Myndigheten för samhällsskydd och beredskap

Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

Resultatredovisning Infosäkkollen 2021

Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

Foto omslag: Johnér
Produktion: Advant

Publikationsnummer: MSB1942 – juni 2022
ISBN: 978-91-7927-252-4

Förord

En av målsättningarna i den nationella strategin för samhällets informations- och cybersäkerhet är att kommuner, regioner och statliga myndigheter ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete. Allt detta underlättas när organisationen kan bedöma på vilken nivå det egna arbetet befinner sig och vilka åtgärder som behöver vidtas för att fortsätta att utveckla och förbättra sitt arbete. Att få en bild av behoven i offentlig förvaltning är också central på samhällsnivå. Det ger möjlighet för inte bara MSB utan även andra myndigheter och aktörer att erbjuda rätt stöd på rätt sätt och i rätt form. Tillsammans kan vi på ett tryggt sätt möta både digitaliseringens möjligheter och dess utmaningar.

Infosäkkollen har därför två huvudsakliga användningsområden. Det ska ge organisationen ett direkt stöd vid uppföljning av det egna informationssäkerhetsarbetet, både avseende bredd, styrkor och utvecklingsområden. Men med Infosäkkollen har vi nu också för första gången etablerat en möjlighet att regelbundet och strukturerat mäta, analysera och dra slutsatser rörande informationssäkerhetsarbetet i en offentlig förvaltning, en mycket central del i samhället.

Att vi nu kan ta fram denna rapport med analyser, slutsatser och rekommendationer har gjorts möjligt genom er medverkan. Jag vill därför rikta ett stort och varmt tack till alla kommuner, regioner och statliga myndigheter som har skickat in sina resultat i Infosäkkollen. Nästan hälften av alla organisationer i offentlig förvaltning har delat sina resultat. Det gör att vi kan konstatera att stora delar av den offentliga förvaltningen inte arbetar systematiskt med informationssäkerhet. Det finns ett starkt fokus på att implementera säkerhetsåtgärder. Vi rekommenderar därför att organisationerna prioriterar det systematiska informationssäkerhetsarbetet från ledningsnivå och nedåt och tilldelar mer resurser om det behövs. Det är viktigt att spetsen inte kommer på bekostnad av bredden. Organisationerna kan i sitt utvecklingsarbete dra nytta av de nya möjligheter till samarbete och samverkan som uppstår genom Infosäkkollen.

Vårt mål är att resultaten, analyserna och rekommendationerna i denna rapport kommer att bidra till och underlätta ert fortsatta systematiska informationssäkerhetsarbete. Vi kommer dock inte att stanna där utan dessutom ta fram nya och mer riktade stöd som svarar mot behoven som framgår av Infosäkkollen och vår övriga samverkan med er. Dessutom kommer vi nu inleda arbete med att vidareutveckla Infosäkkollen så att vi i nästa omgång kan erbjuda ny och förbättrad funktionalitet, nya ämnesområden och välkomna nya organisationer.

Följ gärna arbetet med Infosäkkollen på www.msb.se/infosakkollen. Vi uppmuntrar också till att besöka www.msb.se/informationssakerhet för att hitta metodstöd och vägledningar.

Varmt välkomna att delta i nästa mätning, som kommer att genomföras 2023! Tillsammans kommer vi att nå nya nivåer av systematiskt informationssäkerhetsarbete!

Stockholm, 22 juni 2022

Åke Holmgren,

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

Innehåll

Sammanfattning

Sammanfattning

I maj 2021 lanserade MSB Infosäkkollen, en uppföljningsstruktur för det systematiska informationssäkerhetsarbetet som ger kommuner, regioner och statliga myndigheter stöd i sitt uppföljnings- och förbättringsarbete. Organisationerna erbjöds också att skicka in sina svar, som grund för övergripande återkoppling och analys. Ungefär hälften av organisationerna valde att dela med sig av sina resultat.

Baserat på svaren redovisas i denna rapport en samlad bedömning av nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen 2021. Rapporten innehåller också rekommendationer till målgrupperna utifrån en tolkning av de inskickade svaren och en redovisning av hur MSB avser att utveckla stödet till den offentliga förvaltningen utifrån resultatet av uppföljningen.

Resultatet visar att stora delar av den offentliga förvaltningen inte arbetar systematiskt med sin informationssäkerhet. Arbetet är eftersatt hos majoriteten av de svarande statliga myndigheterna trots att de har omfattats av MSB:s föreskrifter med krav på detta sedan 2009.

Det låga resultatet var delvis väntat, dels för att det är första gången en mätning görs på detta sätt och på grund av hur Infosäkkollen är konstruerad, dels för att det redan var känt att många organisationer av olika anledningar har svårt att få till helheten. En positiv observation är att det finns relativt goda förutsättningar för att substantiellt höja det samlade resultatet till nästa mätning 2023.

Bristen på bredd i arbetet är vad som håller tillbaka många organisationers resultat i Infosäkkollen. Vissa arbetsområden är generellt sett särskilt eftersatta, men nivån behöver höjas även inom de områden där organisationer har genomfört åtgärder. Det finns ett fokus på att implementera säkerhetsåtgärder, men ofta brister arbetssätten som stödjer framtagandet av säkerhetsåtgärder genom omvärldsbevakning, riskanalys och andra aspekter. En ännu större utmaning är bristande arbetssätt för att följa upp arbetet och säkerhetsåtgärderna. En central del av det systematiska arbetet saknas därmed då organisationerna inte kan se om arbetssätt och åtgärder som införts har haft avsedd effekt.

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. Ett stort antal organisationer anger resursbrist som det främsta hindret för att nå högre nivåer i arbetet. MSB instämmer i bedömningen att många organisationer, i synnerhet många kommuner, behöver mer resurser. Samtidigt bedömer MSB också att arbetet kan göras mer effektivt.

Baserat på slutsatserna i analysen har MSB tagit fram en rad rekommendationer, varav ett antal är specifika för kommuner, regioner respektive statliga myndigheter. Följande rekommendationer riktas till samtliga organisationer i den offentliga förvaltningen.

- Prioritera det systematiska informationssäkerhetsarbetet från ledningsnivå och nedåt och tilldela mer resurser om det behövs.
- Säkerställ en organisation som bygger på etablerade. kommunicerade och beslutade processer, rutiner och metoder istället för personberoenden.
- Använd uppföljning och förbättringar i utvecklingen av informationssäkerhetsarbetet.
- Arbeta aktivt för att skapa en god informationssäkerhetskultur där informationssäkerhet är prioriterat på alla nivåer inom organisationen.
- Stärk arbetet med kontinuitetshantering.
- Se till att spetsen inte kommer på bekostnad av bredden.
- Dra nytta av de nya möjligheter till samarbete och samverkan som uppstår genom Infosäkkollen.

Inledning

1. Inledning

1.1 Bakgrund

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. I uppdraget ingick även att lämna en första samlad bedömning av nivån på det systematiska informationssäkerhetsarbetet, baserat på den framtagna uppföljningsstrukturen. Uppdraget skulle redovisas den 1 mars 2021.

Covid-19-pandemin innebar en ökad belastning på många organisationer i målgruppen under 2020. Därför valde MSB, i samråd med regeringskansliet, att senarelägga lanseringen av uppföljningen till sommaren 2021.

I uppdragsredovisningen den 1 mars 2021 fokuserade MSB därför på hur uppföljningsstrukturen utformats, hur utvecklingsarbetet skett i dialog och samverkan med målgruppen samt hur uppföljningsstrukturen skulle kunna utvecklas i framtiden inklusive övergripande slutsatser. De delar av regeringsuppdraget som förutsatte att uppföljningen genomförts redovisades inte.

I maj 2021 lanserade myndigheten uppföljningsstrukturen, under namnet Infosäkkollen, till kommuner, regioner och statliga myndigheter. Under senare delen av 2021 genomfördes övergripande analyser av inkomna svar. Som stöd för både analysarbetet och återkopplingen till målgrupperna utvecklade MSB även ett verktyg för att redovisa benchmarks.

Baserat på svar från Infosäkkollen redovisar myndigheten i denna rapport en första samlad bedömning av nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen 2021, och en bedömning av hur MSB utifrån resultatet kan utveckla stödet till den offentliga förvaltningen.

I regeringsuppdraget ingick även att regelbundet ge regeringen en samlad bedömning avnivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. MSB kommer därför vartannat år att genomföra motsvarande uppföljning och redovisning, med stöd av Infosäkkollen. Målgruppens svar kommer att analyseras och sammanställas på sätt som möjliggör jämförelser över tid.

1.2 Disposition

I kapitel 2 beskrivs vilka slutsatser och rekommendationer till kommuner, regioner och statliga myndigheter som kan göras utifrån den genomförda analysen. Kapitlet innehåller även ett antal satsningar som MSB planerar, med anledning av resultatet. I kapitel 3 ges en närmare beskrivning av Infosäkkollen och tillhörande benchmarkverktyg ur ett användarperspektiv. Kapitel 4 innehåller analys och resultat, både på övergripande nivå och indelat utifrån kommuner, regioner och statliga myndigheter. För statliga myndigheter ges även en indikation påefterlevnaden av MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Slutligen redogörs i kapitel 5 för den fortsatta utvecklingen av Infosäkkollen.

1.3 Begreppsförklaring

Här följer en lista med begrepp som används och deras innebörd i denna rapport. Mer information om begreppen finns i kapitel 3 *Hur resultatet tagits fram* samt i bilaga 2 *Hur informationssäkerhetsarbetet mäts.*

Arbetsområden är en ämnesmässig uppdelning av de frågor som ingår i Infosäkkollen utifrån olika delar av det systematiska informationssäkerhetsarbetet.

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. Läs mer om benchmarks i avsnitt 3.3.1.

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

Infosäkkollen är ett verktyg för uppföljning av det systematiska informationssäkerhetsarbetet i en organisation. Resultat från organisationer som genomfört Infosäkkollen ligger till grund för denna rapport.

Nivå beskriver hur långt en organisation kommit med sitt informationssäkerhetsarbete 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”.

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. Läs mer om resultattal i avsnitt 3.3.2.

Typkommunen, typregionen och **typmyndigheten** är sammanvägda beskrivningar baserat på alla deltagande kommuners, regioners eller myndigheters resultat. Se även Benchmarks.

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

1.4 Varför resultatet i Infosäkkollen är viktigt

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

Infosäkkollen är en modell som används inom ramen för en struktur där organisationers systematiska informationssäkerhetsarbete följs upp i två-årscykler. Likt andra modeller kan Infosäkkollen enbart göra anspråk på att beskriva en *approximation* av hur verkligheten ser ut hos en enskild organisation. Modellens 40 frågor täcker en bred uppsättning aspekter som ingår i ett systematiskt informationssäkerhetsarbete, men de täcker inte allt som kan ingå (exempelvis innehåller Infosäkkollen inga frågor om *specifika säkerhetsåtgärder*, såsom åtgärder kopplade till behörighetshantering). Medan Infosäkkollen alltså ger *en* bild, är det inte säkert att den ger en *fullödig* bild. Det är fullt möjligt att det finns ytterligare aspekter som hade kunnat mätas och som hade kunnat ställa enskilda organisationer i såväl bättre som sämre dager.

På motsvarande sätt kan Infosäkkollen endast göra anspråk på att beskriva en approximation av vad en organisation behöver satsa på för att utveckla sitt systematiska informationssäkerhetsarbete. Enskilda organisationer kan ha större behov av andra åtgärder än de Infosäkkollen visar att de behöver genomföra för att nå en högre nivå.

Med det sagt finns det ett antal skäl till att det är viktigt för organisationer att använda Infosäkkollen för att följa upp sitt systematiska informationssäkerhetsarbete, och att det är viktigt att nå höga nivåer i Infosäkkollen:

Infosäkkollen omfattar noggrant utvalda områden: Det som modellen följer upp är resultatet av 1,5 års arbete med att sammanställa en begränsad uppsättning frågor om olika delar av det systematiska informationssäkerhetsarbetet. 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 informationssäkerhetsarbete: Organisationer får en bild av statusen på sitt systematiska informationssäkerhetsarbete, och de kan jämföra bilden de får med den bild som andra organisationer får. Det gör att de kan se om de har missat något, får bättre förutsättningar för samarbete och kan sätta mål tillsammans.

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

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

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

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

När MSB i kapitel 2 framhäver vikten av att höja organisationers övergripande nivå, handlar de slutsatserna och rekommendationerna alltså om de ovanstående skälen, snarare än att goda resultat i Infosäkkollen har ett egenvärde.

Slutsatser och rekommendationer

2. Slutsatser och rekommendationer

2.1 Slutsatser

Det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.

Arbetet med att efterleva MSB:s föreskrifter med krav på ett systematiskt informationssäkerhetsarbete är eftersatt hos majoriteten av de svarande statliga myndigheterna trots att de har omfattats av sådana krav sedan 2009. Det finns anledning att anta att detta även gäller myndigheter som inte har skickat in sina svar till MSB.

Det är särskilt viktigt att organisationer i den offentliga förvaltningen följer upp de åtgärder som de har vidtagit med anledning av förändrade omständigheter orsakade av pandemin.

Det är också angeläget att organisationer bygger upp sin förmåga inom kontinuitetshantering. Omställningen till hemarbete och säkerhetsläget i Europa är två faktorer som gör förmåga inom det här området särskilt viktigt.

Det behöver fördelas mer resurser till det systematiska informationssäkerhetsarbetet, men det behövs också mer effektiva sätt att bedriva arbetet. Näringslivet kan bidra med nya lösningar som möjliggör sådana effektivitetsökningar i den offentliga förvaltningen.

Det är realistiskt att förvänta sig en höjning av den övergripande nivån hos upp till en tredjedel av de svarande organisationerna till nästa mättillfälle – om deras respektive ledningar beslutar sig för att satsa på det systematiska informationssäkerhetsarbetet.

Det finns goda förutsättningar för samarbete i form av att dela erfarenheter och lärande mellan organisationer. Samtidigt finns det några områden där endast några få organisationer har lyckats väl. Myndigheter som MSB, och det privata näringslivet, kan göra som mest nytta genom att stötta organisationer inom dessa områden.

Arbetet med Infosäkkollen har visat att förmågan, att kunna hantera säkerhetsskyddsklassificerade uppgifter, hos de organisationer inom den offentliga förvaltningen som har en roll inom totalförsvaret behöver fortsätta stärkas och utvecklas.

2.1.1 Den övergripande bilden

Stora delar av den offentliga förvaltningen arbetar inte systematiskt med sin informationssäkerhet. Cirka en tiondel av de svarande organisationerna förefaller inte arbeta så mycket med informationssäkerhet överhuvudtaget. Det finns ett starkt fokus på att implementera säkerhetsåtgärder, men ofta brister arbetssätten som stödjer framtagandet av åtgärder genom omvärldsbevakning, analys av risk och andra aspekter. En ännu större utmaning är bristande arbetssätt för att följa upp arbetet och säkerhetsåtgärderna. Även kontinuitetshanteringen är bristfällig, både med avseende på att många saknar ett arbetssätt för sin kontinuitetshantering, men framförallt för att endast en liten andel övar den. Medarbetarna ges inte förutsättningar och verktyg att på egen hand bidra till säkerheten. Organisationer i den offentliga förvaltningen verkar i regel inte veta ifall de insatser som gjorts för att utbilda personalen har gett någon effekt eller tillämpas i praktiken. Följden blir att organisationer digitaliserar med en hög grad av osäkerhet kring vilka risker det medför – och med påföljande brister i förmågan att hantera de risker som uppstår[1].

Den mest centrala slutsatsen från MSB:s analys av de inskickade svaren är därför att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Resultaten bekräftar en bild som såväl MSB som andra organisationer har kommit fram till förut.

Arbetet med systematisk informationssäkerhet är eftersatt hos majoriteten av de svarande statliga myndigheterna trots att de har omfattats av MSB:s föreskrifter med krav på detta sedan 2009. Det finns anledning att anta att detta även gäller myndigheter som inte har skickat in sina svar till MSB. Infosäkkollens resultat tillsammans med tidigare undersökningar[2] visar att det troligen har varit fallet under en längre tid. Efterlevnaden av föreskrifterna om statliga myndigheters informationssäkerhet omfattas inte av tillsyn. MSB tillhandahåller ett generellt utformat stöd för myndigheternas efterlevnad av föreskriftskraven, och har inte arbetat med att ge sådan vägledning och inriktning till enskilda myndigheter som tillsyn innebär. Om tillsyn över tillämpningen av föreskrifterna skulle ha underlättat de statliga myndigheternas arbete och därmed ha lett till ett bättre resultat än det nuvarande går inte att säga med säkerhet, men det kan heller inte uteslutas.

Vissa arbetsområden är generellt sett särskilt eftersatta, men nivån behöver även höjas inom de områden där organisationer har genomfört åtgärder. För att lyckas kan ytterligare särskilda satsningar behövas från myndigheter som MSB (såväl som andra organisationer). Det handlar om satsningar inom dels områden där organisationer har svårt att på egen hand komma vidare, dels områden där det finns få organisationer som har lyckats väl och som genom delning av erfarenheter kan hjälpa andra att genomföra åtgärder och höja sin nivå.

1. Sådana risker handlar om att system och tjänster konstrueras med inbyggda fel som inte märks förrän de tas i bruk, exempelvis genom att de fallerar, att de gör saker de inte ska göra eller att de (eller informationen i dem) är sårbara. Riskerna handlar också om att medarbetare och andra kan komma att agera på sätt som orsakar eller möjliggör incidenter, eller att de inte agerar på sätt som de behöver agera för att förhindra att incidenter uppstår.

2. Se exempelvis https://www.msb.se/sv/publikationer/en-bild-av-myndigheternas-informationssakerhetsarbete-2014--tillampning-av-msbs-foreskrifter/

Stöd från organisationer som MSB kan dock bara göra skillnad om det finns en motpart som kan ta emot stödet och använda det. I många organisationer saknas resurser för det. Därför krävs det framförallt ökad resurstilldelning för arbetet inom de organisationer som behöver nå högre nivåer i sitt informationssäkerhetsarbete.

Satsningar på sådana åtgärder som ger ett lite högre resultat inom arbetsområdet Säkerhetsåtgärder och förbättringsåtgärder (jämfört med andra arbetsområden), bör till viss del förstås mot bakgrund av pandemin.[3] Många organisationer har i sina svar till MSB angett att pandemin har medfört att resurser har fått prioriteras om, exempelvis för omställning till hemarbete. Mycket av arbetet har skett på kort tid, och med begränsade möjligheter att på ett ordnat sätt bereda hur omställningen ska gå till. Som ett svar på att nya it-funktioner har byggts upp har tillhörande it-säkerhetsåtgärder hastigt fått införas. Svaren till MSB antyder att informationssäkerhetsarbetet ofta ses som en it-fråga – eller att det reduceras till en it-fråga när resurser måste omprioriteras i pressade lägen.

