Fördjupningsinformation

- Uppföljningsstrukturen för systematiskt informationssäkerhetsarbete i offentlig sektor

Innehåll

Innehåll

Varför en uppföljning av systematiskt informationssäkerhetsarbete?

MSB har tagit fram uppföljningsmodellen - Infosäkkollen - för att stödja organisationer i den offentliga förvaltningen (kommuner, regioner och statliga myndigheter) i deras förbättringsarbete på informationssäkerhetsområdet. I det ingår bland annat automatisk återkoppling om vilken nivå organisationen befinner sig på och om vilka utvecklingsområden som är viktiga för framtiden.

När underlaget rapporteras in till MSB får organisationen också kompletterande återkoppling, exempelvis möjlighet att jämföra sitt resultat med de aggregerade resultaten hos andra verksamheter. MSB kommer att använda inrapporterat underlag för att utveckla myndighetens stöd och lämna en samlad bedömning till regeringen.

Infosäkkollen utgår från föreskrifter, stöd och ISO-standard

Uppföljningsmodellen utgår från det systematiska informationssäkerhetsarbetet som det beskrivs i MSB:s föreskrifter och stöd, som i sin tur bygger på standardserien ISO/IEC 27000.

Modellen ger stöd till uppföljning på en strategisk nivå. Resultatet visar i vilken utsträckning organisationen bedriver ett systematiskt informationssäkerhetsarbete, det vill säga har förutsättningar att bygga ett gott skydd för sin information. Modellen mäter inte om den enskilda organisationens skydd är tillräckligt.

Så kan ni arbeta med Infosäkkollen

Uppföljningsmodellen är omsatt i ett verktyg i Excel. Kärnan i verktyget är ett formulär med frågor om centrala delar av det systematiska informationssäkerhetsarbetet (se fliken ”Nivåfrågor”).

Infosäkkollen har skickats ut till din myndighets registratur. Den senaste versionen av verktyget återfinns alltid på www.msb.se/infosakkkollen.

Samla in underlag från olika delar av organisationen

Eftersom era svar avser kommunen, regionen eller den statliga myndigheten i sin helhet behövs underlag från olika delar av organisationen. Ett bra sätt att samla in den nödvändiga informationen är en workshop där olika funktioner och roller deltar. Organisationens informationssäkerhets-samordnare kan med fördel hålla ihop arbetet (alternativt någon i stabsfunktionen). Det samlade svaret bör förankras hos ledningen

Hur lång tid tar det att svara på frågorna?

Hur lång tid det tar att svara på frågorna beror på många faktorer och är därför svårt att uppskatta. Effektiv tid bedöms vara minst en eller ett par dagar, men ledtiden för att samla in informationen kan vara längre. Beroende på organisation och arbetssätt kan det i vissa fall röra sig om några veckor eller en ännu längre period.

Alla organisationer behöver inte svara på alla frågor för att få ett resultat. Anledningen till det är att även organisationer som inte har kommit så långt ska kunna använda uppföljningsmodellen. För en organisation som är i början av sitt arbete med informationssäkerhet kan det till exempel räcka att svara på frågorna under nivå 1, och några frågor på nivå 2.

Svaren måste fyllas i och lämnas in säkert

Svaren som lämnas i verktyget behöver hanteras och rapporteras in till MSB på ett säkert sätt. Följ de anvisningar som finns i under fliken ”Säker hantering”. MSB vill av säkerhetsskäl inte ta emot informationen på andra sätt än de som anges där.

Skicka in svaren senast 30:e september 2021

Era svar behöver komma in till MSB senast den 30:e september för att er organisation ska kunna få kompletterande återkoppling från MSB och bidra till den samlade bedömningen på nationell nivå.

Ni får återkoppling när ni har fyllt i svaren

Direkt när ni har fyllt i svaren kan ni se vilken nivå organisationen befinner sig på och vilka arbetsområden som behöver utvecklas. Återkopplingen presenteras på fliken ”Återkoppling”. Där återfinns också tips på relevant stöd, och länkar finns även på www.msb.se/infosakkollen. Infosäkkollen ger en översiktsbild som ni kan använda som underlag för diskussion i till exempel en ledningsgrupp.

Underlag för att arbeta med förbättringar

Tänk på att nyligen genomförda förbättringar inte kommer att få fullt genomslag i den återkoppling ni får, eftersom uppföljningen avser de senaste två åren. Uppföljningen tittar bakåt i tiden, men själva nyttan med resultatet handlar om att se framåt. Tanken är att få fram ett underlag till arbetet med ständiga förbättringar, och att främja en positiv uppföljningskultur över tid, snarare än att fokusera på resultatet i sig.

