSB att samfinansiering i form av stödfinansiering med motprestationskrav av säkerhetsarbetet i offentlig sektor bör övervägas. MSB bedömer att NCC-SE skulle kunna utgöra en funktion för att genomföra sådan samfinansiering.

Samtidigt bedömer MSB att säkerhetsarbetet bör kunna bedrivas effektivare, och att ökad effektivitet skulle kunna frigöra resurser för att arbeta bredare, och därigenom nå högre nivåer. Här finns en roll för näringslivet i att utveckla och tillhandahålla verktyg, teknologi och tjänster som kan bistå den offentliga förvaltningen i det systematiska cybersäkerhetsarbetet.

256 organisationer från offentlig förvaltning deltog i It-säkkollen[2] 2024. Resultatet i It-säkkollen 2024 motsvarande nästan nivå 3 av 4 i modellen, vilket motsvarar ”visst skydd”. Det är en resultatförbättring på 2,7 procent

Not 2. It-säkkollen är en självskattningsmätning. Självskattningsenkäter har inbyggda metodproblem och därför bör slutsatserna läsas med försiktighet och ses som indikatorer. It-säkkollen kommer vidareutvecklas för att få samma metodologiska robusthet som Infosäkkollen till mättillfället 2025.

jämfört med 2023 års mätning. Att resultatförbättringen är mer begränsad än Infosäkkollen bör förstås utifrån tidigare resultat. Då det redovisats betydligt bättre resultat i It-säkkollen är det rimligt att också resultatförbättringen är procentuellt sett mindre.

It-säkkollen uppvisar 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 oftast har tillgång till organisationens ledningsgrupp och därför har mer påverkan på att arbetet prioriteras och resurssätts. En CISO saknar ofta motsvarande mandat. Detta kan utgöra en del av förklaringen till varför resultatet från It-säkkollen 2024 visar på att många av organisationerna anser sig ha bättre förutsättningar för systematiskt it-säkerhetsarbete än vad resultatet i Infosäkkollen säger om förutsättningarna att bedriva systematiskt informationssäkerhetsarbete.

De arbetsområden där offentliga förvaltningar presterar bäst är Skydd av utrustning och it-utrymmen, Behörighetshantering samt Skydd och övervakning av nätverk och informationssystem. De arbetsområden där offentliga förvaltningar presterar svagast är Förutsättningar för systematiskt it-säkerhetsarbete, Kryptering samt Redundans och återställning.

Svarsfrekvensen hos offentlig förvaltning har minskat för varje mättillfälle. Utifrån det säkerhetspolitiska läget och vikten av ökad motståndskraft behöver deltagandet utifrån ett totalförsvarsperspektiv istället öka. Ju fler organisationer som deltar, desto bättre samlad bild får MSB av Sveriges cybersäkerhetsnivå. Vidare bidrar ökat deltagande också till att säkerställa att de rekommendationer som utfärdas blir träffsäkrare och att MSB:s metodstöd möter samhällsviktiga verksamheters faktiska behov.

Precis som i mätningen 2023 rapporterades det in så få svar från näringslivet, särskilt NIS-leverantörer, att dessa inte kunde inkluderas i resultatredovisningen. När Cybersäkerhetslagen träder i kraft kommer den stora majoriteten av samhällsviktiga verksamheter inom cyberdomänen utgöras av organisationer i privat sektor. För att MSB ska kunna ta fram en samlad nationell lägesbild över cybersäkerhetsnivån i Sverige måste alla samhällsviktiga verksamheter aktivt delta i relevanta cybersäkerhetsmätningar såsom Cybersäkerhetskollen.

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 och medverkan är frivillig. Uppdraget har redovisats två gånger före denna redovisning, 22 juni 2022[3] och 1 mars 2024[4].

Regeringen gav den 23 mars 2023 i uppdrag till MSB att även redovisa till Regeringskansliet (Försvarsdepartementet) hur nivån på it-säkerheten ser ut för organisationerna. MSB redovisade resultatet av It-säkkollen första gången 1 mars 2024.[5]

Baserat på svar från Cybersäkerhetskollen, bestående av Infosäkkollen och It-säkkollen, redovisar myndigheten i denna rapport en samlad bedömning av nivån på det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen 2024. Detta inkluderar 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.

Not 3. Resultatredovisning Infosäkkollen 2021: https://rib.msb.se/filer/pdf/30002.pdf.

Not 4. Resultatredovisningen av Infosäkkollen och It-säkkollen 2023: https://rib.msb.se/filer/pdf/30598.pdf.

Not 5. Resultatredovisningen av Infosäkkollen och It-säkkollen 2023: https://rib.msb.se/filer/pdf/30598.pdf.

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.

Cybersäkerhet definieras som all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.[6] Definitionen inkluderar informationssäkerhet, it-säkerhet, ot-säkerhet och leveranskedjesäkerhet.

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”.

Not 6. Definitionen är i enlighet med Cybersäkerhetsakten: https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881.

De fyra nivåerna i Infosäkkollen är:

- Nivå 1: Grunderna i informations- och cybersäkerhetsarbetet
- Nivå 2: Informations- och cybersäkerhetsarbetet bedrivs med viss systematik och organisationen 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).

1.4 Resultatet i Cybersäkerhetskollen är viktigt

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

Cybersäkerhetskollen är en modell som används inom ramen för en struktur där organisationers systematiska cybersäkerhetsarbete följs upp. Likt andra modeller kan Cybersäkerhetskollen enbart göra anspråk på att beskriva en approximation av hur verkligheten ser ut hos en enskild organisation. Modellens frågor täcker en bred uppsättning aspekter som ingår i ett systematiskt informations- och it-säkerhetsarbete, men de täcker inte allt. Medan Cybersäkerhetskollen 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 Cybersäkerhetskollen endast göra anspråk på att beskriva en approximation av vad en organisation behöver satsa på för att utveckla sitt systematiska cybersäkerhetsarbete. Enskilda organisationer kan ha större behov av andra åtgärder än de modellen 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 Cybersäkerhetskollen för att följa upp sitt säkerhetsarbete, och att det är viktigt att nå höga nivåer i modellen:

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.

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 informations- och cybersäkerhetsarbete: 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 informations- och cybersäkerhetsarbetet: Modellens respektive övergripande nivåer motsvarar naturliga utvecklingssteg som organisationer kan följa för att successivt utveckla helheten i det systematiska 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 säkert. 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.

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

Cybersäkerhetskollen förutsätter att organisationen inte väljer bort något centralt område: Genom att nå högre nivåer kan organisationer utveckla det systematiska 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 Cybersäkerhetskollen har ett egenvärde.

1.5 NIS-leverantörers medverkan

Sammantaget mottog MSB 13 svar till Cybersäkerhetskollen 2024 från aktörer som angav sig vara NIS-leverantörer[7]. Av dessa uppgav tio att de var registrerade leverantörer av samhällsviktiga och digitala tjänster (bekräftade NIS-leverantörer). Utav ovan 13 organisationer svarade alla utom en även på It-säkkollen.

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 ett antal insatser för att öka deltagandet från näringslivet, särskilt NIS-leverantörerna.

Not 7. 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.

Slutsatser och rekommendationer

2. Slutsatser och rekommendationer

I detta kapitel presenteras slutsatser och rekommendationer för Cybersäkerhetskollen 2024. Cybersäkerhetskollen bestod 2024 av Infosäkkollen och It-säkkollen och båda mätningarna redovisas separat. Cybersäkerhetskollen lanserades 3 april 2024 och inrapporteringen var öppen till och med 13 september 2024.

2.1 Slutsatser från Infosäkkollen 2024

48,9 procent av organisationerna inom offentlig förvaltning deltog i Infosäkkollen 2024.[8] Deltagarantalet hos offentlig förvaltning 2024 har sjunkit med 4,4 procentenheter jämfört med 2023. Deltagarfrekvensen 2024 är högst inom aktörsgruppen regioner (57,1 procent), följt av myndigheter (50,6 procent) och till sist kommuner (46,9 procent).

111 organisationer, 41,4 procent, uppnådde nivå 1 eller högre i Infosäkkollen 2024. Nivå 1 i Infosäkkollen motsvarar att man har de grundläggande inslagen i ett systematiskt informations- och cybersäkerhetsarbete på plats. Det betyder samtidigt att 58,6 procent av alla deltagande organisationer saknar de grundläggande inslagen som modellen mäter. Jämförbar siffra 2023 var 69,4 procent.

För helhetsresultatet är dock det mest avgörande att antalet deltagande kommuner, som är den aktörsgrupp som presterar svagast, har minskat. Detta betyder att antalet myndigheter, som är den aktörsgrupp som presterar bäst, har ökat relativt mot hela populationen. Därför kan resultatet för 2024 vid en första anblick se bättre ut jämfört med tidigare mätningar än det faktiskt är.

14,2 procent uppnådde nivå 2 eller bättre, och 5,2 procent uppnådde nivå 3 eller 4 i modellen. I 2023 års mätning hade 10,3 procent uppnått nivå 2 eller bättre, och 2,8 procent nådde upp till nivå 3 eller 4 i modellen.

193 organisationer deltog både 2023 och 2024. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 12,4 procentig resultatförbättring av hela Infosäkkollen. De har genomfört i snitt 12,3 fler åtgärder 2024 jämfört med 2023.

Not 8. Domstolsverket har rapporterat in ett svar för alla domstolars räkning.

98 organisationer deltog enbart 2023 och 75 organisationer deltog enbart 2024. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 3,6 procentig resultatförbättring för de organisationer som endast deltog 2024 jämfört med de som endast deltog 2023. Den procenten är under de 12,4 procent som noterades för organisationer som deltog vid båda mättillfällena. Förbättringen i antalet genomförda åtgärder är 2,8 fler för de organisationer som endast deltog 2024 jämfört med de som endast deltog 2023. Det kan jämföras med 12,3 åtgärder för de som deltagit både 2023 och 2024.

De organisationer som deltog både 2023 och 2024 har i genomsnitt genomfört 111,1 åtgärder. De organisationer som endast deltog 2024 har i jämförelse endast genomfört i genomsnitt 82 åtgärder. Det är en skillnad 29,1 åtgärder. Trots att de organisationer som endast deltog 2024 presterar bättre jämfört med de organisationer som endast deltog 2023, är därmed resultatet för de organisationer som deltog endast 2024 en grupp som sänker helhetsresultatet. Eftersom det var 23 färre organisationer som endast deltog 2024 jämfört med 2023, sänktes dock helhetsresultatet av denna grupp mer 2023 än 2024.

Resultatjämförelsen mellan de organisationer som deltar i Cybersäkerhetskollen varje år visavi de som deltar sporadiskt är det en indikator på att de organisationer som arbetar systematiskt över tid också är de organisationer som utvecklas såväl bäst som snabbast.

I den enkätundersökning som genomfördes bland de som rapporterade in Infosäkkollen 2024 svarade 67,9 procent av respondenterna att de inte har den personal som krävs för att fullt ut implementera förbättringsarbetet. 52,2 procent uppgav att de arbetar deltid eller mindre med informations- och cybersäkerhet. Vidare uppgav 50,3 procent viss eller omfattande personalomsättning under den senaste tvåårsperioden. Samtidigt uppgav 56,4 procent att organisationen besitter nödvändig kompetens.

Vidare svarade 72,7 procent 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 47,3 procent av respondenterna *stämmer knappt* eller *stämmer inte*.

Sammantaget är den bild som framkommer att organisationsledningarna inte engagerar sig, prioriterar eller tillför de resurser till förbättringsarbetet i den utsträckning som krävs.

Det samlade resultatet från Infosäkkollen visar att ledningens engagemang korrelerar med organisationens resultat, det vill säga att ju högre engagemang ledningen visar, desto bättre resultat i Infosäkkollen. 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.

Cybersäkerheten hos samhällsviktiga verksamheter måste stärkas och det snabbt. För att kunna arbeta systematiskt måste cybersäkerhetsarbetet prioriteras och tilldelas resurser.

Övriga centrala iakttagelser och slutsatser sammanfattas kortfattat nedan.

1. Svarsfrekvensen hos offentlig förvaltning har minskat för varje mättillfälle. Utifrån det säkerhetspolitiska läget och vikten av ökad motståndskraft behöver deltagandet istället öka. Ju fler organisationer som deltar, desto bättre samlad bild får MSB av den nationella cybersäkerhetsnivån. Vidare bidrar ökat deltagande också till att säkerställa att de rekommendationer som utfärdas blir träffsäkrare.
2. Precis som i mätningen 2023 rapporterades det in så få svar från näringslivet, särskilt NIS-leverantörer, att dessa inte kunde inkluderas i resultatredovisningen. När Cybersäkerhetslagen träder i kraft kommer den stora majoriteten av samhällsviktiga verksamheter inom cyberdomänen att utgöras av NIS-leverantörer. För att MSB ska kunna ta fram en samlad nationell lägesbild över cybersäkerhetsnivån i Sverige måste denna grupp delta aktivt i relevanta cybersäkerhetsmätningar såsom Cybersäkerhetskollen.
3. 5,2 procent av alla deltagande organisationer uppnådde nivå 3 eller 4 i modellen. Nivå 3, kvalificerat innehåll, har MSB även 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. I Infosäkkollen 2024 uppfyller 8 av 120 myndigheter nivå 3.
4. Deltagande organisationer presterar bäst inom de arbetsområden i Infosäkkollen som ligger närmast it-säkerhetsarbetet. Det är i linje med de resultat MSB noterat i tidigare mätningar. Samtidigt bör dessa bättre resultat förstås utifrån kontexten att helhetsresultatet på Infosäkkollen 2024 visar på brister inom andra arbetsområden, varför det finns utvecklingspotential även här.
5. De arbetsområden där minst antal deltagande organisationer klarat nivå 1 i modellen är 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 2024 jämfört med 2023 inom arbetsområdena för Uppföljning och utvärdering (19,3 procent), Medarbetarnas kunskaper och utbildningsverksamhet (18,8 procent) och Upprättande och utveckling av säkerhetskultur (16,2 procent).

7. Bland de organisationer som deltog vid båda mättillfällena syns minst förbättring 2024 jämfört med 2023 inom arbetsområdena för Upphandling (9,9 procent) och Ledningens styrning och kontroll samt Informationsklassning (båda 10,1 procent).
8. Deltagande kommuner är genomgående den aktörsgrupp som har svagast resultat. Myndigheterna är den aktörsgrupp som genomgående presterar bäst.
9. En typförvaltning 2024 har genomfört 16,3 procent fler åtgärder än typförvaltningen 2023. 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 såväl inom som mellan aktörsgrupperna. 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 2024

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.

256 organisationer från offentlig förvaltning deltog i it-säkkollen 2024, vilket utgör 46,7 procent av offentlig förvaltning. Av dessa var 131 kommuner, 11 regioner och 114 myndigheter. Jämfört med 2023 har deltagandet sjunkit med 2,2 procentenheter. Antalet deltagande kommuner minskade mellan mättillfällena med 6,4 procent och antalet regioner med 38,9 procent. Däremot var det 4,6 procent fler myndigheter som deltog 2024 jämfört med 2023.

Resultatet i It-säkkollen 2024 motsvarade nästan nivå 3 av 4 i modellen, vilket motsvarar ”visst skydd”. Resultatet i It-säkkollen 2024 är 2,7 procent bättre än föregående års mätning. Det är fortsatt 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 oftast har tillgång till 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 ofta saknar samma mandat som en it-chef ofta 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 2024 påvisar att organisationerna, relativt sett, är bättre på de arbetsområden som kan ha större betydelse för att säkra organisationens it-miljö, nämligen Analys och hantering av informationssäkerhetsrisker, Informationsklassning samt Säkerhetsåtgärder och förbättringsarbete. Det förklarar också varför resultatet från It-säkkollen 2024 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.

De arbetsområden där offentliga förvaltningar presterar bäst är Skydd av utrustning och it-utrymmen, Behörighetshantering samt Skydd och övervakning av nätverk och informationssystem. De arbetsområden där offentliga förvaltningar presterar svagast är Förutsättningar för systematiskt it-säkerhetsarbete, Kryptering och Redundans och återställning.

Majoriteten av offentlig förvaltning uppger att de utkontrakterat en betydande andel av sin it-drift. Vidareutvecklingen av It-säkkollen[9] 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.

Resultatspridningen visar på en förhållandevis stor skillnad mellan de starkaste och svagaste tio procenten, men sammantaget tyder svarsfördelningen på att arbetet har nått längre. Resultatspridningen var som minst för arbetsområdet Redundans och återställning, och som mest för arbetsområdet för Kryptering.

En viss förbättring har skett hos samtliga aktörsgrupper mellan de två mättillfällena. Att kommuner och myndigheter, de två större populationerna, utvecklats i ungefär samma takt är rimligt utifrån att de hade liknande resultat såväl 2023 som 2024.

Att resultatet 2024 ligger så nära resultat från 2023, trots förändringarna i populationen[10], antyder att it-säkerhetsarbetet bedrivs på en relativt likvärdig nivå för alla offentliga förvaltningar. Det antyder också att relativt få nya åtgärder implementerats mellan de två tillfällena.

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 tidigare mätningar, resursbrist som det främsta hindret för utvecklingsarbetet. Enkätundersökningen, som genomfördes med deltagande organisationer efter inrapportering, stärker detta ytterligare. MSB instämmer i bedömningen att många organisationer, i synnerhet många kommuner, behöver mer resurser.

Not 9. För information om vidareutvecklingen av It-säkkollen se 3.4.

Not 10. Färre kommuner, som är den generellt svagaste aktörsgruppen, och fler myndigheter, som är den starkast aktörsgruppen, deltog i It-säkkollen 2024 jämfört med 2023.

MSB:s bedömning är att förändringstakten inte motsvarar behovet, särskilt inte utifrån det rådande säkerhetspolitiska läget. Avsaknaden av väsentliga förbättringar inom de områden som lyftes fram redan år 2021 innebär att rekommendationer från tidigare mätningar kvarstår. Sveriges motståndskraft behöver höjas och det omgående.

MSB bedömer att organisationsledningarna hos samhällsviktiga verksamheter behöver öka sitt engagemang för cybersäkerhetsarbetet. För att höja nivån i den utsträckning som krävs för att kunna garantera säkerhet och tillförlitlighet i samhällsviktiga tjänster, måste resurser tillföras. It-incidenter är dessutom kostsamma och ur ett samhällsperspektiv är det 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 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[11] (kommuner, regioner och myndigheter) bör ha möjlighet att hitta andra organisationer som de kan samarbeta med.[12] 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 2024 är myndigheterna den mest heterogena gruppen, som alltså har störst potential för denna typ av samverkan, följt av kommunerna och sist regionerna.

Utifrån analysen av Infosäkkollen 2024 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.

Not 11. MSB har gjort antagandet att det är enklare, och ibland mer givande, att organisationer inom samma aktörsgrupp samarbetar.

Not 12. 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.

De är i synnerhet:

- uppföljning (i synnerhet uppföljning av utbildningsinsatser),
- undersökningar av medarbetarnas kunskaper,
- undersökningar av hinder och framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt, och
- kontinuitetshantering (i synnerhet övningar).

2.4 Rekommendationer

Det säkerhetspolitiska läget i Sverige och Europa har varit ansträngt i flera år och visar inga tecken på närstående förbättring. Vikten av att stärka totalförsvaret och samhällets motståndskraft har återkommande lyfts. Mot den bakgrunden kan inte de begränsade framsteg som framkommer av resultatet från Infosäkkollen 2024 gällande den offentliga förvaltningens systematiska cybersäkerhetsarbete betraktas som tillräckliga. MSB bedömer att förbättringstakten måste öka.

58,6 procent av samtliga organisationer som har rapporterat in sina resultat i Infosäkkollen 2024 saknar de mest grundläggande delarna i ett systematiskt cybersäkerhetsarbete. 8 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[13]. Det har funnits, i olika versioner, sedan 2009. Totalt nådde 14 av 268 organisationer (5,2 procent) nivå 3, kvalificerat innehåll, i Infosäkkollen 2024.

Rekommendationerna nedan grundar sig på de samlade slutsatserna från analysen av Cybersäkerhetskollen 2024 och de brister som har noterats i samband med mätningen. Alla svarande kommuner, regioner och myndigheter har inte alla de listade bristerna, men ett stort antal organisationer har flera av dem.

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. Resultatet från Infosäkkollen 2024 visar också att de organisationer som arbetar systematiskt och inrapporterar återkommande utvecklas såväl bättre som snabbare.

Not 13. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

2.4.1 Rekommendationer till regeringen

Inom ramen för redovisningen rekommenderar MSB att regeringen överväger:

1. att ge i uppdrag till tillsynsmyndigheterna att anvisa organisationer som omfattas av NIS-reglering att använda Cybersäkerhetskollen för att sedan kunna använda inrapporterade resultat som urval för val av tillsynsobjekt.
2. en särskild satsning inom ramen för arbetet med civilt försvar avseende finansiering till stöd för små och medelstora företag som har genomfört Cybersäkerhetskollen eller som utvecklar tjänster som adresserar bristerna som redovisningen av Cybersäkerhetskollen lyfter. En sådan satsning skulle komplettera den satsning som nu görs på offentliga aktörer inom det civila försvaret. Stöd till små och medelstora privata aktörer kan kanaliseras genom NCC-SE vid MSB.
3. om det bör införas ett särskilt mål i den nationella cybersäkerhetsstrategin om att alla organisationer som bedriver samhällsviktig verksamhet senast 2030 ska ha uppnått nivå 3 i Cybersäkerhetskollen.

Gällande punkt ett skulle MSB samverka med tillsynsmyndigheterna om en modell för hur resultat i Cybersäkerhetskollen ska användas, så att inrapporterade resultats korrekthet säkerställs.

2.4.2 Rekommendationer till offentlig förvaltning

Inom detta stycke avhandlas de rekommendationer som gäller samtliga organisationer inom offentlig förvaltning.

Samtliga organisationer som genomfört Cybersäkerhetskollen 2024 har ett erbjudande om att kontakta Cybersäkerhetsrådgivningen för uppföljningssamtal om sitt eget resultat och få särskild stöttning kring sitt vidareutvecklingsarbete. Cybersäkerhetsrådgivningen är en funktion på MSB som stödjer det förebyggande arbetet och underlättar för en organisation att anpassa cybersäkerhetsarbetet till den specifika verksamheten.[14]

Då resultatet för Infosäkkollen 2024 i hög utsträckning liknar resultatet från 2021 och 2023 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 för bristande förbättringsarbete. 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

Not 14. Kontakta Cybersäkerhetsrådgivningen via: https://www.msb.se/sv/verktyg--tjanster/cybersakerhetsradgivning/.

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 ett starkare engagemang för att identifiera, analysera och hantera risker samt 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 stärka 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 rekommendationer 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.[15]
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 Cybersäkerhetskollen. Då får ni reda på hur långt ni kommit med ert systematiska cybersäkerhetsarbete. Be om en resultatredovisning.

2.4.3 Rekommendationer till kommunerna

En majoritet av deltagande kommuner i Infosäkkollen, 70,6 procent, uppnår inte nivå 1. Motsvarande siffra 2023 var 76,5 procent. Även om resultatet visar på viss utveckling inom aktörsgruppen sedan mätningen 2023, är det en blygsam förbättring sett utifrån den låga grundnivån. Rekommendationerna från 2021 och 2023 bedöms därmed vara av fortsatt relevans:

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

Not 15. https://www.msb.se/sv/publikationer/ledningens-roll-inom-informationssakerhet---stod-for-dig-med-en-ledande-funktion/.

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, eller
- 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 mer än 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, eller
- följts upp och utvärderats minst en gång.

Av de som har kontinuitetsplaner för sina olika verksamheter har ungefär fyra femtedelar övat arbetssätten i planerna, men bland de som har övat arbetssätt är det en minoritet som har övat kontinuitet i mer än 50 procent av verksamheterna. Bland de som har såväl ett arbetssätt för kontinuitetshantering såväl som genomfört övningar, är det drygt 40 procent som enbart övat arbetssättet i 0–25 procent av verksamheterna.

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 tvåårsperioden utbildat 0–25 procent av sina medarbetare i informationssäkerhet. Även om kommunen har undersökt om medarbetarna vet hur de ska göra för att arbeta på ett informationssäkert sätt, har man inte undersökt huruvida de tillämpar sina kunskaper i sitt arbete.

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. De 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 en majoritet av kommunerna 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. Hälften av kommunerna har under perioden inte heller följt upp resultatet av sitt systematiska informations- och cybersäkerhetsarbete genom att sammanställa och analysera antingen:

- resultatet av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete,
- resultatet av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt,
- skillnaden mellan införda och beslutade säkerhetsåtgärder,
- resultatet av genomförda informationsklassningar och analyser av informationssäkerhetsrisker, eller
- resultatet av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet.

Medan tre fjärdedelar av kommunerna har haft ett arbetssätt för att hantera informationssäkerhetsincidenter och avvikelser, svarar cirka 45 procent att arbetssättet inte omfattar analys av inträffade incidenter, deras grundorsaker och hantering eller återförande av erfarenheter till det förebyggande arbetet.

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

40 procent av kommunerna har under den senaste tvåårsperioden 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, eller
- 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

Regionernas resultat visar på en övergripande förbättring jämfört med mätningen 2023. Trots resultatförbättringen kvarstår emellertid liknande problematik, varför MSB bedömer att rekommendationerna från föregående år 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. Även om resultatet visar att regionerna har gjort insatser för att stärka informations- och cybersäkerhetskulturen i sina organisationer, kvarstår områden där förbättring är av stor vikt.

Det är positivt att de allra flesta av regionerna har undersökt om medarbetarna, efter genomförd utbildning i informationssäkerhet, vet hur de ska arbeta på ett informationssäkert sätt, samt om medarbetarna tillämpar sina kunskaper i sitt arbete. Hälften av kommunerna svarar att de emellertid inte har 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, eller
- vad medarbetarna ska göra om en informationssäkerhetsincident inträffar.

Att tre fjärdedelar av regionerna har undersökt vilka hinder och framgångsfaktorer som påverkar deras möjligheter att arbeta informationssäkert och som de möter i sin verksamhet är en ytterligare förbättring. I den grupp av regioner som undersökt detta, har dock majoriteten enbart undersökt hinder respektive framgångsfaktorer i arbetet hos 0–25 procent hos medarbetarna.

Hos en majoritet av regionerna har heller inte ledningen 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.

I fråga om att inventering av informationsmängder och informationssystem, inklusive nätverk, har typregionen under perioden gjort det i enbart 50–75 procent av organisationens verksamheter. Även om det är en förbättring jämfört med mätningen föregående år, är resultatet fortfarande lägre än de övriga 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.

Resultatet visar att typregionens arbetssätt för utbildning i informations- och cybersäkerhet innehåller flera viktiga inslag. Under den senaste tvåårsperioden har exempelvis regionerna i snitt utbildat 50–75 procent av sina medarbetare i informationssäkerhet, men samtidigt visar regionerna tydliga brister gällande uppföljningen, exempelvis har regionerna inte i tillräcklig utsträckning undersökt om medarbetarna använder sina kunskaper efter genomförd utbildning.

4. Följ upp fler av säkerhetsåtgärderna och om de informationssäkerhetskrav som har ställts vid upphandling efterföljs.
En majoritet av regionerna har följt upp både analys och hantering av informationssäkerhetsrisker samt hantering av informationssäkerhetsincidenter och avvikelser under de senaste två åren. Därutöver har en majoritet, åtminstone på några punkter, följt upp resultatet av sitt systematiska informationssäkerhetsarbete.

Uppföljningen uppvisar dock vissa brister. Hälften av regionerna har utvärderat om införda säkerhetsåtgärder har varit ändamålsenliga i mindre än 50 procent av regionens verksamheter. En fjärdedel har utvärderat enbart 0–25 procent av implementerade säkerhetsåtgärder.

Tre fjärdedelar av regionerna har heller inte följt upp huruvida de krav som ställdes i samband med upphandlingar var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

2.4.5 Rekommendationer till myndigheterna

Även om myndigheterna har det starkaste resultatet jämfört med övriga två aktörsgrupper och dessutom förbättrats sedan föregående mätning, finns det stort utrymme för förbättring. Enbart sju procent av myndigheterna nådde den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet. MSB:s bedömning är därför att rekommendationerna från 2021 och 2023 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. Strax under hälften av samtliga deltagande myndigheter i Infosäkkollen 2024 nådde inte ens modellens första nivå, och bedöms således vara förhållandevis långt från att nå upp till de krav som de omfattas av.

2. Stärk ledningens engagemang i det systematiska informations- och cybersäkerhetsarbetet.
En majoritet av de svarande myndigheterna anger att de i flera avseenden har en ledning som aktivt deltar i det systematiska informationssäkerhetsarbetet, vilket är positivt. Ledningens styrning och kontroll hör emellertid till ett av de arbetsområden där myndigheterna presterar svagare, och få framsteg har gjorts inom detta område sedan såväl år 2021 som år 2023. 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.

75 procent av myndigheterna har under den senaste tvåårsperioden haft ett arbetssätt för kontinuitetshantering. Men inom denna grupp har en tredjedel enbart övat arbetssättet inom 0–25 procent av organisationens verksamheter. Ytterligare en femtedel har inte övat arbetssättet överhuvudtaget.

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.

85 procent av myndigheterna uppger att de under den senaste tvåårsperioden haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker. Arbetssättet har också tillämpats i hög grad, och omfattat flera av de delar som är viktiga för en välfungerande riskhantering. Typmyndighetens arbetssätt på området brister dock avseende värdering av riskers sannolikhet och centrala delar i en ordnad riskhanteringsprocess.

Hos den överhängande majoriteten hos myndigheterna har dock inte arbetssättet för analys och hantering av informationssäkerhetsrisker under de senaste två åren 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, eller
- 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.

För en majoritet av myndigheterna har arbetssätt för riskhantering under de senaste två åren omfattat att:

- varje identifierad informationssäkerhetsrisk har en riskägare,
- 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), och
- status för informationssäkerhetsrisker följs upp utifrån definierade intervall.

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

De allra flesta myndigheter har under den senaste tvåårsperioden undersökt medarbetarnas kunskap inom informations- och cybersäkerhet. Under perioden har cirka sextio procent av myndigheterna också utbildat fler än tre fjärdedelar av sina medarbetare i ämnet, vilket för merparten av myndigheterna har efterföljts av en undersökning om huruvida medarbetarna vet hur de ska arbeta på ett informationssäkert sätt. Myndigheterna har dock i lägre utsträckning undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

6. Följ upp arbetet och de utkontrakterade tjänsterna.

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

Majoriteten av 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,
- resultatet av genomförda informationsklassningar och analyser av informationssäkerhetsrisker, eller
- resultatet av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet.

I de allra flesta av 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.

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:

Cybersäkerhetsrådgivningen: Stödjer det förebyggande arbetet och underlättar för en organisation att anpassa cybersäkerhetsarbetet till den specifika verksamheten. Samtliga som genomfört Cybersäkerhetskollen 2024 har ett erbjudande om att kontakta Cybersäkerhetsrådgivningen för uppföljningssamtal om sitt eget resultat och få särskild stöttning kring sitt vidareutvecklingsarbete.[16]

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

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 gjordes en översyn av konceptet och det kommer att göras tillgängligt för personer i ledande befattningar inom alla samhällsviktiga verksamheter. 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 Cybersäkerhetskollen 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 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.

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

Not 16. Kontakta Cybersäkerhetsrådgivningen via: https://www.msb.se/sv/verktyg--tjanster/cybersakerhetsradgivning/.

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

Utifrån resultatet konstateras att det behöver tillföras mer resurser till det systematiska cybersäkerhetsarbetet för att höja cybersäkerhetsnivån hos samhällsviktiga verksamheter. Mer behöver göras, men mer behöver också göras effektivare, 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 offentliga förvaltningar att tillsammans se över möjligheterna att samarbeta kring nya sätt att lösa de uppgifter som ingår i det systematiska cybersäkerhetsarbetet, samt att analysera i vilka delar av säkerhetsarbetet de skulle kunna ha särskild nytta av externt stöd.

De nedanstående områdena 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 medarbetarnas möjligheter att arbeta på ett informationssäkert sätt,
- kontinuitetshantering (i synnerhet övningar).

2.6.1 Områden där kommunerna behöver stöd

Följande frågor i Infosäkkollen 2024 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 16**: De senaste två åren, har organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 20**: Har organisationen, de senaste två åren, klassat sin information enligt sitt arbetssätt för informationsklassning?
- **Fråga 21**: De senaste två åren, har organisationen analyserat sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker?
- **Fråga 22**: De senaste två åren, har organisationen använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker?
- **Fråga 23**: De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?
- **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 2024 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 5**: Har organisationen de senaste två åren undersökt medarbetarnas kunskaper om informationssäkerhet?
- **Fråga 22:** De senaste två åren, har organisationen använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker?
- **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 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 2024 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 27:** Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 35:** De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala typer av sannolikhetsbedömning?

Hur resultatet tagits fram

3. Hur resultatet tagits fram

Cybersäkerhetskollen omfattar två mätningar, Infosäkkollen och It-säkkollen. Nedan beskrivs de två mätningarna var för sig.

3.1 Om Infosäkkollen

Det ena målet med Infosäkkollen är att ge den offentliga förvaltningens organisationer stöd i att följa upp sitt systematiska informationssäkerhetsarbete. 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 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.

MSB har dessutom ett återkopplingsverktyg för Infosäkkollen, 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. Mätningen 2024 ligger utanför tvåårsintervallet och genomfördes utifrån en justering i MSB:s regleringsbrev för 2024.[17]

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

Not 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).

MSB:s bedömning av 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 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 Illustration över

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

Not 18. Närmast föreskrifterna om informationssäkerhet för statliga myndigheter, MSBFS 2020:6.

Not 19. https://www.msb.se/cybersakerhetskollen.

3.1.1 Om analysunderlaget

Denna rapport är baserad på svaren som MSB fick ta del av under den tredje inrapporteringen av Infosäkkollen, som genomfördes från april till september 2024. Jämförelser görs med de svar som MSB fått inrapporterade från tidigare mätningar 2021 och 2023.

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 verifiera att inrapporteringen gått rätt till.

Hur verktyget använts och hur arbetet med att besvara frågorna gått till har utvärderats efter varje mättillfälle. Enkätundersökningen 2024 besvarades av 165 organisationer från offentlig förvaltning, vilket representerar drygt 62 procent av svarsunderlaget i Infosäkollen. Av dessa svarade nästan 82 procent att Infosäkkollen är värdefull för sin organisations informations- och cybersäkerhetsarbete. Cirka 73 procent uppgav att de genomför Infosäkkollen i egen regi årsvis eller mer frekvent än så. Mer information om enkätundersökningens resultat återfinns i kapitel 4.1.7.

3.1.1.1 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.

3.1.2 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.