Av de svarande organisationerna, har 39 procent inte angett en informationssäkerhetsrelaterad person som deltagare i arbetet med Infosäkkollen och har därmed troligen inte en sådan person inom organisationen. En stor andel av dessa organisationer har låga resultat och inriktningen mot säkerhetsåtgärder är särskilt tydlig.

Det är bristen på bredd i arbetet som håller tillbaka många organisationers resultat i Infosäkkollen.[4] I synnerhet är avsaknaden av uppföljning och utvärdering påtaglig. Detta innebär att många organisationer saknar en central del av det systematiska arbetet, då de inte kan se om arbetssätt och åtgärder som införs har den avsedda effekten. MSB bedömer att detta är ett av de viktigaste utvecklingsområdena för att höja nivån på det systematiska informationssäkerhetsarbetet i offentlig förvaltning.

Ett annat centralt område med betydande luckor är kontinuitetshantering. Många saknar ett arbetssätt för kontinuitetshantering. Bland de som har ett sådant arbetssätt är det få som har övat det under den senaste tvåårsperioden. Många organisationer har under den här perioden börjat nyttja nätbaserade arbetssätt för att möjliggöra hemarbete. Det innebär förändrade behov när det gäller alternativa arbetssätt som kan utgöra reservförfarande vid störningar. Samtidigt har den säkerhetspolitiska situationen i Europa förvärrats på senare tid, och det kan inte uteslutas att risken för angrepp mot informationssystem är förhöjd. Om mängden angreppsförsök ökar så ökar sannolikt också mängden incidenter där faktisk skada uppstår. Då är det mycket viktigt att så snabbt som möjligt kunna upprätta alternativa sätt att bedriva verksamheten, samt att återställa eller ersätta skadade informationssystem.

3. Detta underbyggs av vad organisationerna själva har angett i fritext iInfosäkkollen, men också av incidentrapporteringen som MSB mottar.

4. Se avsnitt 1.4 för mer information om hur Infosäkkollen fungerar.

I samband med inrapporteringen av resultat i Infosäkkollen under hösten 2021 har organisationerna haft tillfälle att öva sin förmåga att hantera känsliga uppgifter (i vissa fall säkerhetsskyddsklassificerade) och att nyttja säkra kommunikationer. Arbetet med Infosäkkollen visar att förmågan inom det här området behöver stärkas och utvecklas.

2.1.2 Hur nivån på den offentliga förvaltningens systematiska informationssäkerhetsarbete kan höjas

Ett stort antal organisationer anger resursbrist som det främsta hindret för att nå högre nivåer i det systematiska arbetet. MSB instämmer i bedömningen att många organisationer, i synnerhet många kommuner, behöver mer resurser. Men MSB bedömer också att arbetet ofta bör kunna göras mer effektivt, och att en ökad effektivitet skulle kunna frigöra resurser för att arbeta bredare, och därigenom nå högre nivåer. MSB bedömer dessutom att få organisationer kommer att tillföra så pass mycket resurser att resurstillskottet, i sig, ska kunna höja organisationens nivå tillräckligt mycket. Ett mer effektivt nyttjande av resurserna som tillhandahålls är därför en viktig komponent i en satsning mot en högre nivå. Här finns en roll för näringslivet i att utveckla och tillhandahålla verktyg, teknologi och tjänster som kan bistå den offentliga förvaltningen i det systematiska informationssäkerhetsarbetet.

En positiv observation är att det finns relativt goda förutsättningar för att substantiellt höja det samlade resultatet till nästa mätning 2023. Cirka en tredjedel av de svarande organisationerna skulle med bibehållet resultat och maximalt fem ytterligare åtgärder kunna nå en högre övergripande nivå vid mätningen 2023. Dessutom kommer några organisationer per automatik att uppnå något bättre resultat vid nästa mätning, så länge de bibehåller de resultat som de redan har uppnått[5].

Det låga resultatet från mätningen 2021 var väntat, dels på grund av hur Infosäkkollen är konstruerad[6], dels för att organisationerna inte har haft kännedom om frågorna på förhand och dels för att det redan var känt att många organisationer av olika anledningar har svårt att få till helheten. MSB bedömer att det är realistiskt att förvänta sig en höjning av den övergripande nivån hos mellan en sjättedel och en tredjedel av de svarande organisationerna till nästa mättillfälle – om deras respektive ledningar beslutar sig för att satsa på det systematiska informationssäkerhetsarbetet.

I arbetet med Infosäkkollen har MSB återkommande mottagit önskemål om att organisationer ska ges bättre förutsättningar att nå längre i sitt informationssäkerhetsarbete genom att samarbeta. 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

5. I avsnitt 1 i Infosäkkollen, i frågorna 7-13, är det möjligt att svara att man inte har haft ett arbetssätt under hela två-årsperioden, men att man har ett nu – eller att man har ett under utveckling. Merparten av de som har svarat så på de frågorna kommer att ha haft de arbetssätten i minst två år vid nästa mättillfälle.

6. Infosäkkollen fäster stor vikt vid att få till helheten genom att ha en bredd i det systematiska informationssäkerhetsarbetet. Frågorna är dessutom alla utformade som en tillbakablick på det som en organisation har haft eller har gjort de två senaste åren.

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[7] (kommuner, regioner och statliga myndigheter) bör ha möjlighet att hitta andra organisationer som de kan samarbeta med. 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. Förutsättningarna för att hitta organisationer att lära sig av är störst inom grupper där aktörerna skiljer sig mycket åt (s.k. *heterogena* grupper). I Infosäkkollen 2021 är kommunerna den mest heterogena gruppen, som alltså har störst potential för denna typ av samverkan, följt av myndigheterna och sist regionerna. Detta återspeglas i den relativt långa lista av frågor där förutsättningar för samarbete finns mellan kommunerna, och de kortare listor som har genererats för de andra två grupperna[8].

Metoden avslöjar också några områden där särskilda stöd från MSB och andra myndigheter, såväl som privata aktörer, kan vara särskilt avgörande (eftersom det finns relativt få organisationer som andra kan lära sig av). De är i synnerhet

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

2.2 Rekommendationer

Rekommendationerna nedan grundar sig på brett förekommande brister som har noterats i de resultat som har skickats in till MSB. Alla svarrande organisationer inom respektive aktörsgrupp (kommuner, regioner och statliga myndigheter) har inte alla de listade bristerna, men många organisationer har många av dem. Bilden av läget i respektive grupp redovisas i avsnitt 4.3 för kommuner, avsnitt 4.4 för regioner och avsnitt 4.5 för statliga myndigheter.

Rekommendationerna grundar sig på slutsatserna från denna analys. Samtidigt är det viktigt att komma ihåg att alla organisationer är olika och att det systematiska informationssäkerhetsarbetet 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.

För att få en så relevant bild som möjligt bör organisationer också använda verktyget Infosäkkollen benchmark. Verktyget kan generera en lista på åtgärder som en organisation behöver genomföra för att nå egna målsättningar, nå samma resultat som en grupp man jämför sig med, eller klara kraven i MSB:s föreskrifter

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

8. Se Förutsättningar för samarbeten i respektive aktörsgrupps avsnitt i kapitel 4.

om informationssäkerhet för statliga myndigheter[9]. Verktyget hänvisar också till tillgängligt stöd från MSB som kan vara till nytta för organisationer i utvecklingsarbetet. Infosäkkollen benchmark kan laddas ned från www.msb.se/infosakkollen.

Rekommendationerna nedan presenteras i fetstil, dels övergripande, dels för respektive aktörsgrupp. Under rekommendationerna för aktörsgrupperna anges ett urval av data som ligger till grund för rekommendationen.

2.2.1 Övergripande rekommendationer

Prioritera det systematiska informationssäkerhetsarbetet från ledningsnivå och nedåt och tilldela mer resurser om det behövs.
En stor andel av de svarande organisationerna anger resursbrist som den tyngst vägande faktorn bakom att man inte kommer vidare i informationssäkerhetsarbetet. Att tillföra mer resurser är inte alltid ett bra sätt att hantera ett problem – men när en betydande andel av organisationerna inte har en person som (åtminstone en viss del av tiden) dedikerat arbetar med informationssäkerhet förefaller mer resurser i många fall vara en nödvändig del av lösningen. I organisationer där man inte har minst en sådan person kan det dessutom vara så att man inte ens vet vilka resursbehov man har. Organisationer behöver ha dedikerad personal som har som minsta uppgift att hålla samman arbetet och visa på vilka resurser som krävs för att uppnå ledningens ambitionsnivå.

Dra nytta av de nya möjligheter till samarbete och samverkan som uppstår genom Infosäkkollen.
Inom de olika grupperna (kommuner, regioner och myndigheter) av svararande 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 som Infosäkkollen kan bistå med att upprätta finns det också möjligheter till samverkan genom nätverken KIS, HoSIS och SNITS.

Se till att spetsen inte kommer på bekostnad av bredden.
De allra flesta av de svarande organisationerna har några arbetsområden där de inte har satsat så mycket medan andra har många.

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.

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

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

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 det systematiska informationssäkerhetsarbetet, och mycket av det som görs går att formalisera och hantera på sätt som gör att andra tar vid om den man för närvarande är beroende av skulle bli otillgänglig för organisationen.

Arbeta aktivt för att skapa en god informationssäkerhetskultur där informationssäkerhet 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 informationssäkerheten. God informationssäkerhetskultur leder till att medarbetare känner både ett starkare engagemang för att identifiera, analysera och hantera risker och ett ägandeskap och ansvar för organisationens informationssäkerhet.

Använd uppföljning som grund för löpande förbättringar i utvecklingen av informationssäkerhetsarbetet.
Det område som uppvisar de största bristerna 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 gjorts fungerar som tänkt. 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 informationssäkerhet eftersom de saknar den återkoppling som behövs för att kunna förbättra arbetet i de delar där det inte har avsedd verkan. 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.

Stärk arbetet med kontinuitetshantering.
Under pandemin har många organisationer ändrat hur de arbetar, och de 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 ett 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.

2.2.2 Rekommendationer till kommunerna

Stärk ledningens engagemang i det systematiska informationssäkerhetsarbetet.
De flesta kommunledningar har någon gång satt en övergripande inriktning för arbetet och beslutat om en informationssäkerhetspolicy och andra övergripande principer för arbetet.

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

Den resulterande bilden är därför att kommunernas ledningar inte aktivt ser till att den inriktning som de har satt faktiskt efterföljs, och inte heller att de justerar inriktningen eller ändrar resurstilldelning eller mandat när situationen förändras (exempelvis genom omställningen till hemarbete under pandemin). 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.

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 är det en majoritet av kommunerna som saknar ett arbetssätt för analys och hantering av informationssäkerhetsrisker som under den senaste två-årsperioden har

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

I brist på etablerade arbetssätt som är gemensamma för hela, eller åtminstone delar, av kommunerna får medarbetarna löpande hantera risker i den utsträckning de kan. När arbete med risker genomförs beror det på enskilda engagerade medarbetare, vilket innebär att arbetet är personberoende och inte sker på likartat sätt eller likartad grund. När risker inte identifieras, analyseras eller åtgärdas i en gemensam ordning, får kommunen i stort leva med risker som finns men inte är kända eller inte åtgärdats på bra sätt, och som ibland realiseras utan att mildrande åtgärder finns på plats.

Etablera ett arbetssätt för kontinuitetshantering och öva det.
Endast strax över en tredjedel av kommunerna har under perioden haft ett arbetssätt för kontinuitetshantering som har:

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

Av dem som har kontinuitetsplaner för sina olika verksamheter har ungefär hälften övat arbetssätten i planerna – men bland de som har övat arbetssätten har två tredjedelar endast övat 0–25 procent av sina verksamheter.

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

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

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

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

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

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

Medan typkommunen har haft ett arbetssätt för att hantera informationssäkerhetsincidenter och avvikelser, har det inte ingått att man ska analysera inträffade incidenter, deras grundorsaker och hantering, samt återföra erfarenheter till det förebyggande arbetet. Eftersom typkommunen inte haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling så har det inte heller bedrivits ett systematiskt arbete enligt en på förhand beslutad struktur att följa upp om ställda krav var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

Etablera ett arbetssätt för att säkerställa informationssäkerhet vid upphandling och kvalitetssäkra det.
En majoritet av kommunerna har under den senaste två-årsperioden inte haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling som har

- varit beslutat eller på annat sätt medvetet valt av kommunen
- omfattat fördelning av roller och ansvar

- innehållit en kommungemensam modell för informationssäkerhet vid upphandling
- varit beskrivet i stöd och vägledning för medarbetarna
- följts upp och utvärderats minst en gång.

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

- klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras eller anskaffas
- identifiera behovet av säkerhetsåtgärder utifrån resultatet av informationsklassningen och riskanalysen
- införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
- ställa krav på säkerhetsåtgärder som den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat ska införa
- följa upp om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats
- följa upp om de ställda kraven var ändamålsenliga och tillräckliga.

2.2.3 Rekommendationer till regionerna

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

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

Typregionen har undersökt medarbetarnas kunskaper på flera områden, men har inte undersökt vad de vet om

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

Typregionen 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. Typregionens ledning har inte följt upp och vid behov beslutat om organisationens arbete med att ta bort eller reducera identifierade hinder respektive införa eller stärka framgångsfaktorer.

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

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

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

Följ upp fler av säkerhetsåtgärderna och följ upp om informationssäkerhetskrav som har ställts vid upphandling efterföljs.
Till skillnad från de andra aktörsgrupperna har regionerna följt upp några av de arbetssätt som är centrala för det systematiska informationssäkerhetsarbetet de senaste två åren. Därutöver har man, också till skillnad från de andra aktörsgrupperna, i några hänseenden följt upp *resultatet* av sitt systematiska informationssäkerhetsarbete.

Uppföljningen uppvisar dock vissa brister. Typregionen har utvärderat om införda säkerhetsåtgärder har varit ändamålsenliga i endast upp till 25 procent av regionens verksamheter. Det har inte skett någon uppföljning av om de krav som ställdes i samband med upphandlingar var ändamålsenliga och tillräckliga, eller om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

2.2.4 Rekommendationer till statliga myndigheter

Följ MSB:s föreskrifter om statliga myndigheters informationssäkerhet.
Statliga myndigheter ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt (19 § förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap). Som stöd för detta arbete har MSB sedan 2009 utfärdat föreskrifter med detaljerade

krav på hur ett systematiskt informationssäkerhetsarbete ska bedrivas. Det ska omfatta all behandling av information som myndigheten ansvarar för, och integreras med myndighetens befintliga sätt att leda och styra sin organisation. Resultatet i Infosäkkollen 2021 visar att många myndigheter är ganska långt ifrån att nå upp till kraven de omfattas av.

Stärk ledningens engagemang i det systematiska informationssäkerhetsarbetet.
Det är visserligen så att en majoritet av de svarande myndigheterna anger att de i flera avseenden har en ledning som aktivt deltar i det systematiska informationssäkerhetsarbetet. Majoriteten är dock ofta liten (51–55 procent), och bland de myndigheter som inte hör till majoriteten är ledningens deltagande i arbetet i allmänhet betydligt mindre aktivt. De statliga myndigheter som hör till den här minoriteten behöver informera sig om statusen på organisationens systematiska informationssäkerhetsarbete, besluta om inriktning och nivå på informationssäkerhetsarbetet, tillsätta resurser så att beslutade åtgärder ska kunna genomföras och aktivt ta bort hinder och stärka framgångsfaktorer för att underlätta det systematiska informationssäkerhetsarbetet.

Öva kontinuitetshantering.
Typmyndigheten har under den senaste tvåårsperioden haft ett arbetssätt för kontinuitetshantering som är beslutat eller på annat sätt medvetet valt av organisationen, som omfattar fördelning av roller och ansvar och som har följts upp och utvärderas minst en gång. Men arbetssättet har inte övats. 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.

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

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

- hur ofta risken kan väntas inträffa givet de rådande omständigheterna
- när risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna
- hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder införs

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

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

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

- 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 (d.v.s. att analysen genomförs igen för att se vilken riskreducerande effekt den eller de införda säkerhetsåtgärderna har medfört)
- status för informationssäkerhetsrisker följs upp utifrån definierade intervall.

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

Under perioden har typmyndigheten utbildat upp till 75–100 procent av sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning. Under samma period har [typmyndigheten] undersökt upp till 25 procent av medarbetarnas kunskaper om informationssäkerhet. Man har dock inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder kunskaperna i sitt arbete.

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

- vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- de regler och krav som styr informationssäkerhetsarbetet inom organisationen
- vad medarbetarna ska göra om en informationssäkerhetsincident inträffar

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

Följ upp arbetet och de utkontrakterade tjänsterna.
Typmyndigheten har under perioden inte följt upp eller utvärderat arbetssätten för hantering av informationssäkerhetsincidenter och -avvikelser, omvärldsbevakning; eller säkerställande av informationssäkerhet vid upphandling.

Myndigheterna har de senaste två åren inte heller följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera

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

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

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

2.3 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:

Facilitering av samarbeten: Organisationer som har rapporterat in sina svar i Infosäkkollen ska beredas möjlighet att hitta andra organisationer att samarbeta med för att komma vidare i sitt systematiska informationssäkerhetsarbete. Baserat på resultaten i Infosäkkollen kan MSB hjälpa organisationer som redovisat olika styrkor och utvecklingsbehov att hitta varandra för kunskapsdelning och erfarenhetsutbyte.

MSB kommer också att tillhandahålla material till stöd för organisationer som vill samarbeta med varandra kring olika delar av det systematiska informationssäkerhetsarbetet.

Behovsundersökning: Resultaten från Infosäkkollen visar på de brister målgrupperna har i sitt systematiska informationssäkerhetsarbete. För att få en tydligare bild av vilka underliggande behov som finns relaterat till dessa brister kommer MSB att tillsammans med målgrupperna undersöka vad de behöver för att utveckla sitt arbete. Syftet med utredningen är att tydliggöra vad som hindrar utvecklingen samt hur råd och stöd kan utformas för att på bästa sätt hjälpa målgrupperna framåt.

Utbildning: MSB vidareutvecklar sina utbildningsaktiviteter, både sin kurs i strategiskt och systematiskt informationssäkerhetsarbete och sin kurs för myndighetschefer i den offentliga förvaltningen, med utgångspunkt i resultatet från Infosäkkollen för att bidra till att adressera de brister som framkommit.

Utbildning för utbildare: MSB analyserar möjligheten att genomföra aktiviteter riktade mot aktörer som erbjuder tjänster och utbildningar inom informationssäkerhet, i syfte att ge en orientering kring systematiskt informationssäkerhetsarbete i den offentliga förvaltningen och de krav som ställs.

Metodstöd: Nya och uppdaterade vägledningar för analys och hantering av informationssäkerhetsrisker kommer att publiceras inom ramen för MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

Riskbild: MSB ska påbörja utveckling av en form av grundläggande riskbilder som är gemensamma för organisationer i den offentliga förvaltningen, i syfte att ge en grund för riskanalysarbetet som på så sätt får en gemensam grundplåt att utgå ifrån.