Att mäta systematiskt informationssäkerhetsarbete är komplext och kan göras på olika sätt. Återkopplingen ger en kvalificerad bedömning utifrån de svar ni gett.

Rapportera in svaren och få mer återkoppling

När svaren rapporteras in till MSB kommer er organisation att få kompletterande återkoppling. I den ingår en jämförelse med snittet för andra, liknande organisationer. Jämförelsen utgår från det samlade underlaget.

Vad betyder egentligen ”ett systematiskt informationssäkerhetsarbete”?

Informationssäkerhet är ett gemensamt ansvar för hela organisationen. Säkerhet är en förutsättning för att organisationen ska kunna använda sin information på avsett sätt och därigenom nå sina mål. Att bedriva ett systematiskt arbete med informationssäkerhet betyder att det finns en tydlig och strukturerad styrning i enlighet med ledningens vision och mål.

Det övergripande syftet med systematiskt informationssäkerhetsarbete är att skydda informationen på rätt nivå genom ständiga förbättringar och anpassningar till en föränderlig värld.

De grundläggande stegen vid allt systematiskt informationssäkerhetsarbete är att:

- identifiera organisationens informationstillgångar
- värdera informationstillgångarna utifrån konfidentialitet, riktighet och tillgänglighet
- bedöma de risker som kan förekomma när informationstillgångarna hanteras
- införa ändamålsenliga och proportionerliga säkerhetsåtgärder.

Uppföljning och utvärdering av arbetets olika delar sker återkommande och är ett centralt underlag i styrningen.

Planera, genomför, följ upp, utvärdera och förbättra

Att arbeta systematiskt innebär att man arbetar medvetet och metodiskt genom stegen planera, genomföra, följa upp, utvärdera och förbättra. Konkret innebär det att organisationen, för de olika delarna i informationssäkerhetsarbetet:

1. medvetet väljer arbetssätt (exempelvis beslutar och dokumenterar i form av riktlinjer, rutiner, instruktioner, modeller eller verktyg)
2. implementerar och tillämpar arbetssätten i alla relevanta situationer och verksamhetsprocesser
3. följer över tid vilka resultat tillämpningen av arbetssätten leder till
4. utvärderar och förbättrar arbetssätten.

Koppla ihop arbetssätten till en sammanhållen process

Systematik innebär också att olika arbetssätt kopplas ihop till en sammanhållen process i organisationen. Till exempel bör resultatet av organisationens arbete med riskanalys användas vid valet av säkerhetsåtgärder, men även som underlag för att utforma medarbetarnas utbildning.

Främja en god säkerhetskultur

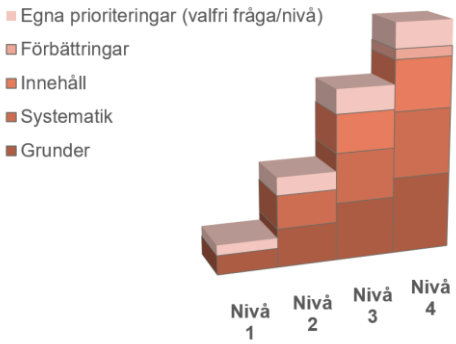
Informationssäkerheten i organisationen påverkas inte bara av de olika arbetsmomenten i informationssäkerhetsarbetet och de tekniska eller administrativa säkerhetsåtgärder som införs. Också säkerhetskulturen i organisationen spelar en avgörande roll för att både det systematiska arbetet och skyddet ska fungera.

Säkerhetskulturen består av tankemönster, värderingar och beteenden hos grupper och individer. Vilka kunskaper medarbetarna har, vilka signaler ledningen och kollegorna ger samt hur individens arbetssituation ser ut är några exempel på faktorer som påverkar informationssäkerhetsarbetet.

Modellen visar vilken nivå organisationens informationssäkerhetsarbete ligger på

Uppföljningsmodellen delar in det systematiska informationssäkerhetsarbetet i fyra nivåer, som är tänkta att svara mot ett stegvis utvecklingsarbete:

Nivå 1	Organisationer som har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad utsträckning.
Nivå 2	Organisationer som bedriver informationssäkerhetsarbetet med en viss systematik, och som är bättre på grunderna än på nivå 1.
Nivå 3	Organisationer som har ett kvalificerat innehåll i sitt informationssäkerhetsarbete, och som är bättre på både grunderna och systematiken än på nivå 2.
Nivå 4	Organisationer som arbetar avancerat med ständiga förbättringar, samt är bättre på såväl grunderna som systematiken och innehållet än på nivå 3.



Gemensamt för alla nivåer är att de bygger vidare på och fördjupar innehållet från föregående nivå. Till exempel har en organisation på nivå 2 inte bara utvecklat viss systematik i sitt arbete utan också kommit längre med informationssäkerhetens grunder än en organisation på nivå 1.