3.1.2.1 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.

3.1.2.2 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.

3.1.2.3 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 tydligt sätt.

3.2 Om It-säkkollen 2024

It-säkkollen är framtagen i enlighet med regeringsuppdraget Fö2023/00697 som uppdrogs MSB 23 mars 2023. It-säkkollen genomfördes, som en del av Cybersäkerhetskollen, för andra gången 3 april 2024. It-säkkollen är en enkät med 41 frågor där respondenten självskattar 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.

Resultat av Infosäkkollen 2024

4. Resultatet av Infosäkkollen 2024

I det här kapitlet redogörs för resultatet i Infosäkkollen 2024 för alla organisationer i offentlig förvaltning och hos de olika aktörsgrupperna, det vill säga kommuner, regioner och myndigheter.

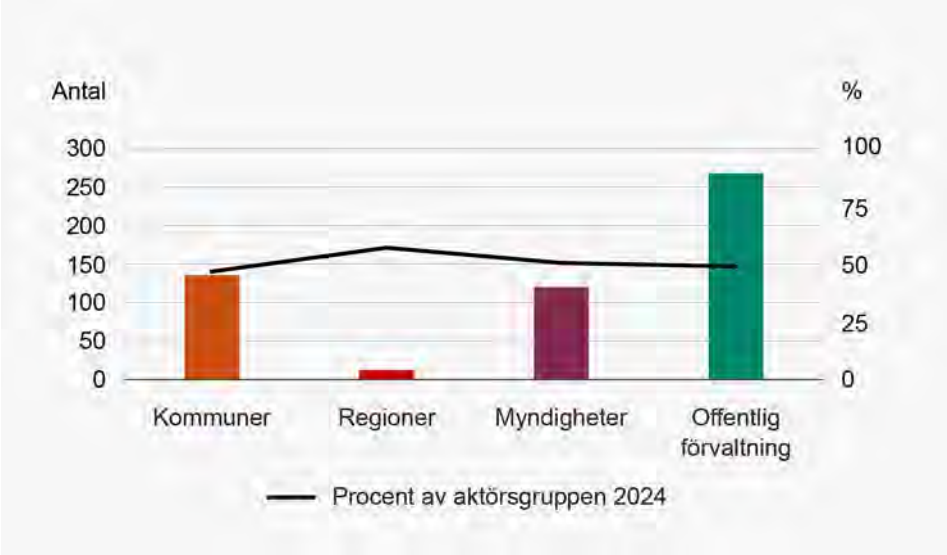
4.1 Offentlig förvaltning

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

4.1.1 Deltagande

48,9 procent av organisationerna inom offentlig förvaltning deltog i Infosäkkollen 2024.[20] Vid de två tidigare mättillfällena (2021 och 2023) har en majoritet av de offentliga förvaltningarna deltagit. Deltagarfrekvensen 2024 är högst inom aktörsgruppen regioner (57,1 procent), följt av myndigheter (50,6 procent) och till sist kommuner (46,9 procent). Samtidigt är underlaget omfattande nog för att resultaten med säkerhet kan extrapoleras för slutsatser och rekommendationer.

Diagram 1. Deltagande i Infosäkkollen 2024

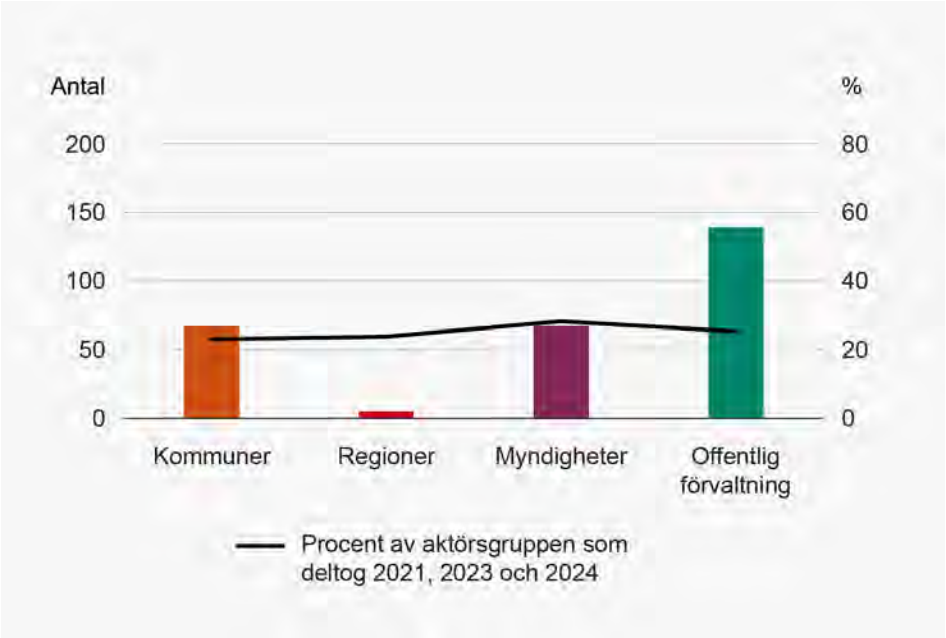


Not 20. Domstolsverket har rapporterat in ett svar för alla domstolars räkning.

Deltagarantalet hos offentlig förvaltning 2024 har sjunkit med 4,4 procentenheter jämfört med 2023, och 6,2 procentenheter jämfört med 2021. Jämfört med 2023 har deltagandet bland kommuner minskat med 5,9 procentenheter, och bland regionerna har deltagandet minskat med hela 28,6 procentenheter. Antalet myndigheter är oförändrat då exakt 120 myndigheter deltog såväl 2023 som 2024.

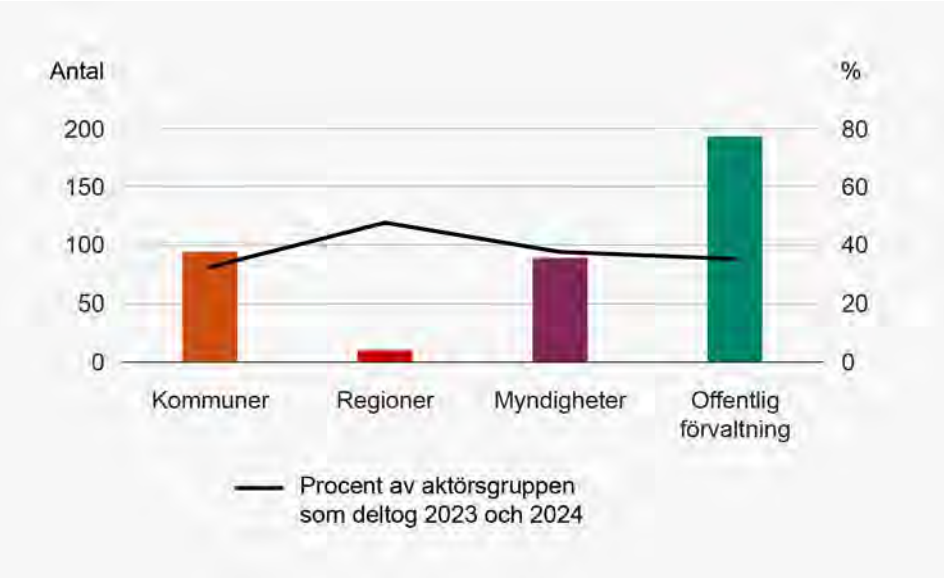
Kommuner är alltjämt den största aktörsgruppen i Infosäkkollen. Det minskande antalet kommuner mellan mätningarna 2023 och 2024, 17 färre kommuner, samtidigt som antalet myndigheter är exakt samma, får dock en stor påverkan på populationen och det sammantagna resultatet för offentliga förvaltningar i Infosäkkollen 2024. Detta beror på att kommunerna är den aktörsgrupp som presterar svagast i Infosäkkollen, medan myndigheter presterar bäst. När populationen, kompositionen utifrån typen av deltagande organisationer, förändras påverkar det jämförbarheten mellan mätningarna. Det är en viktig faktor för förståelsen kring hur Infosäkkollens resultat 2024 ska förstås, särskilt när jämförelser görs med resultat från tidigare års mätningar.

Diagram 2. Organisationer som deltog både 2021, 2023 och 2024



139 organisationer har inrapporterat sina svar till MSB vid samtliga tre mättillfällen. Dessa utgör tillsammans cirka en fjärdedel av alla organisationer i den offentliga förvaltningen. Bland kommuner och regioner har cirka 23 procent av alla organisationer inom respektive aktörsgrupp deltagit alla tre gånger, medan motsvarande siffra för myndigheter är 28,3 procent.

Diagram 3. Organisationer som deltog både 2023 och 2024



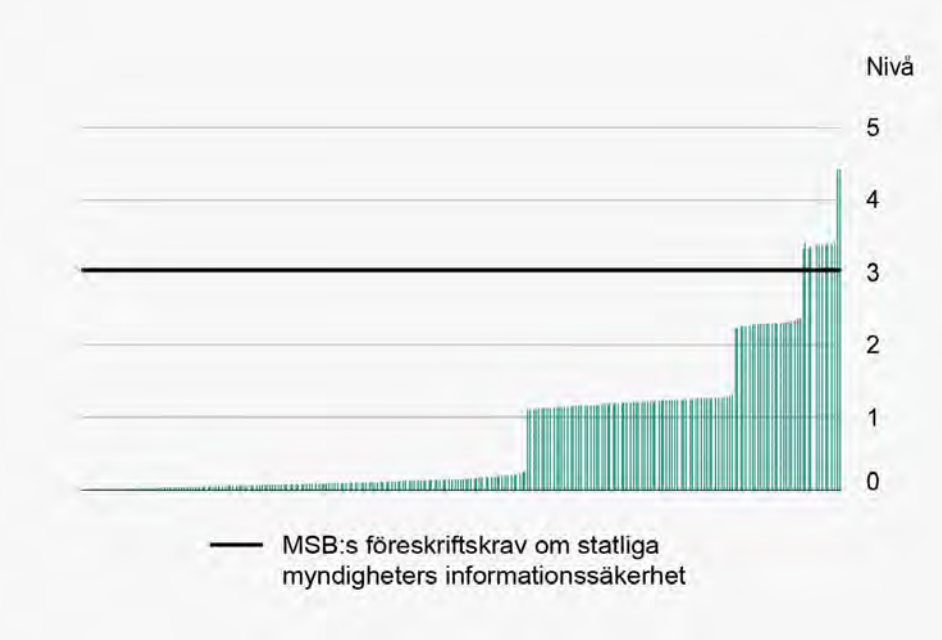
193 organisationer deltog såväl 2023 som 2024, vilket motsvarar 72 procent av alla organisationer som deltog i Infosäkkollen 2024. 69,1 procent av alla kommuner som deltog 2024 deltog även 2023. Motsvarande siffra för regioner var 83,3 procent, och för myndigheter 74,2 procent.

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.

111 organisationer, 41,4 procent, uppnådde nivå 1 eller högre i Infosäkkollen 2024. Nivå 1 i Infosäkkollen motsvarar att man har de grundläggande inslagen i ett systematiskt informations- och cybersäkerhetsarbete på plats. Det betyder samtidigt att 58,6 procent av alla deltagande organisationer inte uppnår nivå 1 i modellen. Jämförbar siffra 2023 var 69,4 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. Resultattal för samtliga 268 organisationer



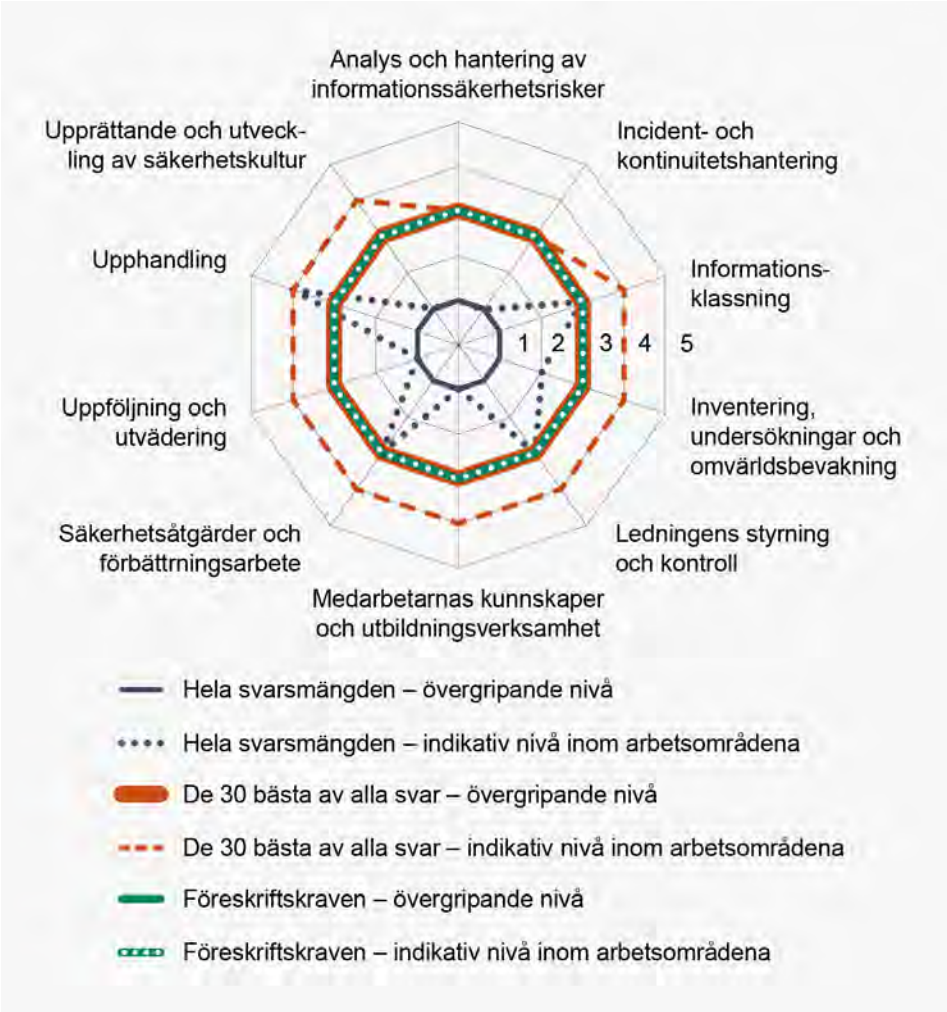
Den svarta linjen i diagrammet motsvarar den nivå som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet.

41,4 procent av deltagande organisationer uppnådde alltså nivå 1 eller bättre, 14,2 procent uppnådde nivå 2 eller bättre, och 5,2 procent uppnådde nivå 3 eller 4 i modellen. I 2023 års mätning hade 30,6 procent av deltagande organisationer uppnått nivå 1 eller bättre, 10,3 procent klarade nivå 2 eller bättre, och 2,8 procent nådde upp till nivå 3 eller 4 i modellen. Det är alltså en betydande större andel organisationer som klarat av nivå 1 2024 jämfört med 2023, en ökning med 29,1 procentenheter. Även om det är fler organisationer som uppnått nivå 2, samt nivå 3 eller 4, så är de ökningarna blygsammare med 3,1 respektive 2,4 procentenheter.

4.1.3 Utfall per arbetsområde

Benchmarken för hela svarsmängden visar att typförvaltningen uppnår nivå 1 i modellen. 2024 är första mättillfället där det uppnås. Den indikativa nivån påvisar också att typförvaltningen klarar nivå 3 på fyra arbetsområden. Att den indikativa nivån för arbetsområdet Ledningens styrning och kontroll uppnår nivå 3 är särskilt beaktansvärt, men i nedan redogörelse kommer det visa sig att det delvis beror på att det är det enskilda arbetsområdet med störst resultatspridning, såväl inom arbetsområdet som mellan aktörsgrupperna. Ledningens styrning och kontroll är fortfarande det arbetsområde där minst antal organisationer uppnått nivå 1.

Diagram 5. Resultat i Infosäkkollen för offentlig förvaltning



De arbetsområden där flest deltagande förvaltningar uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete (97,4 procent), följt av Informationsklassning (82,8 procent) och därefter Medarbetarnas kunskaper och utbildningsverksamhet (75 procent). Minst antal deltagande förvaltningar har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll (52,6 procent), följt av Uppföljning och utvärdering (56,7 procent) samt Incident- och kontinuitetshantering (65,3 procent).

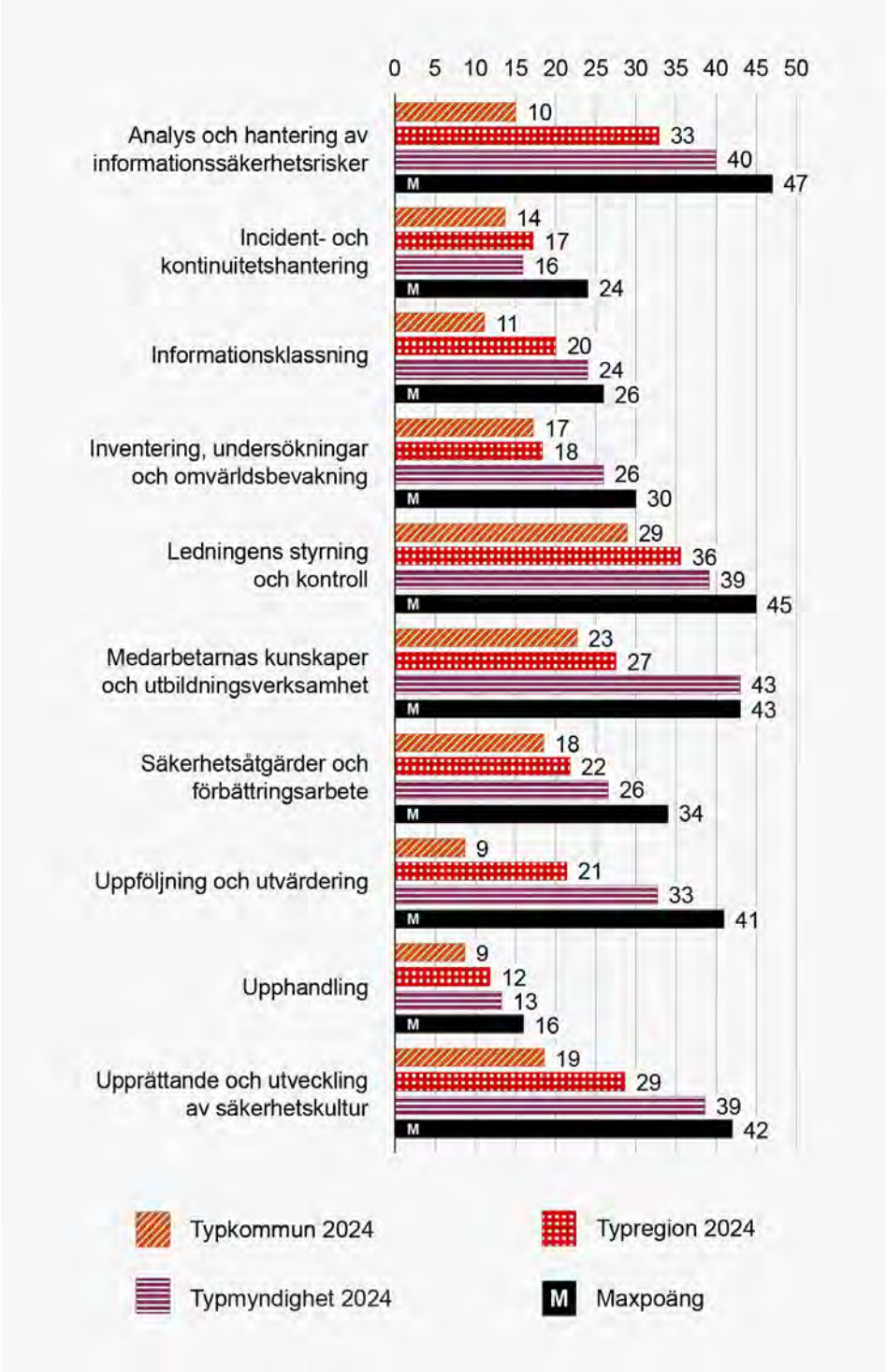
De arbetsområden där flest deltagande förvaltningar uppnått nivå 3 eller bättre är inom Upphandling (41,4 procent), följt av Informationsklassning (36,2 procent) och därefter Inventering, undersökningar och omvärldsbevakning (25,7 procent). Minst antal deltagande förvaltningar har nått nivå 3 eller bättre inom arbetsområdet för Uppföljning och utvärdering (11,6 procent), följt av Incident- och kontinuitetshantering (12,7 procent), samt Analys och hantering av informationssäkerhetsrisker (13,1 procent).

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, samt Incident- och kontinuitetshantering.

4.1.4 Generella resultat

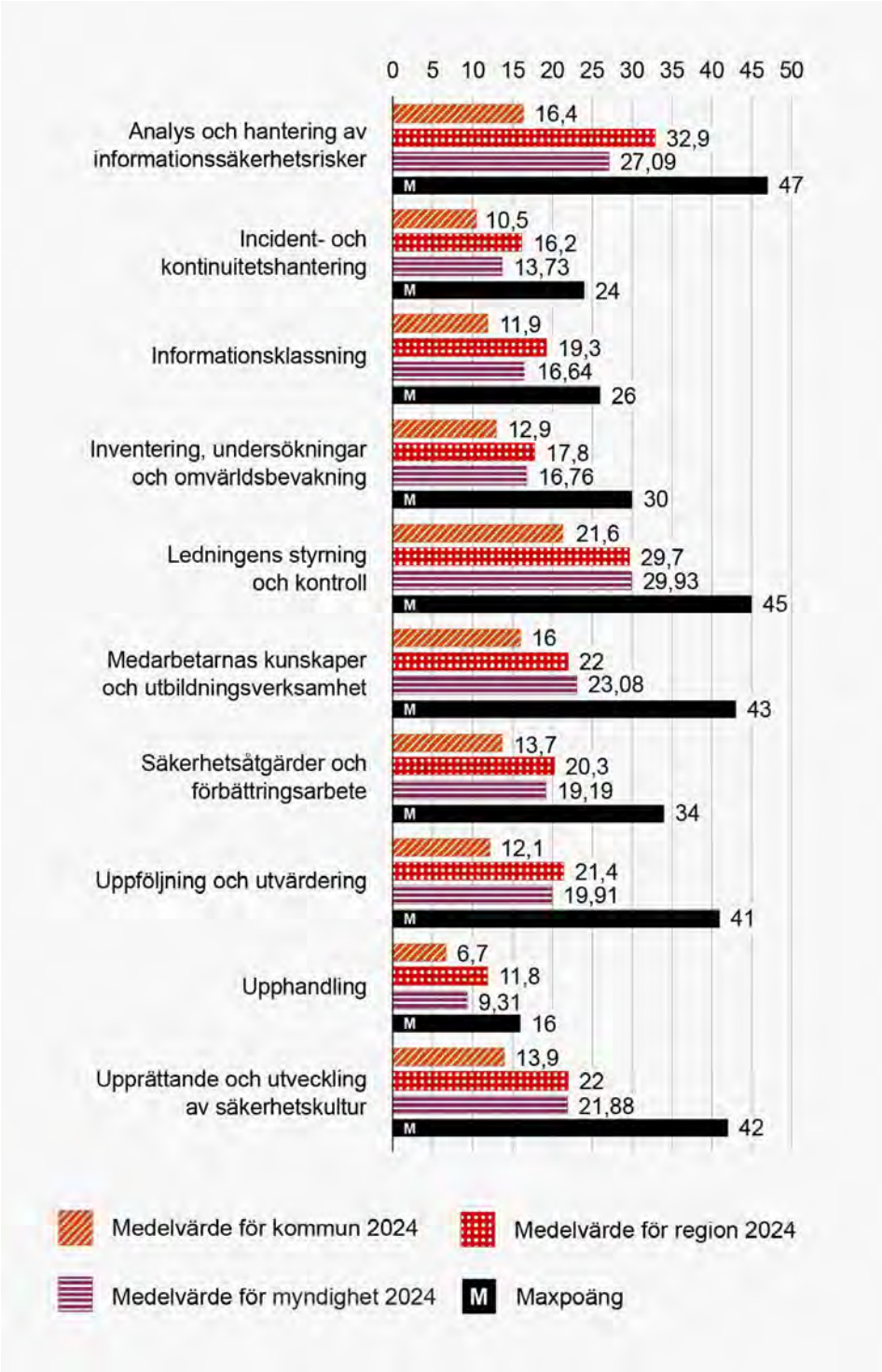
Med generella resultat avses uträkningar utifrån en aktörsgrupp och dess resultat.

Diagram 6. Antal genomförda åtgärder per arbetsområde för alla aktörsgrupper



Deltagande kommuner är den aktörsgrupp med svagast resultat i samtliga arbetsområden. Myndigheterna är bäst inom alla arbetsområden förutom Incident- och kontinuitetshantering där regionerna är bättre.

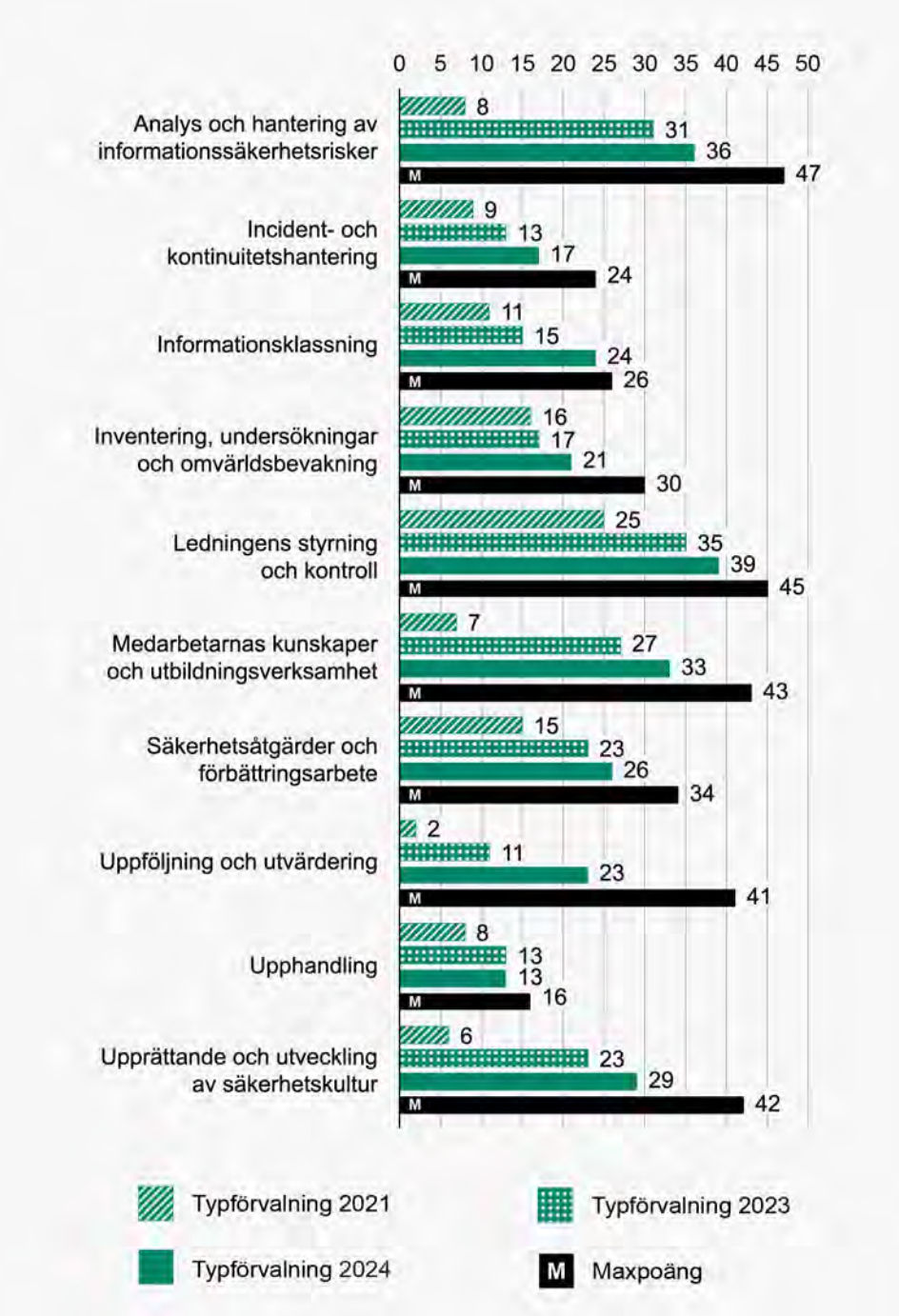
Diagram 7. Antal genomförda åtgärder per arbetsområde för alla aktörsgrupper utifrån medelvärdet



Till skillnad från diagram 6 ovan, som är baserat på majoritetssvaret på varje enskild fråga för att skapa en typaktör inom aktörsgruppen, så redovisar diagram 7 varje aktörsgrupps resultat i varje arbetsområde utifrån medelvärdet inom aktörsgruppen. Skillnaderna mellan diagrammen beror på den omfattande resultatspridningen bland kommuner och myndigheter. Att de

allra flesta deltagande organisationer har så pass svaga resultat får effekt på beräknade medelvärden. Regionerna, som är en mindre och mer homogen grupp, har en högre lägstanivå. Detta avspeglas i att den aktörsgruppen utifrån sitt medelvärde presterar bättre än myndigheterna på åtta arbetsområden.

Diagram 8. Antal genomförda åtgärder per arbetsområde 2021, 2023 och 2024 för offentlig förvaltning



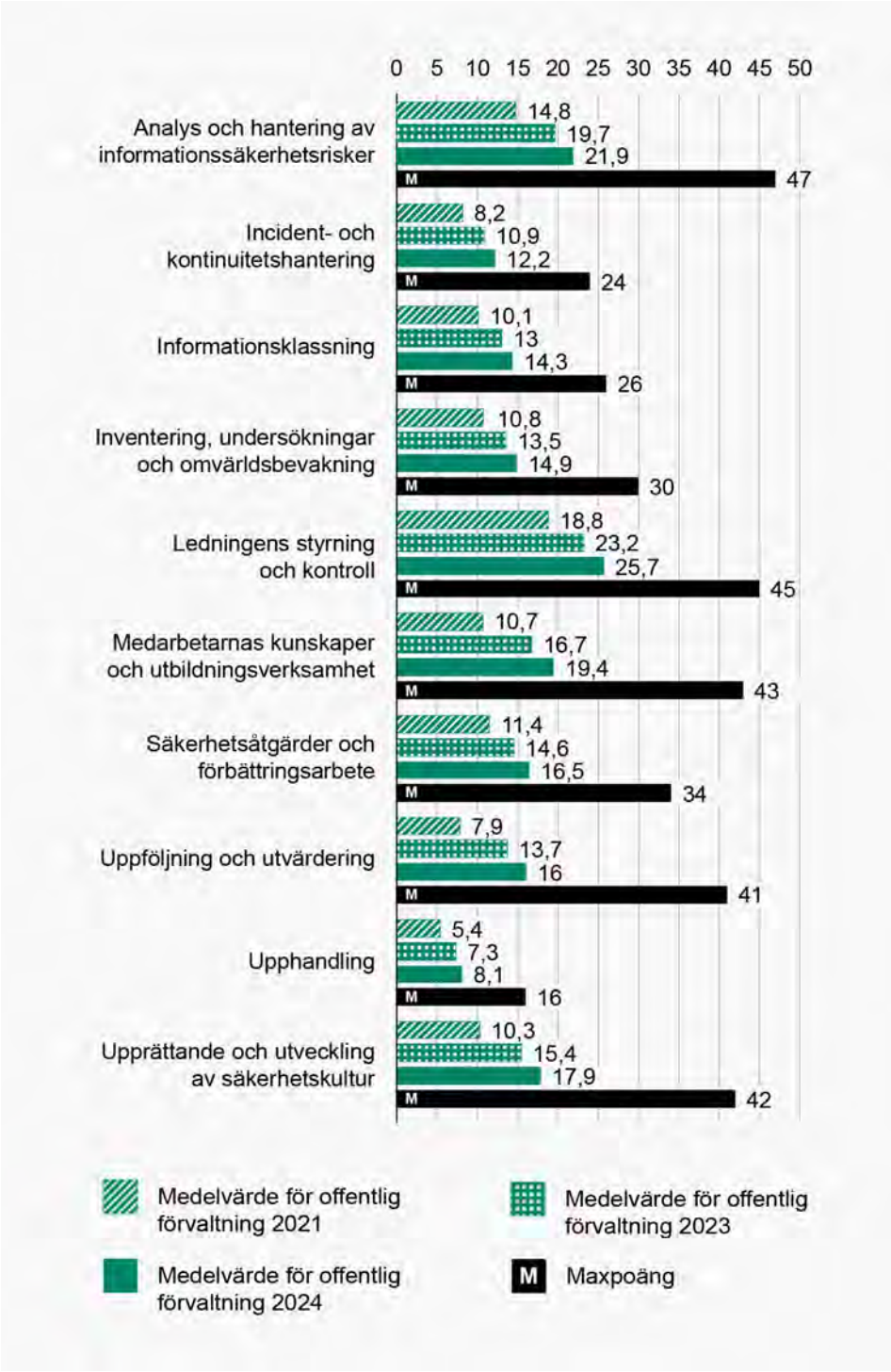
Ovan diagram är baserat på benchmarks för en typförvaltning. Vissa resultat kan antyda att en högre nivå i modellen borde uppnåtts. Det förklaras av att arbetssätt kan finns på plats i större utsträckning, samt innehålla ändamålsenliga inslag, men endast tillämpas i begränsad utsträckning. Detta tar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

I de flesta arbetsområden syns en omfattande förbättring 2024 jämfört med resultatet från 2021. Störst förbättring 2024 jämfört med 2021 ses för arbetsområdena för Analys och hantering av informationssäkerhetsrisker, Medarbetarnas kunskaper och utbildningsverksamhet, samt Upprättande och utveckling av säkerhetskultur. De arbetsområden med störst förbättring 2024 jämfört med 2023 är Uppföljning samt utvärdering och Informationsklassning.

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 2024 jämfört med både 2023 och 2021, men alltjämt tillämpas endast i begränsad utsträckning. Detta eftersom typförvaltningen 2024 fortfarande inte klarar åtgärderna som undersöks på nivå 2 i modellen. Det omvända gäller arbetsområdet för Ledningens styrning och kontroll där ovan diagram visar på en relativt liten förbättring 2024 jämfört med 2023, men där diagram 5 påvisade att typförvaltningen uppnått nivå 1 i mätningen, och indikativ nivå 3.