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

MSB kommer också att publicera Mognadsdialogen, ett pedagogiskt verktyg som syftar till att skapa bättre förutsättningar för dialog och ömsesidig förståelse för ledningar, informationssäkerhetspersonal och andra berörda. Verktyget ger en indikation på hur organisationen ligger till mognadsmässigt inom det systematiska informationssäkerhetsarbetet och bidrar härigenom till att skapa samsyn om nuläget och vad som behöver prioriteras framåt.

Stöd till rättsavdelningar och internrevisorer: MSB kommer att utöka sina informationsinsatser om föreskrifterna om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) i syfte att stödja andra myndigheters rättsavdelningar i uttolkningen av kraven. MSB kommer också att rikta informationsinsatser mot myndigheters internrevisioner för att informera om föreskriftskraven och hur Infosäkkollen kan användas för att indikera hur kraven efterlevs.

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

Forskning: MSB kommer under hösten 2022 att starta en ny forskningsutlysning om ekonomiska perspektiv på informations- och cybersäkerhet motsvarande 20 miljoner kronor. Inom ramen för utlysningen kommer det vara möjligt att söka stöd för forskning om hur resurstillsättning, riskvärdering och andra aspekter med koppling till hur informationssäkerhetsarbetet inom den offentliga förvaltningen ser ut och kan förbättras. Dessutom pågår redan forskning kring informationssäkerhetskultur och informationsklassning och hur arbetet med det kan underlättas för organisationer. Under 2022 etablerar MSB också det nationella samordningscentret för forskning och innovation (NSC) som syftar till att underlätta tillgång till forskningsmedel och främja forskning och innovation på informations- och cybersäkerhetsområdet.

Se även kapitel 5 för mer information om hur MSB kommer att utveckla Infosäkkollen.

2.4 Samarbete och näringslivets roll

Denna rapports mest centrala slutsats är att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Mer behöver göras, men mer behöver också göras mer effektivt så att begränsade resurser kan ge mer effekt i det systematiska informationssäkerhetsarbetet.

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

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

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

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

2.4.1 Områden där kommunerna behöver särskilt stöd

Följande frågor i Infosäkkollen representerar områden där kommunerna har få kommuner att vända sig till för att lära sig av andras erfarenheter, och där externa aktörer därför kan göra en särskilt viktig insats:

- **Fråga 14:** Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 15:** Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 17:** Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 26:** Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?
- **Fråga 27:** Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30:** De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 31:** De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?
- **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?

2.4.2 Områden där regionerna behöver särskilt stöd

Följande frågor i Infosäkkollen representerar områden där regionerna har få regioner att vända sig till för att lära sig av andras erfarenheter, och där externa aktörer därför kan göra en särskilt viktig insats:

- **Fråga 39:** De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

2.4.3 Områden där de statliga myndigheterna behöver särskilt stöd

Följande frågor i Infosäkkollen representerar områden där myndigheterna har få myndigheter att vända sig till för att lära sig av andras erfarenheter, och där externa aktörer därför kan göra en särskilt viktig insats:

- **Fråga 17:** Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 27:** Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30:** De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 39:** De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?
- **Fråga 40:** De senaste två åren, har organisationens ledning arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?

Hur resultatet tagits fram

3. Hur resultatet tagits fram

3.1 Om strukturen för uppföljning

Det ena målet med strukturen är att ge den offentliga förvaltningens organisationer stöd i att följa upp det systematiska informationssäkerhetsarbetet. Detta görs i form av verktyget Infosäkkollen, där organisationen genom att svara på frågor om sitt arbete direkt får återkoppling om vilken nivå organisationen befinner sig på och viktigare utvecklingsområden.

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

Strukturen har dessutom vidareutvecklats med ett återkopplingsverktyg, Infosäkkollen Benchmark, där en organisation kan jämföra sitt eget resultat med sammanställda resultat 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, alltså nästa gång 2023. Tvåårsintervallet är valt för att nivån på informationssäkerhetsarbetet är resultatet av arbete och val som har gjorts över tid. Då både förändringar och uppföljning tar tid att genomföra blir det inte effektivt att mäta för ofta.

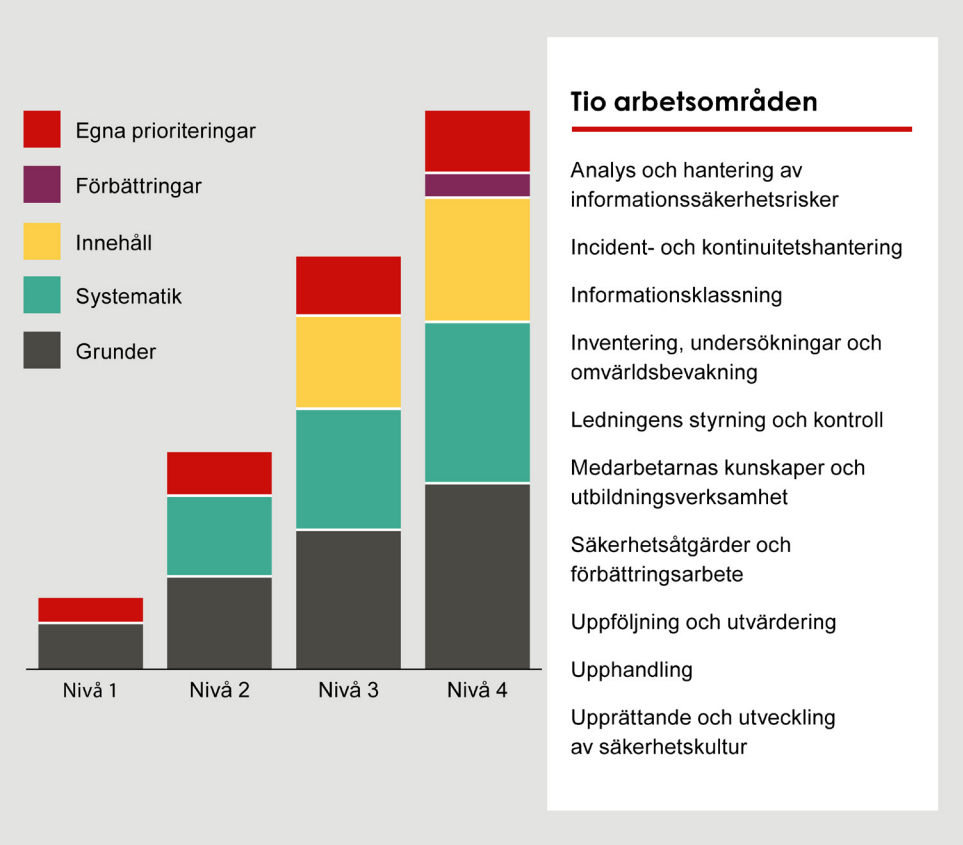
Uppföljningen är inriktad på det systematiska informationssäkerhetsarbetet, det vill säga att organisationen arbetar medvetet och metodiskt med att analysera, planera, genomföra samt följa upp och förbättra sin informationssäkerhet, samt att de olika delarna av arbetet kopplas ihop till en helhet. Uppföljningen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

MSB:s uppfattning om hur en organisation bör bedriva sitt systematiska informationssäkerhetsarbete framgår av myndighetens föreskrifter[10] 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.

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

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

Illustration 1. Infosäkkollens modell för uppföljning



Närmare bakgrund till och beskrivning av den modell som ligger till grund för nivåindelning och resultatberäkning finns i den första redovisningen från mars 2021, *En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.*

3.2 Om analysunderlaget

Denna rapport är baserad på svaren som MSB fick ta del av under den första inrapporteringsperioden för resultat från Infosäkkollen, som genomfördes från maj till september 2021.

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

3.2.1 Svarsfrekvens

Lanseringen av Infosäkkollen riktades till 651 organisationer i den offentliga förvaltningen. Listan inkluderade alla domstolar, men Domstolsverket har rapporterat in ett svar för alla domstolars räkning (88 organisationer). Sammantaget ingår svar från 301 organisationer i underlaget. Ett fåtal inkomna svar har lämnats utanför på grund av att de inkommit försent, inte varit möjliga att läsa in eller kommer från organisationer utanför målgruppen. Svaren i underlaget fördelar sig mellan målgrupperna enligt följande: 169 kommuner, 10 regioner, 122 statliga myndigheter.

Ungefär hälften av organisationerna har alltså valt att dela sina resultat för MSB:s analys. Den höga svarsfrekvensen ger ett utmärkt underlag för analys och slutsatser kring det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.

Bland statliga myndigheter kan noteras att få bevakningsansvariga myndigheter rapporterat in sina svar. En möjlig orsak är det regeringsuppdrag som dessa myndigheter hade under samma period, gällande rapportering kring totalförsvarsarbetet.

Spridningen i resultat bland de organisationer som delat sina svar tyder inte på någon omfattande ovilja att dela med sig även om resultatet varit lågt.

Det särskilda förfarandet för överföring av resultat till MSB har av vissa organisationer upplevts som utmanande/krångligt. Det kan inte uteslutas att några organisationer som varit positivt inställda till att dela sina resultat ändå har avstått från att göra det av denna anledning.

Att så många organisationer valt att bidra till MSB:s analys har givetvis flera anledningar, men den omfattande kommunikationsinsats som gjordes inför lanseringen tycks ha varit framgångsrik. Insatsen använde olika forum och kanaler, och budskapen lyfte fram värdet för de enskilda organisationerna i att dela med sig av sina svar och främjandet av en positiv uppföljningskultur.

Samarbete med målgrupperna och fokus på förankring i utvecklingsprocessen har sannolikt också bidragit till att verktyget blivit känt och uppfattats positivt. Åtskilliga organisationer har i samband med inrapportering av sina svar lämnat kommentarer om hur verktyget är till stor hjälp, även (kanske rent av särskilt) för organisationer som inte kommit så långt med informationssäkerhetsarbetet.

Samtidigt finns ett stort antal organisationer som inte är representerade, som antingen använt verktyget internt utan att dela sina resultat eller inte använt verktyget alls.

3.2.2 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.

Hur verktyget använts och hur arbetet med att besvara frågorna gått till kommer att undersökas vid en utvärdering som genomförs inför nästa omgång av inrapportering 2023. Om möjligt kommer utvärderingen också att titta närmare på den grupp organisationer som inte svarat samt tänkbara orsaker till detta.

3.3 Sammanställning och analys av resultaten

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

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

3.3.1 Benchmarks

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

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

3.3.2 Resultattal

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

En mer utförlig förklaring av begreppen finns i Bilaga 2.

3.3.3 Om redogörelsen för resultaten

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

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

Den samlade bilden för offentlig förvaltning

4. Den samlade bilden för offentlig förvaltning

4.1 Inledning

I det här kapitlet presenterar vi resultaten i Infosäkkollen 2021, dels på övergripande nivå, och dels nedbrutet på de tre aktörsgrupperna (kommuner, regioner och statliga myndigheter).

För att göra texten mer tillgänglig har vi valt att presentera resultatet utifrån vad olika benchmarks visar. Det är därför viktigt att ha en förståelse för vad vi menar med det begreppet (se kapitel 3 ovan), samt hur vi genererar de benchmarks som framställningen grundar sig på.

För att ytterligare tydliggöra där det råder stor likhet respektive stora skillnader mellan de organisationer vars resultat har legat till grund för benchmarksen vi presenterar, har vi i några fall indikerat resultat som grundar sig på svaga majoriteter. För klarhets skull har vi även i några särskilt viktiga fall redovisat det statistiska utfallet på en viss fråga.

Formuleringarna som används i respektive aktörsgrupps avsnitt *Resultat inom arbetsområdena* är, med små grammatiska justeringar, alla hämtade direkt ifrån Infosäkkollens frågor och svarsalternativ. Avsnitten är skrivna så för att det ska vara enkelt att se varifrån vi har fått data till stöd för det som sägs.

Vissa uppgifter upprepas inom flera arbetsområden. Skälet till det är för att vissa uppgifter ligger till grund för utfallet inom fler än ett arbetsområde. Fråga 16 i Infosäkkollen, om organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning, är ett exempel på det. Resultatet på den frågan används dels som en grund för bedömning inom arbetsområdet Medarbetarnas kunskaper och utbildningsverksamhet, men också inom arbetsområdet Upprättande och utveckling av säkerhetskultur.

Avsnitten är också skrivna så att det ska vara tydligt vad olika aktörsgrupper i allmänhet *inte* har eller har gjort. Skälet till det är för att det ska vara enkelt att göra jämförelser mellan aktörsgrupperna.

4.2 Övergripande bild

Strax över 300 organisationer rapporterade in sina resultat i Infosäkkollen 2021 till MSB. Av dem var strax över 170 kommuner, 10 regioner och strax över 120 myndigheter. Några resultat rapporterades för sent för att kunna omhändertas i denna analys, varför resultatet som presenteras här grundar sig på 169 kommuner, 10 regioner och 122 myndigheter.

De övergripande resultaten i Infosäkkollen 2021 är genomgående låga, med undantag för några organisationer som har betydligt högre resultat än snittet. Samtidigt skiljer sig resultaten på gruppnivå åt på flera sätt när resultaten inom Infosäkkollens tre aktörsgrupper (kommuner, regioner och statliga myndigheter) jämförs med varandra.

Diagram 2. Alla inrapporterade organisationers resultattal

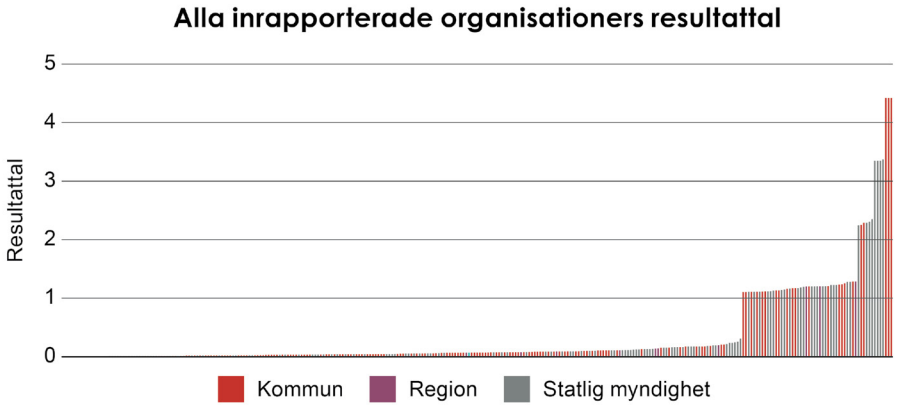


Diagram 3. Utfall i Infosäkkollens arbetsområden för alla svarande

Organisationernas resultat spänner över ett spektrum där vissa endast har uppnått enstaka poäng (nästan en tiondel av organisationerna har under tio poäng), och där några har nått mycket höga poäng. Många organisationer är starka inom några områden, samtidigt som man inte har satsat på andra (i synnerhet uppföljning och utvärdering och kontinuitetshantering), och följden av det har blivit att många inte har uppnått någon övergripande nivå i Infosäkkollen[11] (nästan en sjättedel av organisationerna som har rapporterat in sina svar har fått över 100 av Infosäkkollens 200 poäng, men ändå inte uppnått någon övergripande nivå).

11. Det finns fyra nivåer som kan uppnås i modellen. Organisationer som inte uppnår någon av dem har inte uppnått någon nivå, och deras resultat representeras av en liten ring i mitten av spindeldiagrammet ovan.

Tabell 1. Andel organisationer som har uppnått någon nivå inom respektive arbetsområde

Arbetsområde	% av kommunerna med nivå >0	% av regionerna med nivå >0	% av myndigheterna med nivå >0
Analys och hantering av informationssäkerhetsrisker	48%	80%	68%
Incident och kontinuitetshantering	32%	70%	57%
Informationsklassning	59%	90%	68%
Inventering, undersökningar och omvärldsbevakning	42%	70%	57%
Ledningens styrning och kontroll	58%	100%	69%
Medarbetarnas kunskaper och utbildningsverksamhet	42%	70%	46%
Säkerhetsåtgärder och förbättringsarbete	91%	100%	89%
Uppföljning och utvärdering	25%	60%	43%
Upphandling	42%	80%	61%
Upprättande och utveckling av säkerhetskultur	33%	70%	51%

I fråga om hur omfattande arbete man bedriver är så är variationen störst bland kommunerna (det finns tre kommuner som redovisar att de har genomfört en, två respektive tre åtgärder vardera under den senaste två-årsperioden och det finns också tre kommuner som endast saknar tre, tre respektive fyra av de 132 åtgärder som Infosäkkollen omfattar). Variationen är mindre bland statliga myndigheter (även om det finns tre myndigheter som har genomfört tre, tre respektive fyra åtgärder vardera) och den är som minst bland regionerna.

Det är tydligt att de flesta organisationer inom den offentliga förvaltningen (medvetet eller omedvetet) har satsat på spets inom några arbetsområden, snarare än bredd. Samtidigt finns det skillnader mellan aktörsgrupperna i fråga om balansen mellan bredd och spets. Bland kommunerna är satsningen på spets inom några arbetsområden som mest utpräglad (något som dock kan vara en följd av att många kommuner inte har satsat så mycket på informationssäkerhetsarbetet överhuvudtaget), vilket tydligt återspeglas i spindeldiagrammet om kommunerna nedan. De statliga myndigheterna uppvisar också en tydlig spretighet i sina satsningar, även om de har färre arbetsområden som är tydligt eftersatta i jämförelse med andra. Regionerna har även i den här frågan den största graden av homogenitet.

Med undantag för regionerna råder det en tydlig korrelation mellan organisationer som har ett lågt resultat och organisationer som inte har haft en informationssäkerhetsrelaterad[12] person angiven bland de som har arbetat med att genomföra Infosäkkollen. 61% av alla svarande, varav 62% bland kommuner, 70% bland regioner och 61%, har angett att en informationssäkerhetsrelaterad person har deltagit i arbetet med Infosäkkollen. Den troligaste förklaringen, i de flesta fall, till att en organisation inte har haft en sådan person med i processen är att man inte *har* en sådan person inom organisationen.

Den övergripande bilden som framkommer är att organisationer inom den offentliga förvaltningen främst har arbetat med att införa säkerhetsåtgärder. Samtidigt har man under perioden haft brister i såväl processerna som ska stödja organisationerna i att på ett rationellt sätt avgöra om de behöver säkerhetsåtgärder, och i så fall vilka, såväl som i processerna som ska stödja organisationen i att rationellt avgöra om säkerhetsåtgärderna fungerar och når de resultat de är tänkta att ge. Medan en sådan situation *kan* innebära att en organisation i delar ändå har en god informationssäkerhet (exempelvis genom engagemang hos individuella anställda när det gäller riskhantering eller genom förkovran och nyhetsförmedling på fritiden när det gäller omvärldsbevakning) så innebär det troligen i de flesta fall att organisationer inte upprättar och upprätthåller den informationssäkerhet som deras verksamhet behöver. I sådana fall där en organisation som brister i det systematiska informationssäkerhetsarbetet men kompenserar för det genom individuella medarbetares engagemang uppstår ofta för organisationen osunda personberoenden – och om en sådan person försvinner så kan mycket av den informationssäkerhet som man ändå hade gå förlorad.