Nivåbedömningen i Infosäkkollen utgår från svar på frågorna i fliken ”Nivåfrågor”, som grupperats i avsnitt för respektive nivå.

Nivå 1: organisationer som har grunderna i informationssäkerhetsarbetet

Frågorna i detta avsnitt mäter om organisationen har de grundläggande delarna i informationssäkerhetsarbetet på plats. Frågorna undersöker bland annat:

- om ledningen är engagerad i informationssäkerhetsarbetet
- om organisationen har inventerat informationstillgångar
- om organisationen har arbetssätt på centrala områden (som informationsklassning och risk)
- om organisationen har undersökt medarbetarnas kunskaper inom informationssäkerhetsarbete.

För att uppfylla kraven för nivå 1 räcker det att de grundläggande delarna finns på plats i begränsad utsträckning. Något resultat behöver uppvisas inom varje frågeområde, men det finns inga krav på särskild systematik eller innehåll i arbetet. Det behandlas istället på högre nivåer.

Nivå 2: organisationer som bedriver informationssäkerhetsarbetet med viss systematik och är bättre på grunderna

Frågorna i avsnittet fokuserar på om informationssäkerhetsarbetet sker med viss systematik. Frågorna undersöker därför om organisationen tillämpar sina arbetssätt och om de olika delarna kopplar till varandra. Ett exempel på det är om säkerhetsåtgärderna bygger på en riskanalys.

En del av områdena från nivå 1 utvecklas med fördjupande frågor, till exempel om medarbetarnas kunskaper.

Nivå 3: organisationer som har ett kvalificerat innehåll i informationssäkerhetsarbetet samt är bättre på både grunderna och systematiken

Frågorna i avsnittet handlar om huruvida det systematiska informationssäkerhetsarbetet har ett kvalificerat innehåll. Utgångspunkten är bland annat MSB:s föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6. Frågorna undersöker om organisationens arbetssätt är utformade på ett sätt som kan förväntas vara ändamålsenligt.

Nivå 4: organisationer som arbetar avancerat med ständiga förbättringar samt är bättre på grunderna, systematiken och innehållet

Frågorna i avsnittet syftar till att fånga ett avancerat arbete med ständiga förbättringar, avseende att identifiera hinder och framgångsfaktorer samt ledningens uppföljning. På nivå 4 uppvisar organisationen mycket höga resultat på alla frågor. Informationssäkerhetsarbetet karaktäriseras genomgående av systematik och ändamålsenlighet.

Olika organisationer kan behöva prioritera olika delar av arbetet

Infosäkkollen tar hänsyn till att olika organisationer kan behöva prioritera olika delar av informationssäkerhetsarbetet. Därför kan respektive nivå uppnås på delvis olika sätt, genom viss flexibilitet för egna prioriteringar (se beskrivningen av poängberäkningen nedan). Modellen främjar samtidigt ett helhetsgrepp på informationssäkerhetsarbetet, eftersom organisationer som satsar på spets på bekostnad av bredd inte når modellens högre nivåer.

Nivån räknas fram genom poäng och andel säkra bedömningar

Det krävs ett visst antal poäng för att uppnå varje nivå. Poängen beräknas utifrån svar på frågorna i fliken ”Nivåfrågor”, som grupperats i avsnitt för respektive nivå. För att nå en viss nivå behövs en

totalpoäng, som består av två delar: lägstapoäng per fråga och rörliga poäng (egna prioriteringar). Dessutom krävs säkra bedömningar för en viss andel av de frågor som har besvarats.

Lägstapoängen per fråga beror på nivån. För att nå nivå 1 behöver frågorna i det avsnittet ge minst 1 poäng. För att nå nivå 2 behövs 2 poäng på varje fråga i nivåavsnitt 1-2, osv. För varje nivå krävs alltså bättre resultat på frågorna i de föregående avsnitten. Rörliga poäng kan samlas på olika sätt. Ett sätt är att samla mer än lägstapoängen på någon eller några frågor. Ett annat sätt är att svara på någon eller några frågor från högre nivåer.

Tabellen visar översiktligt hur upplägget fungerar:

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.

Ekvation för poängkraven

Kraven för att nå en viss nivå kan även sammanfattas i följande ekvation:

$$\textit{Poängkrav för nivå } X = (X+0{,}5) * \textit{Antalet frågor som måste besvaras på nivån}$$

X är nivånumret och är även liktydigt med lägstapoängen som behövs per fråga för att nå nivån.