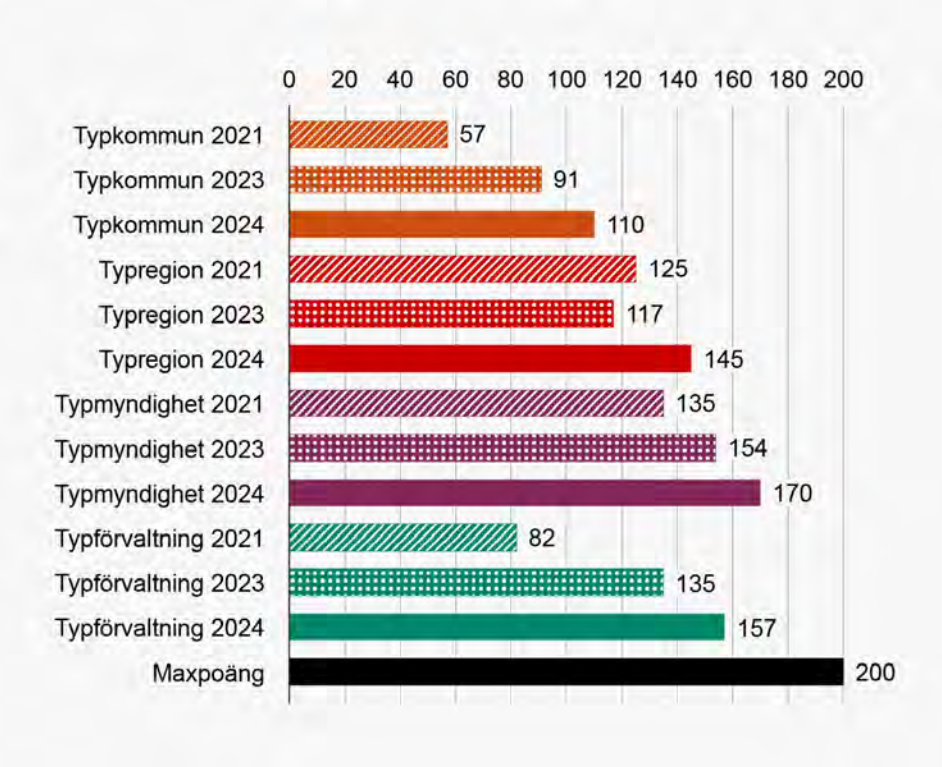
Minst förbättring från de två senaste mättillfällena gäller för arbetsområdena för Upphandling, som år 2023 var det arbetsområde där typförvaltningen presterade starkast, samt Säkerhetsåtgärder och förbättringsarbete.

Diagram 9. Antal genomförda åtgärder per arbetsområde 2021, 2023 och 2024 för offentlig förvaltning utifrån medelvärdet



Till skillnad från diagram 8, som är baserat på svaret från en typförvaltning under de olika åren, så redovisar Diagram 9 resultatet från varje mätning för varje arbetsområde utifrån medelvärdet inom aktörsgruppen. Skillnaderna mellan diagrammen beror på den omfattande resultatspridningen. Faktumet att de allra flesta deltagande organisationer har så pass svaga resultat påverker medelvärdet. Diagram 9 påvisar dock med ökad tydlighet behovet av att lägstanivån höjs hos den stora majoriteten av offentliga förvaltningar och att det inte sker i nödvändig takt.

Diagram 10. Totalt antal genomförda åtgärder per aktörsgrupp 2021, 2023 och 2024



En deltagande typförvaltning 2024 har genomfört 91,5 procent fler åtgärder än en typförvaltning 2021, och en deltagande typförvaltning 2024 har genomfört 16,3 procent fler åtgärder än en typförvaltning 2023.

Den aktörsgrupp som förbättrats mest 2024 jämfört med 2023 är regionerna, som höjt sig med 25,9 procent. 2023 deltog 18 av 21 regioner vilket påverkat resultatet och undersöks vidare i kapitel 4.3.

En typmyndighet har 2024 förbättrat sig med 10,4 procent jämfört med 2023, och en typkommun med 17,3 procent. Att en typkommun har en bättre förbättring än en typmyndighet förklaras delvis av utgångspunkten, det vill säga ett betydligt svagare resultat i tidigare mätning och därför fler möjliga åtgärder som kunde implementeras mellan mättillfällena.

Diagram 11. Totalt antal genomförda åtgärder per aktörsgrupp 2021, 2023 och 2024 utifrån medelvärdet

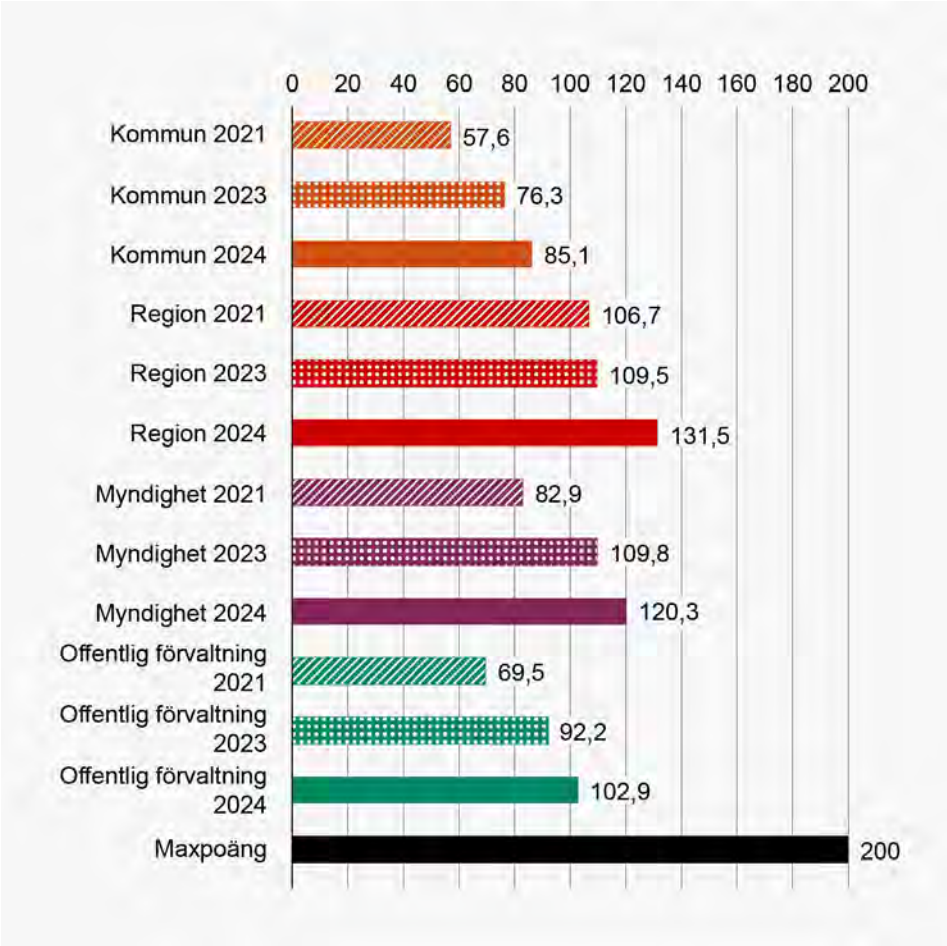


Diagram 11 redogör för den genomsnittliga mängden implementerade åtgärder för varje aktörsgrupp och år. Det är märkbart stor skillnad jämfört med typ-aktörens resultat. Detta förklaras återigen av en omfattande resultatspridning, där den svagt presterande majoriteten sänker medelvärdet och därmed resultatet för hela gruppen.

Diagram 12. Totalt antal genomförda åtgärder per aktörsgrupp bland de organisationer som enbart deltog 2023 eller 2024

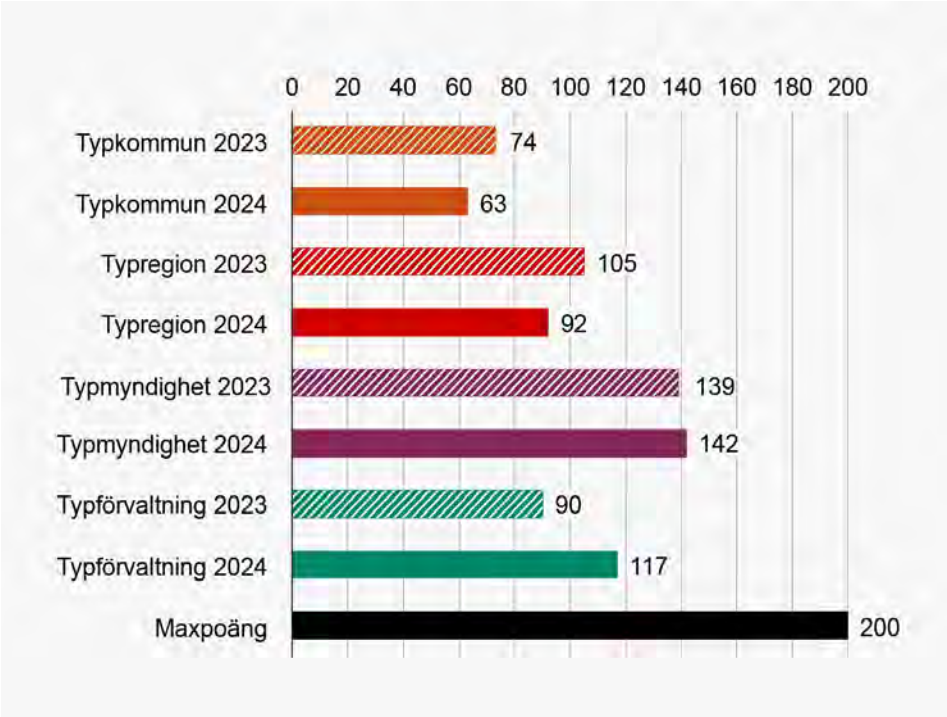


Diagram 12 visar resultatet för en typorganisation som deltog antingen 2023 eller 2024, men inte deltog vid båda mätningarna. Resultatet påverkas mycket av hur många organisationer i varje aktörsgrupp som endast deltog 2023 respektive 2024. År 2023 deltog 59 kommuner, 8 regioner och 31 myndigheter, totalt 98 organisationer som alltså inte inrapporterade sitt resultat 2024. 2024 tillkom 42 kommuner, 2 regioner och 31 myndigheter, totalt 75 organisationer som inte deltog 2023.

För typkommunen och typregionen har resultatet försämrats 2024 jämfört med 2023, vilket betyder att inom dessa aktörsgrupper så har de som endast deltog 2024 ett svagare resultat än de som endast deltog 2023. För typmyndigheten har resultatet förbättrats något.

Antalet deltagande organisationer inom de olika aktörsgrupperna påverkar utfallet. Det blir som mest synligt i resultatet för typförvaltningen 2024 jämfört med 2023. En typkommun och typregion har utfört fler åtgärder 2023 jämfört med 2024, men samtidigt har typförvaltningen infört färre åtgärder 2023 visavi 2024. Det förklaras av att det är betydligt fler kommuner som endast deltog 2023. Då kommunerna har svagast resultat drar det ner resultatet för typförvaltningen under den mätningen. Förändringen i populationen bör därför särskilt beaktas i förståelsen av typförvaltningens resultat.

Diagram 13. Totalt antal genomförda åtgärder per aktörsgrupp bland de organisationer som enbart deltog 2023 eller 2024 utifrån medelvärdet

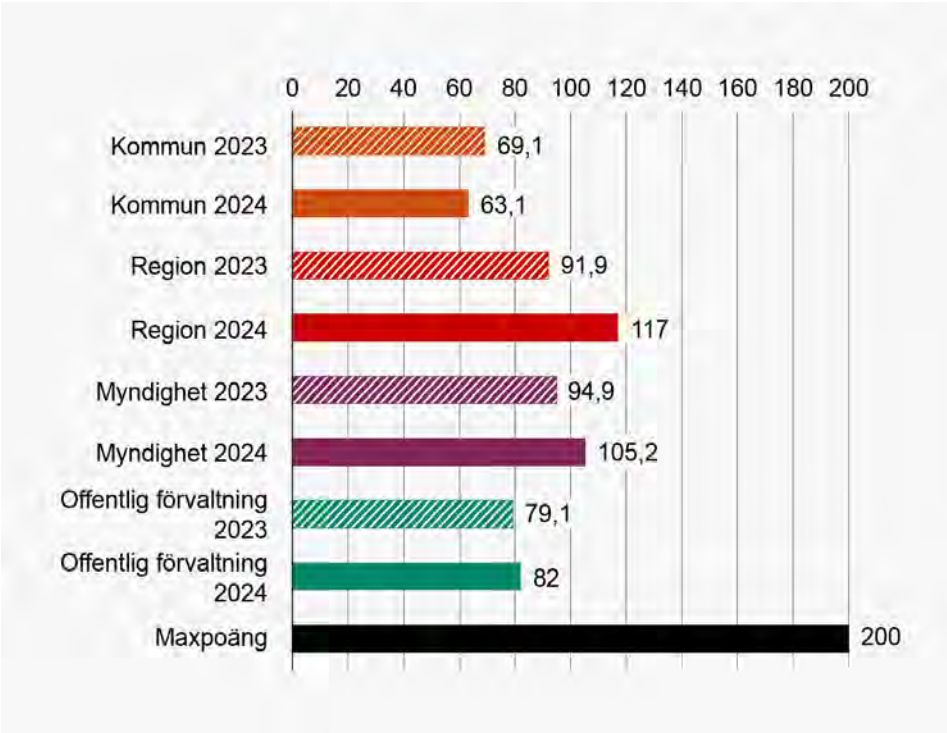


Diagram 13 redogör för den genomsnittliga mängden implementerade åtgärder för varje aktörsgrupp utifrån de som endast deltog vid en av mätningarna 2023 eller 2024. Förutom att det följer samma mönster som tidigare kring resultatspridningens påverkan på medelvärdet är diagrammet viktigt för att förstå helhetsresultatet på Infosäkkollen 2024. Populatationsförändring, där antalet kommuner minskat och antalet myndigheter därför ökat i relativa termer, bör även förstås utifrån att även om de deltagande kommunerna 2024 är svagare än de kommuner som endast deltog 2023 handlar det om en minskning på i genomsnitt sex åtgärder. Detta ska jämföras mot de myndigheter som endast deltog 2024, vilka har genomfört i snitt 10,3 fler åtgärder än de myndigheter som endast deltog 2023. Eftersom myndigheterna, den starkaste aktörsgruppen, har ökat i relativt antal och förbättrat sitt resultat samtidigt som kommunerna, den svagaste aktörsgruppen, har minskat får faktumet att de nytillkomna kommunerna 2024 presterar sämre än de nytillkomna kommunerna 2023 mindre påverkan på helhetsresultatet än föregående mätning.

Diagram 14. Totalt antal genomförda åtgärder hos de 30 bästa kommunerna och myndigheterna 2021, 2023 och 2024

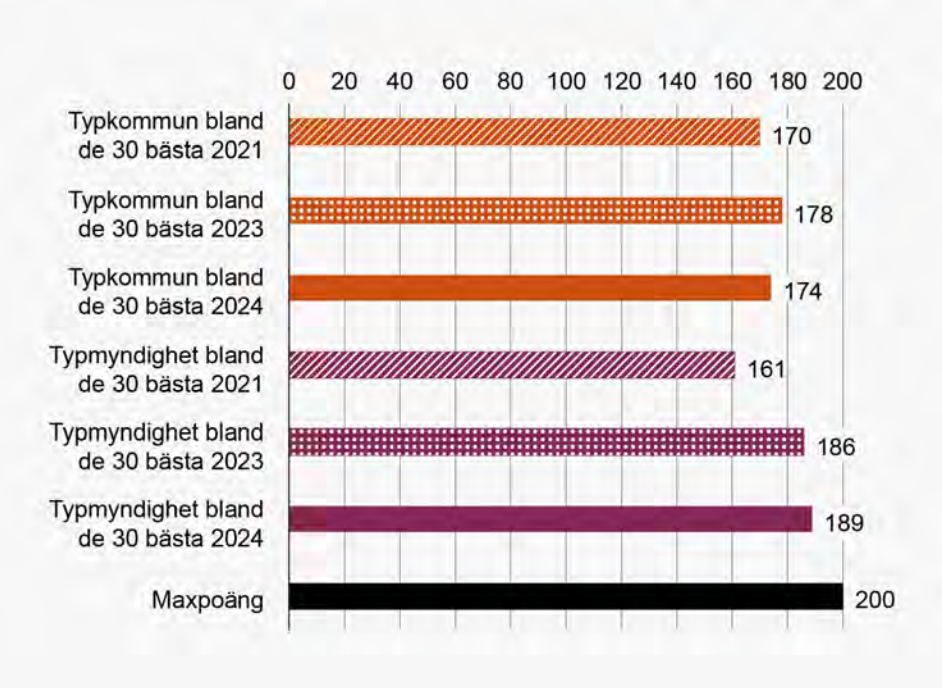
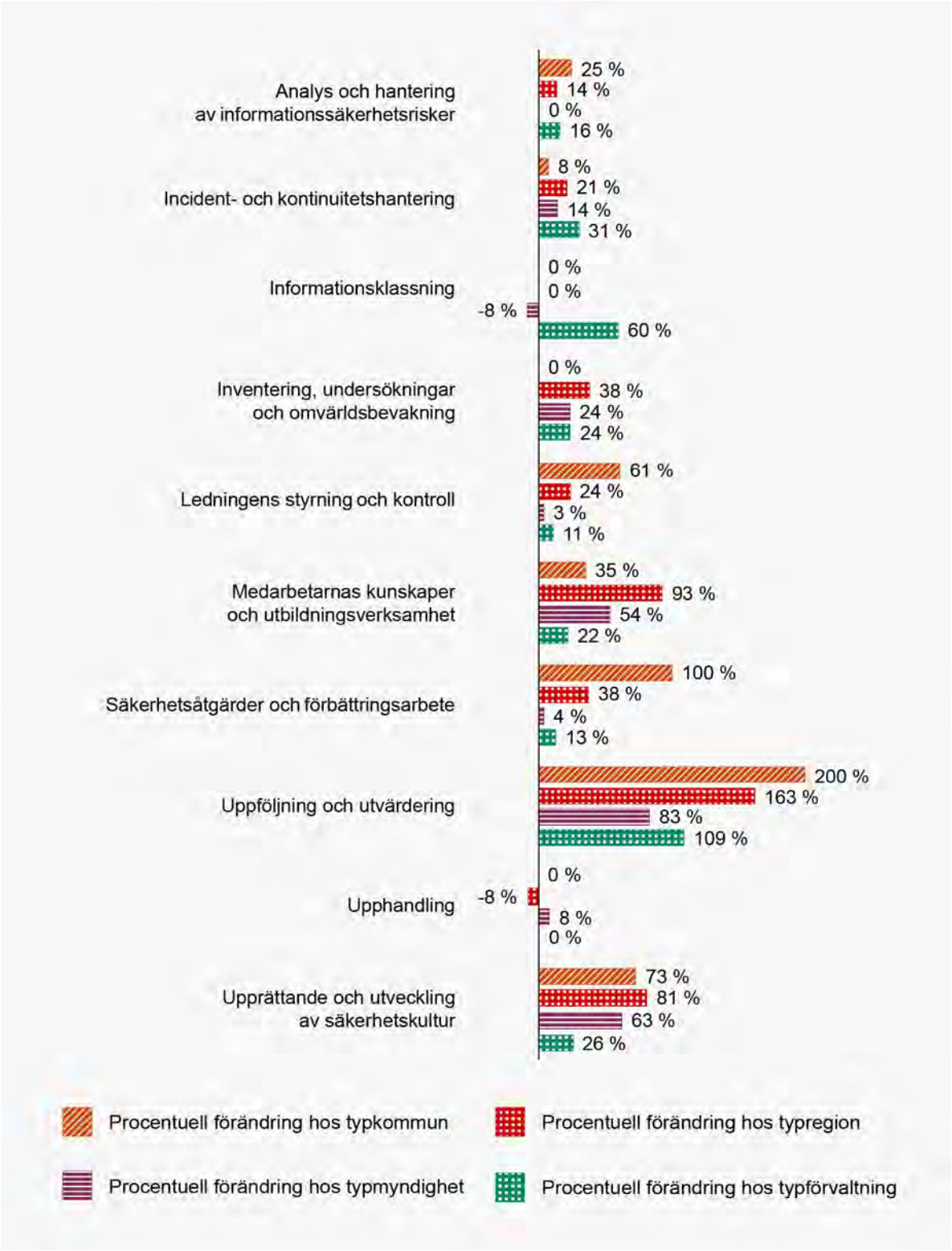


Diagram 10 ovan påvisade att typkommunen och typmyndigheten har infört fler åtgärder för varje mätning, men i diagram 14, där de 30 bästa inom de två aktörsgrupperna undersöks ses inte samma utfall. Bland de 30 bästa kommunerna ses faktiskt en minskning i antalet införda åtgärder 2024 jämfört med 2023. Det förklaras av att några av de kommunerna med bäst resultat 2023 inte deltog i mätningen 2024. För de 30 bästa myndigheterna ses förvisso en liten ökning mellan 2023 och 2024 bestående av tre fler införda åtgärder. Resultatet antyder samtidigt att fler myndigheter, givet att några fler åtgärder tillförs så att systematiken bibehålls över samtliga arbetsområden, bör uppnå nivå 3 i mätningen 2025.

En lärdom sett utifrån att totalresultatet i Infosäkkollen har förbättrats, är att det ändå är helheten av organisationer som blivit något bättre och bidragit till ett bättre helhetsresultat.

Diagram 15. Förändring i procent av antal genomförda åtgärder per arbetsområde 2024 jämfört med 2023 för alla aktörsgrupper



Ovan diagram ska utläsas med försiktighet. Stora procentuella förbättringar beror på ett relativt svagt resultat 2023 och framstår som ännu större inom de arbetsområden som har relativt få mätbara åtgärder. Typexemplet är den 200 procentiga förbättringen hos en typkommun gällande Uppföljning och utvärdering, där en typkommun gått från tre genomförda åtgärder 2023 till nio genomförda åtgärder 2023. Vidare motsvarar 9 av 41 genomförda åtgärder enbart 22 procent av den maxpoäng som kan uppnås på arbetsområdet.

Det är en generellt positiv utveckling på samtliga arbetsområden. Arbetsområdet för Uppföljning och utvärdering, som varit ett av de arbetsområden där organisationerna varit svagast i tidigare mätningar, har utvecklats mest. Även Upprättande och utveckling av säkerhetskultur samt Medarbetarnas kunskaper och utbildningsverksamhet visar på god utveckling. Samtidigt är det så att förbättringen sker från låg nivå i tidigare mätningar. Exempelvis har en typförvaltning inom arbetsområdet Upprättande och utveckling av säkerhetskultur gått från 23 till 29 genomförda åtgärder utav 41 möjliga, och en typkommun inom arbetsområdet Säkerhetsåtgärder och förbättringsarbete har gått från 9 till 18 genomförda åtgärder utav 34 möjliga.

En typregion har färre antal genomförda åtgärder inom arbetsområdet för Upphandling 2024 jämfört med 2023. Även typmyndigheten har färre antalet genomförda åtgärder inom arbetsområdet för Informationsklassning 2024 jämfört med 2023. I båda fallen är det en åttaprocentig försämring, en försämring på en åtgärd för typregionen och två åtgärder för typmyndigheten. I båda fallen uppnåddes bra resultat inom arbetsområdena för aktörsgrupperna såväl 2024 som 2023.

De arbetsområden där minst skillnad mellan mättillfällena syns är för Upphandling, Ledningens styrning och kontroll, samt Säkerhetsåtgärder och förbättringsarbete, vilket antyder att dessa arbetsområden har haft lägre prioritet.

4.1.5 Resultatspridning

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

Diagram 16. Resultatspridning hos offentlig förvaltning

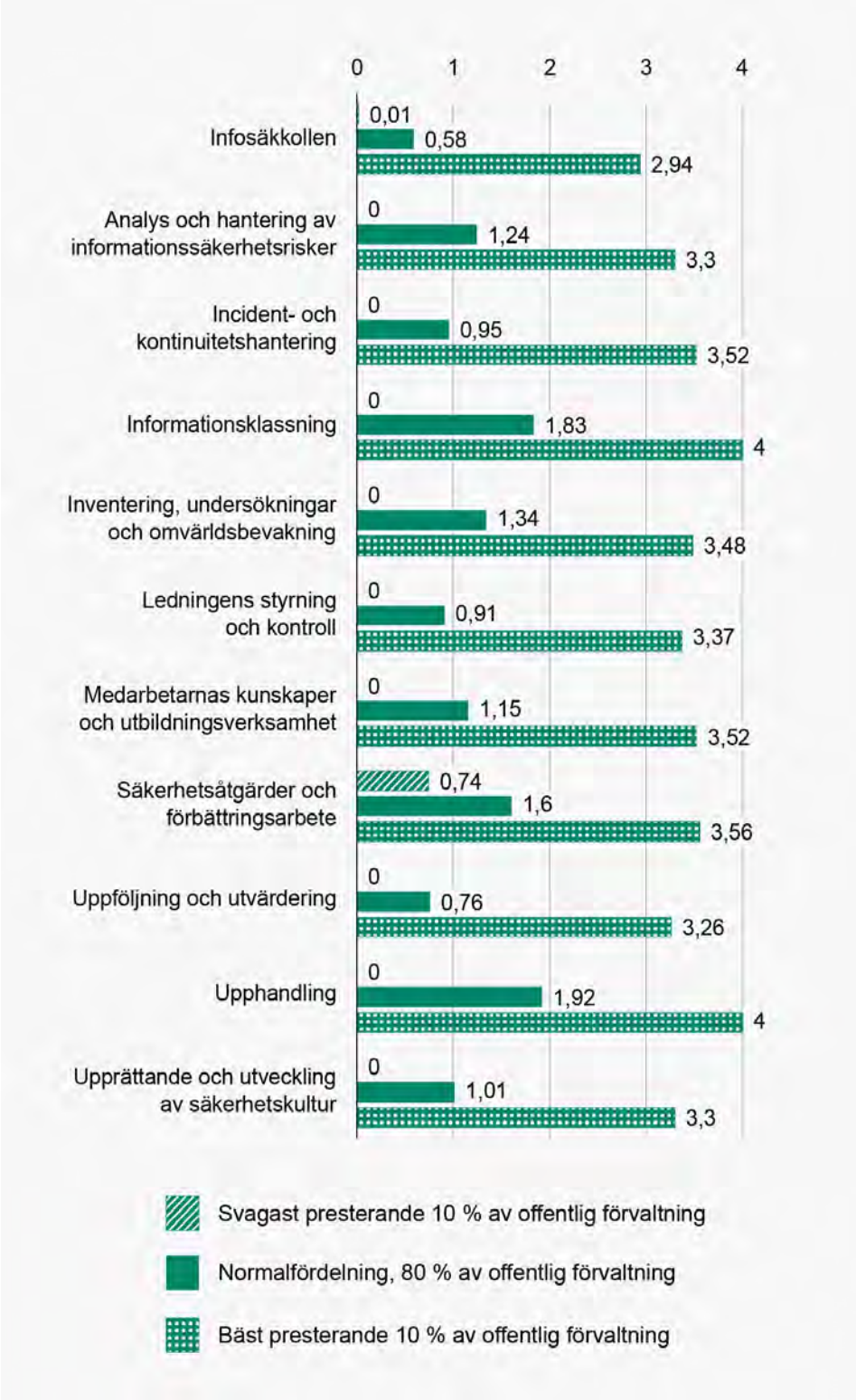


Diagram 16 tydliggör hur mycket de 10 procent bäst presenterande organisationerna drar upp resultatet för en typorganisation inom sin aktörsgrupp. Det är en kraftig skillnad mellan resultatet för de 10 procent bästa visavi de 80 procent som här återges som normalfördelning.

Säkerhetsåtgärder och förbättringsarbete är det enda arbetsområde där de svagaste 10 procenten inom offentlig förvaltning har uppnått en genomsnittlig nivå som är högre än noll. Mer information om potentiella förklaringar för att just det arbetsområdet har ett relativt bra resultat återfinns i kapitel 5 om It-säkkollen.

Diagram 17. Nivåresultat per arbetsområde för offentlig förvaltning

I diagram 17 visas hur många organisationer som uppnått Infosäkkollens fyra nivåer. Det arbetsområde där flest organisationer uppnått en nivå är, precis som 2023, inom Säkerhetsåtgärder och förbättringsarbete, där hela 261 organisationer, alltså 97,4 procent, har klarat modellens krav för nivå 1.

Det svagaste resultatet finns, återigen precis som 2023, inom arbetsområdet för Ledningens styrning och kontroll där 141 organisationer, eller 52,6 procent, av helheten, har klarat av nivå 1. Det är dock en förbättring jämfört med 2023 då motsvarande siffra var 43,9 procent. Den till synes stora förbättringen förklaras dock till övervägande del av att färre kommuner deltog 2024 jämfört med antalet myndigheter, som är den aktörsgrupp som i samtliga mätningar haft det starkaste resultatet.

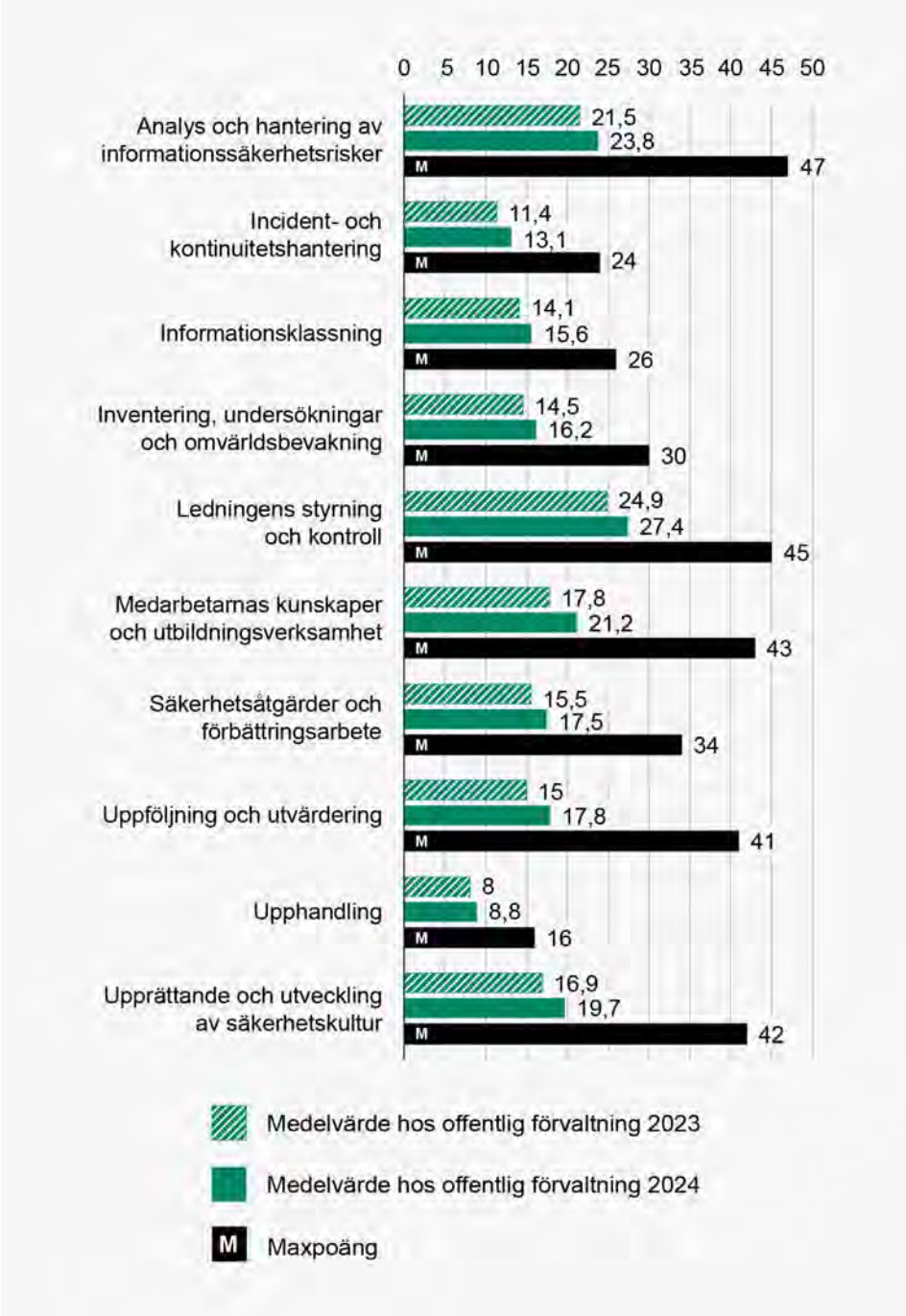
Arbetsområdet för Uppföljning och utvärdering är där minst antal organisationer, 32,5 procent, uppnått nivå 2 eller högre. Det är också det arbetsområde där minst antal organisationer, 11,6 procent, klarat nivå 3 eller 4. Återigen är det likstämmigt med mätningen 2023. Brist på uppföljning och utvärdering riskerar att innebära att implementerade åtgärder inte uppnår förväntad effekt.

Upphandling är det arbetsområde där flest organisationer uppnår modellens högre nivåer. Detta trots att arbetsområdet bara placerar sig på fjärdeplats utifrån hur många organisationer som uppnår nivå 1. 111 organisationer, 41,4 procent, når nivå 3 eller 4 i modellen för arbetsområdet Upphandling. Även detta är likstämmigt med resultatet från tidigare mätningar.

4.1.6 Förändring i resultatet från 2023 till 2024

193 organisationer deltog såväl 2023 som 2024. 98 organisationer deltog enbart 2023, och motsvarande antal för 2024 var 75 organisationer. Dessa grupper är särskilt intressanta att studera för att se resultatförändring mellan de två mättillfällena.