Som noterat förefaller organisationer i den offentliga förvaltningen huvudsakligen ha arbetat med att införa säkerhetsåtgärder, inklusive sådana som har koppling till totalförsvarsverksamhet. Man har dock inte följt upp de införda säkerhetsåtgärderna. Samtidigt har man antingen redan haft eller under perioden infört eller uppdaterat vissa grundläggande inslag i arbetet, såsom en informationssäkerhetspolicy. Ledningen har beslutat om viss övergripande inriktning, men har sedan inte i särskilt stor utsträckning följt upp arbetet eller förhört sig om arbetets status. Viss grundläggande utbildningsverksamhet har bedrivits, men enbart en liten andel av medarbetarna har i allmänhet fått utbildning i informationssäkerhet under perioden. En påtaglig skillnad mellan kommunerna å ena sidan och regionerna och myndigheterna å den andra sidan är att den senare gruppen i stor utsträckning har ett arbetssätt för att säkerställa informationssäkerhet vid upphandling, och att man dessutom tillämpar det arbetssättet i hög grad. Regionerna når särskilt höga resultat inom det här området då de även har säkerställt att arbetssättet omfattar flera centrala inslag[13].

12. En informationssäkerhetssamordnare, en informationssäkerhetschef eller någon annan relevant person och/eller roll.

13. Specifikt: Klassning av information och analyser av informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas, bedömning av behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat, samt identifiering av säkerhetsåtgärder, införande av de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv samt kravställning på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat.

Det bristande aktiva engagemanget från ledningen kombinerat med begränsade utbildningsinsatser och avsaknaden av uppföljning innebär att arbetet med att upprätta och utveckla en (informationssäkerhets)kultur inom organisationerna har blivit lidande. Den mest genomgående bristen är att få organisationer har genomfört uppföljning av sitt informationssäkerhetsarbete, men en ytterligare brist är att organisationer ofta inte har ett arbetssätt för kontinuitetshantering – och även om de har ett sådant arbetssätt så har de inte övat det.

4.2.1 Omständigheter som har påverkat informationssäkerhetsarbetet under den senaste två-årsperioden

Ungefär hälften av organisationerna har svarat på om de under en längre tid de senaste två åren påverkats av omständigheter som de bedömer har haft stor inverkan på deras informationssäkerhetsarbete. Av dessa har en stor majoritet angett att covid-19-pandemin varit en sådan omständighet. Vissa har bara angett pandemin som sådan medan vissa specificerat att det handlat om ett ökat distansarbete, förhöjda säkerhetskrav på grund av distansarbete, förändrade rutiner eller att resurser som vanligtvis använts i informationssäkerhetsarbetet behövt lösa andra uppgifter. Det finns även organisationer som angett att det inte funnits några omständigheter under de senaste två åren som fått en sådan påverkan. Dessa är i en klar minoritet med cirka en åttondel sådana svar av de som besvarat frågan för kommuner och cirka en femtedel sådana svar av de som besvarat frågan för regionerna. För myndigheterna däremot är det cirka en tredjedel av de som besvarat frågan som angett att de inte haft någon sådan påverkan under de senaste två åren. Några ytterligare omständigheter som särskilt kommunerna angett har påverkat deras informationssäkerhetsarbete under perioden är EU-domstolens domslut i fallet som i folkmun gått under benämningen *Schrems II*[14] och hur detta domslut påverkat deras användning av olika molntjänster.

4.2.2 Hinder på vägen mot högre nivåer

Det är även ungefär hälften av organisationerna som besvarat frågan gällande vad de ser som de största hindren för att kunna ta sig till nästa nivå i modellen. En klar majoritet av de som svarat har angett att resursbrist är det största hindret. Vissa har specificerat att det rör sig om resurser såsom tid, personal och/eller ekonomi medan andra bara angett att det handlar om resurser utan ytterligare specificering. Jämfört med kommuner har myndigheter och regioner,

14. Data Protection Commissioner v Facebook Ireland and Maximilian Schrems, juli 2020. Domslutet ogiltigförklarade Privacy Shield, den ordning som satts upp mellan EU och USA för att möjliggöra dataflöden som inkluderar personuppgifter i GDPR:s bemärkelse. Skälet till domslutet var att Privacy Shield, på grund av amerikansk underrättelselagstiftning, inte kunde garantera att EU-medborgares personuppgifter som behandlas av it-tjänsteleverantörer som är verksamma på den amerikanska marknaden, inte hamnar hos amerikanska underrättelsemyndigheter. Det har utöver Privacy Shield också funnits möjlighet att använda standardklausuler för personuppgifter. Men skälen som ledde till att Privacy Shield ogiltigförklarades förefaller också vara applicerbara på sådana klausuler. Effekten av domslutet har blivit att molntjänster och andra it-tjänster från företag som faller under USA:s jurisdiktion löper en risk att inte kunna användas av europeiska organisationer. Förutom att det lett till en begränsning av utbudet har vissa av de it-tjänster som faller under amerikansk jurisdiktion av vissa ansetts ha en säkerhet och funktionalitet som inte nödvändigtvis har kunnat matchas av europeiska konkurrenter. Konsekvenserna på kort och medellång sikt av en legalt framtvingad förflyttning bort från företag som faller under USA:s jurisdiktion kan därför bli att den säkerhet som svenska organisationer har när de nyttjar exempelvis molntjänster inte blir lika hög.

utöver resursbrist, i större utsträckning angett verksamhetsstrukturen, dålig integration mellan informationssäkerhetsfrågor och verksamhetsstyrning och brist på ett systematiskt arbete som anses utgöra hinder för att nå nästa nivå. Kommunerna anger förutom brist på resurser även brister i ledningens stöd för och prioritering av informationssäkerhetsarbetet som klara hinder på vägen mot högre nivåer.

4.2.3 Hantering av säkerhetsskyddsklassificerade uppgifter och nyttjande av säkra kommunikationer

Eftersom innehållet i en organisations resultat kan vara känsligt användes ett särskilt förfarande för att upprätthålla säker hantering vid överföringen. Även om de svarande organisationerna klassificerat informationen olika så har instruktionen för inrapportering utgått ifrån skyddsnivå Begränsat hemlig, för att beakta informationens skyddsvärde i alla led och för att skydda den aggregerade mängden svar.

Det framgår tydligt att det råder varierad nivå på kunskaper och erfarenhet kring att hantera säkerhetsskyddsklassificerade uppgifter bland organisationerna i den svenska offentliga förvaltningen. Vissa organisationer har inte it-miljöer för att kunna arbeta med uppgifterna och det saknas kunskap om exempelvis signalskydd och hur säkerhetsskyddsklassificerade uppgifter ska hanteras. Andra aktörer har mer kunskap och erfarenhet och har processer och verktyg på plats för att hantera information av den här karaktären.

Ur ett vidare perspektiv kan tilläggas att förmågan i den offentliga förvaltningens organisationer att digitalt hantera, bearbeta och dela säkerhetsskyddsklassificerade uppgifter behöver stärkas.

4.2.4 Vad krävs för en högre övergripande nivå för den offentliga förvaltningen?

Det kan finnas två skäl till att man behöver genomföra fler åtgärder för att nå en högre nivå i Infosäkkollen: Antingen behöver man genomföra fler åtgärder för att nå minimipoängen som krävs på individuella frågor, eller så behöver man genomföra fler åtgärder för att nå den totalpoäng som krävs.

Av alla de 301 organisationerna finns det endast en organisation som har tillräckligt högt antal på poäng på varje fråga för att kunna komma vidare till nästa nivå (i det fallet är det ett otillräckligt högt antal säkra bedömningar som håller nivån nere). Samtidigt är det 221 organisationer som har en högre totalpoäng än vad de behöver för att nå en högre nivå än den de har. Bland dem har 119 organisationer upp till fem åtgärder från individuella frågor där de inte når minimikraven kvar, bland dem har 108 organisationer lika många frågor att få poäng på som de har åtgärder att genomföra (vilket indikerar att organisationen behöver bredda sitt informationssäkerhetsarbete till fler arbetsområden).

Av de 221 organisationerna som har en högre totalpoäng än vad de behöver för att nå en högre nivå än den de har så är 115 kommuner (53 med upp till fem återstående åtgärder), 10 regioner (9 med upp till fem återstående åtgärder) och 94 statliga myndigheter (57 med upp till fem återstående åtgärder).

Sammantaget betyder det att ett målmedvetet arbete med att upprätthålla de resultat som redan har uppnåtts, parat med ett tillskott av ytterligare, men relativt begränsade, resurser hos en tredjedel av organisationerna som rapporterade sina resultat under 2021 skulle kunna leda till för en höjning av den generella övergripande nivån till nästa mätning under 2023.

Det som specifikt behöver göras i den här gruppen (i ordning av det som det lägsta antalet gör först) är framförallt att genomföra uppföljning (fråga 14), uppdatera ledningen om statusen på det systematiska informationssäkerhetsarbetet (fråga 15), upprätta ett arbetssätt för kontinuitetshantering (fråga 10) och att upprätta ett arbetssätt för omvärldsbevakning (fråga 11).

Här finns också en relativt stor potential för samverkan då de flesta som brister på någon av de nämnda frågorna inte brister på de andra frågorna. Organisationer som har enstaka av de nämnda bristerna bör därför kunna finna andra organisationer som har genomfört de åtgärder man själv saknar, men som samtidigt brister inom områden där man själv har genomfört åtgärder.

4.3 Kommuner

4.3.1 Inledning

I det här delkapitlet presenterar vi den bild som framkommit genom en sammanställning av 169 inrapporterande kommuners resultat. Delkapitlet redovisar först en övergripande bild av läget bland kommunerna och därefter en detaljerad redogörelse för resultaten inom Infosäkkollens tio arbetsområden. Den detaljerade redogörelsen presenterar huvudsakligen vad benchmarken för alla de svarande kommunerna visar. I förekommande fall har klargörande statistik adderats.

Diagram 4. Kommunernas resultattal i Infosäkkollen 2021

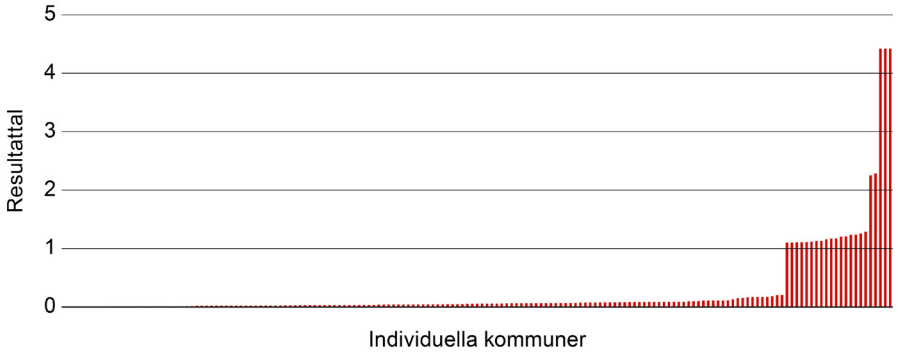
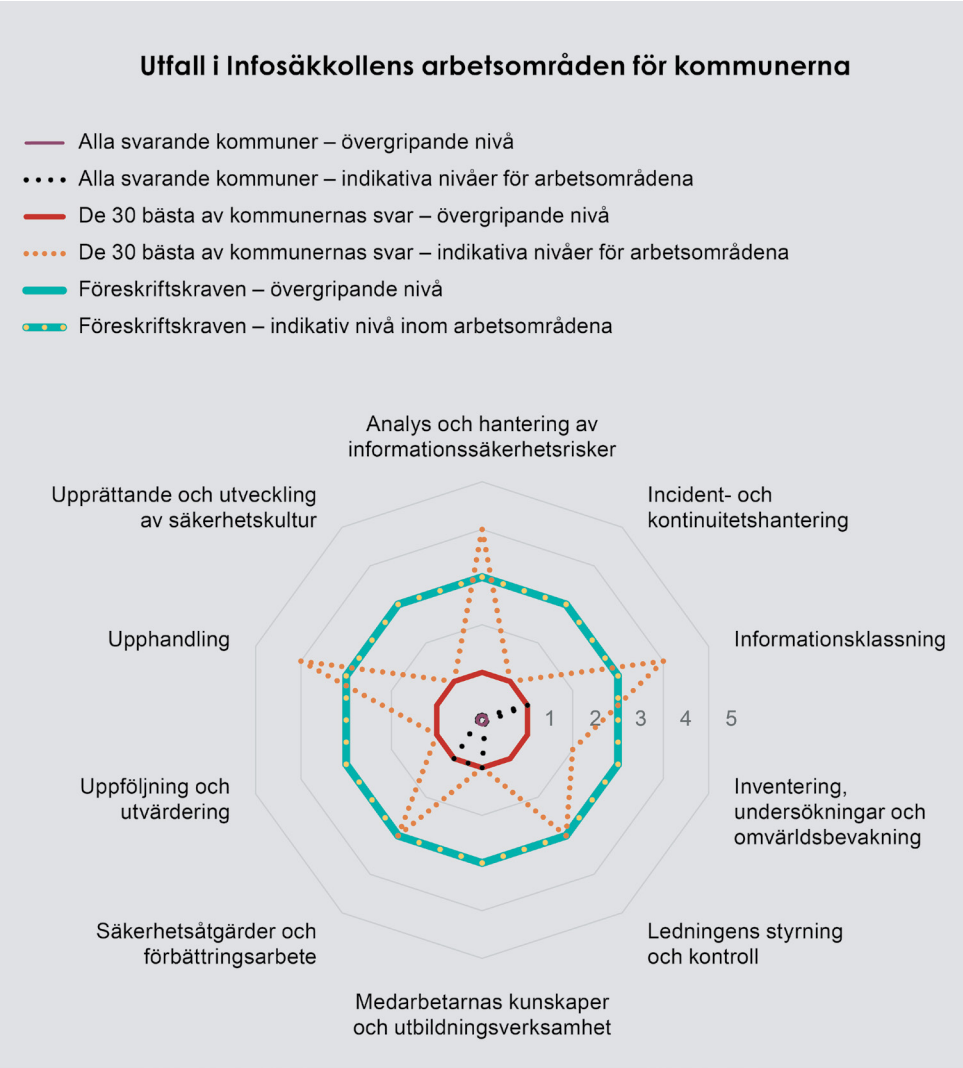


Diagram 5. Utfall i Infosäkkollens arbetsområden för kommunerna



4.3.2 Övergripande bild

Typkommunen har under mätperioden genomfört och haft på plats totalt 43 av Infosäkkollens 132 åtgärder. Samtidigt har den generella representanten för de 30 bäst presterande kommunerna genomfört och haft på plats 117 av åtgärderna. Kommunerna är därmed den mest heterogena bland tre aktörsgrupperna (se spindeldiagrammet ovan för en illustration av skillnaden mellan typkommunen och de 30 bäst presterande kommunerna) – såväl de starkaste som de svagaste resultaten är inrapporterade från kommuner.

Tabell 2.

Antal genomförda åtgärder per arbetsområde Totalt 169 kommuner	Generell kommun	Kommun bland de 30 bästa	Maxresultat
Analys och hantering av informationssäkerhetsrisker	3	44	47
Incident och kontinuitetshantering	10	19	24
Informationsklassning	7	25	26
Inventering, undersökningar och omvärldsbevakning	10	26	30
Ledningens styrning och kontroll	18	36	45
Medarbetarnas kunskaper och utbildningsverksamhet	4	33	43
Säkerhetsåtgärder och förbättringsarbete	8	26	34
Uppföljning och utvärdering	2	31	41
Upphandling	1	15	16
Upprättande och utveckling av säkerhetskultur	6	32	42

MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6) ger en god grund att stå på i informationssäkerhetsarbetet och myndigheten använder därför den uttolkning av föreskriftskraven som har gjorts i Infosäkkollen som ett riktmärke för hur de olika aktörerna ligger till i sitt arbete. Typkommunen har 76 åtgärder kvar att genomföra innan de når föreskriftskraven, medan representanten för de 30 bästa kommunerna har 10 åtgärder kvar att genomföra.

Det bör dock noteras att resultatet som typrepresentanten för de 30 bästa kommunerna uppnår påverkas av att tre kommuner har rapporterat in att de når strax under maxpoäng i modellen.

4.3.3 Förutsättningar för samarbeten

Kommunernas svar på de olika frågorna i Infosäkkollen indikerar att det finns vissa områden där det på systemnivå kan finnas stora fördelar med att samarbeta inom gruppen. Detta gäller främst områden som behandlas i frågor där fördelningen mellan de som fått poäng och de som inte fått poäng är förhållandevis jämn. Samarbeten på dessa frågor har potential att kunna hjälpa många då andelen som inte fått poäng är stor samtidigt som det finns en stor andel som kan erbjuda erfarenheter och stöttning med att förbättra sitt informationssäkerhetsarbete. De frågor där det är jämnt fördelat mellan de som fått poäng och de som inte fått poäng är främst:

- **Fråga 5:** Har organisationen de senaste två åren undersökt medarbetarnas kunskaper om informationssäkerhet?

- **Fråga 7:** Har organisationen haft ett arbetssätt för informationsklassning de senaste två åren?
- **Fråga 8:** Har organisationen haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker de senaste två åren?
- **Fråga 9:** De senaste två åren, har organisationen haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser?
- **Fråga 10:** Har organisationen haft ett arbetssätt för kontinuitetshantering de senaste två åren?
- **Fråga 11:** Har organisationen haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet de senaste två åren?
- **Fråga 12:** Har organisationen haft ett arbetssätt för utbildning i informationssäkerhet de senaste två åren?
- **Fråga 13:** Har organisationen haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren?
- **Fråga 16:** De senaste två åren, har organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning?
- **Fråga 19:** De senaste två åren, har organisationen bevakat utvecklingen på informationssäkerhetsområdet enligt sitt arbetssätt för omvärldsbevakning?
- **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 24:** De senaste två åren, har organisationen beslutat om att tilldela resurser för att kunna införa beslutade säkerhetsåtgärder?
- **Fråga 28:** Har organisationen, de senaste två åren, genomfört upphandling enligt sitt arbetssätt för att säkerställa informationssäkerhet?
- **Fråga 29:** De senaste två åren, har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat följande centrala delar?
- **Fråga 32:** De senaste två åren, har organisationens arbetssätt för informationsklassning omfattat följande centrala delar?
- **Fråga 38:** De senaste två åren, har organisationen undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap?

De frågor där det finns en övervägande majoritet som inte har fått några poäng finns det anledning för centrala myndigheter och andra stöttande organisationer på alla nivåer i samhället att se över sitt stöd. Detta rör främst:

- **Fråga 14:** Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 15:** Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 17:** Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 26:** Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?
- **Fråga 27:** Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?
- **Fråga 30:** De senaste två åren, har organisationen i sin undersökning av medarbetarnas kunskaper undersökt kunskaperna inom följande grundläggande områden?
- **Fråga 31:** De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?
- **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?