Diagram 18. Antalet genomförda åtgärder per arbetsområde 2023 och 2024 för de organisationer som deltog vid båda mättillfällena

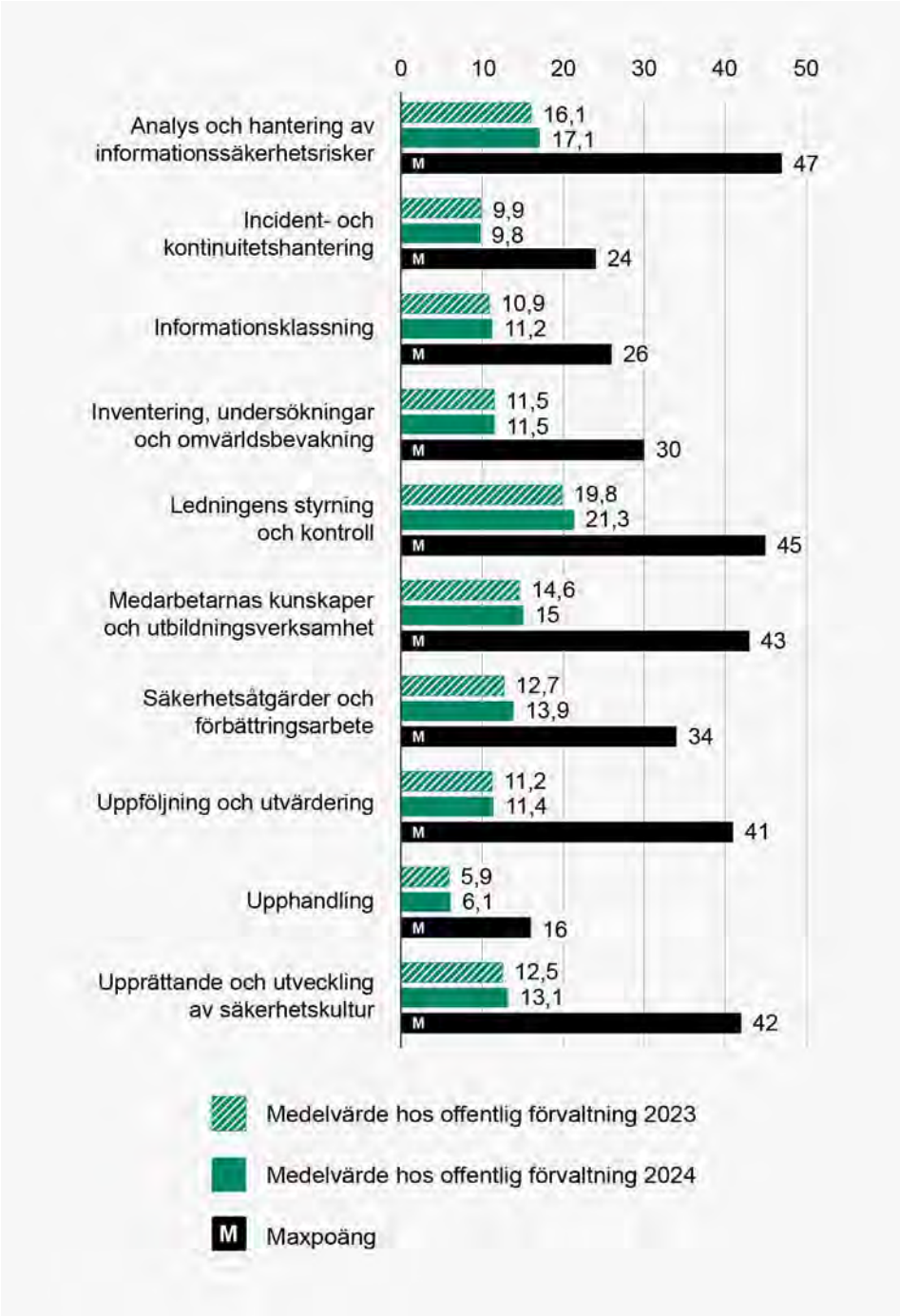


Ett genomsnitt av resultatet för genomförda åtgärder för samtliga organisationer som deltagit vid båda mättillfällena visar på en förbättring inom samtliga arbetsområden hos gruppen. Det arbetsområde med flest nya genomförda åtgärder är Medarbetarnas kunskaper och utbildningsverksamhet och det med minst är Upphandling. I genomsnitt har 2,3 fler åtgärder genomförts per arbetsområde.

Diagram 19. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 för de organisationer som deltog vid båda mättillfällena

Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 12,4 procentig resultatförbättring av totalt antal genomförda åtgärder. De 193 organisationer som deltog i båda de två senaste mätningarna har genomfört i snitt 12,3 fler åtgärder 2024 jämfört med 2023. Detta har bidragit till en resultatförbättring för hela Infosäkkollen.

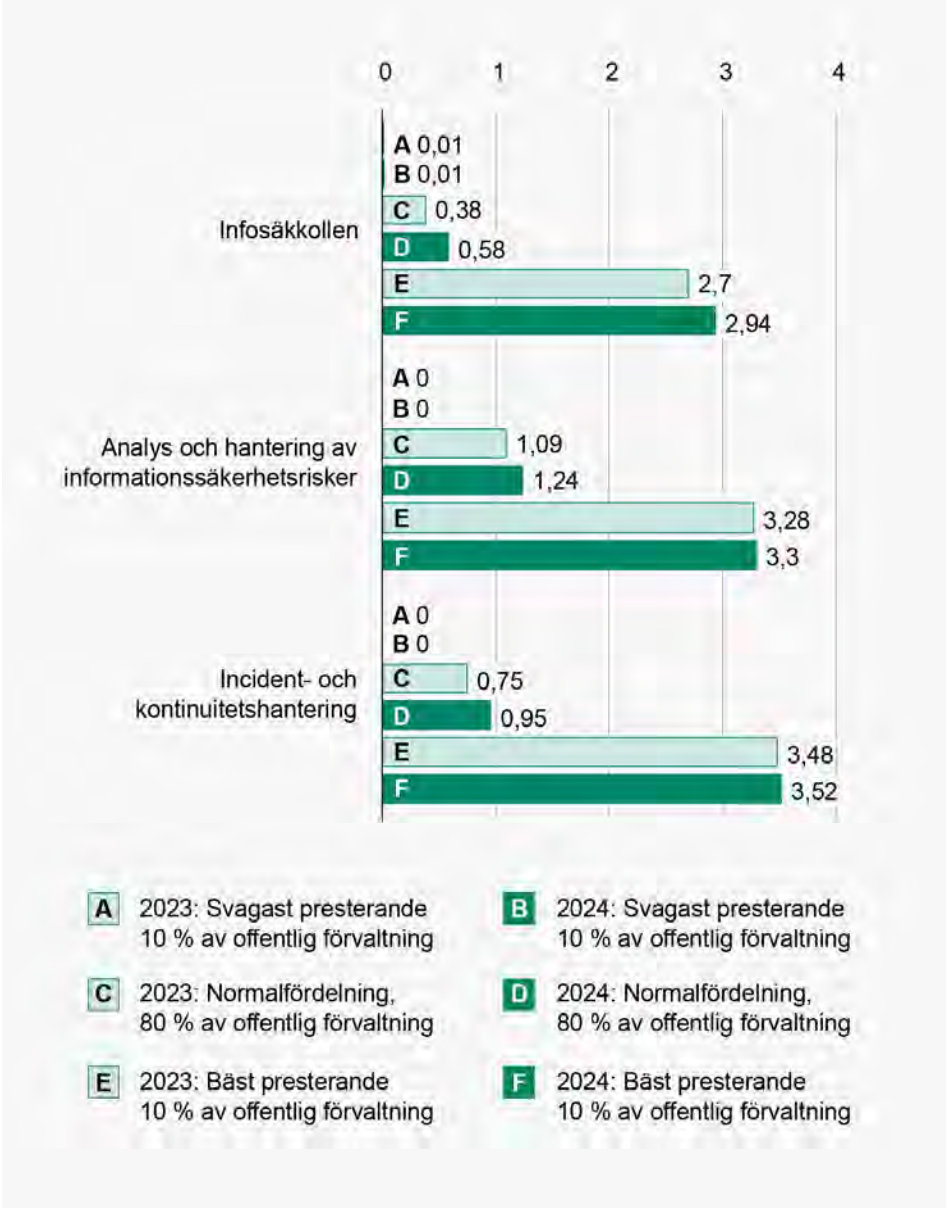
Diagram 20. Antalet genomförda åtgärder per arbetsområde 2023 och 2024 för de organisationer som enbart deltog vid ett av mättillfällena

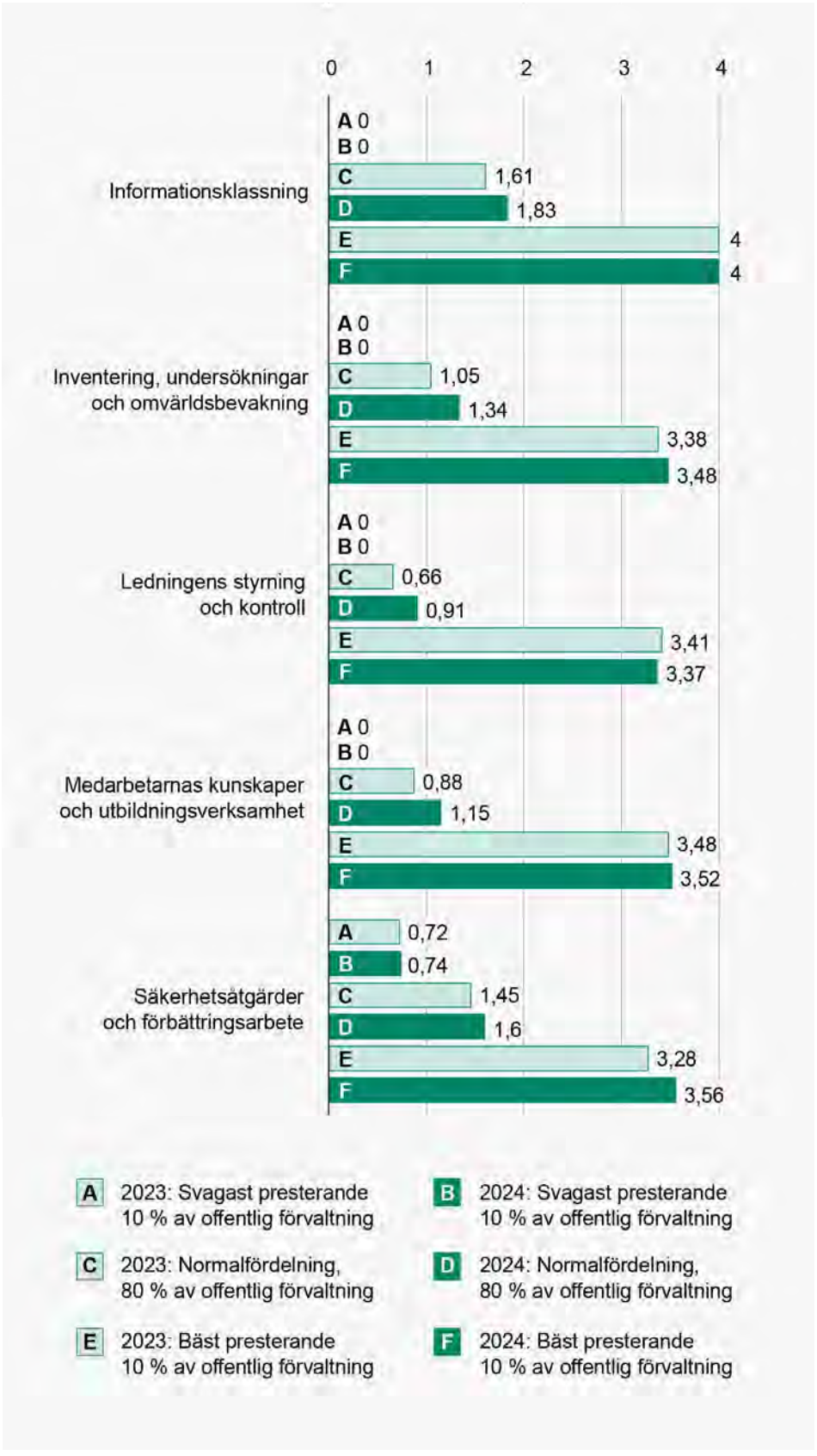


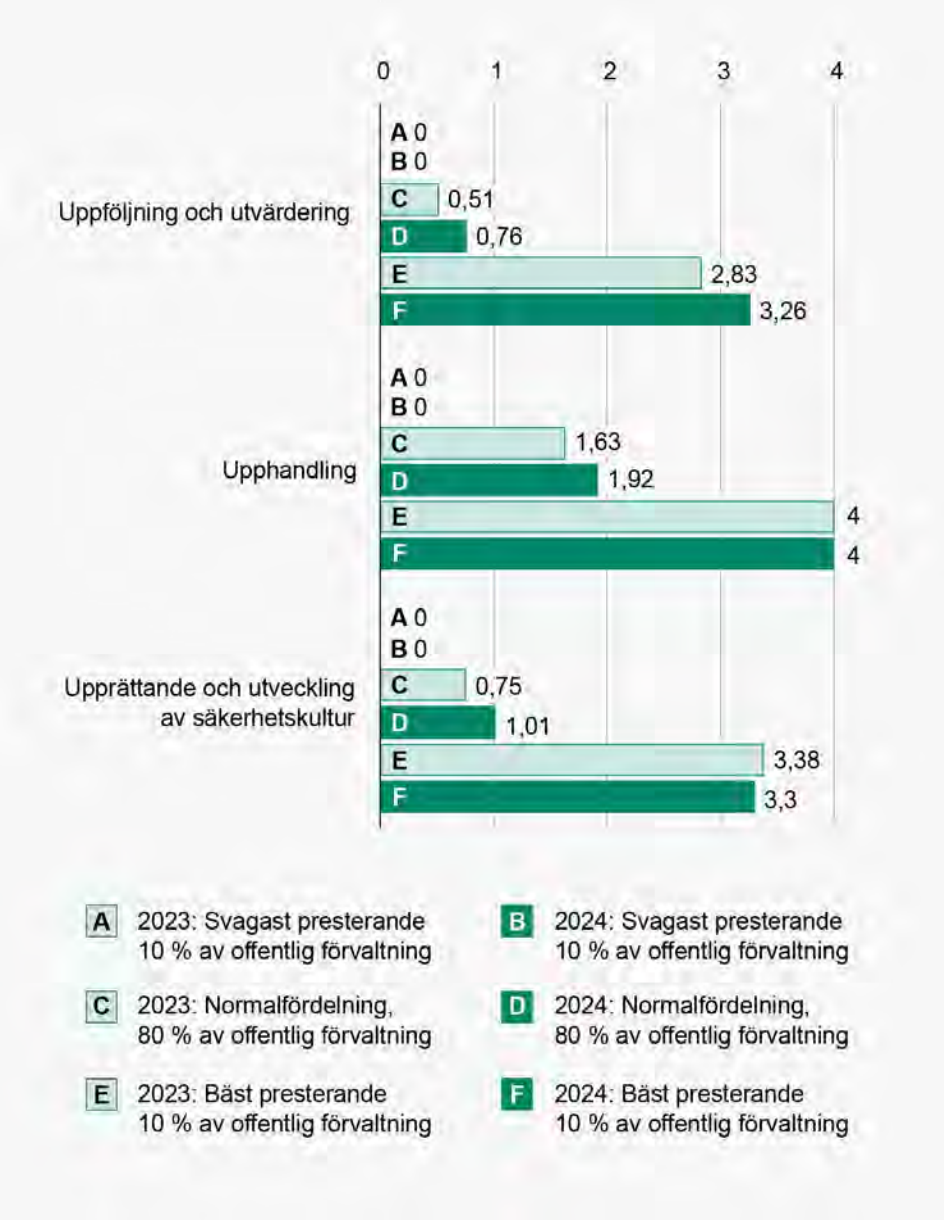
Här jämförs de 98 respektive 75 organisationer som enbart deltog 2023 eller 2024. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 3,6 procentig resultatförbättring av hela Infosäkkollen. Den procenten är mindre än de 12,4 procent som noterades för organisationer som deltagit vid båda mättillfällena. De organisationer som endast deltog 2024 har i snitt genomfört 2,8 fler åtgärder än de som endast deltog 2023. Det kan jämföras med 12,3 åtgärder för de som deltagit både 2023 och 2024.

Vid en jämförelse mellan diagram 18 och diagram 20 utifrån alla de organisationer som deltog 2024 skönjs stora skillnader. De organisationer som deltog både 2023 och 2024 har i genomsnitt genomfört 111,1 åtgärder. Den grupp som deltog för första gången 2024 har i jämförelse endast genomfört 82 åtgärder. Det är en skillnad 29,1 åtgärder. Så trots att de organisationer som endast deltog 2024 presterar bättre jämfört med de organisationer som endast deltog 2023 är resultatet för de organisationer som deltog endast 2024 en grupp som sänker helhetsresultatet. Sammantaget är det en indikator på att de organisationer som arbetar systematiskt över tid också är de organisationer som utvecklas såväl bäst som snabbast.

Diagram 21. Resultatspridning hos offentlig förvaltning 2023 respektive 2024




0
1
2
3
4
Informationsklassning
A 0
B 0
C 1,61
D 1,83
E 4
F 4
Inventering, undersökningar och omvärldsbevakning
A 0
B 0
C 1,05
D 1,34
E 3,38
F 3,48
Ledningens styrning och kontroll
A 0
B 0
C 0,66
D 0,91
E 3,41
F 3,37
Medarbetarnas kunskaper och utbildningsverksamhet
A 0
B 0
C 0,88
D 1,15
E 3,48
F 3,52
Säkerhetsåtgärder och förbättringsarbete
A 0,72
B 0,74
C 1,45
D 1,6
E 3,28
F 3,56
A 2023: Svagast presterande 10 % av offentlig förvaltning
B 2024: Svagast presterande 10 % av offentlig förvaltning
C 2023: Normalfördelning, 80 % av offentlig förvaltning
D 2024: Normalfördelning, 80 % av offentlig förvaltning
E 2023: Bäst presterande 10 % av offentlig förvaltning
F 2024: Bäst presterande 10 % av offentlig förvaltning



Även om ingen av staplarna för den gruppen som i diagrammet utgör normalfördelning uppnår nivå 2, systematik i arbetssätten, så visar diagram 21 på en genomgående förbättring 2024 jämfört med 2023. Resultatspridningen förklarar utifrån förbättringen bland de organisationer som utgör normalfördelningen varför typförvaltningen i mätningen 2024 uppnått nivå 1 i modellen, vilket motsvarar grunderna för ett informations- och cybersäkerhetsarbete.

Det förbättrade resultatet för en typförvaltning förklaras också av att färre kommuner, den aktörsgrupp med det svagaste resultatet, deltog 2024 jämfört med 2023. Detta betyder i sin tur att antalet myndigheter utgör en större andel av alla offentliga förvaltningar och myndigheter är den aktörsgrupp som presterat bäst vid varje mättillfälle. Sammantaget förklaras alltså det förbättrade resultatet 2024 till stor del av en förändring i populationen. Det kommer synliggöras ytterligare i nedan delar som studerar resultatet för varje enskild aktörsgrupp.

4.1.7 Enkätundersökning

Mellan den 10 och 24 november 2024 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 2024.[21] Undersökningen var frivillig och frågorna tog ungefär tio minuter att besvara. Utöver fritextfälten var samtliga frågor obligatoriska. Svaren var anonyma och presenteras på aggregerad nivå nedan.

Totalt svarade 165 organisationer inom offentlig förvaltning. 83 kommuner (50,3 procent), sex regioner (3,6 procent) och 76 myndigheter (46,1 procent) besvarade enkätundersökningen. De som besvarade hade uppgivit att de deltagit aktivt i organisationens genomförande av Infosäkkollen och respondenterna var i huvudsak CISO[22], men också roller såsom it-strateg, it-chef, säkerhetsskyddschef och liknande.

På frågan om Infosäkkollen är värdefull för organisationens informations- och cybersäkerhetsarbete svarade 32,7 procent att det *stämmer helt*, 49,1 procent angav *stämmer väl*, 16,4 procent fyllde i *stämmer knappt*, medan 1,8 procent svarade *stämmer inte*. Att 81,8 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 cybersäkerhetsarbete svarade 57,6 procent *ja, varje år*, 10,3 procent *ja, varje halvår*, 1,8 procent *ja, tertialt*, 3,6 procent *ja, varje kvartal*, medan 26,7 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 73,3 procent genomför Infosäkkollen i egen regi årsvis eller mer frekvent än så. Det är jämfört med enkätundersökningen 2023 en ökning med 12,3 procentenheter.

På frågan om organisationen använder Infosäkkollen för att planera kommande åtgärder uppgav 19,4 procent *stämmer helt*, 43,6 procent *stämmer väl*, 27,3 procent *stämmer knappt* och 9,7 procent *stämmer inte*. Att 63 procent anger att de använder Infosäkkollen är ett gott betyg för verktyget. Det är en ökning med 7,3 procentenheter jämfört med 2023.

Gällande i vilken utsträckning respondenterna arbetar med informations- och cybersäkerhet svarade 43 procent *heltid*, 4,8 procent angav *cirka 75 procent*, 17 procent svarade *halvtid* och 35,2 procent angav *cirka 25 procent*. Antalet som angav *heltid* eller *cirka 75 procent* har minskat med 2,4 procent i mätningen 2024 jämfört med 2023. Det ska påpekas att frågan var personligt ställd och

Not 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.

Not 22. I begreppet CISO inkluderas de som uppgivit informationssäkerhetssamordnare.

organisationens respondent kan ha kollegor som arbetar med frågorna i större utsträckning än respondenten själv. 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 cybersäkerhetsarbetet.

MSB undersökte kontinuiteten i arbetet genom att fråga om samma kollegor var ansvariga för organisationens informations- och cybersäkerhetsarbete som för två år sedan. 19,4 procent uppgav *ja, alla medarbetare är kvar*, 30,3 procent *ja, de flesta medarbetare är kvar*, 35,8 procent *nej, vi har haft viss personalomsättning*, och 14,5 procent *nej, vi har haft omfattande personalomsättning*. Svaren är svårtolkade då MSB saknar data på ”normal” personalomsättning inom branschen och tidsspannet. Antalet som svarade *nej, vi har haft viss/omfattande personalomsättning* ökade dock med 5 procenenheter jämfört med 2023, vilket indikerar att personalomsättningen ökat. Kommunerna uppger större personalomsättning än regioner och myndigheter.

Respondenterna fick ta ställning till om deras organisation har den personal som krävs för att förbättra informations- och cybersäkerhetsarbetet. Svaren fördelades på så vis att 2,4 procent uppgav *stämmer helt*, 29,7 procent *stämmer väl*, 48,5 procent *stämmer knappt*, och 19,4 procent *stämmer inte*. Det förekommer viss resultatspridning mellan aktörsgrupperna, exempelvis anger kommuner i högre utsträckning än regioner och myndigheter att de saknar personal. Sammantaget uppger 67,9 procent av respondenterna *stämmer knappt* eller *stämmer inte*, vilket är samma som vid enkätundersökningen 2023.

MSB undersökte om respondenten ansåg att organisation har den kompetens som krävs för att förbättra informations- och cybersäkerhetsarbetet. 5,5 procent uppgav *stämmer helt*, 50,9 procent *stämmer väl*, 36,4 procent *stämmer knappt* och 7,3 procent *stämmer* inte. Myndigheter uppger sig ha mer kompetens än övriga två aktörsgrupper. Sammantaget uppgav 56,4 procent att organisationen besitter nödvändig kompetens, det är en minskning på 9,1 procentenheter jämfört med 2023. Det kan möjligtvis förklaras av den antytt ökade personalomsättningen.

På frågan huruvida deras organisation har den budget som krävs för att förbättra informations- och cybersäkerhetsarbetet uppgav 3,6 procent *stämmer helt*, 23,6 procent *stämmer väl*, 41,2 procent *stämmer knappt*, medan 31,5 procent svarade *stämmer inte*. Att 72,7 procent uppger *stämmer knappt* eller *stämmer inte* är nedslående, och en liten försämring, 0,7 procentenheter, jämfört med 2023. Att 31,5 procent svarar *stämmer inte* är ännu mer bekymrande. Endast 17,1 procent av de 76 deltagande myndigheterna svarade *stämmer inte*, vilket påvisar en upplevt stor skillnad jämfört med svarande kommuner och regioner.

På frågan om Infosäkkollens resultat presenterats för organisationens högsta ledning svarade 60 procent *ja*, 35,2 procent *nej* och 4,8 procent *vet ej*. MSB rekommenderar samtliga organisationer att föredra resultatet för ledningen före inrapportering. Antalet organisationer som presenterat sitt svar för sin ledning har ökat med 11,7 procentenheter 2024 jämfört med 2023, vilket kan antyda att arbetet har fått högre prioritet hos organisationsledningarna. Bland kommu-

nerna uppgav dock 52,9 procent att de inte presenterat resultatet för sin organisationsledning, vilket visar på skillnader mellan aktörsgrupperna. Att 35,2 procent svarade *nej* och indikerar fortfarande att många ledningar 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 uppgav 11,5 procent *stämmer helt*, 41,2 procent *stämmer väl*, 37 procent *stämmer knappt* och 10,3 procent *stämmer inte*. Resultatspridningen mellan aktörsgrupperna var dock stor. Enligt respondenterna visar myndighetsledningarna betydligt mer engagemang, där 65,8 procent svarade *stämmer helt* eller *stämmer väl*. För kommunerna svarade 60 procent *stämmer knappt* eller *stämmer inte*. Sammantaget har 47,3 procent av respondenterna angett *stämmer knappt* eller *stämmer inte*, vilket förvisso är en förbättring jämfört med 3 procentenheter jämfört med undersökningen 2023, men likväl en omfattande upplevd avsaknad av engagemang hos ledningen.

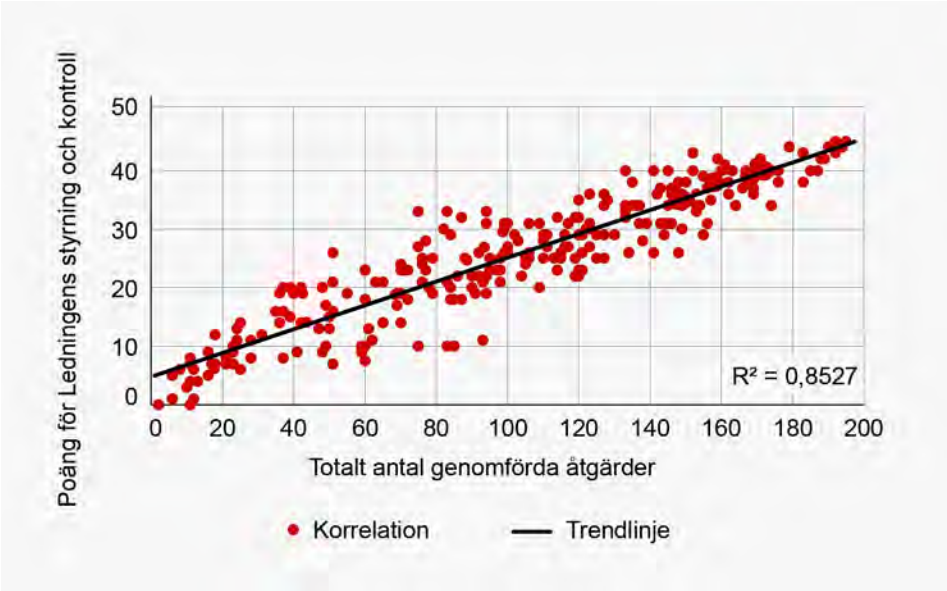
MSB undersökte i enkätundersökningen vad de huvudsakliga hindren för förbättringsarbetet består av. Precis som 2023 svarade de flesta respondenterna resursbrist och avsaknad av engagemang från ledningen som de huvudsakliga. En respondent svarade ”för få personer arbetar med frågan. Ledningen förstår inte frågorna och prioriterar inte arbetet. Digitaliseringen är viktigare”. En annan uttryckte att det ”krävs en kulturförändring och högre mandat för CISO. Kommunikationsbrister och för lågt intresse från ledning”.

Slutligen ställde MSB två frågor kring metodstödet. På frågan om organisationen använder MSB:s metodstöd som stöd för sitt säkerhetsarbete uppgav 15,2 procent *stämmer helt*, 50,9 procent *stämmer väl*, 27,3 procent *stämmer knappt* och 6,7 procent *stämmer inte*. För frågan om huruvida organisationen har de resurser som behövs för att tillgodogöra sig MSB:s metodstöd uppgav 12,1 procent *stämmer helt*, 35,2 procent *stämmer väl*, 40,6 procent *stämmer knappt* och 12,1 procent *stämmer inte*. 66,1 procent svarade således att de nyttjar metodstödet, medan 47,3 procent samtidigt svarar att de har resurserna för att tillgodogöra sig detsamma. Sammantaget tyder det på att metodstödet uppskattas och hade kommit till ännu större nytta om organisationerna hade haft bättre förutsättningar.

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 mätningen 2024 är Ledningens styrning och kontroll. Ett lyckosamt informationssäkerhetsarbete 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.

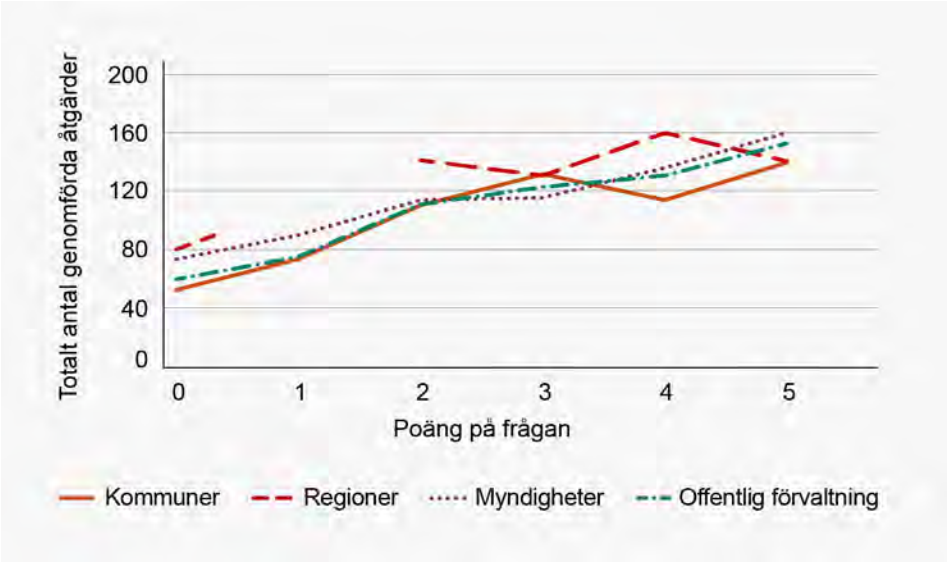
Diagram 22. Korrelation mellan antal poäng i ledningens styrning och kontroll och totalt antal genomförda åtgärder



Diagrammet ovan påvisar en stark korrelation mellan ett bra resultat för arbetsområdet Ledningens styrning och kontroll och ett bra resultat för hela Infosäkkollen 2024.[23] Även om korrelation inte är samma sak som kausalitet är det 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 säkerhetsarbetet.

Not 23. 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, 0,8487, regioner R^2 = 0,9327 och myndigheter R^2 = 0,8398).

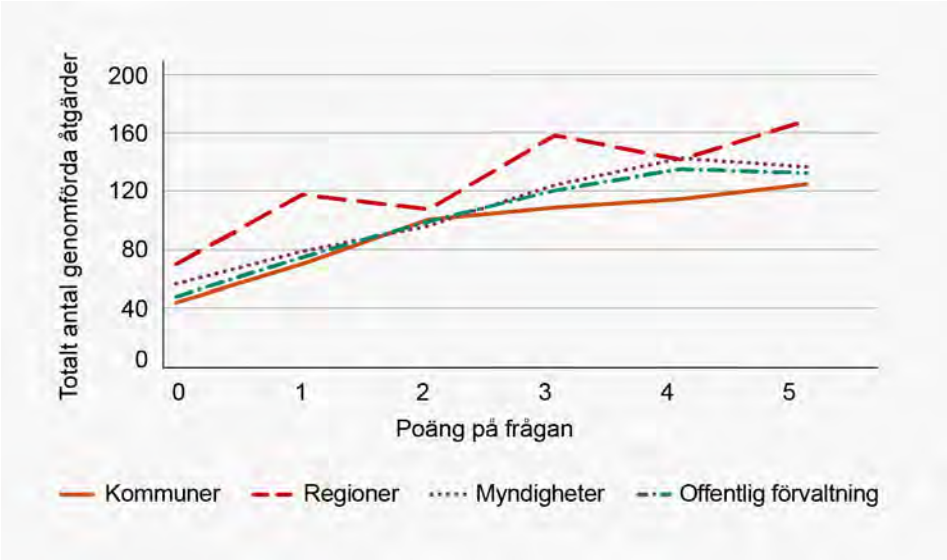
Diagram 23. Har organisationens ledning informerat mig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?



Ingen av de deltagande regionerna i Infosäkkollen 2024 fick 1 poäng på fråga 15, varför det är ett glapp i den linje som representerar totalt antal genomförda åtgärder hos regionerna.

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.

Diagram 24. Har beslutet om att införa säkerhetsåtgärder lett till beslut om att tilldela resurser för att kunna införa beslutande säkerhetsåtgärder?



Fråga 23 i Infosäkkollen 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 de organisationer vars beslutsfattare engagerat sig med informations- och cybersäkerhetsfrågor och beslutat om införande av säkerhetsåtgärder, har också resurser tillförts för dess implementering.

I enkätundersökningen som genomfördes med de som rapporterade in Infosäkkollen 2024 svarade 67,9 procent att de inte har den personal som krävs för att fullt ut implementera förbättringsarbetet. 52,2 procent uppgav att de arbetar deltid eller mindre med informations- och cybersäkerhet.[24] Vidare uppgav 50,3 procent viss eller omfattande personalomsättning under en tvåårsperiod. Samtidigt uppgav 56,4 procent att organisationen besitter nödvändig kompetens.

Att 35,2 procent av respondenterna inte haft en föredragning om resultatet från Infosäkkollen 2024 till sin organisationsledning indikerar att det är svårt att få gehör för frågorna. 47,3 procent av respondenterna svarade också att högsta ledningen saknar det engagemang som krävs för att förbättra informations- och cybersäkerhetsarbetet. 72,7 procent 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 tillför de resurser till förbättringsarbetet i den utsträckning som krävs.

Det positiva är att diagram 22, 23 och 24 påvisar att ledningens engagemang korrelerar med ett bättre resultat i Infosäkkollen. Om ledningens engagemang ökar och nödvändiga resurser tillförs borde därför 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.

Not 24. Frågan var personligt ställd och organisationens respondent kan ha kollegor som arbetar med frågorna i större utsträckning än respondenten själv.