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

4.3.4 Resultat från arbetsområdena

Tabell 3.

Arbetsområde Totalt 169 kommuner	Antal med nivå >0	Antal med nivå >1	Antal med nivå >2
Analys och hantering av informationssäkerhetsrisker	80	25	6
Incident och kontinuitetshantering	53	9	7
Informationsklassning	99	32	18
Inventering, undersökningar och omvärldsbevakning	71	28	11
Ledningens styrning och kontroll	98	15	5
Medarbetarnas kunskaper och utbildningsverksamhet	70	9	4
Säkerhetsåtgärder och förbättringsarbete	153	19	10
Uppföljning och utvärdering	42	6	3
Upphandling	70	39	27
Upprättande och utveckling av säkerhetskultur	56	16	4

Analys och hantering av informationssäkerhetsrisker

Cirka två tredjedelar av de inrapporterande kommunerna har haft ett arbetssätt för hantering och analys av informationssäkerhetsrisker de senaste två åren. Över hälften av kommunerna har under perioden dock saknat ett arbetssätt som har:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Strax över en åttondel har antingen arbetat med att utveckla ett sådant arbetssätt under perioden, eller haft ett arbetssätt under delar, men inte hela, perioden.

Typkommunen har under de senaste två åren därför inte analyserat sina informationssäkerhetsrisker enligt ett arbetssätt för ändamålet. Däremot har typkommunen tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid 0–25% av sina informationsklassningar och analyser av informationssäkerhetsrisker. Bland typkommunens verksamheter har 0–25%

fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker.

Då typkommunen under perioden inte har haft ett arbetssätt där minst en av de ovanstående punkterna stämmer så har de inte heller under perioden (åtminstone inte under hela perioden) haft ett kvalitetssäkrat arbetssätt där:

1. Analysen av informationssäkerhetsrisker har:
    a. Utgått ifrån organisationens informationsklassning av berörda informationsmängder, informationssystem och nätverk
    b. Utgått ifrån en specifik uppgift som ska lösas med stöd av analysen av informationssäkerhetsrisker
    c. Utvärderat riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet
    d. Stötts av medarbetare med särskild kompetens inom analys av informationssäkerhetsrisker
    e. Granskats och godkänns av berörda informationsägare

2. Bedömningen av informationssäkerhetsrisker alltid tar hänsyn till potentiell skadeverkan på:
    a. Informationsmängder, informationssystem och nätverk (den egna organisationens och andras)
    b. Människors liv och hälsa (de egna medarbetarnas och andras)
    c. Finansiella tillgångar och övrig egendom (den egna organisationens och andra människors eller organisationers)
    d. Tillhandahållande av tjänster (den egna organisationens och andra organisationers)
    e. Förtroende (allmänhetens eller andras, för organisationen eller andra organisationer, för egna eller andras tjänster)

3. Bedömningen av informationssäkerhetsrisker alltid värderar:
    a. Hur ofta risken kan väntas inträffa givet de rådande omständigheterna
    b. När risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna
    c. Hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder införs
    d. När risken tidigast, senast och troligast kan väntas inträffa om föreslagna säkerhetsåtgärder införs
    e. Hur säker man kan vara på sannolikhetsbedömningarna givet vad man vet och de antaganden man har gjort

4. Hanteringen av informationssäkerhetsrisker har omfattat att:
    a. Varje identifierad informationssäkerhetsrisk har en riskägare
    b. Organisationen har ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd
    c. Analys av enskilda informationssäkerhetsrisker uppdateras efter att beslutade säkerhetsåtgärder har införts
    d. Inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker
    e. Status för informationssäkerhetsrisker följs upp utifrån definierade intervall

Under perioden har typkommunen haft tillgång till kompetens inom analys och hantering av informationssäkerhetsrisker. Samtidigt har typkommunen inte följt upp resultatet av sitt informationssäkerhetsarbete under perioden, och de har därför inte följt upp resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker. Typkommunens ledning har i allmänhet inte informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete under perioden, och i det ingår att ledningarna inte heller har informerat sig om eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats. Då typkommunen har saknat ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren så har de inte heller under den perioden haft ett arbetssätt som inkluderar:

1. Klassning av information och analyser av informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
2. Bedömning av behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat
3. Införande av de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
4. Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat

Incident- och kontinuitetshantering

Typkommunen har de senaste två åren i allmänhet haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för hantering av informationssäkerhetsincidenter och -avvikelser och det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte följts upp.

Arbetssättet har under perioden i allmänhet saknat sådana centrala inslag som Infosäkkollen efterfrågar, d.v.s.:

- En funktion för att hantera informationssäkerhetsincidenter och -avvikelser med dedikerad personal som har särskild kompetens
- Kanaler som medarbetare inom organisationen kan använda för att nå funktionen och rapportera incidenter och avvikelser
- Kanaler som funktionen kan använda för att nå andra organisationer och rapportera om incidenter, få rapporter om incidenter eller dela information, samt rutiner för deras användning
- En eskaleringsrutin för att hantera stora och allvarliga incidenter, inklusive extern rapportering vid behov
- Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete

Typkommunen har under perioden saknat ett arbetssätt för kontinuitetshantering och de har därför inte övat kontinuitetshantering enligt något sådant arbetssätt.

Typkommunen har under perioden typiskt undersökt upp till 25% av medarbetarnas kunskaper i informationssäkerhet, men undersökningen har inte inkluderat huruvida de vet vad de ska göra om en informationssäkerhetsincident inträffar. Typkommunens arbetssätt för analys och hantering av informationssäkerhetsrisker har under perioden inte omfattat användning av inträffade avvikelser och incidenter som underlag för analys av informationssäkerhetsrisker.

Under perioden har typkommunen inte undersökt eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns. De har däremot i allmänhet kontrollerat eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång.

Informationsklassning

Typkommunen har under de senaste två åren i allmänhet haft ett arbetssätt för informationsklassning. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för klassning med definierade nivåer för skyddskrav med fördefinierade säkerhetsåtgärder och det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte följts upp.

Under perioden har typkommunen haft tillgång till kompetens inom informationsklassning och man har klassat sin information enligt sitt arbetssätt för informationsklassning i upp till 25% av sina verksamheter. Typkommunen har tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid 0–25% av sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typkommunens arbetssätt för informationsklassning har under perioden inte omfattat att informationsklassningen ska:

- Utgå ifrån organisationens inventering av informationsmängder, informationssystem och nätverk
- Beakta tillämplig lagstiftning, inklusive offentlighets- och sekretesslagen, dataskyddsförordningen, säkerhetsskyddslagen, arkivlagen, samt krisberedskapsförordningen eller lagen om extraordinära händelser
- Utgå ifrån krav på tillgänglighet, riktighet och konfidentialitet
- Stödjas av medarbetare med särskild kompetens inom informationsklassning
- Granskas och godkännas av berörda informationsägare

Inventering, undersökningar och omvärldsbevakning

Typkommunen har under perioden minst en gång inventerat sina informationsmängder och informationssystem, inklusive nätverk, i 75–100% av sina verksamheter. Typkommunen har haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet under perioden, men arbetssättet har inte:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Under perioden har typkommunen bevakat utvecklingen på informationssäkerhetsområdet och minst en gång per kvartal spridit information till utpekade medarbetare inom upp till 25% av organisationens verksamheter. Typkommunen har också under perioden tittat på och använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser i upp till 25% av sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typkommunen har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns

- Eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång

Däremot har man inte gått igenom eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns.

Typkommunen har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Ledningens styrning och kontroll

Under perioden har typkommunens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning
- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

Typkommunen har i allmänhet under perioden också haft en informationssäkerhetspolicy (eller motsvarande dokument) som har innehållit:

- En definition av informationssäkerhet och informationssäkerhetsarbete
- Ledningens målsättningar för informationssäkerhetsarbetet (vad som ska uppnås)
- Ledningens inriktning för informationssäkerhetsarbetet (hur det ska uppnås)
- Definierade roller som ledningen har pekat ut som ansvariga för att hantera informationssäkerhet
- Att arbetet ska integreras i myndighetens befintliga sätt att leda och styra sin organisation

Typkommunen har de senaste två åren i allmänhet haft utpekade informationsägare eller motsvarande för sin information de senaste två åren i alla organisationens verksamheter.

Typkommunen har inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren. I det ingår att organisationen, och ledningen, därigenom inte har följt upp:

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

Ledningen har inte heller under perioden informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, och därigenom inte informerat sig om:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- Resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Under perioden har typkommunen beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i upp till 25% av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa 0–25% av sina beslutade säkerhetsåtgärder och man har också infört upp till 25% av de säkerhetsåtgärder som har beslutats.

Typkommunens ledning har under perioden inte arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång ha följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt

- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Medarbetarnas kunskaper och utbildningsverksamhet

Typkommunen har under perioden undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet. Man har också haft ett arbetssätt för utbildning i informationssäkerhet under perioden och det har varit beslutat eller på annat sätt medvetet valt av organisationen. Det har däremot inte omfattat fördelning av roller och ansvar, innehållit en organisationsgemensam modell för utbildning i informationssäkerhet, varit beskrivet i stöd och vägledning för medarbetarna, eller följts upp och utvärderats minst en gång under den tiden. Man har också haft tillgång till kompetens inom utbildning i informationssäkerhet under perioden.

Under perioden har organisationen utbildat upp till 25% av sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning. Man har dock inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

I sin undersökning av medarbetarnas kunskaper har typkommunen inte undersökt huruvida medarbetarna vet:

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

Typkommunens utbildning i informationssäkerhet har under perioden inte varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Ledningens målsättningar för det systematiska informationssäkerhetsarbetet
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet

- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

Typkommunen har i allmänhet inte undersökt medarbetarnas uppfattningar om vilka hinder och framgångsfaktorer som påverkar deras möjligheter att arbeta på ett informationssäkert sätt och som de möter i sin verksamhet.

Säkerhetsåtgärder och förbättringsarbete

Under perioden har typkommunen haft tillgång till särskild kompetens inom arbete med it-säkerhet. Typkommunen har beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i upp till 25% av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa upp till 25% av sina beslutade säkerhetsåtgärder och man har också infört upp till 25% av de säkerhetsåtgärder som har beslutats. Typkommunen har under perioden i allmänhet inte utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typkommunen har under perioden inte följt upp skillnaden mellan införda och beslutade säkerhetsåtgärder eller resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet. Man har inte haft ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd.

Typkommunen har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns

Typkommunens ledning har under perioden inte arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt

- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Uppföljning och utvärdering

Typkommunen har under perioden haft tillgång till kompetens inom uppföljning av informationssäkerhetsarbete, men man har inte följt upp eller utvärderat något av arbetssätten för informationsklassning, analys och hantering av informationssäkerhetsrisker, hantering av informationssäkerhetsincidenter och -avvikelser, kontinuitetshantering, omvärldsbevakning, utbildning i informationssäkerhet eller säkerställande av informationssäkerhet vid upphandling.

Typkommunen har i allmänhet inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete under perioden.

Typkommunen har inte heller undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

Typkommunen har i allmänhet inte utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typkommunen har undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet och informationssäkerhetsarbete, men man har inte undersökt huruvida medarbetarna vet:

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

Medan typkommunen har haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser så har det i det arbetssättet inte ingått att man ska bedriva analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete. Då man i allmänhet inte har haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker så har man heller inte, som en del av arbetssättet, utvärderat riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet. Då man inte heller i allmänhet har haft ett arbetssätt för att

säkerställa informationssäkerhet vid upphandling så har det inte heller ingått i arbetssättet att följa upp om ställda krav var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

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

Upphandling

Typkommunen har under perioden haft tillgång till särskild kompetens inom säkerställande av informationssäkerhet vid upphandling. De har också haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren, men det har i allmänhet inte:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för informationssäkerhet vid upphandling
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Typkommunen har dock inte använt det arbetssättet vid upphandlingar under den senaste två-årsperioden.

Arbetssättet har under perioden inte omfattat att:

- Klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
- Bedöma behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat, samt att identifiera säkerhetsåtgärder
- Införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
- Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat
- Följa upp om de ställda kraven var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats

Upprättande och utveckling av säkerhetskultur

Under perioden har typkommunens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning

- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

Under perioden har ledningen inte informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, och därigenom inte informerat sig om:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- Resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Typkommunen har inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

I sin undersökning av medarbetarnas kunskaper har typkommunen inte undersökt huruvida medarbetarna vet:

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

Typkommunens utbildning i informationssäkerhet har under perioden inte varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Ledningens målsättningar för det systematiska informationssäkerhetsarbetet
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet
- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

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

Typkommunens ledning har under perioden inte arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång ha följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

4.4 Regioner

4.4.1 Inledning

I det här delkapitlet presenterar vi den bild som framkommit genom en sammanställning av 10 inrapporterande regioners resultat. Delkapitlet redovisar först en övergripande bild av läget bland regionerna och därefter en detaljerad redogörelse för resultaten inom Infosäkkollens tio arbetsområden. Den detaljerade redogörelsen presenterar huvudsakligen vad benchmarken för alla de svarande regionerna visar. I förekommande fall har klargörande statistik adderats.

Diagram 6. Regionernas resultattal i Infosäkkollen 2021

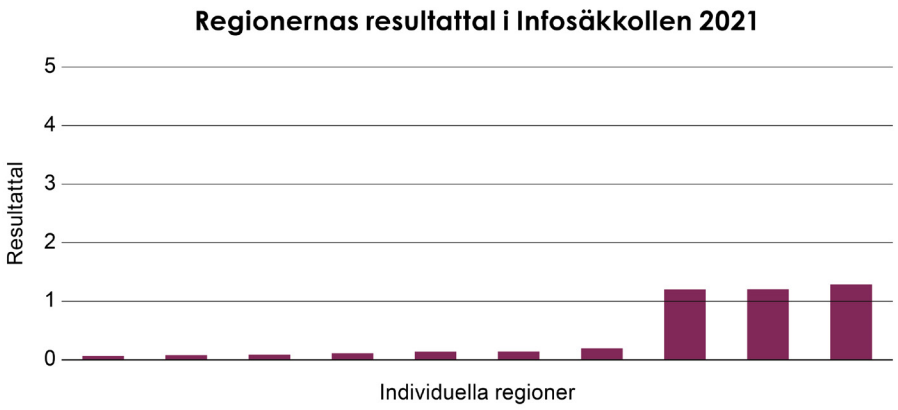
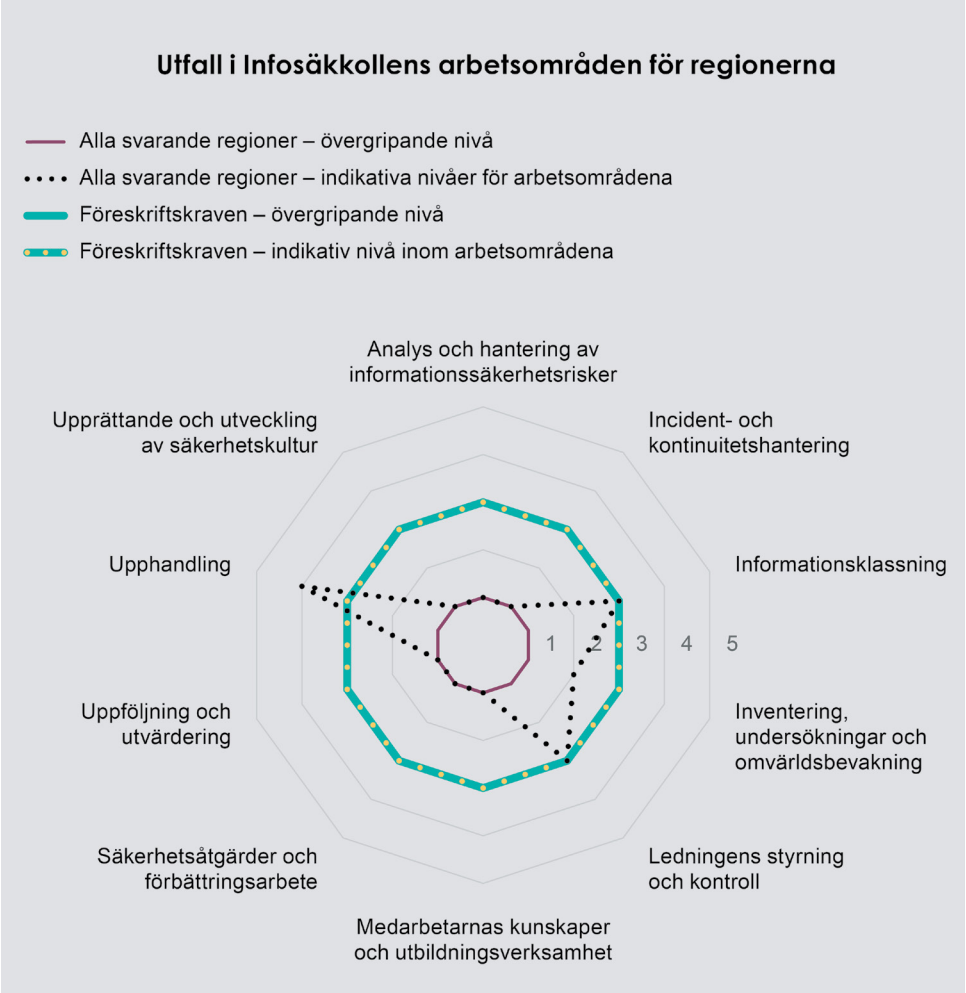


Diagram 7. Utfall i Infosäkkollens arbetsområden för regionerna



4.4.2 Övergripande bild

Typregionen har under mätperioden genomfört och haft på plats totalt 99 av Infosäkkollens 132 åtgärder. Regionerna är de minst heterogena bland tre aktörsgrupperna.

Tabell 4.

Antal genomförda åtgärder per arbetsområde Totalt 10 regioner	Generell region	Maxresultat
Analys och hantering av informationssäkerhetsrisker	32	47
Incident och kontinuitetshantering	17	24
Informationsklassning	20	26
Inventering, undersökningar och omvärldsbevakning	18	30
Ledningens styrning och kontroll	35	45
Medarbetarnas kunskaper och utbildningsverksamhet	16	43
Säkerhetsåtgärder och förbättringsarbete	23	34
Uppföljning och utvärdering	12	41
Upphandling	13	16
Upprättande och utveckling av säkerhetskultur	18	42

MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6) ger en god grund att stå på i informationssäkerhetsarbetet och myndigheten använder därför den uttolkning av föreskriftskraven som har gjorts i Infosäkkollen som ett riktmärke för hur de olika aktörerna ligger till i sitt arbete. Typregionen har 22 åtgärder kvar att genomföra innan den når föreskriftskraven.

Det bör noteras att resultatet som typrepresentanten för regionerna uppnår är avhängigt ett betydligt färre antal inkomna rapporter (10 stycken, att jämföra med 169 för kommunerna och 122 för myndigheterna).