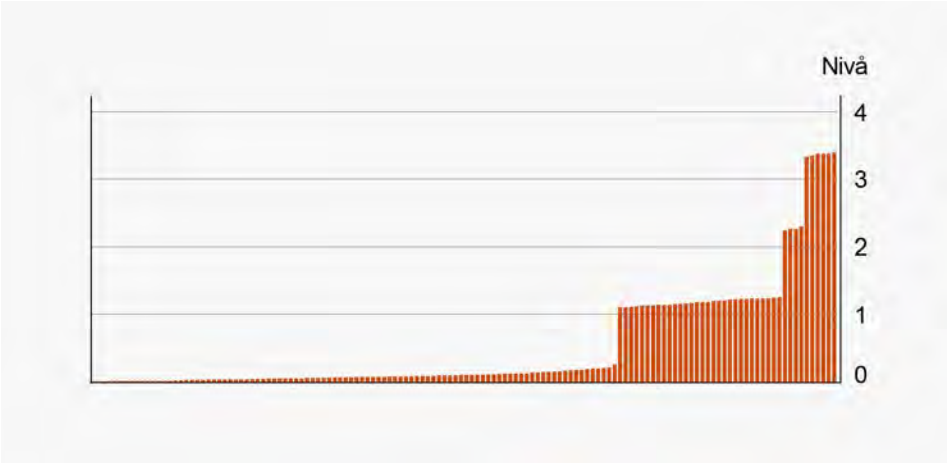
4.2 Kommuner

I det här avsnittet presenteras den bild som framkommit genom sammanställning av 136 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

40 av alla deltagande kommuner uppnådde nivå 1 i modellen. En majoritet, 70,6 procent, uppnår inte nivå 1. Motsvarande siffra 2023 var 76,5 procent. 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 25. Resultattal för samtliga 136 kommuner



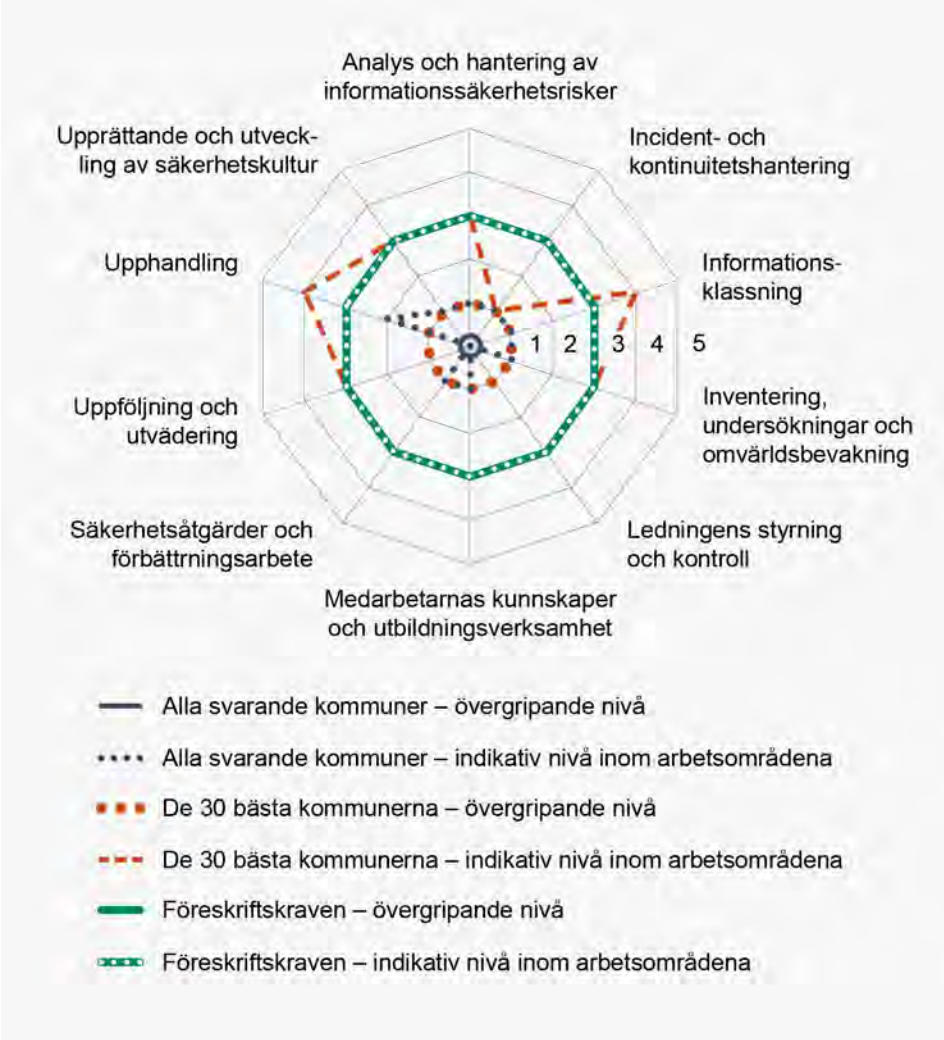
29,4 procent av deltagande kommuner uppnådde nivå 1 eller mer, 7,4 procent uppnådde nivå 2 eller mer, och 4,4 procent uppnådde nivå 3 i modellen.

4.2.2 Utfall per arbetsområde

Gruppen med de 30 bästa kommunerna uppnår modellens nivå 1, och den indikativa nivån når nivå 3 eller bättre i nio arbetsområden. Samma grupp uppnådde nivå 2 förra året, vilket är en följd av att några av de bästa kommunerna från mätningen 2023 inte deltog 2024.

Gruppen med alla svarande kommuner klarar inte att nå nivå 1, men når dock nivå 1 eller bättre på indikativ nivå inom åtta arbetsområden. Det är snarlikt resultatet 2023, med endast förbättring på indikativ nivå inom ett arbetsområde.

Diagram 26. Resultat i Infosäkkollen för samtliga kommuner



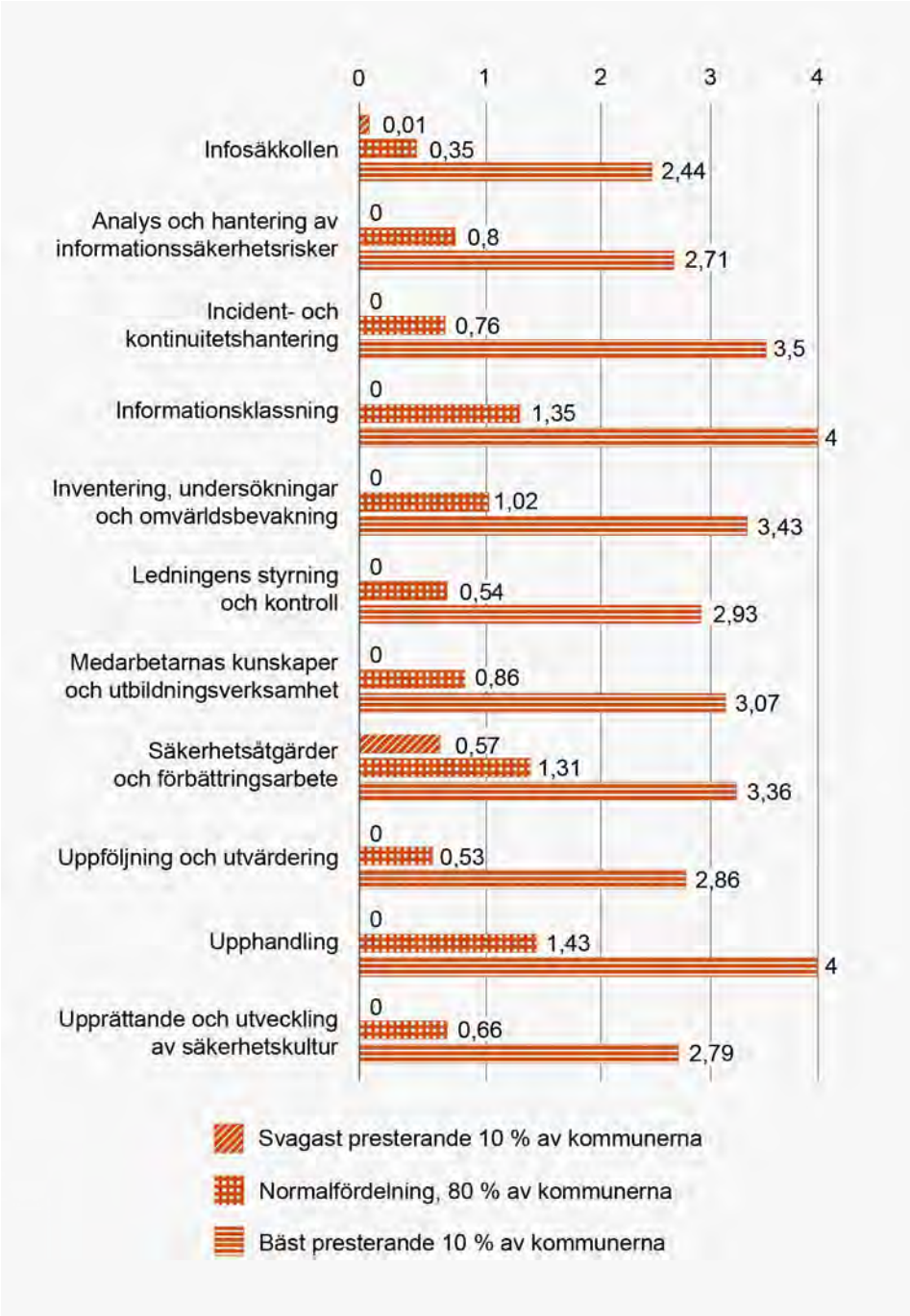
De arbetsområden där flest deltagande kommuner uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete (95,6 procent), följt av Informationsklassning (76,5 procent) och därefter Medarbetarnas kunskaper och utbildningsverksamhet (69,1 procent). Minst antal deltagande kommuner har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll (41,9 procent), följt av Uppföljning och utvärdering (48,5 procent) samt Upprättande och utveckling av säkerhetskultur (55,1 procent). Det är exakt samma arbetsområden som 2023.

De arbetsområden där flest deltagande kommuner uppnått nivå 3 eller bättre är inom Upphandling (31,6 procent), följt av Informationsklassning (21,3 procent) och därefter Inventering, undersökningar och omvärldsbevakning (16,9 procent). Minst antal deltagande kommuner har nått nivå 3 eller bättre inom arbetsområdet för Analys och hantering av informationssäkerhetsrisker (6,6 procent), följt av Upprättande och utveckling av säkerhetskultur (7,4 procent).

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 4.1. Det är en omfattande skillnad mellan resultatet för de 10 procent bästa kommunerna visavi de 80 procent av kommunerna som här motsvarar normalfördelningen.

Diagram 27. Resultatspridning hos kommunerna



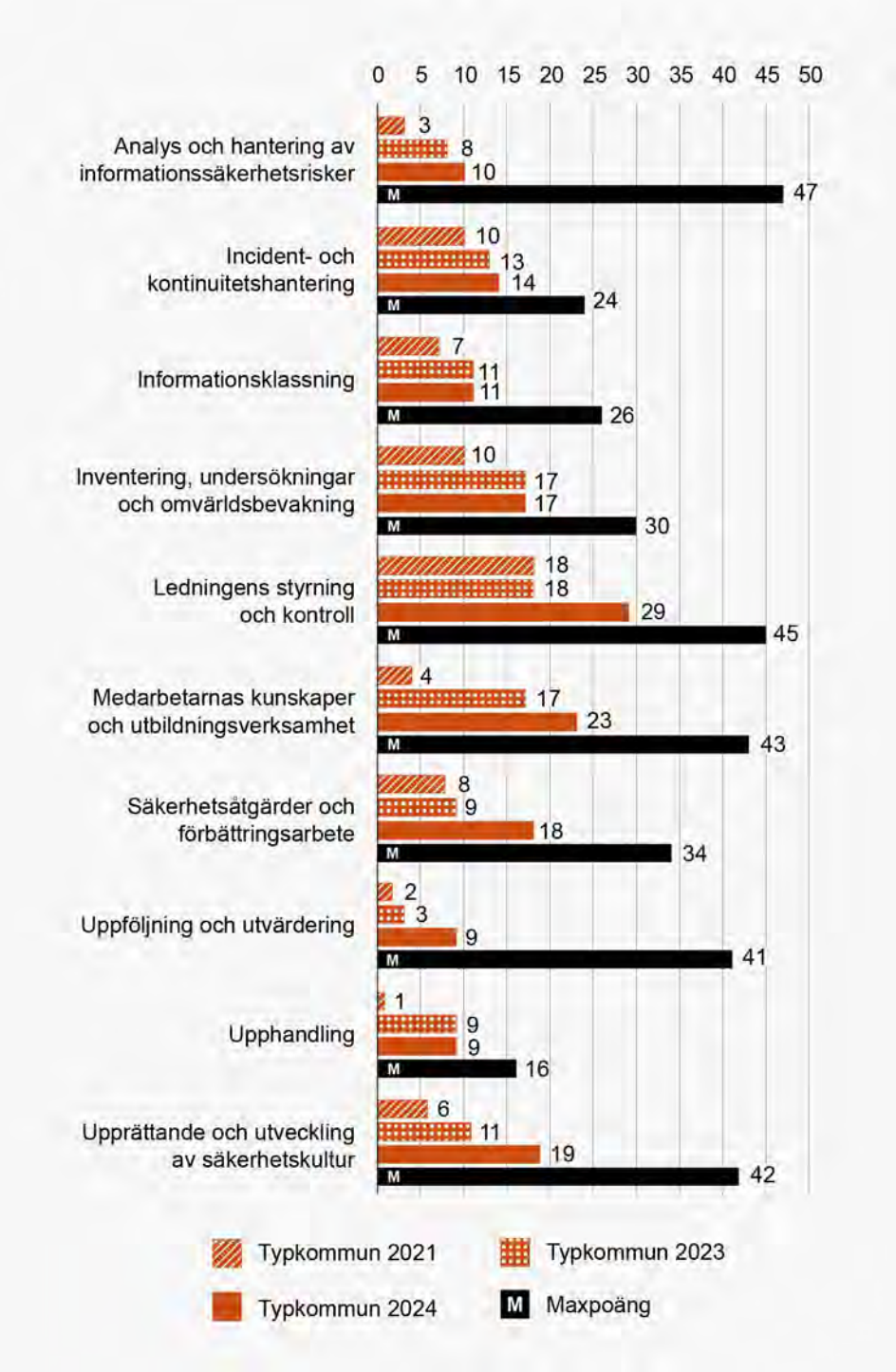
Det enda arbetsområdet där de svagaste 10 procenten av kommunerna ens uppnått ett egentligt resultat är inom Säkerhetsåtgärder och förbättringsarbete. De 10 procent bästa kommunerna har uppnått bäst resultat inom Informationsklassning och Upphandling.

För de 80 procent av kommunerna som återfinns i normalfördelningen är resultaten genomgående nedslående. På Infosäkkollen som helhet har endast 24,1 procent av organisationerna i normalfördelningen klarat nivå 1, vilket kan jämföras mot myndigheternas 51 procent. Sammantaget har gruppen genomfört i genomsnitt 83,9 åtgärder. Inom de olika arbetsområdena har normalfördelningsgruppen, sett utifrån genomsnittet, inte klarat nivå 2 på något arbetsområde, men nivå 1 på fyra arbetsområden.

4.2.4 Resultatförändring mellan mättillfällena

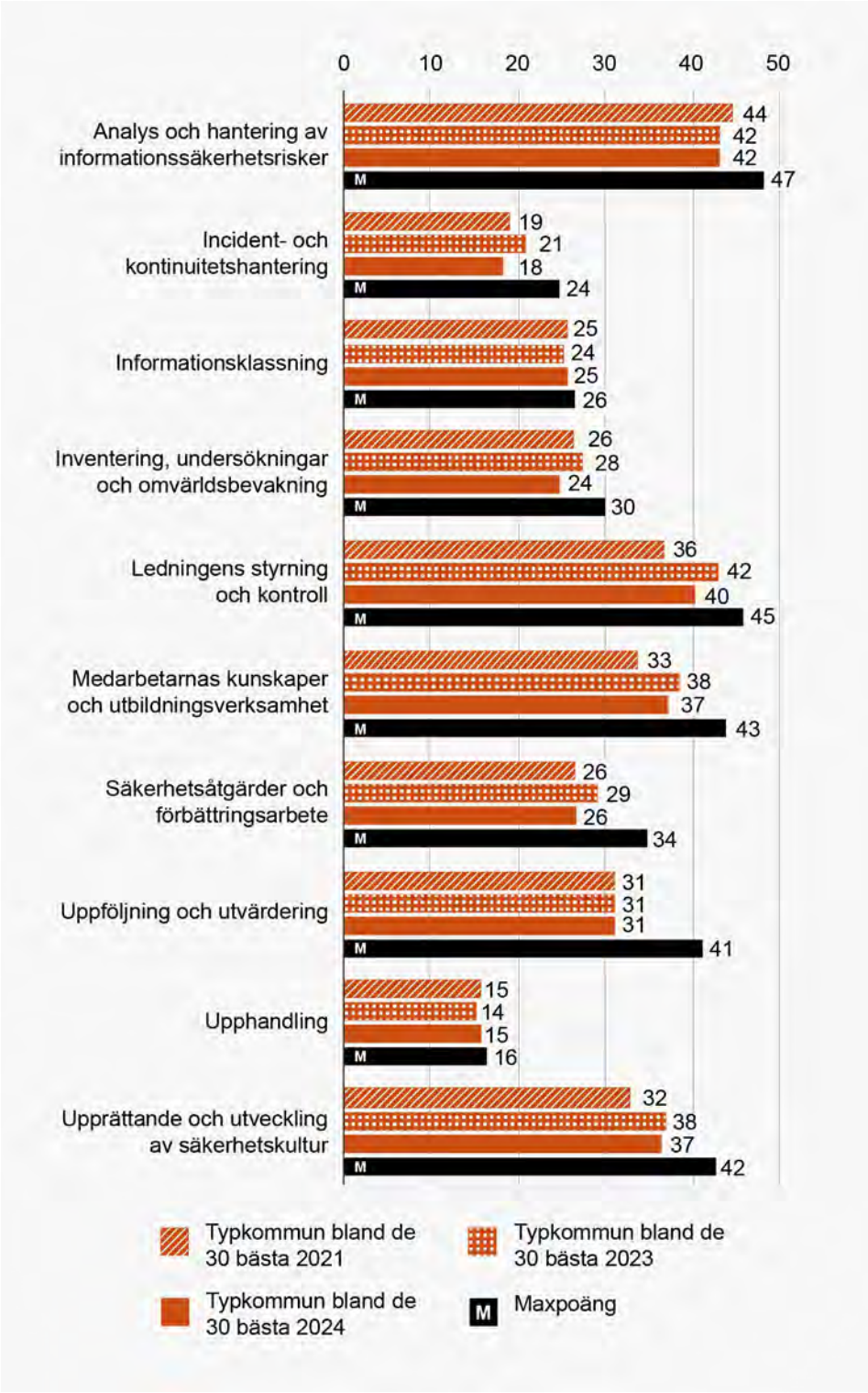
I detta avsnitt kommer resultatförändringen från 2021 till 2024 att redogöras. Vad det anbelangar kommunerna så har typkommunen tagit ett kliv framåt 2024 jämfört med tidigare resultatet.

Diagram 28. Antal genomförda åtgärder per arbetsområde 2021, 2023 och 2024 hos kommunerna



En typkommun 2021 hade genomfört 57 åtgärder (28,5 procent), medan samma typkommun 2023 hade genomfört 91 åtgärder (45,5 procent). Motsvarande antal åtgärder för 2024 är 110 (55,5 procent). Detta utgör en procentuell förbättring 2024 på 20,9 procent jämfört med 2023. Sju av tio arbetsområden har förbättrats sedan det senaste mättillfället. Det är dock viktigt att betänka att en typkommun i tidigare mätningar haft svaga resultat och därmed finns som mest förbättrings-potential inom denna aktörsgrupp.

Diagram 29. Antal genomförda åtgärder per arbetsområde bland de 30 bästa kommunerna 2021, 2023 och 2024



En typkommun av de 30 bästa 2021 hade genomfört 85 procent av möjliga åtgärder, medan en typkommun 2023 hade genomfört 89 procent av alla möjliga åtgärder. År 2024 hade en typkommun bland de 30 bästa genomfört 87 procent av möjliga åtgärder, vilket är en försämring jämfört med 2023 på 2,2 procentenheter.

Att resultatet för typkommunen bland de 30 bästa 2024 är en marginell försämring jämfört med 2023 förklaras av att några av de allra bästa kommunerna i mätningen 2023 inte deltagit 2024.

Diagram 30. Förändring i procent av antal genomförda åtgärder bland de 30 bästa kommunerna 2024 jämfört med 2023

Två arbetsområden visar på en förbättring, medan sju visar på en negativ utveckling. Även om Upphandling förbättras med 7,1 procent så är det enbart en åtgärds skillnad. Att det får så pass stor effekt beror på att Upphandling är det arbetsområdet där minst antal åtgärder mäts.

Diagram 31. Antal genomförda åtgärder per arbetsområde band de 30 bästa kommunerna 2021, 2023 och 2024 utifrån medelvärdet

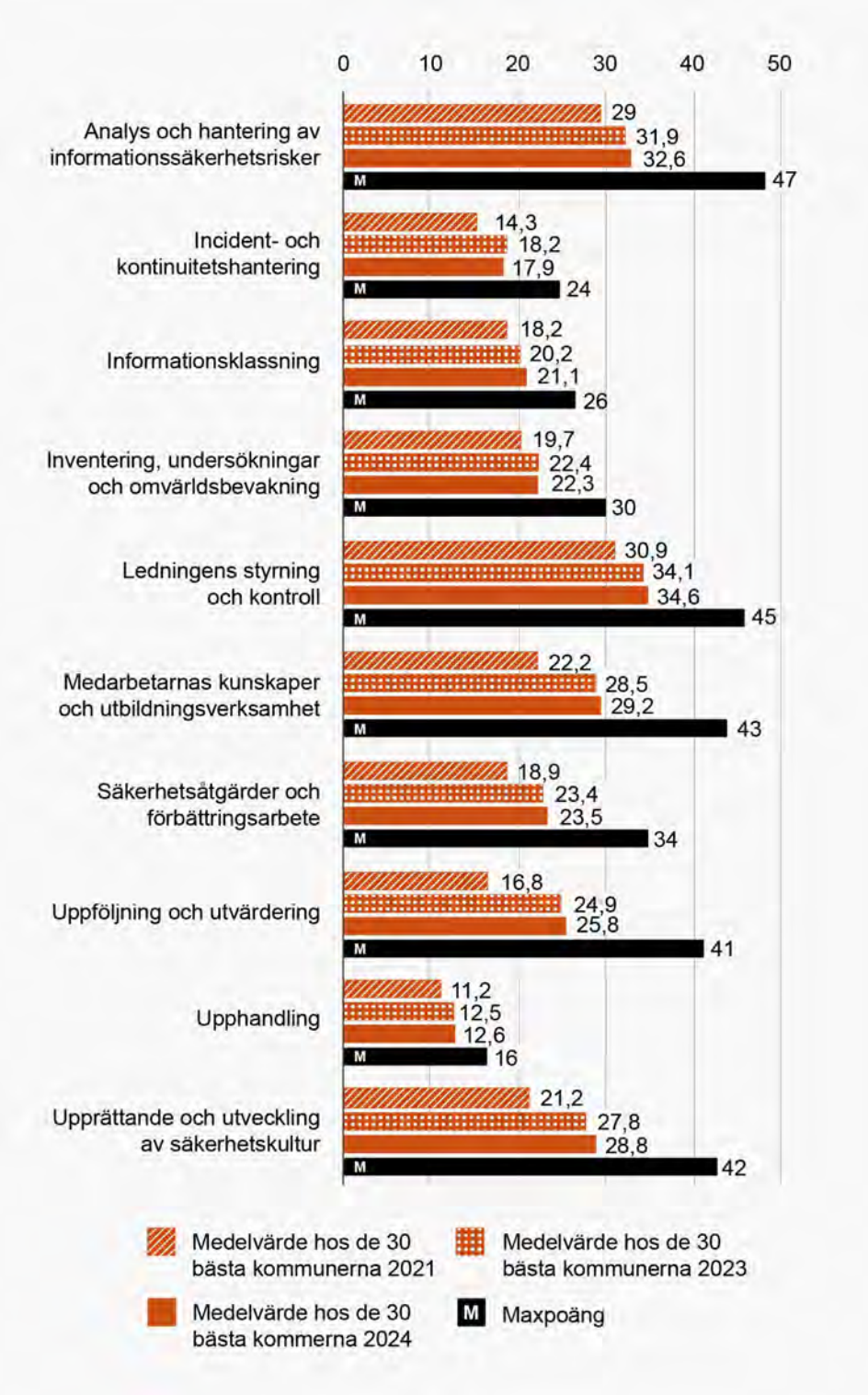


Diagram 29 och 30 ovan redovisade resultatet utifrån benchmarken för en typkommun bland de 30 bästa. Här redovisas istället det genomsnittliga antalet genomförda åtgärder bland de kommuner som var bland de 30 bästa vid de tre olika mättillfällena.

Resultatet ser något annorlunda ut och visar, istället för den marginella försämring som framgick utifrån jämförelsen av typkommunen bland de 30 bästa 2024 jämfört med 2023, istället på en förbättring. Sett utifrån genomsnittet av totalt antal genomförda åtgärder har en kommun bland de 30 bästa 2024 genomfört 149,3 åtgärder, jämfört med 146,2 2023. Detta motsvarar en förbättring på 2,1 procent, trots att några av de allra bästa kommunerna 2023 inte deltog 2024. Att förbättringstakten för gruppen bland de 30 bästa är lägre är att betrakta som naturligt givet att gruppen redan befinner sig på en högre nivå.

Diagram 32. Antalet genomförda åtgärder per arbetsområde bland de kommuner som deltog såväl 2023 som 2024

94 kommuner deltog såväl 2023 som 2024. Ett genomsnitt av resultatet för genomförda åtgärder för de kommuner som deltagit vid båda mättillfällena visar på en förbättring inom samtliga arbetsområden. Mätt i antalet åtgärder har denna grupp i genomsnitt genomfört 14 fler åtgärder 2024 jämfört med 2023.

Totalt 14 fler genomförda åtgärder 2024 hos de kommuner som även deltog 2023 kan jämföras med motsvarande antalet åtgärder för regioner och myndigheter vilka är 10,8 åtgärder för regionerna, respektive 10,6 åtgärder för myndigheterna. Kommunerna är förvisso den aktörsgrupp som genomfört flest åtgärder sedan senaste mätningen, men det bör snarare förstås utifrån kontexten att kommuner presterade svagast i mätningen 2023, varför det fanns fler kvarstående åtgärder att vidta för en genomsnittlig kommun jämfört med de två andra aktörsgrupperna.

Diagram 33. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 för de kommuner som deltog vid båda mättillfällena

De kommuner som deltagit i båda de senaste mätningarna har haft en förbättring på 17,3 procent gällande antalet genomförda åtgärder på hela Infosäkkollen. Det arbetsområde med störst procentuell förbättring är Uppföljning och utvärdering, följt av Incident- och kontinuitetshantering samt Informationsklassning. Det gör att kommunerna är den aktörsgrupp som haft starkast förbättringsutveckling.

Diagram 34. Antalet genomförda åtgärder per arbetsområde bland de kommuner som enbart deltog 2023 eller 2024

De kommuner som enbart deltog 2024 har i snitt genomfört sex färre åtgärder jämfört med de som enbart deltog 2023. Det är endast på ett arbetsområde, Ledningens styrning och kontroll, som fler åtgärder genomförts 2024 jämfört med 2023 och då med en genomsnittlig ökning på 0,2 åtgärder.

Att de kommuner som enbart deltagit 2024 i genomsnitt genomfört färre åtgärder påverkar hela aktörsgruppens resultat negativt. Dock är det endast en skillnad på i genomsnitt 6 färre genomförda åtgärder och antalet kommuner som endast deltog 2023 var 59 stycken, medan antalet kommuner som endast deltog 2024 var 42 stycken. Det betyder att den svagare nya gruppen kommuner som endast deltagit 2024 påverkar hela aktörsgruppen mindre.

Diagram 35. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 bland de kommuner som enbart deltog vid ett av mättillfällena

Den försämring som delgavs i diagram 34 visas i procent i diagram 35 ovan. Antalet nya kommuner, alltså de 42 kommuner som endast deltog 2024, utgör 30,9 procent av det totala antalet deltagande kommuner 2024. Motsvarande procent för 2023 var 38,5 procent. Den försämring som påvisas i diagram 34 och 35 får således ändå en begränsad effekt på hela aktörsgruppens resultat. Förbättringen hos de organisationer som deltog både 2023 och 2024, vilken visades i diagram 32 och 33, är procentuellt sett högre och den populationen är större.

4.2.5 Förutsättningar för samarbeten

På frågorna nedan har en majoritet av kommunerna alternativt den största minoriteten fått enbart ett poäng eller mindre.[25] Frågorna representerar således områden där kommunerna uppvisar brister, samtidigt som de har få andra kommuner att lära från varandras erfarenheter av. Inom dessa områden är det därför av särskild vikt att näringslivet såväl som andra stöttande organisationer på alla nivåer i samhället ser över sitt stöd. Detta berör fråga 14, 16, 18, 20, 21, 22, 23, 26, 27, 30, 33, 34, 35, 36, 37, 39 och 40.

- **Fråga 14**: Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 16**: De senaste två åren, har organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning?
- **Fråga 18**: De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 20**: Har organisationen, de senaste två åren, klassat sin information enligt sitt arbetssätt för informationsklassning?
- **Fråga 21**: De senaste två åren, har organisationen analyserat sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker?
- **Fråga 22**: De senaste två åren, har organisationen använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker?
- **Fråga 23**: De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?
- **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?

Not 25. Under motsvarande rubrik i resultatredovisningen av Cybersäkerhetskollen 2021 och 2023 redovisades frågor där en majoritet av kommunerna inte fått poäng. Givet kommunernas resultatförbättring är det få frågor där en majoritet av svarsunderlaget inte fått några poäng, varför modellen för att identifiera frågor där samarbete är av särskild vikt har justerats i syfte att möta kommunernas utvecklingstakt.

- **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?

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.

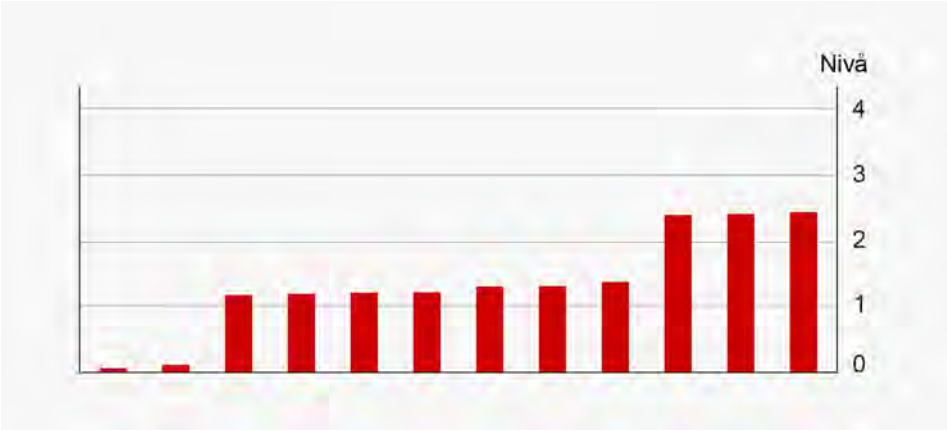
4.3 Regioner

I avsnittet nedan framförs sammanställningen av de tolv 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

Tio utav tolv regioner uppnår nivå 1 eller högre 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 36. Resultattal för samtliga 12 regioner



83,3 procent av deltagande regioner uppnådde nivå 1 eller bättre, 25 procent uppnådde nivå 2. I likhet med 2023 uppnådde ingen region 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 typregionen en indikativ nivå som svarar mot nivå 3.

Diagram 37. Resultat i Infosäkkollen för samtliga regioner

Bland samtliga deltagande regioner har nivå 1 uppnåtts inom fem arbetsområden. Regionerna presterar bäst inom arbetsområdena för Upphandling, Informationsklassning och Säkerhetsåtgärder och förbättringsarbete. Omvänt presterar regionerna svagast inom arbetsområdena för Uppföljning och utvärdering, Upprättande och utveckling av säkerhetskultur och Incident- och kontinuitetshantering.

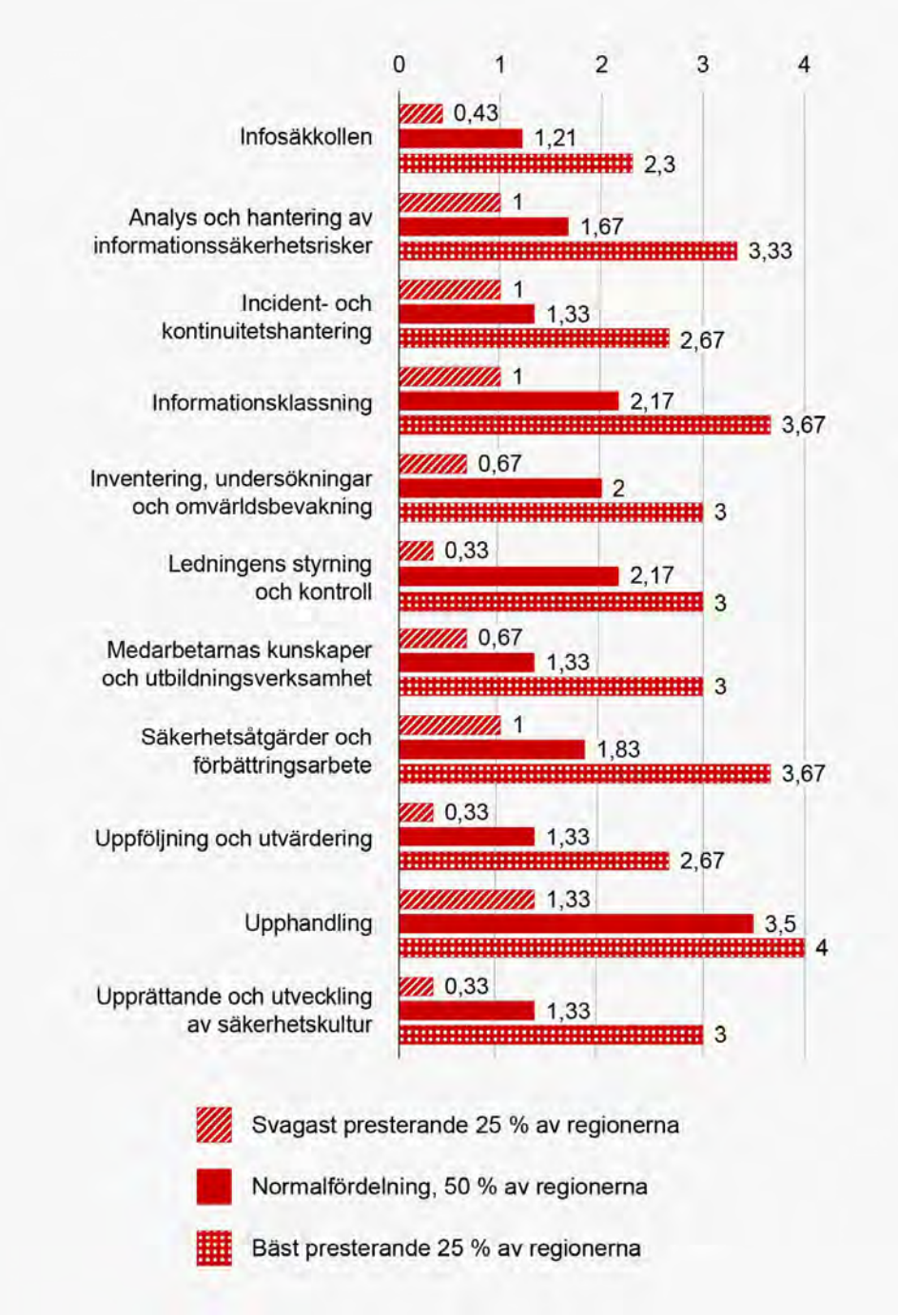
Minst antal deltagande regioner har nått nivå 1 inom arbetsområdet för Uppföljning och utvärdering (83,3 procent), Upprättande och utveckling av säkerhetskultur (83,3 procent) samt Ledningens styrning och kontroll (83,3 procent). Det är exakt samma arbetsområden som 2023.

De arbetsområden där flest deltagande regioner uppnått nivå 3 eller bättre är inom Upphandling (66,7 procent), följt av Informationsklassning (50 procent) och Inventering, undersökningar och omvärldsbevakning (50 procent). Minst antal deltagande regioner har nått nivå 3 eller bättre inom arbetsområdet för Incident- och kontinuitetshantering (16,7 procent) samt Uppföljning och utvärdering (16,7 procent) samt Upprättande och utveckling av säkerhetskultur (25 procent).

4.3.3 Resultatspridning

Diagrammet nedan förtydligar hur mycket de 25 procent bästa regionerna drar upp resultatet för en typregionen i de redovisade diagrammen i kapitel 4.1. Det är en omfattande skillnad mellan resultatet för de 25 procent bästa regionerna jämfört med de 50 procent som här ses som normalfördelningen.

Diagram 38. Resultatspridning hos regionerna



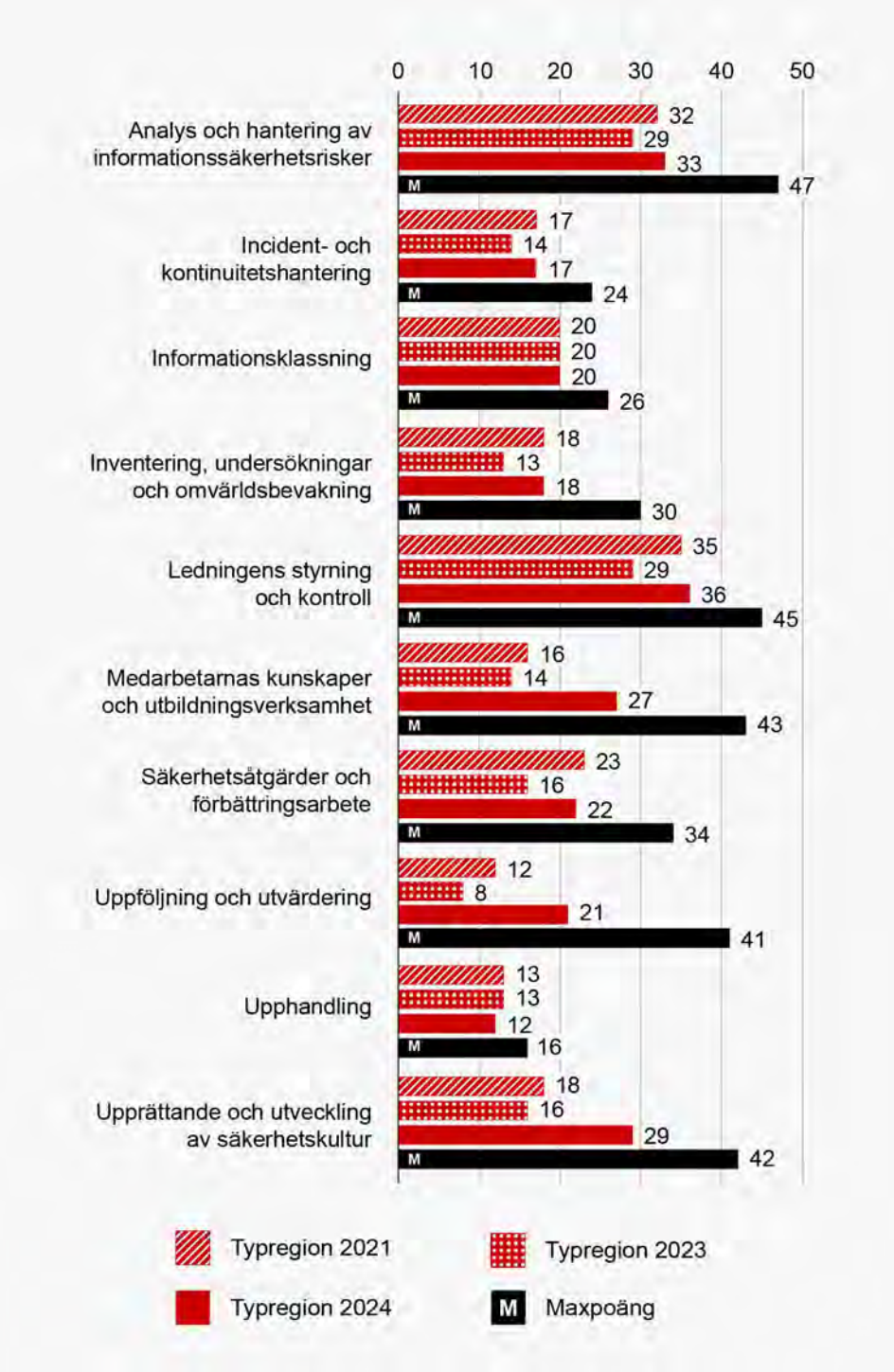
Notera att normalfördelningen i diagrammet är baserad på annan procentsats för regionerna jämfört med kommunerna och myndigheterna. Detta beror på att aktörsgruppen har en liten population, endast 12 organisationer, varför en 10-80-10 struktur som använts för kommuner och myndigheter inte passar för aktörsgruppen regioner.

Det svagaste 25 procenten av regionerna har uppnått nivå 1 inom fem arbetsområden. De 25 procent bästa regionerna har uppnått nivå 3 eller bättre i åtta av modellens arbetsområden. Av de 50 procent av regionerna som utgör normalfördelningen är resultaten varierande. Normalfördelningsgruppen har uppnått nivå 1 på samtliga arbetsområden och nivå 2 eller bättre på fyra arbetsområden.

4.3.4 Resultatförändring mellan mättillfällena

I detta avsnitt redogörs för resultatförändringen mellan de tre mätningar av Infosäkkollen som gjorts. Hos regionerna har typregionen förbättrats 2024 jämfört med resultaten från 2021 och 2023.

Diagram 39. Resultat per arbetsområde 2021, 2023 och 2024 hos regionerna



En typregion 2021 hade genomfört 125 åtgärder (62,5 procent), medan samma typregion 2023 hade genomfört 117 åtgärder (58,5 procent). Motsvarande antal åtgärder för 2024 är 145 (72,5 procent). Resultatet 2024 motsvarar en förbättring på 23,9 procent jämfört med 2023, men 16 procent jämfört med 2021. 2023 deltog 18 av Sveriges samtliga 21 regioner, och i resultatredovisningen för 2023 kunde det konstateras att det ökade antalet deltagande regioner 2023 hade påverkat resultatet negativt jämfört med 2021.

En typregion 2024 presterar bättre på åtta arbetsområden och endast marginellt sämre på kvarvarande två jämfört med resultatet från 2021 och 2023.

Diagram 40. Förändring i procent av antalet genomförda åtgärder hos regionerna mellan 2023 och 2024

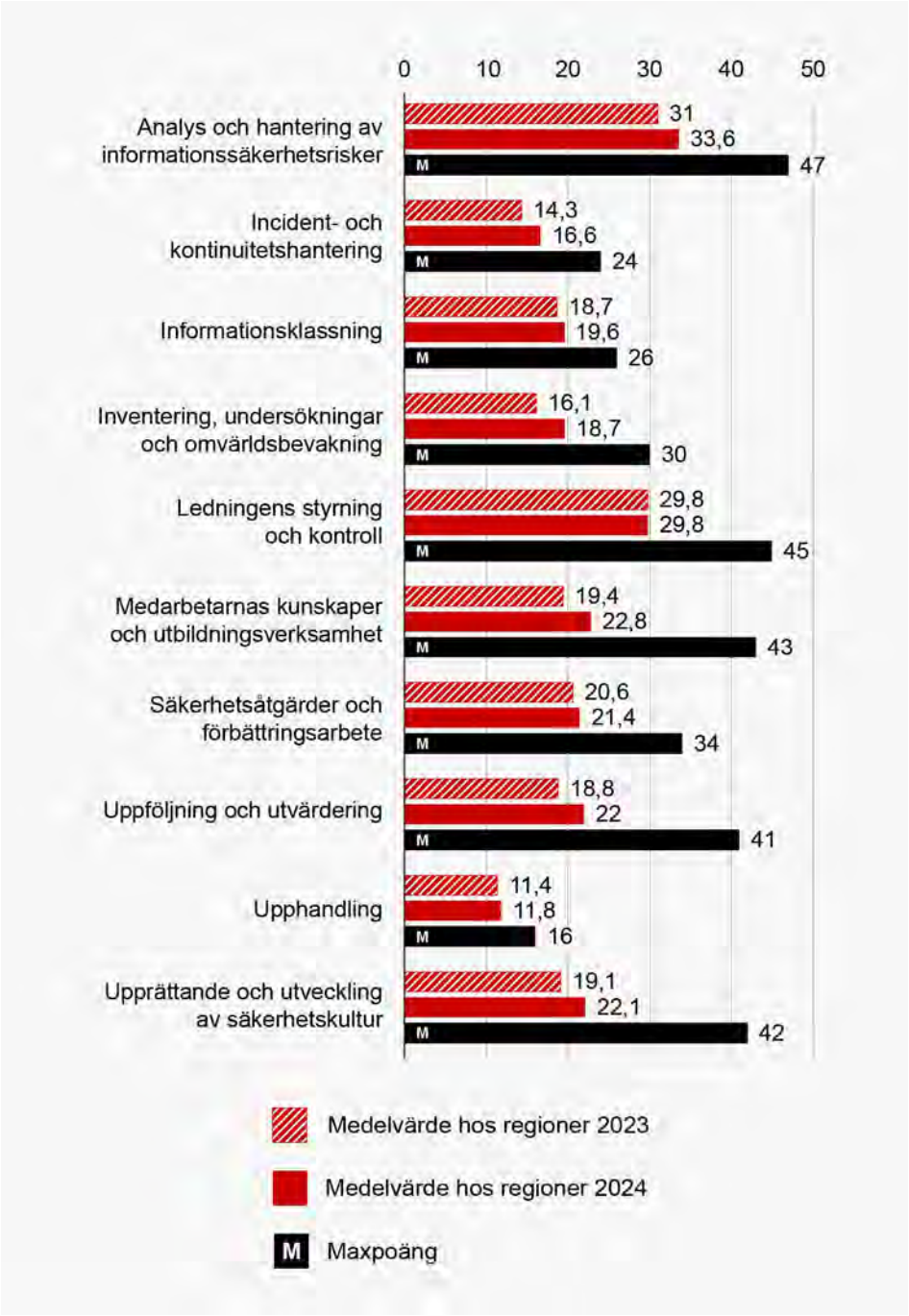
Att antalet deltagande regioner minskat har haft en positiv effekt på resultatet 2024 jämfört med 2023. Detta är dock en chimär som förklaras av att de svagare regionerna som deltog 2023 inte deltagit 2024. Diagram 40 och övriga diagram som jämfört resultaten mellan mätningarna 2024 och 2023 ska förstås i den kontexten och därför utläsas med försiktighet.

Diagram 41. Förändring i procent av antalet genomförda åtgärder hos regionerna mellan 2021 och 2024

Diagrammet ovan jämför förändringen hos en typregion 2024 med resultatet från 2021. Den jämförelsen presenteras inte för aktörsgrupperna kommuner och myndigheter eftersom antalet deltagande organisationer inom de aktörsgrupperna gör det mer värdefullt att jämföra resultaten från de senaste två mätningarna. Som noterats ovan är regionernas deltagande en faktor med stor påverkan på resultatförändringen och aktörsgruppen jämförs i detta fall bäst utifrån mätningarna 2024 och 2021.

På de tre år som passerat mellan mätningarna är det tre arbetsområden där en större förbättring kan ses. Förbättringen inom dessa arbetsområden svarar nästan för hela av den sextonprocentiga förbättringen på helheten. Tre arbetsområden är oförändrade och två arbetsområden uppvisar en försämring. Även om båda försämringarna endast handlar om en åtgärd färre genomförd per arbetsområde 2024 jämfört med 2021, är det noterbart att en försämring ens inträffat.

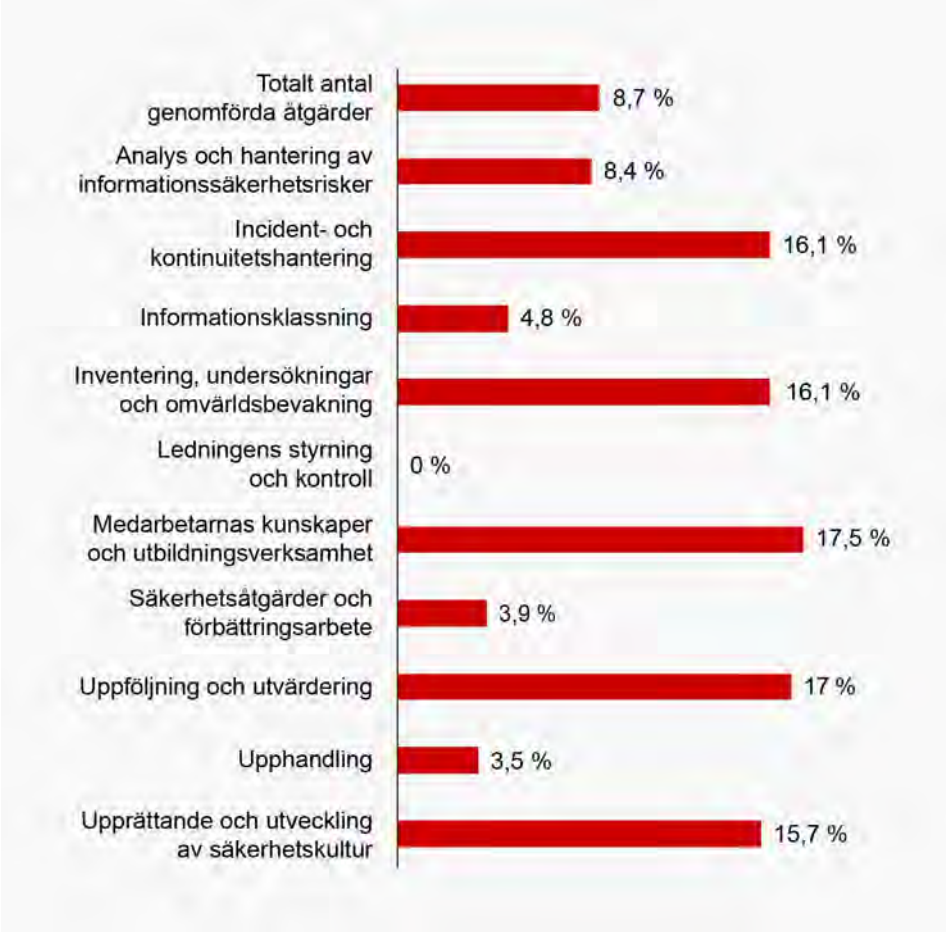
Diagram 42. Antalet genomförda åtgärder per arbetsområde bland de regioner som deltog såväl 2023 som 2024



Det var tio regioner som deltog både 2023 och 2024. Mätt i antalet genomförda åtgärder per region ser utvecklingen inte lika drastisk ut som den gjorde i diagram 35 där typregionens svar jämfördes. Samtidigt har de regioner som deltog både 2023 och 2024 genomfört i genomsnitt 10,8 fler åtgärder 2024 jämfört med 2023.

10,8 fler genomförda åtgärder 2024 hos de regioner som även deltog 2023 kan jämföras med motsvarande antalet åtgärder för kommuner och myndigheter vilka är 14 åtgärder för kommunerna, respektive 10,6 åtgärder för myndigheterna. Regionerna är således den aktörsgrupp som varken genomfört minst eller flest åtgärder sedan senaste mätningen. Detta bör dock snarare förstås utifrån kontexten att kommuner presterade svagast, och myndigheter bäst, i mätningen 2023, varför det därför exempelvis fanns fler kvarstående åtgärder att vidta för en genomsnittlig region jämfört med en myndighet. I detta sammanhang bör det också noteras att skillnaden i antalet genomförda åtgärder för regionerna respektive myndigheterna är liten.

Diagram 43. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 för de regioner som deltog vid båda mättillfällena



De regioner som deltagit i båda de senaste mätningarna har haft en förbättring på 8,7 procent gällande antalet genomförda åtgärder på hela Infosäkkollen. Det gör att regionerna är den aktörsgrupp som har haft svagast förbättringsutveckling.

De arbetsområden med störst procentuell förbättring är Medarbetarnas kunskaper och utbildningsverksamhet, följt av Uppföljning och utvärdering,

Det var åtta regioner som deltog 2023 som inte rapporterade in sitt resultat 2024, och omvänt två regioner som deltog 2024 som inte deltog även 2023. Att det bara är två organisationer som utgör populationen för 2024 gör att MSB avstår från att publicera en jämförelse då enskilda organisationers resultat riskerar att synliggöras.

4.3.5 Förutsättningar för samarbeten

På frågorna nedan har en majoritet av regionerna alternativt den största minoriteten fått enbart ett poäng eller mindre.[26] Frågorna representerar således områden där regionerna uppvisar brister, samtidigt som de har få andra regioner att lära från varandras erfarenheter av. Inom dessa områden är det därför av särskild vikt att näringslivet såväl som andra stöttande organisationer på alla nivåer i samhället ser över sitt stöd. Detta berör fråga 5, 22, 26, 27 och 39.

- **Fråga 5**: Har organisationen de senaste två åren undersökt medarbetarnas kunskaper om informationssäkerhet?
- **Fråga 22:** De senaste två åren, har organisationen använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker?
- **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 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.

Not 26. Under motsvarande rubrik i resultatredovisningen av Cybersäkerhetskollen 2021 och 2023 redovisades frågor där en majoritet av regionerna inte fått poäng. Givet regionernas resultatförbättring finns det inga frågor där en majoritet av svarsunderlaget saknar poäng, varför modellen för att identifiera frågor där samarbete är av särskild vikt har justerats i syfte att möta regionernas utvecklingstakt.

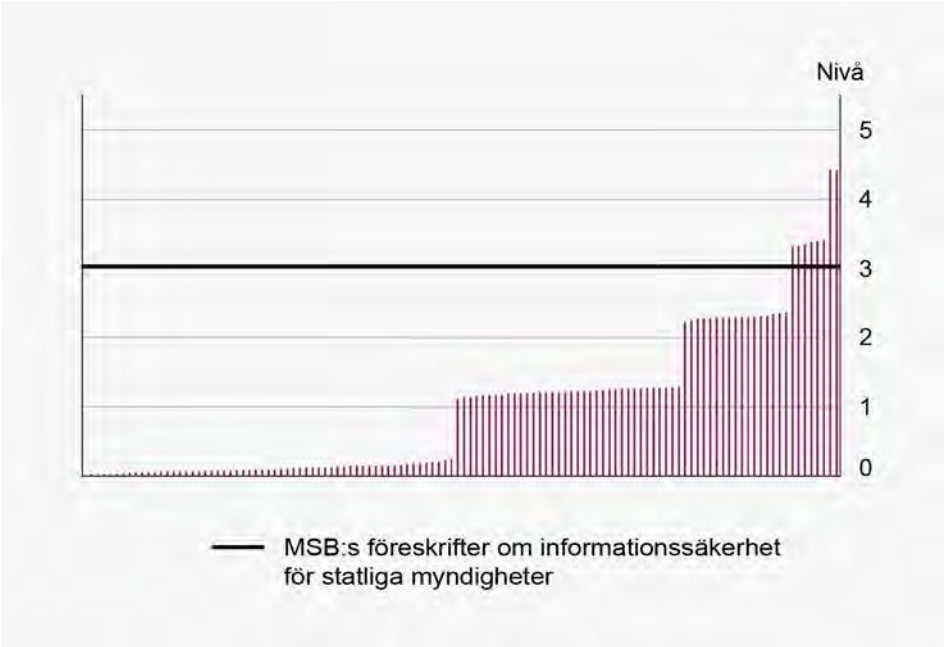
4.4 Myndigheter

I det här kapitlet redogörs för sammanställningen av resultatet för 120 inrapporterande myndigheter. Det är exakt samma antal myndigheter som deltog 2023. 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

61 myndigheter uppnår nivå 1 eller högre i Infosäkkollen 2023. 49,2 procent 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 44. Resultattal för samtliga 120 myndigheter



Den svarta 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.

50,8 procent av deltagande myndigheter uppnådde nivå 1 eller mer, 20,8 procent uppnådde nivå 2 eller mer, och 6,7 procent uppnådde nivå 3 eller 4 i modellen. Motsvarande resultat för 2023 var att 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.

Åtta av 120 myndigheter når det samlade resultat, nivå 3, som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet[27]. Den första utgåvan av föreskrifterna trädde ikraft 2009. Jämfört med resultatet 2023 är det en fördubbling, från fyra till åtta myndigheter, men det innebär samtidigt att 112 av 120 deltagande myndigheter inte klarar föreskriftskraven på informationssäkerhet.

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 sju arbetsområden. Det är på indikativ nivå tre fler arbetsområden jämfört med resultatet 2023. De 30 bästa myndigheterna är däremot svagare än de som deltog 2023. 2023 uppnådde de 30 bästa myndigheterna nivå 3, och därmed även MSB:s föreskriftskrav, men i mätningen 2024 uppnåddes endast nivå 2 av de 30 bästa myndigheterna.

Diagram 45. Resultat i Infosäkkollen för samtliga myndigheter

Not 27. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

De arbetsområden där flest deltagande myndigheter uppnått nivå 1 är inom Säkerhetsåtgärder och förbättringsarbete (99,2 procent), följt av Informationsklassning (88,3 procent) och därefter Analys och hantering av informationssäkerhetsrisker (85 procent). Det är samma arbetsområden som i mätningen 2023.

Minst antal deltagande myndigheter har nått nivå 1 inom arbetsområdet för Ledningens styrning och kontroll (61,7 procent), följt av Uppföljning och utvärdering (63,3 procent) och Incident- och kontinuitetshantering (73,3 procent).

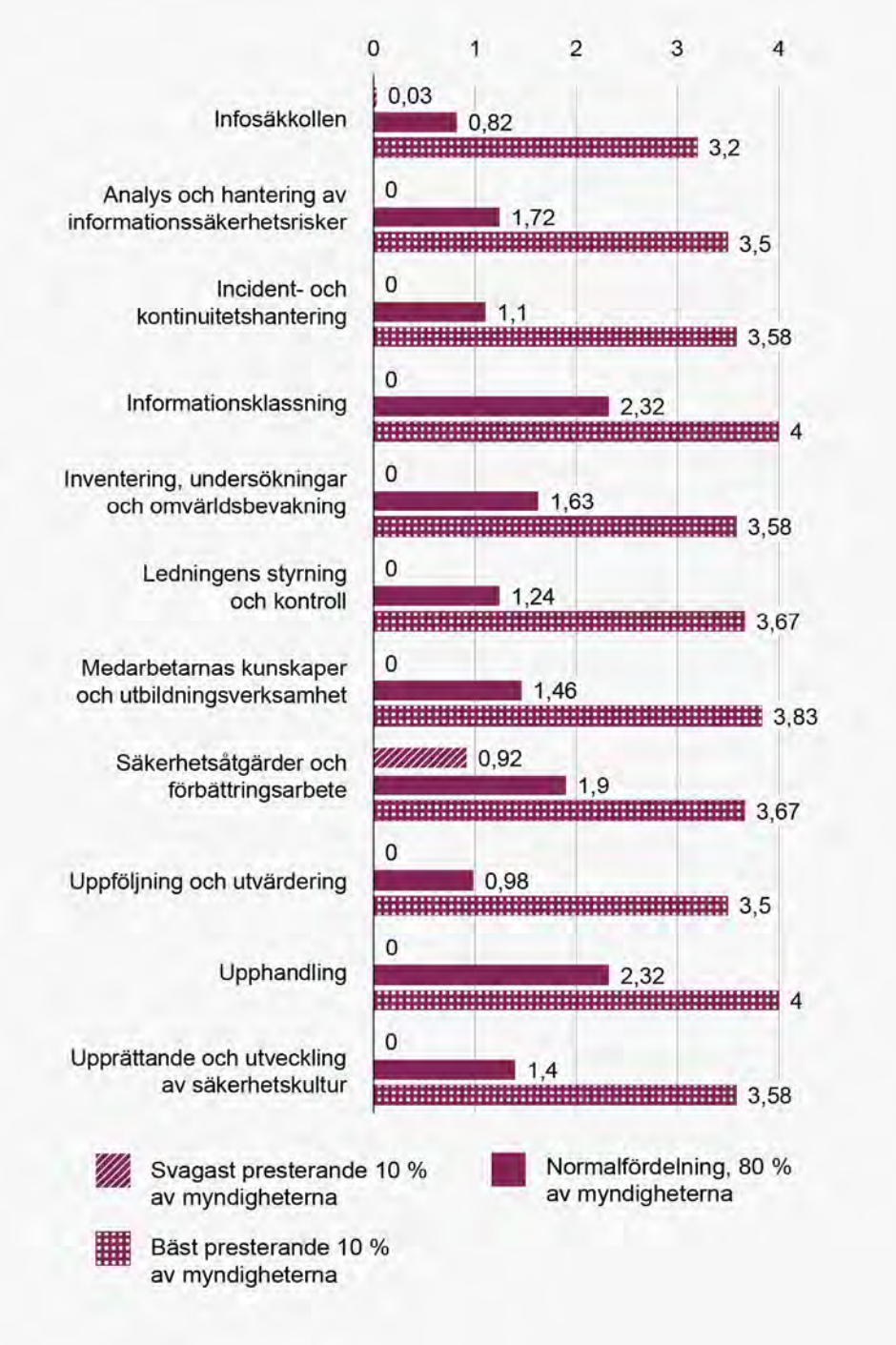
De arbetsområden där flest deltagande myndigheter uppnått nivå 3 eller bättre är inom Informationsklassning (51,7 procent), följt av Upphandling (50 procent) och därefter delas tredjeplatsen av de två arbetsområdena för Inventering, undersökningar och omvärldsbevakning samt Säkerhetsåtgärder och förbättringsarbete (33,3 procent).

Minst antal deltagande myndigheter har nått nivå 3 eller bättre inom arbetsområdet för Incident- och kontinuitetshantering och Uppföljning och utvärdering (båda 15 procent), samt Analys och hantering av informationssäkerhetsrisker (19,2 procent).

4.4.3 Resultatspridning

Diagrammet nedan påvisar, precis som med kommunerna tidigare, hur mycket de 10 procent bästa myndigheterna drar upp resultatet för en typmyndighet i de redovisade diagrammen i kapitel 4.1. 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.

Diagram 46. Resultatspridning hos myndigheterna



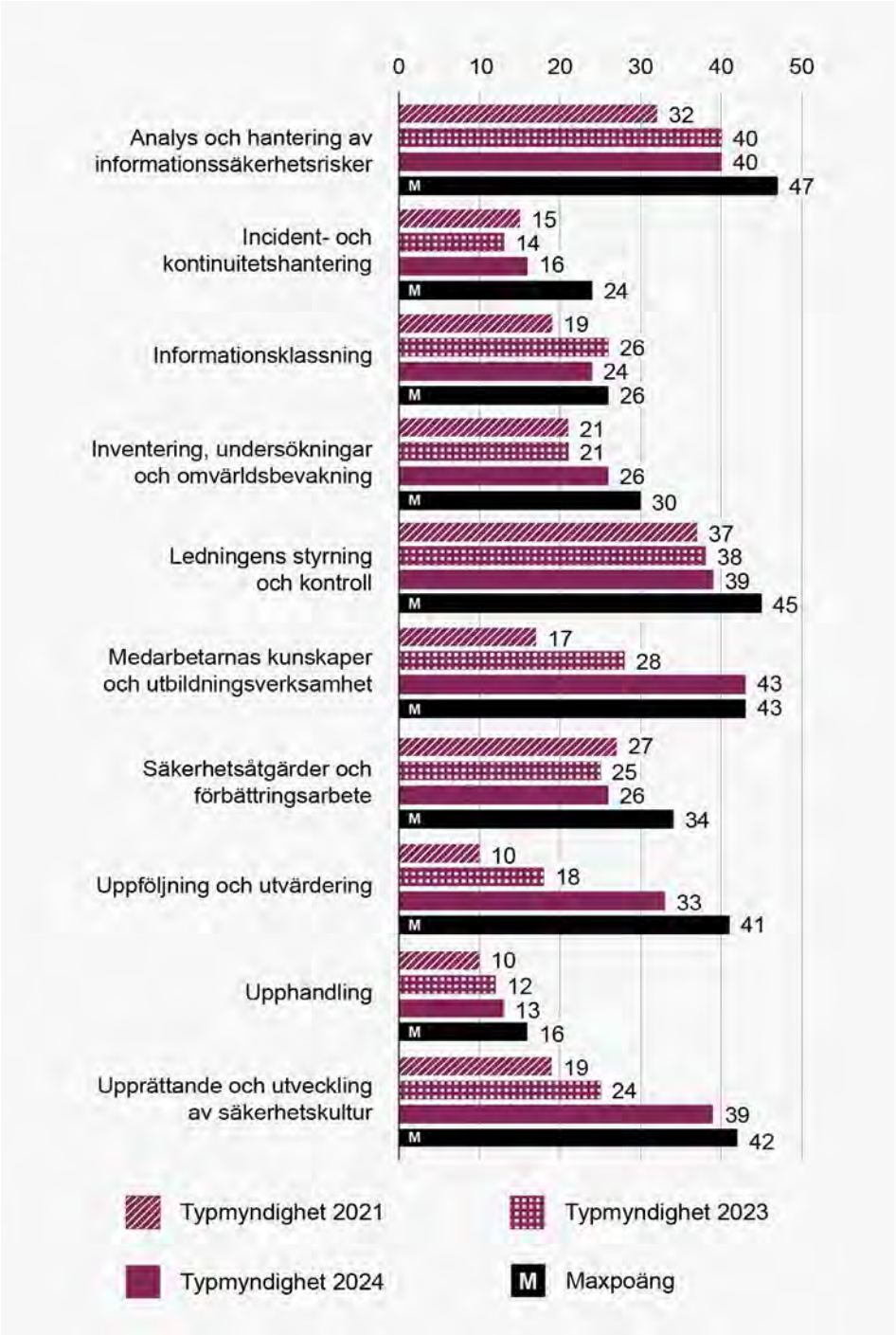
Det svagaste tio procenten av myndigheterna har enbart uppnått ett egentligt påvisbart resultat inom ett arbetsområde, Säkerhetsåtgärder och förbättringsarbete. De tio procent bästa myndigheterna har däremot uppnått nivå 3 inom samtliga arbetsområden, samt maxresultat i modellens arbetsområden för Informationsklassning och Upphandling.

Av de 80 procent av myndigheterna som utgör normalfördelningen är resultatspridningen relativt stor. På Infosäkkollen som helhet når inte gruppen nivå 1 (0,82), även om det är bättre jämfört med kommunerna (0,35). Normalfördelningsgruppen har uppnått nivå 1 eller bättre i nio av modellens tio arbetsområden. Detta inkluderar två arbetsområden där gruppen nått över nivå 2, vilket indikerar att dessa organisationer bedriver sitt informations- och cybersäkerhetsarbetet med en viss systematik. På Infosäkkollen som helhet har 51 procent av myndigheterna i normalfördelningen klarat nivå 1, vilket kan jämföras mot kommunernas 24,1 procent.

4.4.4 Resultatförändring mellan mättillfällena

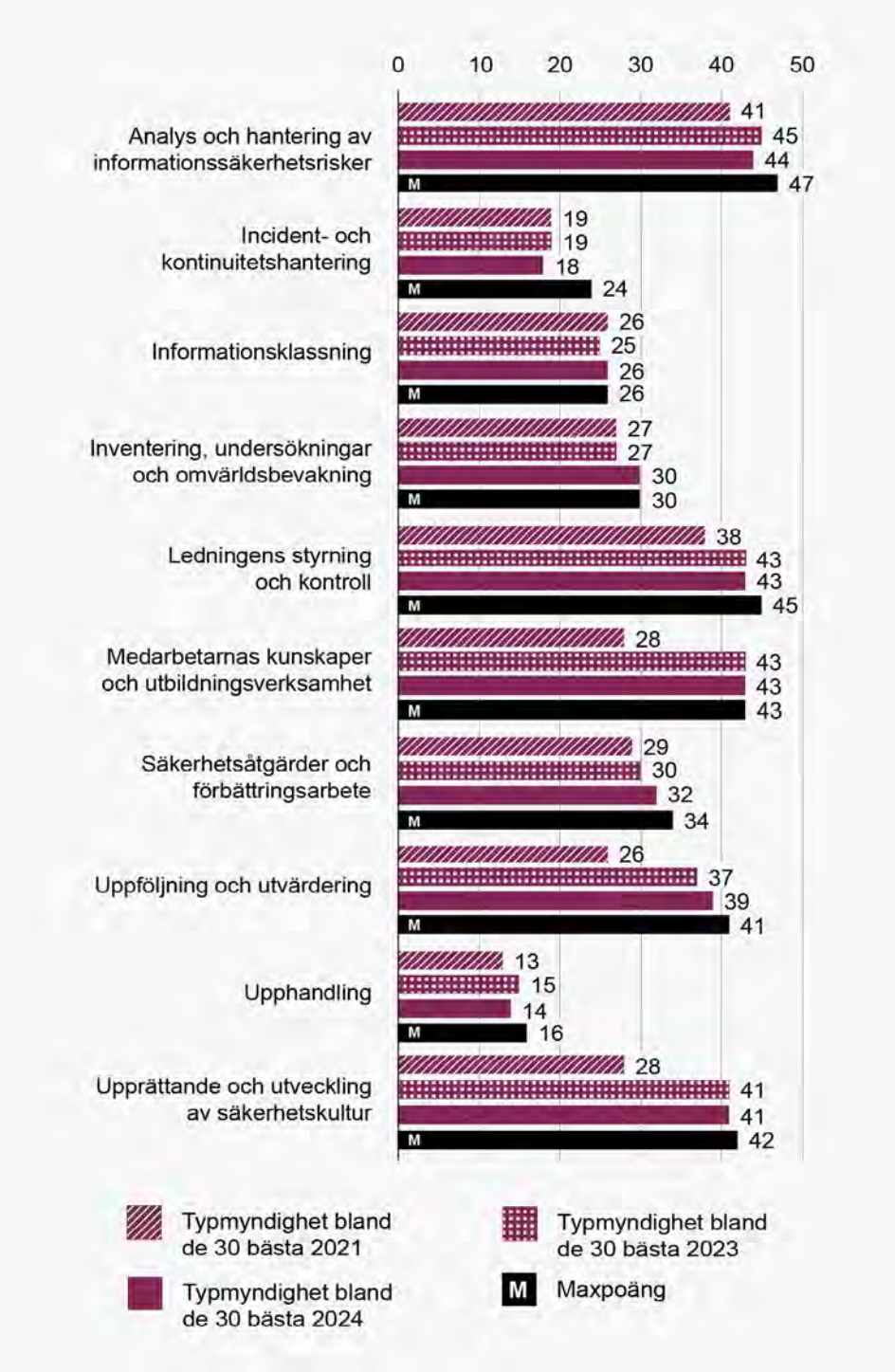
I detta avsnitt kommer resultatförändringen hos myndigheter mellan 2021 till 2024 presenteras. Typmyndigheten har förbättrat sitt resultat 2024 jämfört både resultaten från 2021 och 2023.