4.4.3 Förutsättningar för samarbeten

Regionernas svar på de olika frågorna i Infosäkkollen indikerar att det finns vissa områden där det på systemnivå kan finnas stora fördelar med att samarbeta inom gruppen. Detta gäller främst områden som behandlas i frågor där fördelningen mellan de som fått poäng och de som inte fått poäng är förhållandevis jämn. Samarbeten på dessa frågor har potential att kunna hjälpa många då andelen som inte fått poäng är stor samtidigt som det finns en stor andel som kan erbjuda erfarenheter och stöttning med att förbättra sitt informationssäkerhetsarbete. De frågor där det är jämnt fördelat mellan de som fått poäng och de som inte fått poäng är främst:

- **Fråga 14:** Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?

- **Fråga 17:** Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?
- **Fråga 18:** De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?
- **Fråga 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 40:** De senaste två åren, har organisationens ledning arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?

De frågor där det finns en övervägande majoritet som inte fått några poäng finns det anledning för centrala myndigheter och andra stöttande organisationer på alla nivåer i samhället att se över sitt stöd. Detta rör främst fråga 39[15]. Det är dock viktigt att poängtera att det ytterst är varje organisation som är ansvarig för sitt informationssäkerhetsarbete, att det håller en adekvat nivå och följer de krav som ställs.

4.4.4 Resultat från arbetsområdena

Tabell 5.

Arbetsområde Totalt 10 regioner	Antal med nivå >0	Antal med nivå >1	Antal med nivå >2
Analys och hantering av informationssäkerhetsrisker	8	6	1
Incident och kontinuitetshantering	7	1	1
Informationsklassning	9	6	2
Inventering, undersökningar och omvärldsbevakning	7	5	1
Ledningens styrning och kontroll	10	5	1
Medarbetarnas kunskaper och utbildningsverksamhet	7	3	1
Säkerhetsåtgärder och förbättringsarbete	10	3	2
Uppföljning och utvärdering	6	2	1
Upphandling	8	8	5
Upprättande och utveckling av säkerhetskultur	7	3	1

15. Fråga 39: De senaste två åren, har organisationen undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt?

Analys och hantering av informationssäkerhetsrisker

Fyra femtedelar av de inrapporterande regionerna har haft ett arbetssätt för hantering och analys av informationssäkerhetsrisker de senaste två åren. Arbetssättet har i allmänhet:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

De kvarvarande regionerna har haft ett arbetssätt, men ingen av de ovanstående punkterna har varit realiserad under perioden.

Typregionen har under de senaste två åren analyserat informationssäkerhetsrisker i upp till 50% av sina verksamheter enligt sitt arbetssätt för ändamålet. Typregionen har också tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid mellan 50–100% av sina informationsklassningar och analyser av informationssäkerhetsrisker. Bland typregionens verksamheter har 100% fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker.

Typregionens arbetssätt för analys och hantering av informationssäkerhetsrisker har under perioden omfattat att:

1. Analysen av informationssäkerhetsrisker har:
    a. Utgått ifrån organisationens informationsklassning av berörda informationsmängder, informationssystem och nätverk
    b. Utvärderat riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet
    c. Stötts av medarbetare med särskild kompetens inom analys av informationssäkerhetsrisker
2. Bedömningen av informationssäkerhetsrisker alltid tar hänsyn till potentiell skadeverkan på:
    a. Informationsmängder, informationssystem och nätverk (den egna organisationens och andras)
    b. Människors liv och hälsa (de egna medarbetarnas och andras)
    c. Finansiella tillgångar och övrig egendom (den egna organisationens och andra människors eller organisationers)

   d. Tillhandahållande av tjänster (den egna organisationens och andra organisationers)
   e. Förtroende (allmänhetens eller andras, för organisationen eller andra organisationer, för egna eller andras tjänster)

3. Hanteringen av informationssäkerhetsrisker har omfattat att:
   a. Organisationen har ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd
   b. Inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker

Typregionens arbetssätt har däremot saknat att:

1. Analysen av informationssäkerhetsrisker har:
   a. Utgått ifrån en specifik uppgift som ska lösas med stöd av analysen av informationssäkerhetsrisker
   b. Granskats och godkänns av berörda informationsägare
2. Bedömningen av informationssäkerhetsrisker alltid värderar:
   a. Hur ofta risken kan väntas inträffa givet de rådande omständigheterna
   b. När risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna
   c. Hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder införs
   d. När risken tidigast, senast och troligast kan väntas inträffa om föreslagna säkerhetsåtgärder införs
   e. Hur säker man kan vara på sannolikhetsbedömningarna givet vad man vet och de antaganden man har gjort
3. Hanteringen av informationssäkerhetsrisker har omfattat att:
   a. Varje identifierad informationssäkerhetsrisk har en riskägare
   b. Analys av enskilda informationssäkerhetsrisker uppdateras efter att beslutade säkerhetsåtgärder har införts
   c. Status för informationssäkerhetsrisker följs upp utifrån definierade intervall

Under perioden har typregionen haft tillgång till kompetens inom analys och hantering av informationssäkerhetsrisker. Samtidigt har typregionen inte följt upp resultatet av sitt informationssäkerhetsarbete under perioden, och de har därför inte följt upp resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker. Typregionens ledning har dock i allmänhet informerat sig om statusen på organisationens systematiska informationssäker-

hetsarbete under perioden, och i det ingår att ledningarna har informerat sig om eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats. Typregionens arbetssättför att säkerställa informationssäkerhet vid upphandling har de senaste två åren omfattat:

1. Klassning av information och analyser av informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
2. Bedömning av behovet av åtgärder med anledning av informations-klassningens och riskanalysens resultat
3. Införande av de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
4. Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat

Däremot har arbetssättet inte omfattat uppföljning av om de ställda kraven var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

Incident- och kontinuitetshantering

Regionerna har de senaste två åren i allmänhet haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för hantering av informationssäkerhetsincidenter och -avvikelser, det har varit beskrivet i stöd och vägledning för medarbetarna och det har följts upp.

Arbetssättet har under perioden i allmänhet saknat sådana centrala inslag som Infosäkkollen efterfrågar, d.v.s.:

- En funktion för att hantera informationssäkerhetsincidenter och -avvikelser med dedikerad personal som har särskild kompetens
- Kanaler som medarbetare inom organisationen kan använda för att nå funktionen och rapportera incidenter och avvikelser
- Kanaler som funktionen kan använda för att nå andra organisationer och rapportera om incidenter, få rapporter om incidenter eller dela information, samt rutiner för deras användning
- En eskaleringsrutin för att hantera stora och allvarliga incidenter, inklusive extern rapportering vid behov
- Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete

Typregionen har under perioden haft ett arbetssätt för kontinuitetshantering och det har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte innehållit en organisationsgemensam modell för kontinuitetshantering, inklusive scenarier som organisationen behöver öva och det har inte följts upp. Typregionen har inte övat sina arbetssätt för kontinuitetshantering under perioden.

Typregionen har under perioden typiskt undersökt upp till 25% av medarbetarnas kunskaper i informationssäkerhet och undersökningen har inkluderat huruvida de vet vad de ska göra om en informationssäkerhetsincident inträffar. Typregionens arbetssättför analys och hantering av informationssäkerhetsrisker har under perioden omfattat användning av inträffade avvikelser och incidenter som underlag för analys av informationssäkerhetsrisker.

Under perioden har typregionen undersökt eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns. De har också i allmänhet kontrollerat eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång.

Informationsklassning

Typregionen har under de senaste två åren i allmänhet haft ett arbetssätt för informationsklassning. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för klassning med definierade nivåer för skyddskrav med fördefinierade säkerhetsåtgärder och det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte följts upp.

Under perioden har typregionen haft tillgång till kompetens inom informationsklassning och man har klassat sin information enligt sitt arbetssätt för informationsklassning i mellan 50–75% av sina verksamheter. Typregionen har tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid 75–100% av sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typregionens arbetssättför informationsklassning har under perioden omfattat att informationsklassningen ska:

- Utgå ifrån organisationens inventering av informationsmängder, informationssystem och nätverk
- Beakta tillämplig lagstiftning, inklusive offentlighets- och sekretesslagen, dataskyddsförordningen, säkerhetsskyddslagen, arkivlagen, samt krisberedskapsförordningen eller lagen om extraordinära händelser
- Utgå ifrån krav på tillgänglighet, riktighet och konfidentialitet
- Stödjas av medarbetare med särskild kompetens inom informationsklassning

Däremot har arbetssättet under perioden inte omfattat att utförda informationsklassningar ska granskas och godkänns av berörda informationsägare.

Inventering, undersökningar och omvärldsbevakning

Typregionen har under perioden minst en gång inventerat sina informationsmängder och informationssystem, inklusive nätverk, i 25–50% av sina verksamheter. Typregionen har haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet under perioden och det har:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar

Däremot har arbetssättet inte:

- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Under perioden har typregionen bevakat utvecklingen på informationssäkerhetsområdet och minst en gång per kvartal spridit information till utpekade medarbetare inom alla av organisationens verksamheter. Typregionen har också under perioden tittat på och använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser i upp till 75–100% av sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typregionen har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång

Typregionen har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Ledningens styrning och kontroll

Under perioden har typregionens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning
- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

Typregionen har i allmänhet under perioden också haft en informationssäkerhetspolicy (eller motsvarande dokument) som har innehållit:

- En definition av informationssäkerhet och informationssäkerhetsarbete
- Ledningens målsättningar för informationssäkerhetsarbetet (vad som ska uppnås)
- Ledningens inriktning för informationssäkerhetsarbetet (hur det ska uppnås)
- Definierade roller som ledningen har pekat ut som ansvariga för att hantera informationssäkerhet
- Att arbetet ska integreras i myndighetens befintliga sätt att leda och styra sin organisation

Typregionen har de senaste två åren i allmänhet haft utpekade informationsägare eller motsvarande för sin information i alla organisationens verksamheter.

Typregionen de senaste två åren följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- Skillnaden mellan införda och beslutade säkerhetsåtgärder
- Resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet

Däremot har typregionen inte följt upp resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt samt resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker.

Typregionens ledning har under perioden minst en gång per år informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, inklusive:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Däremot har ledningen inte förhört sig om resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Under perioden har typregionen beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i alla av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa 75–100% av sina beslutade säkerhetsåtgärder och man har också infört upp till 50–75% av de säkerhetsåtgärder som har beslutats.

Typregionens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typregionens ledning, i samband med sådana tillfällen, inte följt upp och vid behov beslutat om organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga

- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer

Medarbetarnas kunskaper och utbildningsverksamhet

Typregionen har under perioden undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet. Man har också haft ett arbetssätt för utbildning i informationssäkerhet under perioden och det har varit beslutat eller på annat sätt medvetet valt av organisationen, omfattat fördelning av roller och ansvar, innehållit en organisationsgemensam modell för utbildning i informationssäkerhet och varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte följts upp och utvärderats minst en gång under den tiden. Man har också haft tillgång till kompetens inom utbildning i informationssäkerhet under perioden.

Under perioden har organisationen utbildat upp till 25% av sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning. Man har dock inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

I sin undersökning av medarbetarnas kunskaper har typregionen undersökt huruvida medarbetarna vet:

- Vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- De regler och krav som styr informationssäkerhetsarbetet inom organisationen
- Vad medarbetarna ska göra om en informationssäkerhetsincident inträffar

Däremot har man inte undersökt:

- Vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt
- Informationssäkerhetsrelaterade hot, sårbarheter och risker

Typregionens utbildning i informationssäkerhet har under perioden varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet
- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

Däremot har regionens utbildning i informationssäkerhet inte varit utformad utifrån ledningens målsättningar för det systematiska informationssäkerhetsarbetet.

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

Säkerhetsåtgärder och förbättringsarbete

Under perioden har typregionen haft tillgång till särskild kompetens inom arbete med it-säkerhet. Under perioden har typregionen beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i alla av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa 75–100% av sina beslutade säkerhetsåtgärder och man har också infört upp till 50–75% av de säkerhetsåtgärder som har beslutats.

Typregionen har under perioden i allmänhet utvärderat om upp till 25% av deras införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typregionen har under perioden följt upp skillnaden mellan införda och beslutade säkerhetsåtgärder och resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet. Man har också haft ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd.

Typregionen har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång

Typregionen har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Typregionens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typregionens ledning, i samband med sådana tillfällen, följt upp och vid behov beslutat om organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer

Uppföljning och utvärdering

Typregionen har under perioden haft tillgång till kompetens inom uppföljning av informationssäkerhetsarbete och man har följt upp och utvärderat sina arbetssätt för analys och hantering av informationssäkerhetsrisker respektive hantering av informationssäkerhetsincidenter och -avvikelser. Typregionen har inte följt upp eller utvärderat något av arbetssätten för informationsklassning, kontinuitetshantering, omvärldsbevakning, utbildning i informationssäkerhet eller säkerställande av informationssäkerhet vid upphandling.

Typregionen de senaste två åren följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- Skillnaden mellan införda och beslutade säkerhetsåtgärder
- Resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet

Däremot har typregionen inte följt upp resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt samt resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker.

Typregionen har inte heller undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

Typregionen har under perioden i allmänhet utvärderat om upp till 25% av deras införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typregionen har undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet och informationssäkerhetsarbete, och i samband med det har man undersökt huruvida medarbetarna vet:

- Vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- De regler och krav som styr informationssäkerhetsarbetet inom organisationen
- Vad medarbetarna ska göra om en informationssäkerhetsincident inträffar

Däremot har man inte undersökt:

- Vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt
- Informationssäkerhetsrelaterade hot, sårbarheter och risker

Typregionen har i allmänhet haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser och i det arbetssättet har det ingått att man ska bedriva analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete. Det har också ingått i typregionens arbetssätt för analys och hantering av informationssäkerhetsrisker att man utvärderar riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet. I typregionens arbetssätt för att säkerställa informationssäkerhet vid upphandling har det inte under perioden ingått att följa upp om ställda krav var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

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

Upphandling

Typregionen har under perioden haft tillgång till särskild kompetens inom säkerställande av informationssäkerhet vid upphandling. De har också haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren, och det har:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för informationssäkerhet vid upphandling
- Varit beskrivet i stöd och vägledning för medarbetarna

Däremot har arbetssättet inte följts upp och utvärderats minst en gång under perioden.

Typregionen har använt det arbetssättet vid 75–100% av sina upphandlingar under den senaste två-årsperioden.

Arbetssättet har under perioden omfattat att:

- Klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
- Bedöma behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat, samt att identifiera säkerhetsåtgärder
- Införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
- Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat

Däremot har arbetssättet inte omfattat att man ska:

- Följa upp om de ställda kraven var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats

Upprättande och utveckling av säkerhetskultur

Under perioden har typregionens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning
- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

De senaste två åren har typregionen inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Typregionens ledning har under perioden minst en gång per år informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, inklusive:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Däremot har ledningen inte förhört sig om resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Typregionen har inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

I sin undersökning av medarbetarnas kunskaper har typregionen undersökt huruvida medarbetarna vet:

- Vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- De regler och krav som styr informationssäkerhetsarbetet inom organisationen
- Vad medarbetarna ska göra om en informationssäkerhetsincident inträffar

Däremot har man inte undersökt:

- Vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt
- Informationssäkerhetsrelaterade hot, sårbarheter och risker

Typregionens utbildning i informationssäkerhet har under perioden varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet
- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

Däremot har regionens utbildning i informationssäkerhet inte varit utformad utifrån ledningens målsättningar för det systematiska informationssäkerhetsarbetet.

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

Typregionens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typregionens ledning, i samband med sådana tillfällen, följt upp och vid behov beslutat om organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer

4.5 Statliga myndigheter

4.5.1 Inledning

I det här delkapitlet presenterar vi den bild som framkommit genom en sammanställning av 122 inrapporterande statliga myndigheters resultat. Delkapitlet redovisar först en övergripande bild av läget bland statliga myndigheterna och därefter en detaljerad redogörelse för resultaten inom Infosäkkollens tio arbetsområden. Den detaljerade redogörelsen presenterar huvudsakligen vad benchmarken för alla de svarande statliga myndigheterna visar. I förekommande fall har klargörande statistik adderats.

Diagram 8. Myndigheternas resultattal i Infosäkkollen 2021

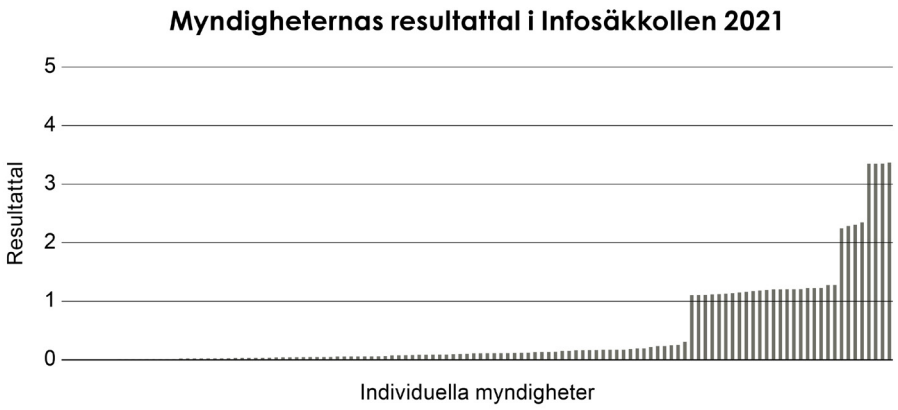
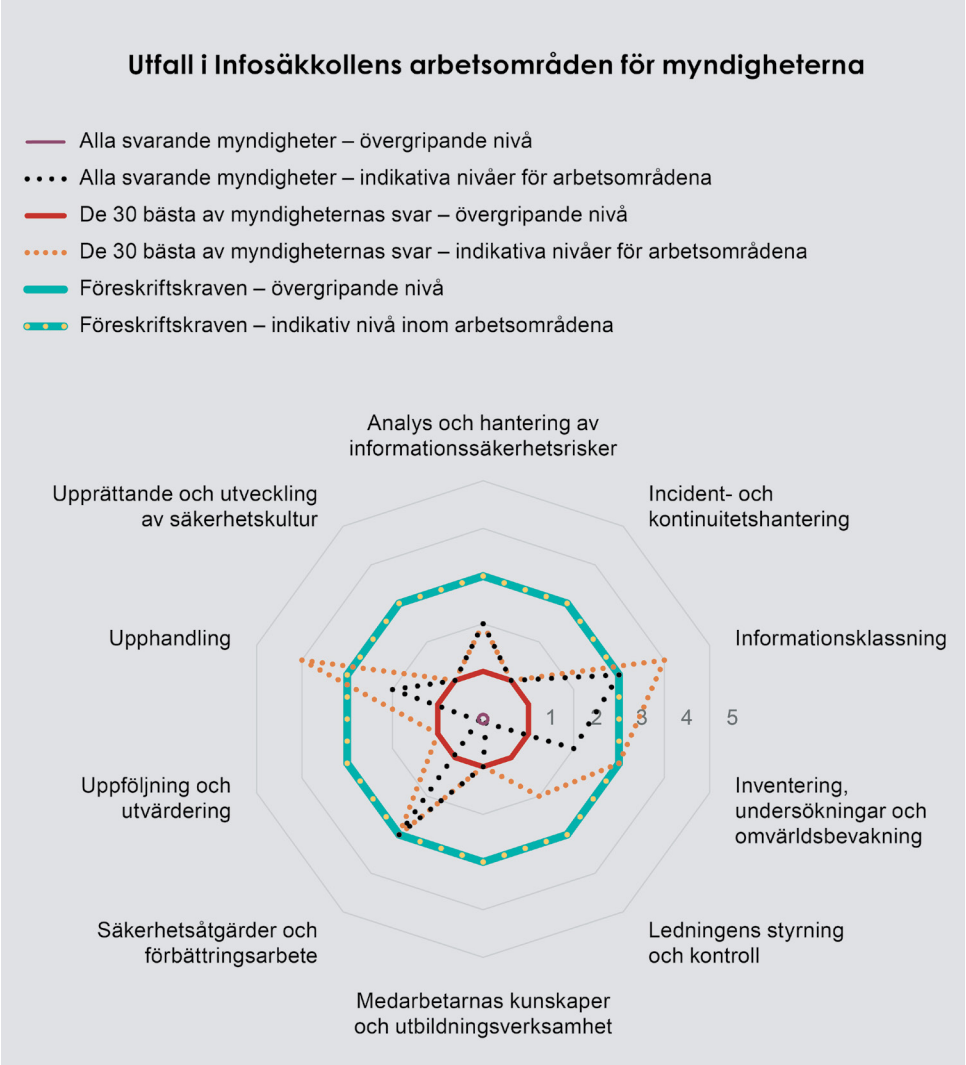


Diagram 9. Utfall i Infosäkkollens arbetsområden för myndigheterna



4.5.2 Övergripande bild

Typmyndigheten har under mätperioden genomfört och haft på plats totalt 94 av Infosäkkollens 132 åtgärder. Samtidigt har den generella representanten för de 30 bäst presterande myndigheterna genomfört och haft på plats 113 av åtgärderna. Myndigheterna är därmed varken mest eller minst heterogen bland tre aktörsgrupperna.