Diagram 47. Antal genomförda åtgärder per arbetsområde 2021, 2023 och 2024 hos myndigheterna



En typmyndighet hade genomfört 135 möjliga åtgärder år 2021 (67,5 procent), medan samma typmyndighet hade genomfört 154 åtgärder 2023 (77 procent). I mätningen 2024 hade en typmyndighet genomfört 170 åtgärder (85 procent). Resultatet 2024 motsvarar en ökning med 10,4 procent jämfört 2023. Resultatet har förbättrats inom åtta arbetsområden, och väsentligt bättre på tre arbetsområden nämligen Medarbetarnas kunskaper och utbildningsverksamhet, Uppföljning och utvärdering och Upprättande och utveckling av säkerhetskultur.

Diagram 48. Antal genomförda åtgärder per arbetsområde bland de 30 bästa myndigheterna 2021, 2023 och 2024

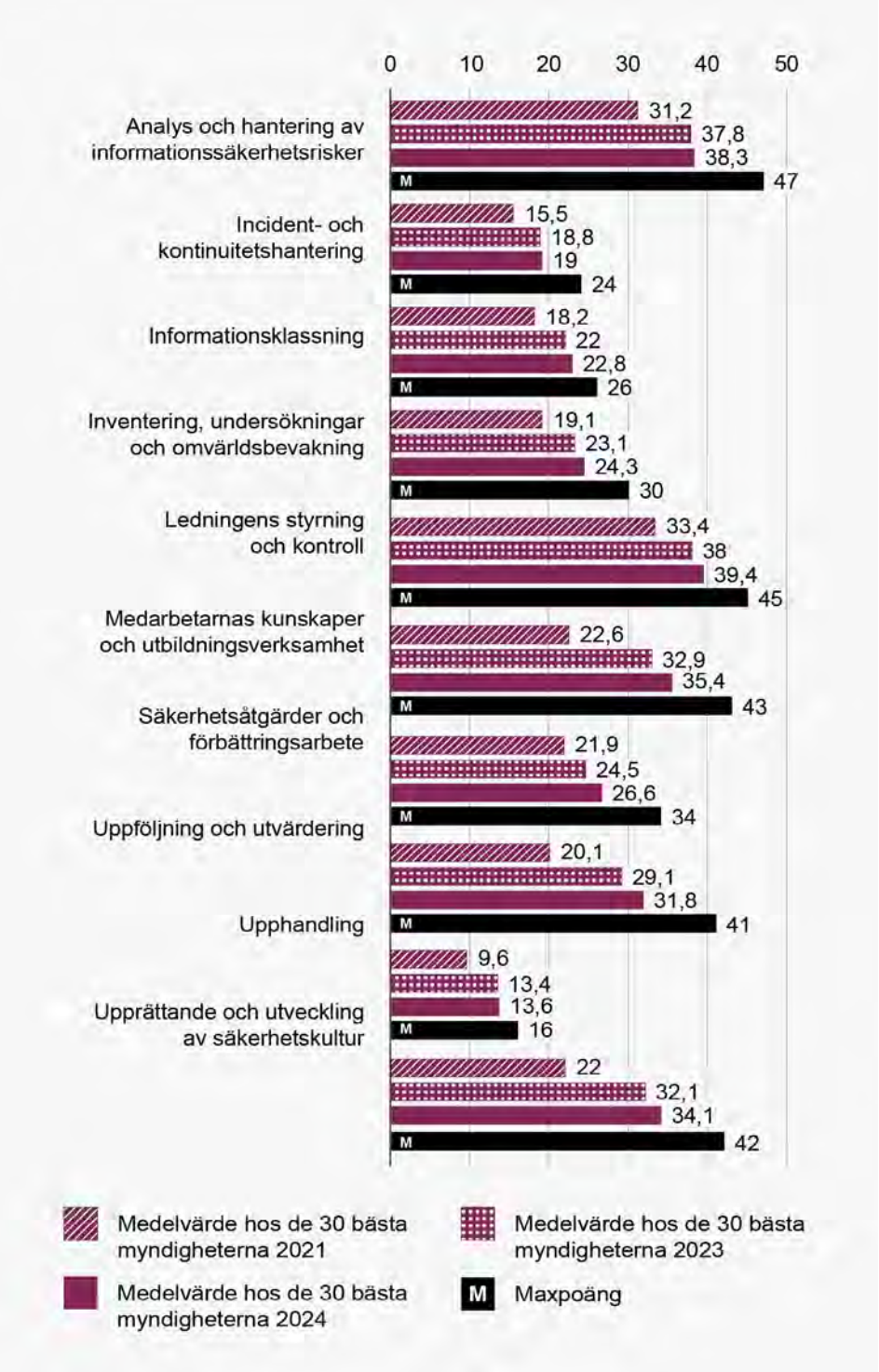


En typmyndighet av de 30 bästa 2021 hade genomfört 80,5 procent av alla möjliga åtgärder, medan samma aktör 2023 hade genomfört 93 procent. Motsvarande för 2024 var 94,5 procent av alla möjliga åtgärder. En typmyndighet bland de 30 bästa 2024 har genomfört tre fler åtgärder jämfört med en typmyndighet 2023.

Diagram 49. Förändring i procent av antalet genomförda åtgärder bland de 30 bästa myndigheterna 2024 jämfört med 2023

Diagram 49 ovan ska utläsas med viss försiktighet. Det är totalt elva åtgärder som förändrats mellan mätningarna, och som konstaterades i diagram 48 ovan så har en typmyndighet bland de 30 bästa genomfört tre fler åtgärder jämfört med samma typmyndighet 2023. Att den procentuella förändringen ser relativt stor ut beror på att det inom varje enskilt arbetsområde inte mäts på så många åtgärder. Dock är procenttalet för helheten, totalt antal genomförda åtgärder, en god indikator och där ses en förbättring på 1,6 procent mellan de två mättillfällena.

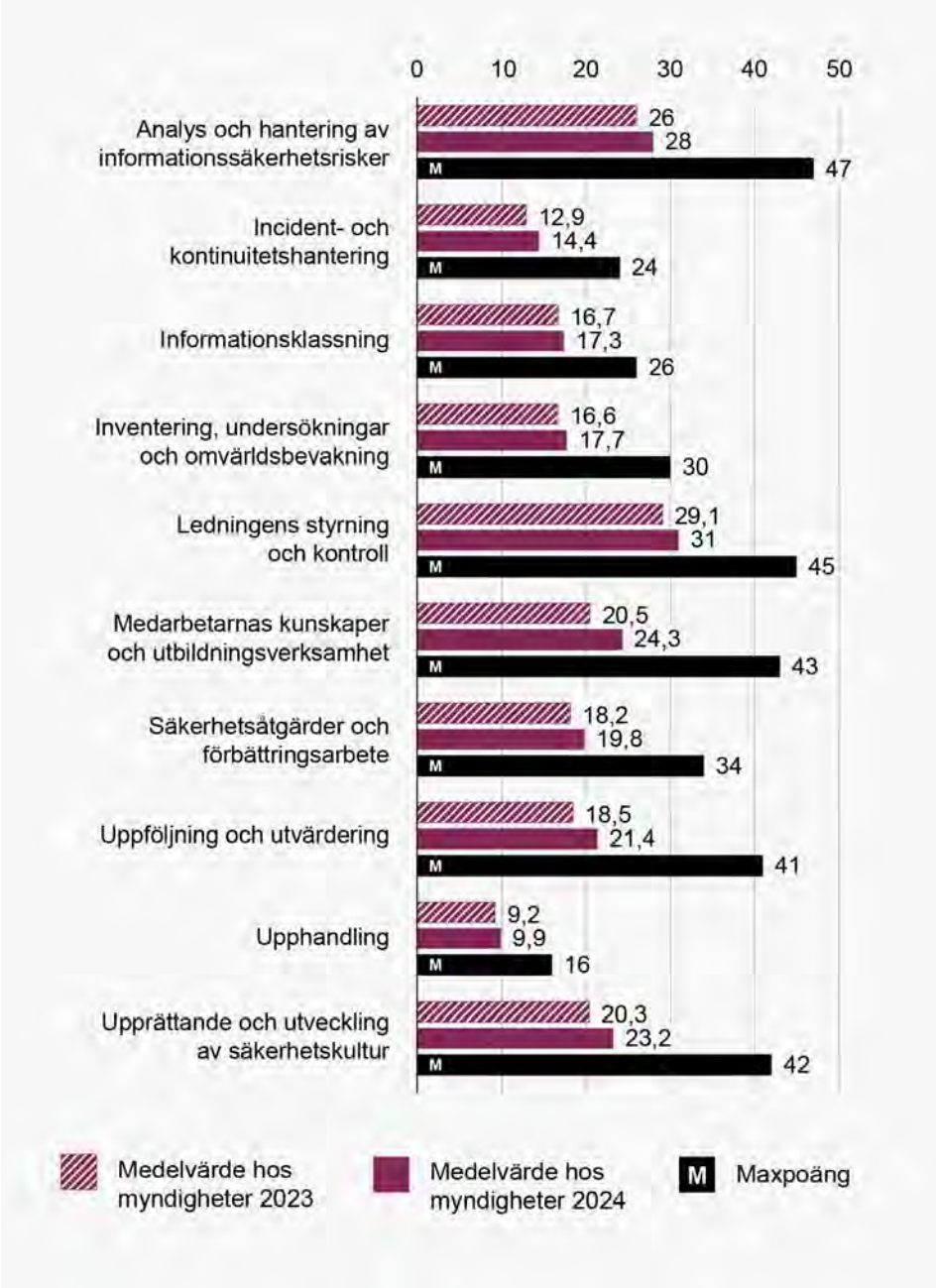
Diagram 50. Antalet genomförda åtgärder per arbetsområde bland de 30 bästa myndigheterna 2021, 2023 och 2024 utifrån medelvärdet



I diagram 48 och 49 ovan redovisades för resultatet utifrån benchmark, en typ-myndighet, bland de 30 bästa. Här redovisas istället det genomsnittliga antalet genomförda åtgärder bland de myndigheter som var bland de 30 bästa vid de tre olika mättillfällena.

Resultatet är förvisso snarlikt, men förtydligar att lägstanivån bland de 30 bästa myndigheterna har höjts i mätningen 2024 jämfört med 2023. Utifrån ett genomsnitt bland de 30 bästa har 6,6 fler åtgärder genomförts 2024 jämfört med 2023.

Diagram 51. Antalet genomförda åtgärder bland de myndigheter som deltog såväl 2023 som 2024



89 myndigheter deltog både 2023 och 2024. Ett genomsnitt av resultatet för genomförda åtgärder för de myndigheter som deltagit vid båda mättillfällena visar på förbättring inom alla arbetsområden.

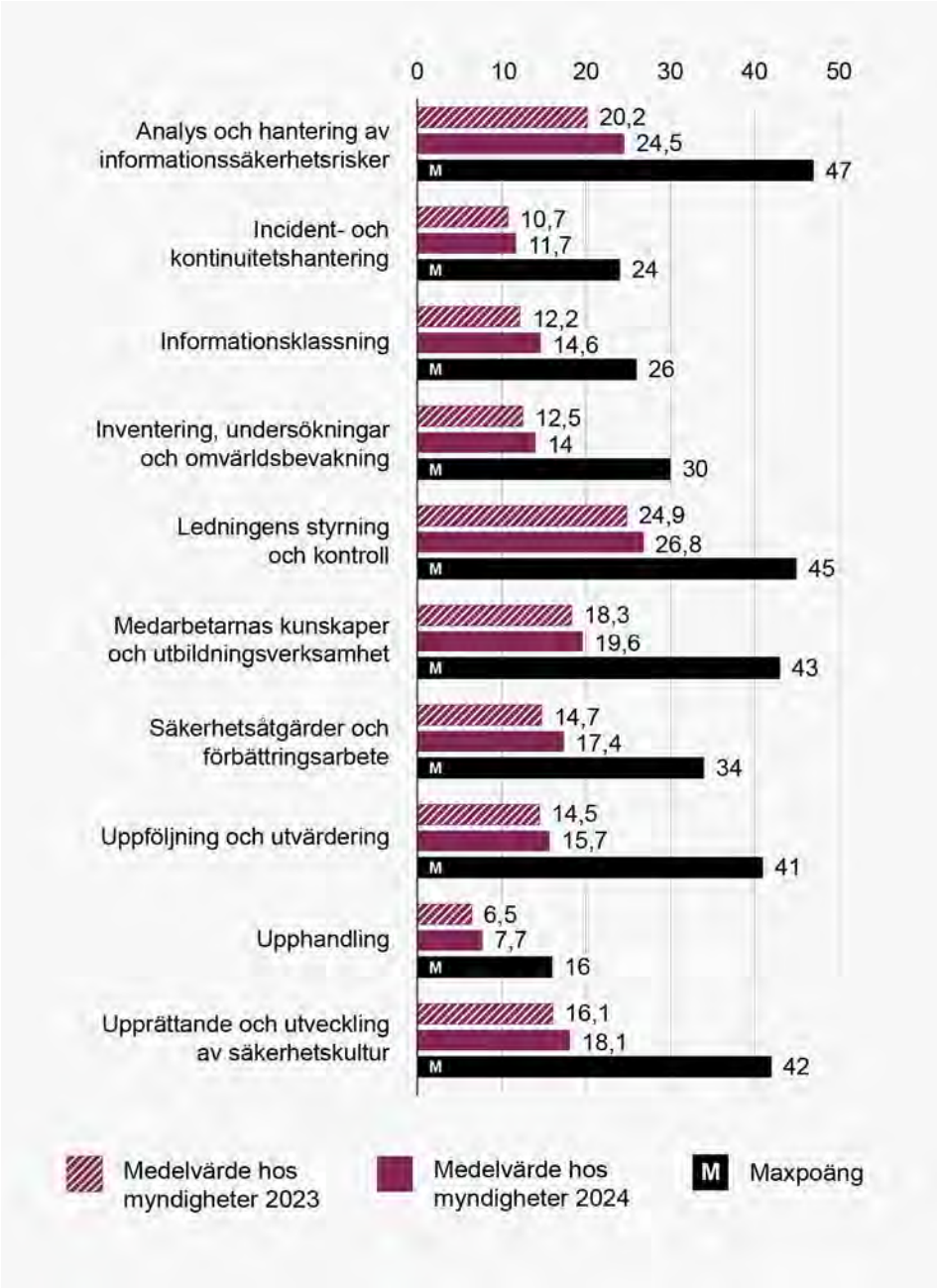
Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 10,6 procentig resultatförbättring av hela Infosäkkollen. Förbättringen är marginellt större än utvecklingen hos de regioner som deltog vid båda mättillfällena, men mindre än den förbättring som de kommuner som deltagit vid båda mätningarna haft. Myndigheterna är dock den aktörsgrupp som hade bäst resultat vid tidigare mätningar, varför de rimligtvis har mindre utrymme för faktisk förbättring jämfört med andra aktörsgrupper.

Diagram 52. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 för de myndigheter som deltog vid båda mättillfällena

Utifrån genomsnittet har de myndigheter som deltog både 2023 och 2024 genomfört 10,6 fler åtgärder 2024 jämfört med 2023. Det motsvarar en förändring på 9,2 procent.

För fyra arbetsområden är förbättringen över tio procent. Den procentuella förändringen ska återigen utläsas med försiktighet. För det arbetsområde där bäst procentuell förbättring förekommit, Medarbetarnas kunskaper och utbildningsverksamhet, har i genomsnitt 3,8 fler åtgärder genomförts 2024 jämfört med 2023, vilket alltså motsvarar en ökning på 18,7 procent.

Diagram 53. Antalet genomförda åtgärder per arbetsområde bland de myndigheter som enbart deltog 2023 eller 2024



31 myndigheter som deltog 2023 avstod från deltagande 2024. Exakt samma antal deltog 2024, men avstod 2023. Diagrammet ovan visar att de myndigheter som endast deltog 2024 har presterat bättre på samtliga arbetsområden. I jämförelse med diagram 51 kan det också konstateras att de organisationer som inrapporterar Infosäkkollen vid varje mättillfälle presterar bättre än de organisationer som gör det sporadiskt. En indikator på att de organisationer som arbetar systematiskt uppnår bättre resultat och ökad förbättringstakt.

Diagram 54. Förändring i procent av antalet genomförda åtgärder 2024 jämfört med 2023 bland de myndigheter som enbart deltog vid ett av mättillfällena

Den genomsnittliga förändringen för totalt antal genomförda åtgärder är en förbättring på 10,9 procent mellan de myndigheter som enbart deltog 2024 jämfört med de som enbart deltog 2023. Detta påvisar att många av de myndigheter med svagast resultat 2023 inte deltagit igen 2024, medan de som enbart deltagit 2024 fått bättre resultat visavi de som deltog 2023.

Således har hela aktörsgruppens övergripande resultat påverkats positivt, även om cybersäkerhetsarbetet för samtliga inom 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. Tio myndigheter fått mindre än 50 poäng, av Infosäkkollens totalt 200 poäng. Ingen av dessa har uppnått nivå 1. 86 myndigheter har fått mer än 100 poäng, men 26 av dem ändå inte uppnått nivå 1 då de har saknat bredden i arbetet, huvudsakligen på grund av brister avseende Uppföljning och utvärdering, Ledningens styrning och kontroll samt Incident- och kontinuitetshantering. 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 åtta 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 fjorton 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

På frågorna nedan har en majoritet av myndigheterna alternativt den största minoriteten fått enbart ett poäng eller mindre.[28] Frågorna representerar således områden där myndigheterna uppvisar brister, samtidigt som de har få andra myndigheter att lära från varandras erfarenheter av. Inom dessa områden är det därför av särskild vikt att näringslivet såväl som andra stöttande organisationer på alla nivåer i samhället ser över sitt stöd. Detta berör fråga 27 och 35.

- **Fråga 27:** Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 35:** De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala typer av sannolikhetsbedömning?

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.

Not 28. Under motsvarande rubrik i resultatredovisningen av Cybersäkerhetskollen 2021 och 2023 redovisades frågor där en majoritet av myndigheterna inte fått poäng. Givet myndigheternas resultatförbättring finns det inga frågor där en majoritet av svarsunderlaget saknar poäng, varför modellen för att identifiera frågor där samarbete är av särskild vikt har justerats i syfte att möta myndigheternas utvecklingstakt.

Resultatet av It-säkkollen 2024

5. Resultatet av It-säkkollen 2024

I det här kapitlet redogörs för resultatet i It-säkkollen 2024 för alla organisationer i offentlig förvaltning. It-säkkollen 2024 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).

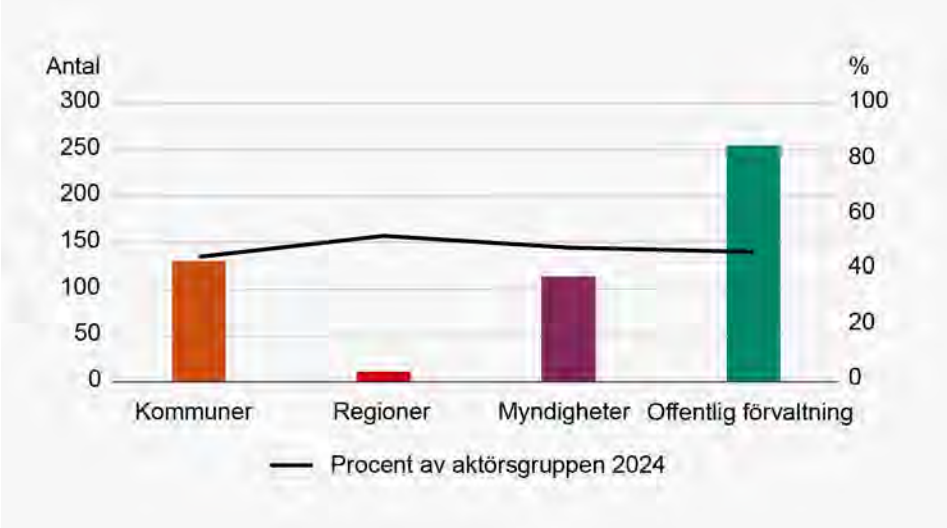
Självskattningsenkäter är problematiska. De lämnar ett stort tolkningsutrymme hos respondenten, vilket påverkar trovärdigheten av insamlade data. Respondenter brukar särskilt överskatta sin egen förmåga. Redogörelsen av resultatet för It-säkkollen kan inte jämställas med trovärdigheten i svaren för Infosäkkollen. De nivåangivelser som anges är inte heller kalibrerade mot MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).[29]

5.1 Övergripande bild

5.1.1 Deltagande

Totalt deltog 256 organisationer från offentlig förvaltning i It-säkkollen 2024. Av dessa var 131 kommuner, 11 regioner och 114 myndigheter. 46,7 procent av offentlig förvaltning deltog i It-säkkollen. Det betyder att deltagandet jämfört med 2023 sjunkit med 2,2 procentenheter. Antalet deltagande kommuner minskade mellan mättillfällena med 6,4 procent och antalet regioner med 38,9 procent. Däremot var det 4,6 procent fler myndigheter som deltog 2024 jämfört med 2023.

Diagram 55. Deltagande i It-säkkollen 2024

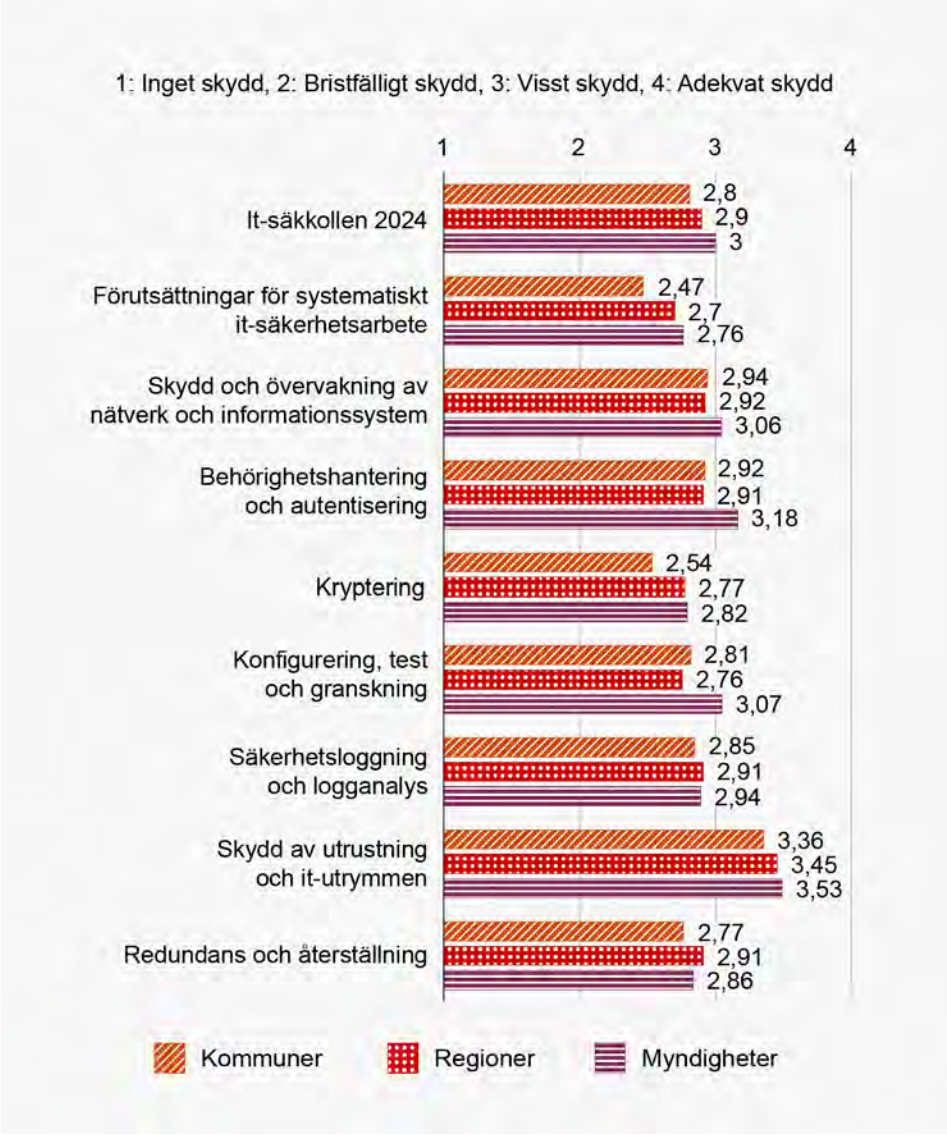


Not 29. För information om It-säkkollens utformning och planerade vidareutveckling, se kapitel 3.

5.1.2 Utfall per arbetsområde

Resultatet i It-säkkollen visar på små skillnader mellan aktörsgrupperna. Detta gäller för såväl helheten som inom varje enskilt arbetsområde. Diagram 2 visar att myndigheterna presterar lite bättre än regionerna, följt av kommunerna som är marginellt svagast.

Diagram 56. Resultat per aktörsgrupp i offentlig förvaltning



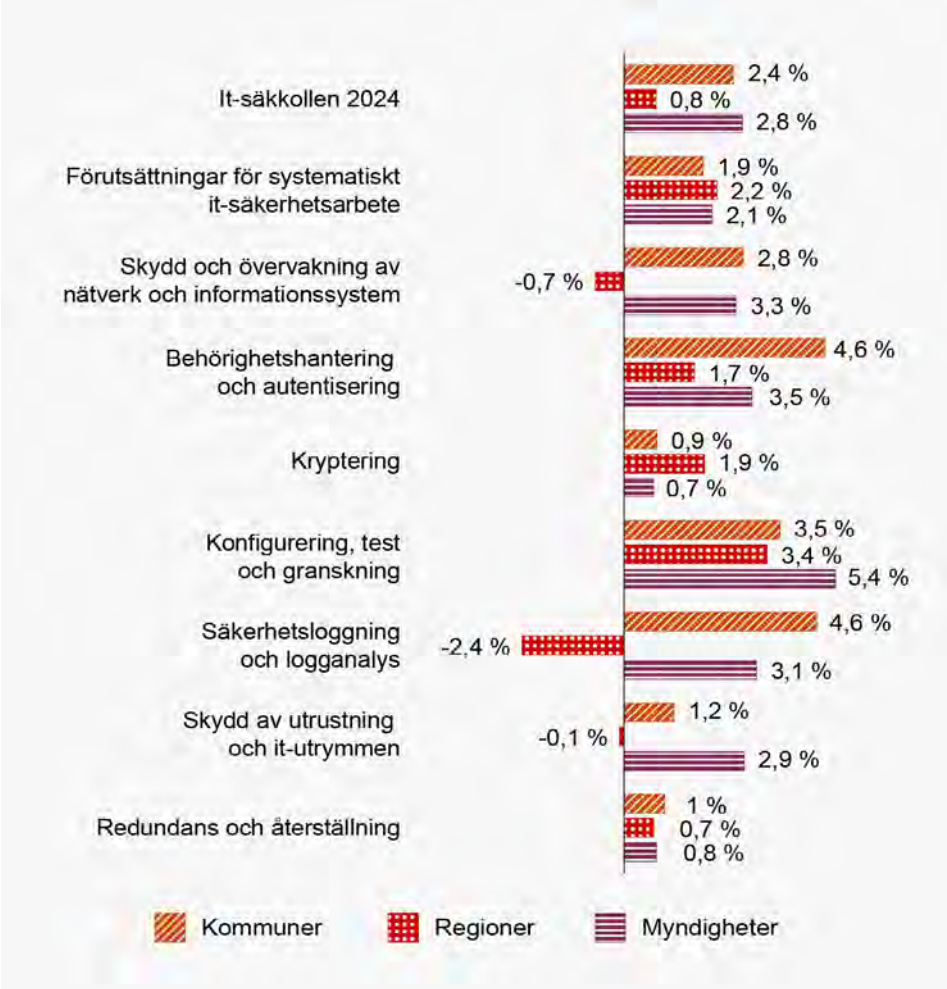
De arbetsområden där kommuner presterar bäst är Skydd av utrustning och it-utrymmen och Skydd och övervakning av nätverk och informationssystem. De arbetsområden där kommuner presterar svagast är Förutsättningar för systematiskt it-säkerhetsarbete och Kryptering.

De arbetsområden där regionerna, precis som kommunerna, presterar bäst är Skydd av utrustning och it-utrymmen och Skydd och övervakning av nätverk och informationssystem. De arbetsområden där regioner presterar svagast är

Förutsättningar för systematiskt it-säkerhetsarbete, samt Konfigurering, test och granskning.

De arbetsområden där myndigheter presterar bäst är Skydd av utrustning och it-utrymmen och Behörighetshantering och autentisering. De arbetsområden där myndigheter presterar svagast är Förutsättningar för systematiskt it-säkerhetsarbete och Kryptering.

Diagram 57. Förändring i procent mellan 2023 och 2024 för alla aktörsgrupper

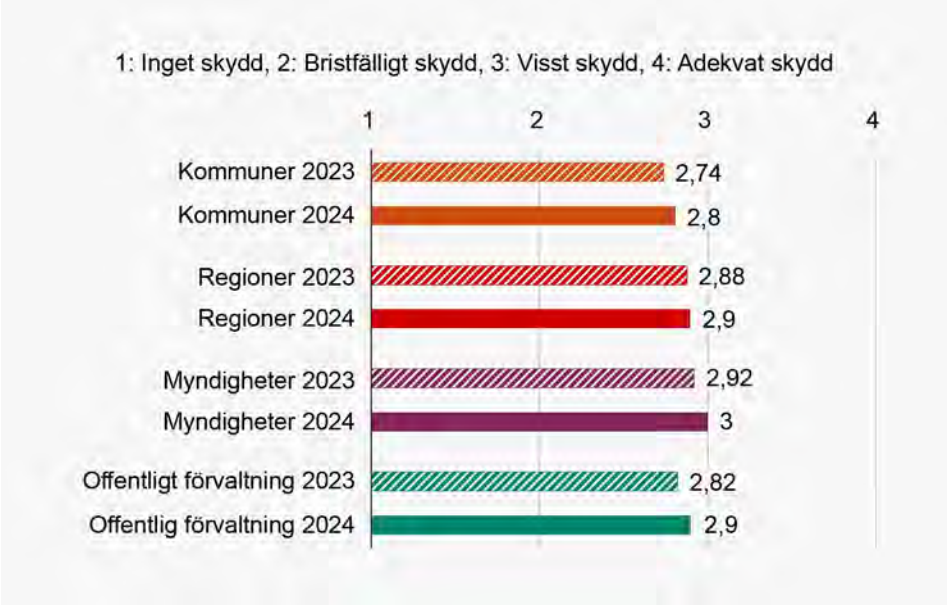


En viss förbättring har skett hos samtliga aktörsgrupper mellan de två mättillfällena. Att kommuner och myndigheter, de två större populationerna, utvecklats i ungefär samma takt är rimligt utifrån att de hade liknande resultat såväl 2023 som 2024.

Att regionerna har utvecklats minst förvånar då aktörsgruppens respondenter i Infosäkkollen visade på tydliga förbättringar 2024 jämfört med 2023. Det förklarades då av att de svagaste regionerna 2023 inte deltog 2024, varför ovan resultat förklaras av att de regioner som deltog 2023 och avstod 2024 hade ett bättre resultat på It-säkkollen 2023. Det finns dock vissa undantag, mest noterbart försämringen inom arbetsområdet för Säkerhetsloggning och analys.

Att den generella förbättringen är begränsad, såväl sett till helheten som inom enskilda arbetsområden, förklaras främst av att resultaten vid mätningen 2023 redan var relativt goda.

Diagram 58. Sammantaget resultat för It-säkkollen 2023 respektive 2024 för alla aktörsgrupper



Resultatet för samtliga offentliga förvaltningar som deltog i It-säkkollen 2024 motsvarar nästan nivå 3 vilket betecknas som ”visst skydd”. Skillnaderna mellan aktörsgrupperna är små. Myndigheterna presterar bäst, följt av regionerna och därefter kommunerna, men skillnaderna mellan aktörsgrupperna är marginella.

Att resultatet 2024 ligger så nära resultat från 2023, trots förändringarna i populationen, antyder att it-säkerhetsarbetet bedrivs på en relativt likvärdig nivå för alla offentliga förvaltningar. Det antyder också att relativt få nya åtgärder implementerats mellan de två tillfällena.

Resultatet i It-säkkollen, såväl 2023 som 2024, antyder ett betydligt starkare it-säkerhetsarbete än informationssäkerhetsarbete i Sveriges förvaltningar. It-säkerhetsarbetet styrs oftast av en it-chef, och genomförs oftast av en mer avgränsad skara medarbetare än informationssäkerhetsarbetet. It-chefen har vanligtvis tillgång till eller medverkar själv i organisationens ledningsgrupp och har därför sannolikt mer påverkan på hur arbetet prioriteras och resurssätts. Detta kan jämföras med att långt ifrån alla organisationer har en CISO på heltid, samt att den rollen saknar det mandatet en it-chef ofta 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 2024 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 2024 visar på att många av organisationerna anser sig ha goda förutsättningar för systematiskt it-säkerhetsarbete, vilket MSB noterar står i kontrast mot vad respondenterna och 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.

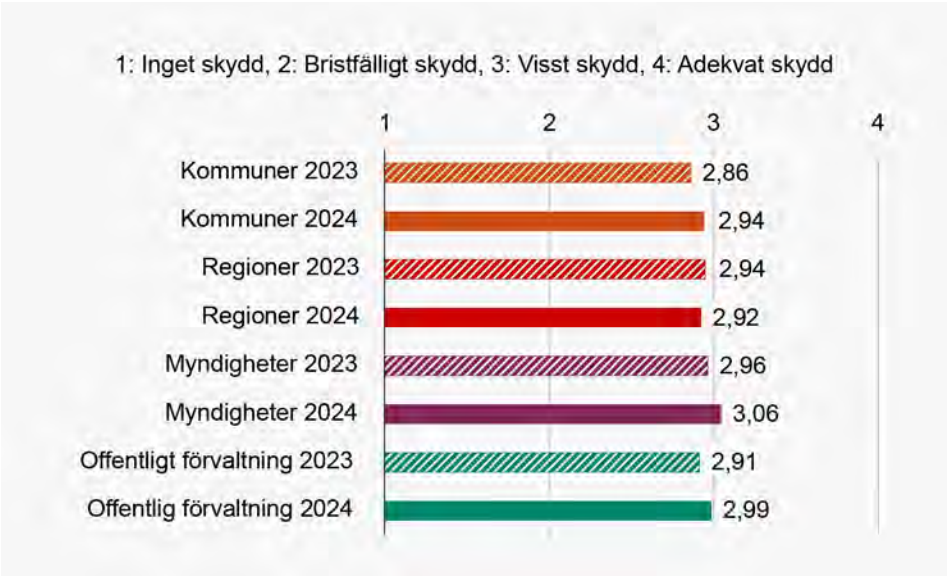
Diagram 59. Förutsättningar för systematiskt it-säkerhetsarbete

Förutsättningar för systematiskt it-säkerhetsarbete är, precis som 2023, det arbetsområde med svagast resultat. Skillnaderna mellan aktörsgrupperna är återigen små, såväl 2023 som 2024. En potentiell förklaring till det svagare resultatet här kan ligga i självskattningsmodellen och att det är relativt vanligt att alla verksamheter, oavsett förutsättningar, önskar de hade ännu mer resurser.

Trots det svaga resultatet jämfört med övriga arbetsområden är det notabelt att organisationerna anser sig ha så pass goda förutsättningar för systematiskt it-säkerhetsarbete. Det kan potentiellt styrka tidigare resonemang kring 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

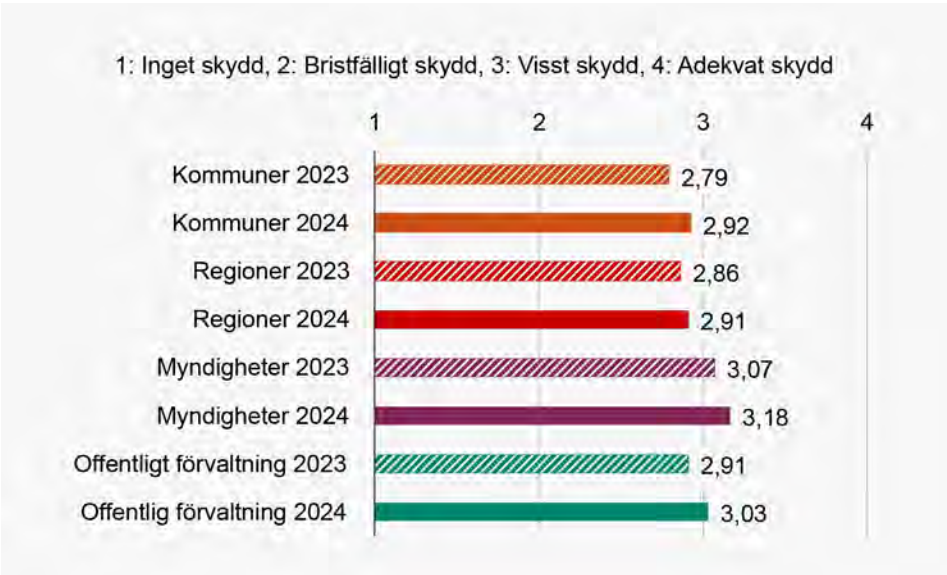
rollen saknar samma mandat och resurser. En annan möjlig förklaring skulle kunna vara att när it-driften är utkontrakterad så förutsätter organisationen att leverantören tar betalt för att bedriva ett ändamålsenligt it-säkerhetsarbete.

Diagram 60. Skydd och övervakning av nätverk och informationssystem



Gällande Skydd och övervakning av nätverk och informationssystem syns återigen knappt någon skillnad i nivån mellan aktörsgrupperna. Kommuner och regioner når nästan upp till nivå 3, vilket motsvarar ”visst skydd”, medan myndigheterna är precis över.

Diagram 61. Behörighetshantering och autentisering



Behörighetshantering och autentisering är grundläggande och förhållandevis enkelt jämfört med andra it-säkerhetsåtgärder. Kommuner och regioner når nästan upp till nivå 3, medan myndigheterna däremot är en bit över.

Diagram 62. Kryptering

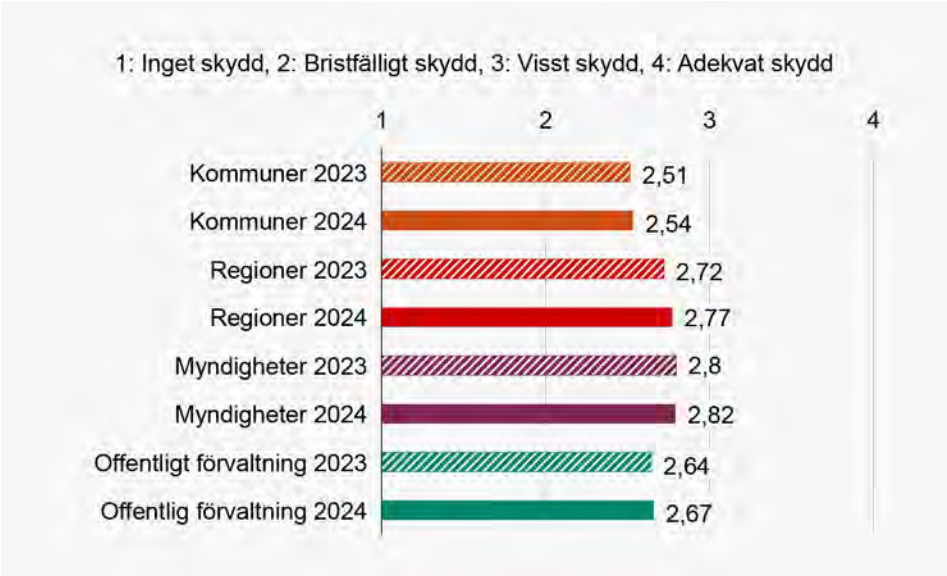
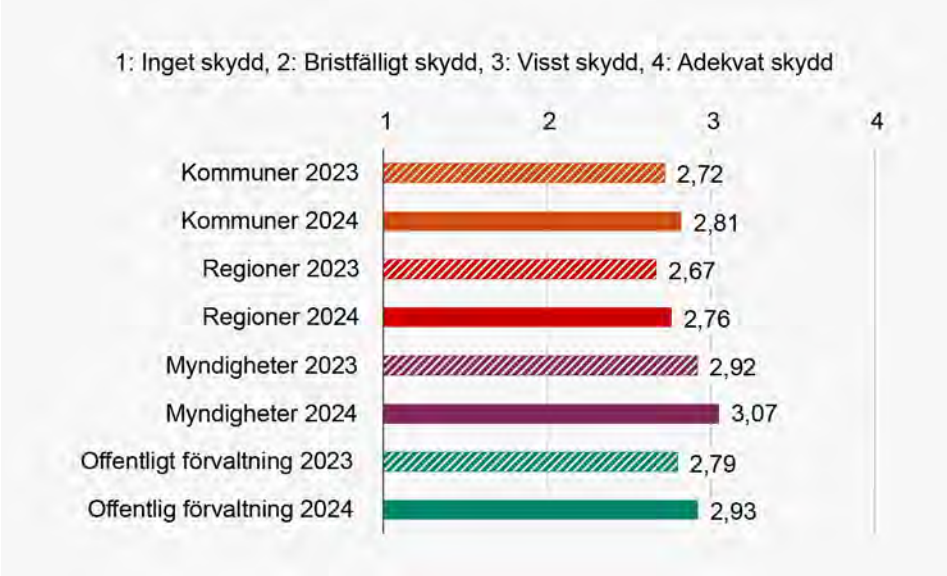


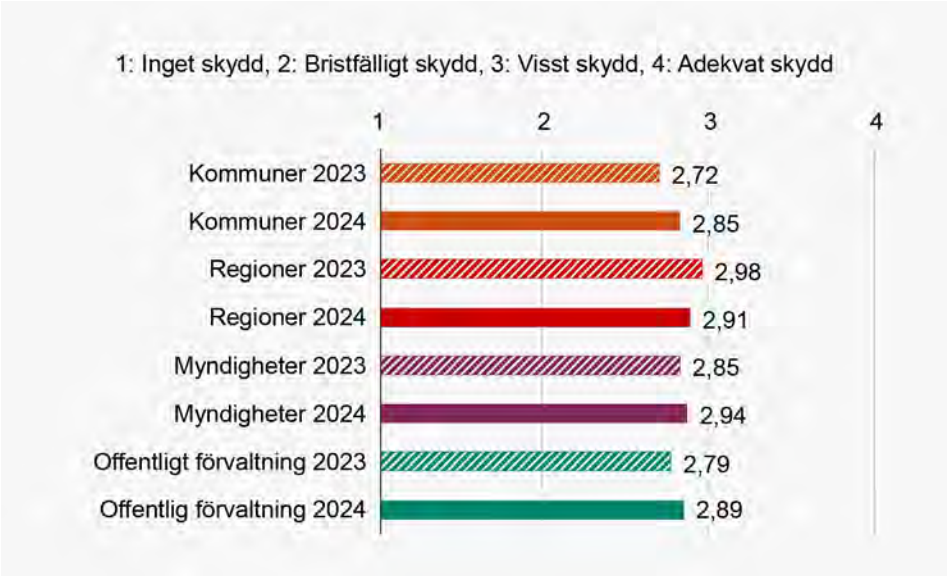
Diagram 62 visar att resultatet för arbetsområdet Kryptering är svagt jämfört med övriga arbetsområden. Med påtalade förändringar i populationen, det vill säga att antalet deltagande kommuner och regioner minskat, samtidigt som antalet myndigheter ökat, är det särskilt noterbart hur lika resultaten är mellan de två mätningarna.

Diagram 63. Konfigurering, test och granskning



Att organisationerna, precis som 2023, skulle prestera svagare på Konfigurering, test och granskning var något förväntat. Dessa åtgärder ligger ofta i slutet av arbetsflödet och prioriteras ofta ner. Svaren på Infosäkkollen för arbetsområdet för Uppföljning och utvärdering påvisar samma mönster. Samtidigt är Konfigurering, test och granskning det arbetsområde där de offentliga förvaltningarna förbättrats mest 2024 jämfört med 2023.

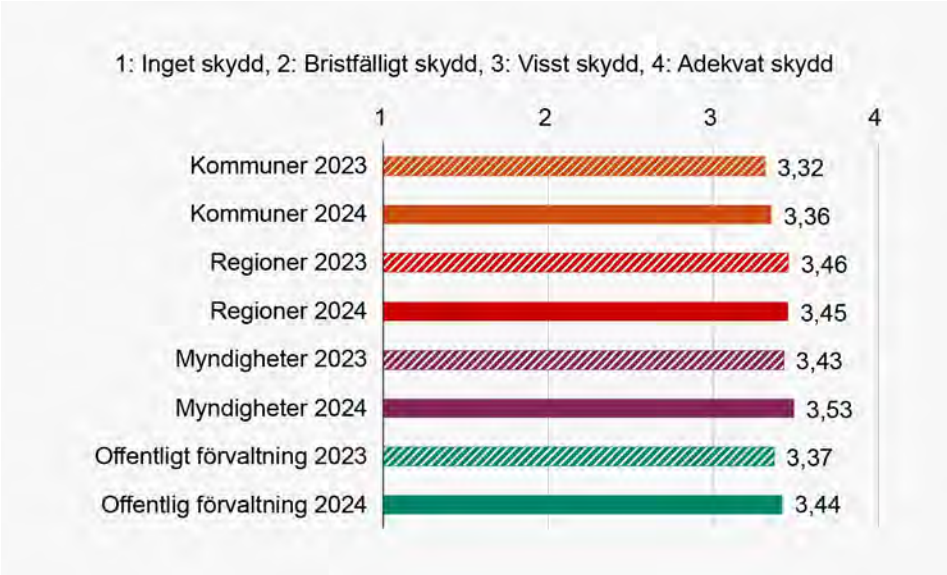
Diagram 64. Säkerhetsinloggning och logganalys



Det kan vara svårt, tidsödande eller resurskrävande att göra fullgoda logganalyser, vilket kan skönjas i att ingen aktörsgrupp når nivå 3 i mätningen. Kommunerna har haft en positiv utveckling mellan de två mättillfällena.

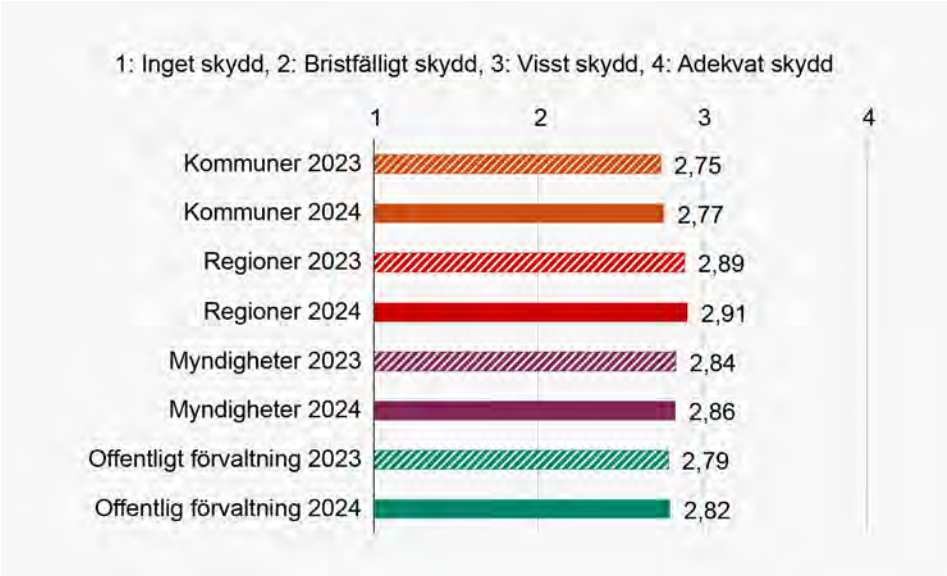
Givet hur frågorna är utformade i It-säkkollen, särskilt gällande avsaknad av detaljer, går det inte att bedöma om den kompetens som krävs för att bedriva kvalitet i detta arbete förekommer. Mer detaljerade frågor i den fullständiga It-säkkollen som lanseras under 2025 kan komma att förändra resultatet.

Diagram 65. Skydd av utrustning och it-utrymmen



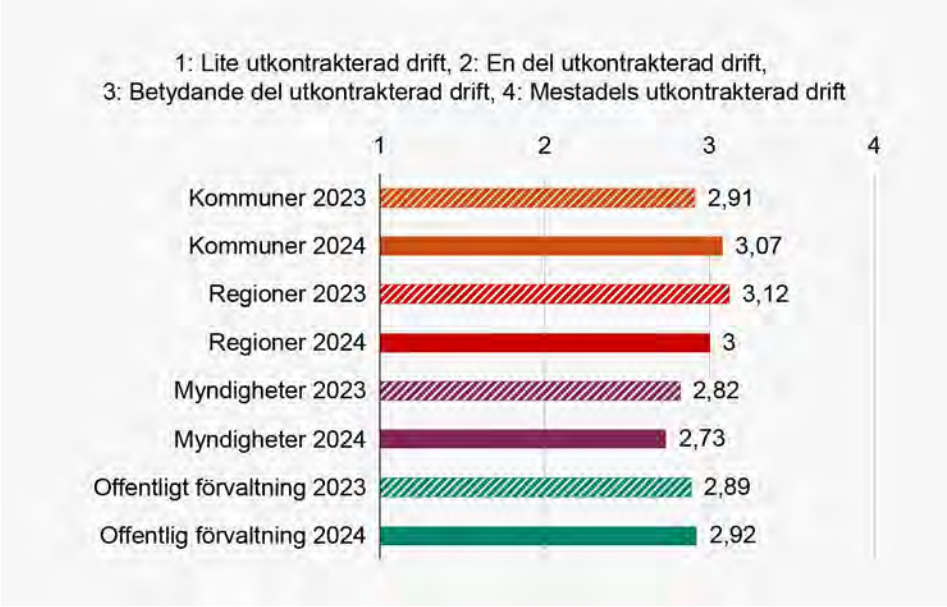
Skydd av utrustning och it-utrymmen är, precis som 2023, det arbetsområde med det klart bästa resultatet, oavsett aktörsgrupp. Det är det minst abstrakta arbetsområdet och kanske därför lättare att förstå vikten av, samt genomföra åtgärder för.

Diagram 66. Redudans och återställning



Arbetsområdet för Redundans och återställning påvisar ett relativt bra resultat, sett till att det är den typen av arbete som ibland prioriteras ner, eftersom det ofta hanterar eventuellt framtida risker. Det är dock samtidigt det arbetsområde med minst förbättring 2024 jämfört med 2023 års resultat.

Diagram 67. Utkontrakterad drift



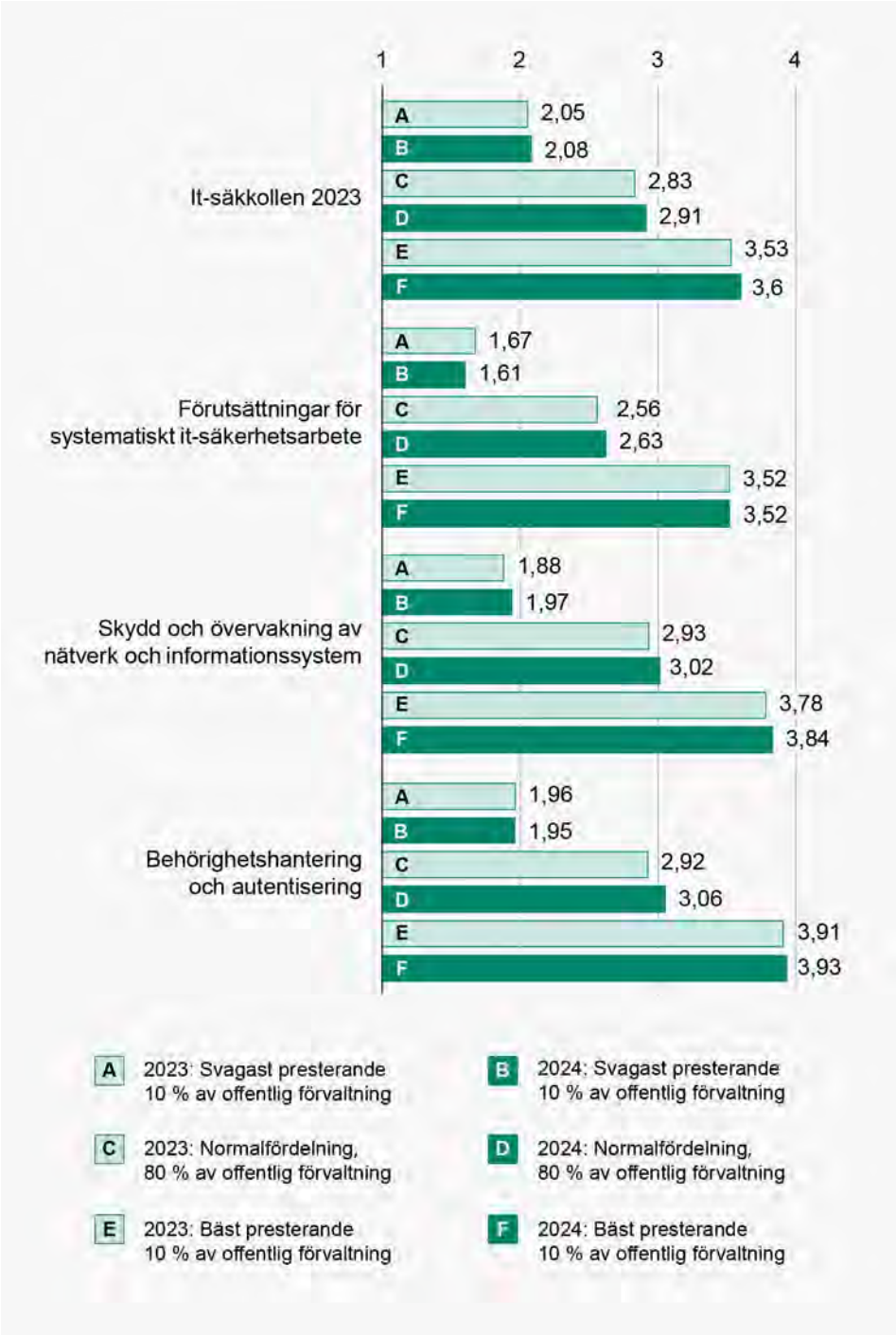
Även om det finns vissa förändringar mellan aktörsgrupperna, exempelvis anger deltagande kommuner att utkontrakteringen ökat samtidigt som deltagande myndigheter uppger att den minskat jämfört med 2023, rör det sig enbart om en marginell ökning för helheten jämfört med resultatet 2023.

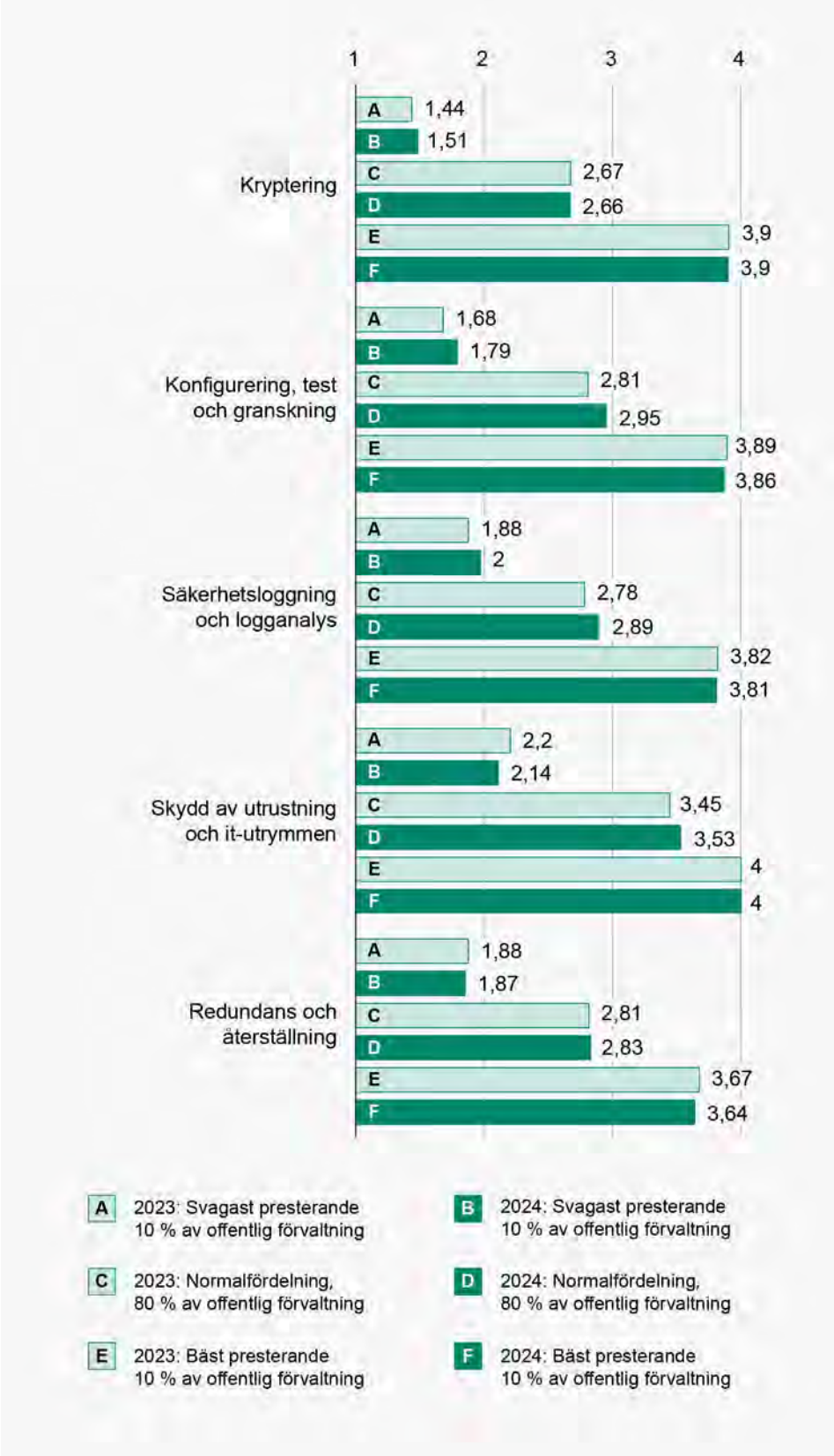
En stor andel av offentlig förvaltning uppger att de utkontrakterat en betydande del av sin it-drift. Frågan lämnar dock ett visst tolkningsutrymme och en modell med bättre metodologi behövs för ett förbättrat kunskapsläge, exempelvis kring vilka delar som är utkontrakterade och hur kritiska dessa bedöms vara.

5.1.3 Resultatspridning

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

Diagram 68. Resultatspridning hos offentlig förvaltning 2023 respektive 2024




1
2
3
4
Kryptering
A 1,44
B 1,51
C 2,67
D 2,66
E 3,9
F 3,9
Konfigurering, test och granskning
A 1,68
B 1,79
C 2,81
D 2,95
E 3,89
F 3,86
Säkerhetsloggning och logganalys
A 1,88
B 2
C 2,78
D 2,89
E 3,82
F 3,81
Skydd av utrustning och it-utrymmen
A 2,2
B 2,14
C 3,45
D 3,53
E 4
F 4
Redundans och återställning
A 1,88
B 1,87
C 2,81
D 2,83
E 3,67
F 3,64
A 2023: Svagast presterande 10 % av offentlig förvaltning
B 2024: Svagast presterande 10 % av offentlig förvaltning
C 2023: Normalfördelning, 80 % av offentlig förvaltning
D 2024: Normalfördelning, 80 % av offentlig förvaltning
E 2023: Bäst presterande 10 % av offentlig förvaltning
F 2024: Bäst presterande 10 % av offentlig förvaltning

För alla offentliga förvaltningar är resultatspridningen relativt liten jämfört med den spridning som den resultatredovisning påvisat för Infosäkkollen. Det är alltjämt en stor skillnad på de bästa och svagaste tio procenten, men sammantaget tyder svarsfördelningen på att it-säkerhetsarbetet generellt kommit längre.

Då de svagaste tio procenten har fler möjliga åtgärder att implementera och därmed hämta in på övriga är det noterbart att det är en så pass liten skillnad mellan mätningarna. Detta tyder på att utvecklingsarbetet bedrivs i ungefär samma takt.

Diagram 69. Resultatspridning hos kommunerna

Resultatspridningen hos kommunerna är mindre än bland myndigheterna, men större än hos regionerna. Det är relativt väl fördelat mellan arbetsområdena, men i Skydd av utrustning och it-utrymmen är skillnaden mellan normalfördelningen

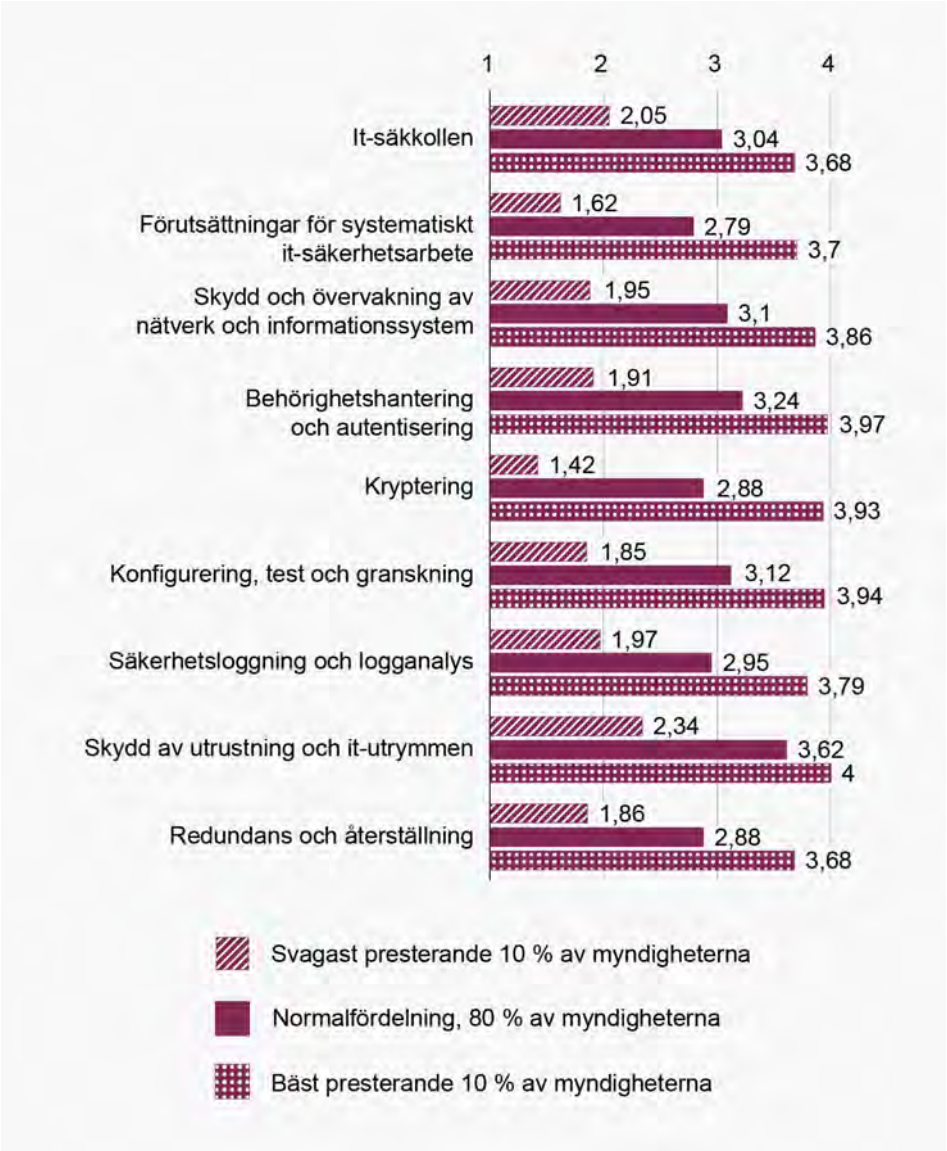
och de bästa tio procenten som minst. Motsatsen hittas inom Kryptering där de tio procent bästa kommunerna presterar mycket bättre än normalfördelningen.

Diagram 70. Resultatspridning hos regionerna

Hos regionerna syns den minsta spridningen mellan organisationerna. Det kan sannolikt förklaras av att det är den minsta aktörsgruppen, samt den mest homogena. Det följer samma mönster som i mätningen 2023. Till följd av den mindre populationen i aktörsgruppen har procentsatserna justerats för en mer rättvis bild av underlaget.

De svagast presterande regionerna har ett betydligt bättre resultat än de svagast presterande kommunerna och myndigheterna. Det omvända gäller också, det vill säga att de bäst presterande kommunerna och myndigheterna har betydligt bättre resultat jämfört med de bästa regionerna.

Diagram 71. Resultatspridning hos myndigheterna



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. Det var likadant i mätningen 2023.

De svagaste tio procenten av myndigheterna klarar bara nivå 2, bristfälligt skydd, inom två av arbetsområdena, och når precis över nivå 2 på helheten.

Utveckningen framåt

6. Utvecklingen framåt

Cybersäkerhetskollen syftar till att stödja uppföljning och därmed utveckling av organisationers systematiska och riskbaserade cybersäkerhetsarbete. Det bidrar i förlängningen till ett stärkt totalförsvar genom ett mer motståndskraftigt samhälle.

Inrapportering av Cybersäkerhetskollen bidrar till en förbättrad och mer heltäckande bild av cybersäkerhetsarbetet i Sverige. Baserat på Cybersäkerhetskollen och andra informationskällor kan MSB göra en bedömning av nivån på cybersäkerheten inom det civila försvaret.

En stor del av samhällsviktiga tjänster, produkter och infrastruktur bedrivs och tillhandahålls av privat sektor. När cybersäkerhetslagen träder i kraft kommer en stor majoritet av de organisationer som bedriver samhällsviktig verksamhet utgöras av organisationer från näringslivet. För att MSB fullt ut ska kunna bedöma nivån på cybersäkerheten utifrån ett totalförsvarsperspektiv är det därför centralt att alla organisationer som bedriver samhällsviktig verksamhet deltar i Cybersäkerhetskollen.

Ny reglering ställer långtgående krav på samhällsviktiga verksamheters cybersäkerhetsarbete. Kraven som kommer att ställas utifrån dessa regleringar gör inte skillnad på om en organisation tillhör offentlig eller privat sektor. Att genomföra Cybersäkerhetskollen ger en organisation en förståelse kring hur de klarar av lagkraven, men också stöd för deras förbättringsarbete. Baserat på detta, kombinerat med vikten av inrapportering utifrån ett totalförsvarsperspektiv, hoppas MSB på ett större deltagande i framtida mätningar.

It-säkkollen var under genomförandet 2024 en självskattningsenkät. Det medför metodologiska svagheter som MSB avser adressera till mätningen 2025. It-säkkollen kommer då följa Infosäkkollens metodik. Detta i huvudsak genom att respondenten istället anger införda säkerhetsåtgärder. Det minskar risken för tolkning och ger samtidigt detaljer som gagnar det analytiska arbetet. It-säkkollen kommer också kartläggas mot MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter[30].

MSB kommer också ta fram två nya mätningar inom ramen för Cybersäkerhetskollen. De kommer att följa samma metodik som idag finns för Infosäkkollen, men undersöka nivån på samhällsviktiga verksamheters ot-säkerhet respektive leveranskedjesäkerhet.

Not 30. MSBFS 2020:7: https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20207/.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2545 – januari 2025 ISBN-nummer 978-91-7927-599-0