Tabell 6.

Antal genomförda åtgärder per arbetsområde Totalt 122 statliga myndigheter	Generell myndighet	Myndighet bland de 30 bästa	Max-resultat
Analys och hantering av informationssäkerhetsrisker	32	41	47
Incident och kontinuitetshantering	15	19	24
Informationsklassning	19	26	26
Inventering, undersökningar och omvärldsbevakning	21	27	30
Ledningens styrning och kontroll	37	38	45
Medarbetarnas kunskaper och utbildningsverksamhet	17	28	43
Säkerhetsåtgärder och förbättringsarbete	27	29	34
Uppföljning och utvärdering	10	26	41
Upphandling	10	13	16
Upprättande och utveckling av säkerhetskultur	19	28	42

MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6) ger en god grund att stå på i informationssäkerhetsarbetet och myndigheten använder därför den uttolkning av föreskriftskraven som har gjorts i Infosäkkollen som ett riktmärke för hur de olika aktörerna ligger till i sitt arbete. Typmyndigheten har 34 åtgärder kvar att genomföra innan de når föreskriftskraven, medan typrepresentanten för de 30 bästa myndigheterna har 18 åtgärder kvar att genomföra.

4.5.3 MSB:s föreskrifter om statliga myndigheters informationssäkerhet

Som analysen i det föregående stycket 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 (41 myndigheter har fått mindre än 50 poäng, av Infosäkkollens totalt 200 poäng – och ingen av dem har uppnått någon övergripande nivå) och där några har fått goda resultat (52 myndigheter har fått mer än 100 poäng, dock har trettio av dem ändå inte uppnått någon nivå

då de har saknat bredden i arbetet – huvudsakligen på grund av brister avseende uppföljning, utbildning och omvärldsbevakning). Bland de myndigheter som har nått höga poäng i Infosäkkollen är det alltså en klar majoritet som har genomfört stora delar av de åtgärder som föreskrifterna kräver – men som samtidigt uppvisar brister inom något eller några arbetsområden.

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 de statliga myndigheterna har omfattats av författningskrav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i 12 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 de statliga myndigheterna, och att det har troligen har varit fallet under en längre tid.

4.5.4 Förutsättningar för samarbeten

Myndigheternas svar på de olika frågorna i Infosäkkollen indikerar att det finns vissa områden där det på systemnivå kan finnas stora fördelar med att samarbeta inom gruppen. Detta gäller främst områden som behandlas i frågor där fördelningen mellan de som fått poäng och de som inte fått poäng är förhållandevis jämn. Samarbeten på dessa frågor har potential att kunna hjälpa många då andelen som inte fått poäng är stor samtidigt som det finns en stor andel som kan erbjuda erfarenheter och stöttning med att förbättra sitt informationssäkerhetsarbete. De frågor där det är jämnt fördelat mellan de som fått poäng och de som inte fått poäng är främst fråga 5, 10, 11, 12, 13, 14, 15, 26, 31, 33, 34, 35, 36, 37, 38 och 40.

- **Fråga 5:** Har organisationen de senaste två åren undersökt medarbetarnas kunskaper om informationssäkerhet?
- **Fråga 10:** Har organisationen haft ett arbetssätt för kontinuitetshantering de senaste två åren?
- **Fråga 11:** Har organisationen haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet de senaste två åren?
- **Fråga 12:** Har organisationen haft ett arbetssätt för utbildning i informationssäkerhet de senaste två åren?
- **Fråga 13:** Har organisationen haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren?

- **Fråga 14:** Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 15:** Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?
- **Fråga 26:** Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?
- **Fråga 31:** De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?
- **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?

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

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

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

4.5.5 Resultat från arbetsområdena

Tabell 7.

Arbetsområde Totalt 122 statliga myndigheter	Antal med nivå >0	Antal med nivå >1	Antal med nivå >2
Analys och hantering av informationssäkerhetsrisker	83	53	12
Incident och kontinuitetshantering	69	21	12
Informationsklassning	83	48	38
Inventering, undersökningar och omvärldsbevakning	70	37	19
Ledningens styrning och kontroll	84	34	12
Medarbetarnas kunskaper och utbildningsverksamhet	56	15	9
Säkerhetsåtgärder och förbättringsarbete	109	53	23
Uppföljning och utvärdering	53	11	7
Upphandling	75	50	29
Upprättande och utveckling av säkerhetskultur	62	20	11

Analys och hantering av informationssäkerhetsrisker

Två tredjedelar av de inrapporterande myndigheterna har haft ett arbetssätt för hantering och analys av informationssäkerhetsrisker de senaste två åren. Arbetssättet har i allmänhet:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Bland de kvarvarande myndigheterna har:

- Strax under en tiondel haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker under perioden, men ingen av de ovanstående punkterna har varit realiserade.
- Strax under en femtedel har under perioden arbetat med att utveckla ett arbetssätt för analys och hantering av informationssäkerhetsrisker, eller så har de haft ett sådant arbetssätt, men inte under hela perioden.

Typmyndigheten har under de senaste två åren analyserat informationssäkerhetsrisker i alla sina verksamheter enligt sitt arbetssätt för ändamålet. Typmyndigheten har också tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid alla sina informationsklassningar och analyser av

informationssäkerhetsrisker. Bland typmyndighetens verksamheter har alla fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker.

Typmyndighetens arbetssätt för analys och hantering av informationssäkerhetsrisker har under perioden omfattat att:

1. Analysen av informationssäkerhetsrisker har:
    a. Utgått ifrån organisationens informationsklassning av berörda informationsmängder, informationssystem och nätverk
    b. Utgått ifrån en specifik uppgift som ska lösas med stöd av analysen av informationssäkerhetsrisker
    c. Utvärderat riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet
    d. Stötts av medarbetare med särskild kompetens inom analys av informationssäkerhetsrisker

2. Bedömningen av informationssäkerhetsrisker alltid tar hänsyn till potentiell skadeverkan på:
    a. Informationsmängder, informationssystem och nätverk (den egna organisationens och andras)
    b. Människors liv och hälsa (de egna medarbetarnas och andras)
    c. Finansiella tillgångar och övrig egendom (den egna organisationens och andra människors eller organisationers)
    d. Tillhandahållande av tjänster (den egna organisationens och andra organisationers)
    e. Förtroende (allmänhetens eller andras, för organisationen eller andra organisationer, för egna eller andras tjänster)

3. Hanteringen av informationssäkerhetsrisker har omfattat att:
    a. Inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker

Typmyndighetens arbetssätt har däremot saknat att:

4. Analysen av informationssäkerhetsrisker har:
    a. Granskats och godkänns av berörda informationsägare

5. Bedömningen av informationssäkerhetsrisker alltid värderar:
    a. Hur ofta risken kan väntas inträffa givet de rådande omständigheterna
    b. När risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna

   c. Hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder införs
   d. När risken tidigast, senast och troligast kan väntas inträffa om föreslagna säkerhetsåtgärder införs
   e. Hur säker man kan vara på sannolikhetsbedömningarna givet vad man vet och de antaganden man har gjort

6. Hanteringen av informationssäkerhetsrisker har omfattat att:
   a. Varje identifierad informationssäkerhetsrisk har en riskägare
   b. Organisationen har ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd
   c. Analys av enskilda informationssäkerhetsrisker uppdateras efter att beslutade säkerhetsåtgärder har införts
   d. Status för informationssäkerhetsrisker följs upp utifrån definierade intervall

Under perioden har typmyndigheten haft tillgång till kompetens inom analys och hantering av informationssäkerhetsrisker. Samtidigt har typmyndigheten inte följt upp resultatet av sitt informationssäkerhetsarbete under perioden, och de har därför inte följt upp resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker. Typmyndighetens ledning har dock i allmänhet informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete under perioden, och i det ingår att ledningarna har informerat sig om eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats.

Typmyndighetens arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren har under den perioden inte omfattat:

1. Klassning av information och analyser av informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
2. Bedömning av behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat
3. Införande av de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
4. Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat

Incident- och kontinuitetshantering

Typmyndigheten har de senaste två åren i allmänhet haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för hantering av informationssäkerhetsincidenter och -avvikelser och det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har inte följts upp.

Arbetssättet har under perioden i allmänhet innehållit sådana centrala inslag som Infosäkkollen efterfrågar, d.v.s.:

- En funktion för att hantera informationssäkerhetsincidenter och -avvikelser med dedikerad personal som har särskild kompetens
- Kanaler som medarbetare inom organisationen kan använda för att nå funktionen och rapportera incidenter och avvikelser
- Kanaler som funktionen kan använda för att nå andra organisationer och rapportera om incidenter, få rapporter om incidenter eller dela information, samt rutiner för deras användning
- En eskaleringsrutin för att hantera stora och allvarliga incidenter, inklusive extern rapportering vid behov
- Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete

Typmyndigheten har under perioden haft ett arbetssätt för kontinuitetshantering och det har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar och det har följts upp. Arbetssättet har inte varit beskrivet i stöd och vägledning för medarbetarna eller innehållit en organisationsgemensam modell för kontinuitetshantering, inklusive scenarier som organisationen behöver öva. Typmyndigheten har i allmänhet inte övat sina arbetssätt för kontinuitetshantering under perioden.

Typmyndigheten har under perioden typiskt undersökt upp till 25% av medarbetarnas kunskaper i informationssäkerhet, men undersökningen har inte inkluderat huruvida de vet vad de ska göra om en informationssäkerhetsincident inträffar. Typmyndighetens arbetssättför analys och hantering av informationssäkerhetsrisker har under perioden omfattat användning av inträffade avvikelser och incidenter som underlag för analys av informationssäkerhetsrisker.

Under perioden har typmyndigheten undersökt eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns. De har också i allmänhet kontrollerat eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång.

Informationsklassning

Typmyndigheten har under de senaste två åren i allmänhet haft ett arbetssätt för informationsklassning. Arbetssättet har varit beslutat eller på annat sätt valt av organisationen, det har omfattat en fördelning av roller och ansvar, innehållit en organisationsgemensam modell för klassning med definierade nivåer för skyddskrav med fördefinierade säkerhetsåtgärder och det har varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har också följts upp.

Under perioden har typmyndigheten haft tillgång till kompetens inom informationsklassning och man har klassat sin information enligt sitt arbetssätt för informationsklassning i mellan 50–75% av sina verksamheter. Typmyndigheten har tittat på, och när det har varit relevant, använt underlag från sin omvärldsbevakning vid alla av sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typmyndighetens arbetssättför informationsklassning har under perioden omfattat att informationsklassningen ska:

- Utgå ifrån organisationens inventering av informationsmängder, informationssystem och nätverk
- Beakta tillämplig lagstiftning, inklusive offentlighets- och sekretesslagen, dataskyddsförordningen, säkerhetsskyddslagen, arkivlagen, samt krisberedskapsförordningen eller lagen om extraordinära händelser
- Utgå ifrån krav på tillgänglighet, riktighet och konfidentialitet
- Stödjas av medarbetare med särskild kompetens inom informationsklassning
- Granskas och godkänns av berörda informationsägare

Inventering, undersökningar och omvärldsbevakning

Typmyndigheten har under perioden minst en gång inventerat sina informationsmängder och informationssystem, inklusive nätverk, i 75–100% av sina verksamheter. Typmyndigheten har haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet under perioden och det har:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar

Däremot har arbetssättet inte:

- Innehållit en organisationsgemensam modell för analys av informationssäkerhetsrisker
- Varit beskrivet i stöd och vägledning för medarbetarna
- Följts upp och utvärderats minst en gång

Under perioden har typmyndigheten bevakat utvecklingen på informationssäkerhetsområdet och minst en gång per kvartal spridit information till utpekade medarbetare inom alla av organisationens verksamheter. Typmyndigheten har också under perioden tittat på och använt resultat från sin omvärldsbevakning vid informationsklassningar och analyser i alla sina informationsklassningar och analyser av informationssäkerhetsrisker.

Typmyndigheten har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång

Typmyndigheten har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Ledningens styrning och kontroll

Under perioden har typmyndighetens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning
- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

Typmyndigheten har i allmänhet under perioden också haft en informationssäkerhetspolicy (eller motsvarande dokument) som har innehållit:

- En definition av informationssäkerhet och informationssäkerhetsarbete
- Ledningens målsättningar för informationssäkerhetsarbetet (vad som ska uppnås)
- Ledningens inriktning för informationssäkerhetsarbetet (hur det ska uppnås)
- Definierade roller som ledningen har pekat ut som ansvariga för att hantera informationssäkerhet
- Att arbetet ska integreras i myndighetens befintliga sätt att leda och styra sin organisation

Typmyndigheten har de senaste två åren i allmänhet haft utpekade informationsägare eller motsvarande för sin information i alla organisationens verksamheter.

Typmyndigheten de senaste två åren inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera:

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

Typmyndighetens ledning har under perioden minst en gång per år informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, inklusive:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Däremot har ledningen inte förhört sig om resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Under perioden har typmyndigheten beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i alla av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa alla sina beslutade säkerhetsåtgärder och man har också infört 75–100% av de säkerhetsåtgärder som har beslutats.

Typmyndighetens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typmyndighetens ledning, i samband med sådana tillfällen, inte följt upp och vid behov beslutat om organisationens arbete med att mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer.

Medarbetarnas kunskaper och utbildningsverksamhet

Typmyndigheten har under perioden undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet. Man har också haft ett arbetssätt för utbildning i informationssäkerhet under perioden och det har varit beslutat eller på annat sätt medvetet valt av organisationen, omfattat fördelning av roller och ansvar, innehållit en organisationsgemensam modell för utbildning i informationssäkerhet och varit beskrivet i stöd och vägledning för medarbetarna. Arbetssättet har följts upp och utvärderats minst en gång under den tiden. Man har också haft tillgång till kompetens inom utbildning i informationssäkerhet under perioden.

Under perioden har organisationen utbildat upp till 75–100% av sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning. Man har dock inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

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

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

Typmyndighetens utbildning i informationssäkerhet har under perioden varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Ledningens målsättningar för det systematiska informationssäkerhetsarbetet
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet
- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

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

Säkerhetsåtgärder och förbättringsarbete

Under perioden har typmyndigheten haft tillgång till särskild kompetens inom arbete med it-säkerhet.

Under perioden har typmyndigheten beslutat om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i alla av organisationens verksamheter. Samtidigt har man beslutat om att tilldela resurser för att kunna införa alla sina beslutade säkerhetsåtgärder och man har också infört 75–100% av de säkerhetsåtgärder som har beslutats.

Typmyndigheten har under perioden i allmänhet utvärderat om 50–75% av deras införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typmyndigheten har under perioden inte följt upp skillnaden mellan införda och beslutade säkerhetsåtgärder och resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet. Man har därutöver inte haft ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd.

Typmyndigheten har under perioden minst en gång undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap. I samband med den eller de undersökningarna har man gått igenom:

- Vilka, om några, informationsmängder som kan omfattas av säkerhetsskydd, samt vid behov genomfört säkerhetsskyddsanalys och säkerställt att påkallade säkerhetsåtgärder är införda
- Vilka, om några, informationsmängder som skulle vara nödvändiga för samverkan och ledning i händelse av kris eller höjd beredskap, samt vid behov säkerställt att påkallade säkerhetsåtgärder är införda
- Eventuellt behov av att kunna upprätta, dela och ta emot säkerhetsskyddsklassificerade uppgifter samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns
- Eventuellt behov av tillgång till alternativ ledningsplats samt vid behov säkerställt sådan tillgång

Typmyndigheten har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Typmyndighetens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typmyndighetens ledning, i samband med sådana tillfällen, inte följt upp och vid behov beslutat om organisationens arbete med att mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer.

Uppföljning och utvärdering

Typmyndigheten har under perioden haft tillgång till kompetens inom uppföljning av informationssäkerhetsarbete och man har följt upp och utvärderat sina arbetssätt för informationsklassning, analys och hantering av informationssäkerhetsrisker, kontinuitetshantering och utbildning i informationssäkerhet. Typmyndigheten har inte följt upp eller utvärderat arbetssätten för hantering av

informationssäkerhetsincidenter och -avvikelser, omvärldsbevakning, eller säkerställande av informationssäkerhet vid upphandling.

Typmyndigheten de senaste två åren inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera:

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

Typmyndigheten har inte heller undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

Typmyndigheten har under perioden i allmänhet utvärderat om 50–75% av deras införda säkerhetsåtgärder är ändamålsenliga och tillräckliga.

Typmyndigheten har undersökt upp till 25% av medarbetarnas kunskaper om informationssäkerhet och informationssäkerhetsarbete, men i samband med det har man inte undersökt huruvida medarbetarna vet:

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

Typmyndigheten har i allmänhet haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser och i det arbetssättet har det ingått att man ska bedriva analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete. Det har också ingått i typmyndighetens arbetssätt för analys och hantering av informationssäkerhetsrisker att man utvärderar riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet. I typmyndighetens arbetssätt för att säkerställa informationssäkerhet vid upphandling har det inte under perioden ingått att följa upp om ställda krav var

ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.

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

Upphandling

Typmyndigheten har under perioden haft tillgång till särskild kompetens inom säkerställande av informationssäkerhet vid upphandling. De har också haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren, och det har:

- Varit beslutat eller på annat sätt medvetet valt av organisationen
- Omfattat fördelning av roller och ansvar
- Innehållit en organisationsgemensam modell för informationssäkerhet vid upphandling
- Varit beskrivet i stöd och vägledning för medarbetarna

Däremot har arbetssättet inte följts upp och utvärderats minst en gång under perioden.

Typmyndigheten har använt det arbetssättet vid alla sina upphandlingar under den senaste två-årsperioden.

Arbetssättet har under perioden inte omfattat att:

- Klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas
- Bedöma behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat, samt att identifiera säkerhetsåtgärder
- Införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv
- Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat
- Följa upp om de ställda kraven var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats

Upprättande och utveckling av säkerhetskultur

Under perioden har typmyndighetens ledning i allmänhet deltagit i styrningen av organisationens informationssäkerhetsarbete på en övergripande nivå genom att minst en gång ha beslutat om eller sett över tidigare beslut om:

- Målsättning och inriktning
- Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet
- Resurser som informationssäkerhetsarbetet kräver
- Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
- Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande

De senaste två åren har typmyndigheten inte följt upp resultatet av sitt systematiska informationssäkerhetsarbete genom att sammanställa och analysera resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Typmyndighetens ledning har under perioden minst en gång per år informerat sig om statusen på organisationens systematiska informationssäkerhetsarbete, inklusive:

- Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
- I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
- Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
- Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet

Däremot har ledningen inte förhört sig om resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt.

Typmyndigheten har inte undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt och inte heller om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.

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

- Vad som menas med informationssäkerhet och informationssäkerhetsarbete, samt varför det är viktigt för organisationen
- De regler och krav som styr informationssäkerhetsarbetet inom organisationen
- Vad medarbetarna ska göra om en informationssäkerhetsincident inträffar

- Vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt
- Informationssäkerhetsrelaterade hot, sårbarheter och risker

Typmyndighetens utbildning i informationssäkerhet har under perioden varit utformad enligt de följande aspekterna:

- Medarbetarnas roller, uppgifter, ansvar och behov
- Medarbetarnas kunskapsnivå
- Ledningens målsättningar för det systematiska informationssäkerhetsarbetet
- Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet
- Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

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

Typmyndigheten har under perioden i allmänhet inte undersökt vilka hinder respektive framgångsfaktorer som påverkar medarbetarnas möjligheter att arbeta på ett informationssäkert sätt.

Typmyndighetens ledning har under perioden arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet genom att minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att:

- Ta bort eller reducera identifierade hinder för att arbeta på ett informationssäkert sätt
- Införa eller stärka identifierade framgångsfaktorer för att arbeta på ett informationssäkert sätt
- Utvärdera säkerhetsåtgärderna och vid behov ersätta, justera eller komplettera de säkerhetsåtgärder som inte har bedömts vara ändamålsenliga eller tillräckliga
- Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen

Däremot har typmyndighetens ledning, i samband med sådana tillfällen, inte följt upp och vid behov beslutat om organisationens arbete med att mäta resultaten av informationssäkerhetsarbetet med hjälp av indikatorer.

Utvecklingen framåt

5. Utvecklingen framåt

Huvudsyftet med Infosäkkollen är att stödja uppföljning och utveckling av organisationers systematiska och riskbaserade informationssäkerhetsarbete och därigenom bidra till ett säkrare, robustare samhälle och i förlängningen ett stärkt civilt försvar. För att fullt ut kunna tillvarata de möjligheter en etablerad struktur för uppföljning ger att stödja och inrikta samhällets aktörer arbetar MSB kontinuerligt med att identifiera möjligheter till vidareutveckling av Infosäkkollen och dess benchmarkverktyg. Den vidareutveckling som nu planeras handlar både om mindre tillägg avseende funktionaliteten i nuvarande version och större utvecklingssteg avseende både innehåll och målgrupper.

När det gäller funktionalitetsförbättringar kommer MSB exempelvis att utöka möjligheterna att jämföra sina resultat i Infosäkkollen med andra individuella organisationer samt komplettera benchmarkverktyget med funktionalitet för tids- och resurssättning av åtgärder.

Avseende innehåll handlar det om att låta Infosäkkollen även stödja uppföljning av organisationernas it-säkerhetsarbete i enlighet med MSB:s föreskrifter om säkerhetsåtgärder i informationssystem (MSBFS 2020:7). Infosäkkollens nuvarande uppföljning av det systematiska informationssäkerhetsarbetet fokuserar på vilka förutsättningar en organisation har att nå en tillräcklig informations- och it-säkerhet. Målsättningen är att Infosäkkollen efter utvidgningen även ska ge stöd för organisationens bedömning av om införda it-säkerhetsåtgärder motsvarar organisationens behov.

När det gäller målgrupp bedömer MSB att det är lämpligt att även erbjuda leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer) att delta i Infosäkkollen. Dessa organisationer tillhandahåller viktig funktionalitet i samhället som är beroende av fungerande informationssystem. Att även tillhandahålla stöd för uppföljning till NIS-leverantörerna kommer inte bara att stärka samhällets förmåga att hantera och förebygga it-incidenter och it-relaterade kriser utan även arbetet med att utveckla det civila försvaret. Infosäkkollen kommer även att bidra till en förbättrad och mer heltäckande bild av arbetet med informations- och cybersäkerhet i Sverige.

I MSB:s arbete med samhällets informations- och cybersäkerhet ger Infosäkkollen en stärkt förmåga att inte bara bedöma och analysera informationssäkerhetsarbetet hos en målgrupp utan även, främst genom benchmarkverktyget, ge direkt och organisationsanpassat stöd för det fortsatta arbetet med informationssäkerhet.

Bilagor

Bilagor

Bilaga 1: Regeringsuppdraget

2019-09-19 Ju2019/03058/SSK Ju2019/02421/SSK

Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen Regeringens beslut Regeringen uppdrar åt Myndigheten för samhällsskydd och beredskap (MSB) att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Med den offentliga förvaltningen avses i detta uppdrag statliga myndigheter, kommuner och landsting. I de delar av uppdraget som berör kommuner och landsting ska MSB ha en löpande dialog med Sveriges Kommuner och Landsting (SKL). Vid behov bör MSB även samverka med Myndigheten för digital förvaltning och andra relevanta myndigheter. Uppföljningsstrukturen ska syfta till att aktörer i offentlig förvaltning regelbundet ska erbjudas att medverka i uppföljningen och få återkoppling som omfattar en bedömning om vilken nivå deras informationssäkerhetsarbete befinner sig på samt förslag på åtgärder som bör vidtas för att uppnå en högre nivå på informationssäkerhetsarbetet. I uppdraget ingår därmed att ta fram en skala med beskrivna nivåer för det systematiska informationssäkerhetsarbetet. Uppföljningsstrukturen ska även syfta till att MSB regelbundet ger regeringen en samlad bedömning om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Uppföljningsstrukturen ska utformas på ett sådant sätt att resultaten kan följas och jämföras över tid. Uppföljningsstrukturen ska lanseras och erbjudas till aktörer i offentlig förvaltning under 2020.

Uppdraget ska redovisas till Regeringskansliet (Justitiedepartementet) senast den 1 mars 2021. Utöver en beskrivning av uppdragets genomförande ska redovisningen innehålla en första samlad bedömning om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen baserat på den framtagna uppföljningsstrukturen. Redovisningen ska även innehålla en beskrivning av hur uppföljningsstrukturen kan vidareutvecklas och en bedömning av hur MSB utifrån resultatet av uppföljningen kan utveckla stödet till den offentliga förvaltningen. Skälen för regeringens beslut Som framgår av regeringens skrivelse Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213) finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. En av målsättningarna i strategin är att bl.a. statliga myndigheter, kommuner och landsting ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete.

Idag saknas det en struktur för att kunna följa upp informationssäkerhetsarbetet över tid i den offentliga förvaltningen. Regeringen bedömer att informationssäkerhetsarbetet kommer att underlättas om aktörer i offentlig förvaltning får återkoppling om vilken nivå de befinner sig på samt konkreta förslag på åtgärder för att utveckla informationssäkerhetsarbetet utifrån sin specifika nivå. Behovet av mer strukturerade former för uppföljning av informationssäkerhetsarbetet inom den offentliga förvaltningen lyfts också fram i betänkandet Reboot – en omstart för den digitala förvaltningen (SOU 2017:114).

Uppföljningsstrukturen kommer utgöra en viktig komponent inom ramen för regeringens prioritering i den nationella strategin om att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.

Bilaga 2: Hur informationssäkerhets-arbetet mäts

Uppföljningen i Infosäkkollen består av 40 frågor om olika aspekter på informationssäkerhetsarbetet. Resultatet utvärderas utifrån en modell med fyra nivåer och tio arbetsområden. I det följande beskrivs mer ingående hur resultaten beräknats och jämförts. En detaljerad förklaring av hur modellen är uppbyggd finns i den första redovisningen från mars 2021, *En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*.

Nivåer

Modellen består av fyra nivåer som speglar ett stegvist utvecklingsarbete: Organisationer på nivå 1 har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad utsträckning. Organisationer på nivå 2 är bättre på grunderna och bedriver dessutom informationssäkerhetsarbetet med viss systematik. På motsvarande sätt är organisationer på nivå 3 ännu bättre på grunderna, arbetar mer systematiskt och uppvisar därutöver ett kvalificerat innehåll i det som görs. Organisationer på nivå 4 har ett informationssäkerhetsarbete på en mycket hög nivå, inklusive ett avancerat arbete med ständiga förbättringar.

Nivåerna representerar en utvecklingstrappa, där man avancerar genom att utveckla arbetet på nya områden parallellt med att man bibehåller och förstärker det man redan uppnått. Modellen främjar ett helhetsgrepp på informationssäkerhetsarbetet; för att nå en nivå krävs tillräckliga resultat i alla delar. Samtidigt kan olika organisationer behöva prioritera olika delar av informationssäkerhetsarbetet, modellen gör det möjligt att uppnå nivåer på delvis olika sätt.

Tabellen visar översiktligt hur nivåresultatet beräknas.

Tabell 8.

Nivå	Frågorna på nivå 1	Frågorna på nivå 2	Frågorna på nivå 3	Frågorna på nivå 4	Krav
1	Behöver besvaras	Behöver inte besvaras	Behöver inte besvaras	Behöver inte besvaras	Minst 23 poäng behövs för att uppnå nivå 1. Alla 15 frågorna i avsnittet för nivå 1 behöver besvaras med minst 1 poäng. Högst 50% av svaren får vara osäkra bedömningar.
2	Behöver besvaras	Behöver besvaras	Behöver inte besvaras	Behöver inte besvaras	Minst 70 poäng behövs för att uppnå nivå 2. Alla 28 frågorna i avsnitten för nivå 1–2 behöver besvaras med minst 2 poäng. Högst 40% av svaren får vara osäkra bedömningar.
3	Behöver besvaras	Behöver besvaras	Behöver besvaras	Behöver inte besvaras	Minst 133 poäng behövs för att uppnå nivå 3. Alla 38 frågorna i avsnitten för nivå 1–3 behöver besvaras med minst 3 poäng. Högst 30% av svaren får vara osäkra bedömningar.
4	Behöver besvaras	Behöver besvaras	Behöver besvaras	Behöver besvaras	Minst 180 poäng behövs för att uppnå nivå 4. Alla 40 frågorna i avsnitten för nivå 1–4 behöver besvaras med minst 4 poäng. Högst 20% av svaren får vara osäkra bedömningar.

Arbetsområden

Utöver nivåindelningen delas sakinnehållet in i tio arbetsområden som speglar väsentliga delar i det systematiska informationssäkerhetsarbetet: ledningens styrning och kontroll; medarbetarnas kunskap och utbildningsverksamhet; inventering, undersökningar och omvärldsbevakning; informationsklassning; analys och hantering av informationssäkerhetsrisker; incident- och kontinuitetshantering; säkerhetsåtgärder och förbättringsarbete; uppföljning och utvärdering; upphandling; samt upprättande och utveckling av säkerhetskultur.

Områdena omfattar frågor och i vissa fall svarsalternativ som berör den specifika delen av informationssäkerhetsarbetet. En fråga och ett svarsalternativ kan ingå i flera arbetsområden, exempelvis räknas fråga 23 – om beslut om säkerhetsåtgärder fattas utifrån genomförda riskanalyser – till två områden då den omfattar både riskhantering och säkerhetsåtgärder. På liknande sätt räknas svaren på fråga 14 – om organisationen följt upp sitt systematiska informationssäkerhetsarbete – till olika arbetsområden då svarsalternativen speglar uppföljning inom olika delar av arbetet.

I Infosäkkollens återkoppling anges *indikativ nivå* för de olika arbetsområdena för att underlätta förståelse av resultaten och vidare utveckling av organisationens arbete. Att nå en viss indikativ nivå inom alla arbetsområden betyder inte nödvändigtvis att samma nivå nås i det övergripande resultatet (eftersom extra

poäng från egna prioriteringar också behövs, utöver de fasta poängkraven för respektive nivå). Den övergripande nivån representerar den formella bedömningen av resultatet.

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.

Benchmarks genereras i en funktion enligt den följande metoden:

1. Först väljs den grupp som det ska skapas en benchmark för (såsom Alla svarande regioner, eller de 30 bästa bland myndigheterna)
2. Därefter tittar funktionen på utfallet under Summa-fältet på varje enskild fråga (varje fråga i Infosäkkollen har ett sådant fält) i varje inrapporterad Infosäkkollen från en organisation som hör till gruppen.
    a. Först kontrollerar funktionen om det finns en majoritet av ja-svar på frågan. Kontrollen jämför då antalet giltiga ja-svar (d.v.s. svar som inte är motsägelsefulla och som innehåller både ett svar på frågan och en bedömning) med antalet andra utfall under Summa-fältet (såsom nej-svar, eller olika typer av felmeddelanden).
    b. Om det är en majoritet för ett ja-svar på frågan så försöker funktionen avgöra vilka poänggivande svarsalternativ som benchmarken ska ha ikryssade. Det gör den genom att titta på gruppen av alla de rapporter där organisationen har svarat ja på frågan och har fått poäng. Om det finns svarsalternativ som en majoritet inom den gruppen har kryssat i så blir det det eller de svarsalternativen som benchmarken har ikryssade (detta kallas i modellen för ett *majoritetssvar*). Om det inte finns svarsalternativ som en majoritet inom den gruppen har kryssat i så blir det det eller de svarsalternativ som den största minoriteten har kryssat i (detta kallas i modellen för ett *minoritetssvar*).
    c. Om det istället är en majoritet av svar som inte ger poäng på frågan (såsom nej-svar, eller olika typer av felmeddelanden) så blir benchmarkens svar på frågan ett nej.

Tabellerna illustrerar hur funktionen fungerar:

Tabell 9. Exempel 1: Benchmark med majoritet av poänggivande ja-svar

Organisation	Poänggivande ja-svarsalternativ 1	Poänggivande ja-svarsalternativ 2	Poänggivande ja-svarsalternativ 3	Poänggivande ja-svarsalternativ 4	Poänggivande ja-svarsalternativ 5	Nej-svar	Summa
Kommun 1	x						1
Kommun 2		x	x				2
Kommun 3	x			x			2
Kommun 4						x	0
Kommun 5		x					1
Kommun 6						x	0
Kommun 7						x	0
Benchmark	x	x					2

Exempel 1: Fyra av sju kommuner har fått poäng på frågan, varför en majoritet finns för ett ja-svar. Inget av de poänggivande svarsalternativen har kryssats i av en majoritet av de som har fått poäng på frågan. Funktionen väljer därför det eller de svarsalternativ som har kryssats i av den största minoriteten, i det här fallet ja-svarsalternativ 1 och 2.

Tabell 10. Exempel 2: Benchmark med majoritet av nej-svar

Organisation	Poänggivande ja-svarsalternativ 1	Poänggivande ja-svarsalternativ 2	Poänggivande ja-svarsalternativ 3	Poänggivande ja-svarsalternativ 4	Poänggivande ja-svarsalternativ 5	Nej-svar	Summa
Kommun 1	x						1
Kommun 2		x	x				2
Kommun 3	x			x			2
Kommun 4						x	0
Kommun 5						x	0
Kommun 6						x	0
Kommun 7						x	0
Benchmark						x	0

Exempel 2: Fyra av sju kommuner har svarat nej på frågan, varför en majoritet finns för ett nej-svar.

Benchmarks ger en bild av hur den övergripande situationen ser ut inom en viss grupp. Det är samtidigt viktigt att komma ihåg att det inte nödvändigtvis är så att någon individuell organisation har ett resultat i Infosäkkollen som precis överensstämmer med vad en benchmark visar. Det är också viktigt att komma ihåg att benchmarks inte i sig visar om det är stor eller liten variation mellan medlemmarna i gruppen som benchmarken genereras ifrån. Ett viktigt komplement till benchmarksen är därför att titta på om benchmarkens ja- eller nej-svar är baserade på starka majoriteter, samt om dess poänggivande ja-svar är majoritets- eller minoritetssvar. Det är också bra att jämföra en benchmarks resultattal med resultattalen som dess medlemmar har fått.

Benchmarks används i Infosäkkollen och denna rapport som ett sätt att beskriva den övergripande situationen i olika grupper. När vi i resultatkapitlet nedan exempelvis talar om den ”typkommunen” så avser vi det vi ser i benchmarken för alla svarande kommuner. I verktyget Infosäkkollen benchmark är det också möjligt att använda benchmarksen för att ta reda på vilka åtgärder ens egen organisation behöver genomföra för att ”komma ikapp” snittresultatet i den egna gruppen.

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 resultat jämförs sedan i tur och ordning nivåer inom arbetsområdena, uppnådd totalpoäng samt uppnått poängresultat för arbetsområdena.

Bedömningen av resultat fungerar på så sätt att det som väger tyngst är den övergripande nivån. Om den ena organisationen har en högre övergripande nivå än den andra så kommer den alltid att bedömas som högre. Om två organisationer har samma övergripande nivå så jämförs nivåerna de har uppnått inom arbetsområdena. Så om två organisationer har samma övergripande nivå men den ena organisationen har uppnått en högre summa av nivåer inom arbetsområdena så bedöms den organisationen högre. Om två organisationer har nått samma övergripande nivå och har likvärdiga resultat* med avseende på nivåerna de har uppnått inom arbetsområdena så jämförs deras totalpoäng. Om de är lika även där jämförs de slutligen med avseende även på poängen de har samlat inom arbetsområdena (som kan vara högre än totalpoängen då viss överlappning förekommer mellan arbetsområdena).

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1942 – juni 2022 ISBN 978-91-7927-252-4