Antalet rörliga poäng, alltså poäng som kan hämtas från vilken fråga som helst, beräknas som *0,5 * Antalet frågor som måste besvaras på nivån.*

Hur Infosäkkollens frågor besvaras

Svara på frågorna i verktyget genom att markera med ett X under de svarsalternativ som stämmer för organisationen. Svarsrutor finns direkt under respektive svarsalternativ. Komplettera svaret med hur säker organisationen är på svaren som lämnas.

Rutan under ”Summa” speglar de svar som markerats, antingen genom att visa poäng som samlats eller genom att indikera om svaret är ofullständigt eller ogiltigt.

Två typer av frågor

Infosäkkollen omfattar två typer av frågor: flervalsfrågor och angränsande flervalsfrågor.

Flervalsfrågorna kan besvaras med fler än ett svarsalternativ. De första fem svarsalternativen ger 1 poäng, övriga svarsalternativ ger 0 poäng. Poängsumman motsvarar alltså antalet valda poänggivande svarsalternativ. Flervalsfrågorna kan ge maximalt 5 poäng.

Angränsande flervalsfrågor kan också besvaras med fler än ett svarsalternativ, men bara om svarsalternativen angränsar till varandra och inte motsäger varandra. Svarsalternativen är formulerade som intervall. De angränsande flervalsfrågornas svarsalternativ ger antingen 5, 4, 3, 2, 1 eller 0 poäng. Svaret ”Alla …” ger 5 poäng, medan lägre andelar ger lägre poäng i fallande skala. Om organisationen väljer fler än ett svarsalternativ bestäms poängen av det alternativ som ger lägst poäng.

Säker och osäker bedömning

För varje fråga behöver ni bedöma hur säkert svaret eller svaren är. Det kan vara en fördel när organisationer har goda skäl att tro, men inte helt säkert vet, att en viss del av det systematiska informationssäkerhetsarbetet ser ut på ett visst sätt. Välj bara alternativet ”Säker bedömning” om det finns dokumenterade och tydliga belägg för att svaret är korrekt.

Ju högre nivå, desto högre måste andelen säkra bedömningar vara.

Om ni kryssar i flera svarsalternativ betyder ”Säker bedömning” att det finns dokumenterade och tydliga belägg för *alla* svarsalternativ ni väljer.

Infosäkkollen följer upp de senaste två åren

Alla frågor i Infosäkkollen handlar om den senaste tvåårsperioden, eftersom nivån på organisationens informationssäkerhetsarbete 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. Det är också en fördel att mätperioden sammanfaller med hur ofta uppföljningen genomförs. Vartannat år kommer att MSB skicka ut verktyget till offentlig förvaltning och be att resultaten rapporteras in.

Infosäkkollen använder måttet ”andel av verksamheter”

I de frågor som handlar om i vilken utsträckning något tillämpas (till exempel ett arbetssätt) förekommer måttet ”andel av verksamheter”. Det är ett trubbigt mått, men MSB bedömer att det är bättre att mäta något som är enklare att kontrollera för, men som ger en lägre precision, än att mäta något som är svårt att kontrollera för, men som ger en hög precision om man lyckas.

Med verksamhet menas större organisationsindelningar, till exempel förvaltningar eller avdelningar beroende på hur organisationen är strukturerad.

Infosäkkollen stödjer tillämpning av MSB:s föreskrifter

Statliga myndigheter är skyldiga att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete, i enlighet med MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6). Även organisationer som inte omfattas av föreskrifterna kan använda dem som stöd för arbetet och för att hitta rätt ambitionsnivå. Infosäkkollen är utformad så att den kan indikera i vilken utsträckning organisationen uppfyller olika krav i föreskrifterna. Tanken med det är att stödja tillämpningen av föreskrifterna.

Indikation om att kraven är uppfyllda förutsätter minst nivå 3 i modellen. Dessutom innebär kraven att vissa specifika svarsalternativ behöver vara uppfyllda på enskilda frågor.

Det är viktigt att komma ihåg att modellen bara kan ge en indikation, den är inte tänkt att omfatta hela författningen eller alla sätt som kraven kan uppnås på. Till exempel berör modellen inte fysiskt skydd. Ni kan läsa mer om hur indikationen tas fram på www.msb.se/infosakkollen.

Modellen mäter inte hur organisationens arbete förhåller sig till specifika krav i andra författningar, exempelvis dataskyddsförordningen och säkerhetsskyddslagen.

MSB använder inte svaren för att kontrollera om föreskrifterna följs

MSB avser inte använda Infosäkkollen för att kontrollera hur enskilda organisationer efterlever de regler som finns. Det är inte syftet med modellen och MSB har inte heller i uppgift att utöva tillsyn över tillämpningen av föreskrifterna på informationssäkerhetsområdet. Indikationen ska inte heller i övrigt tas till intäkt för en bedömning av efterlevnad från MSB i det enskilda fallet.

Reflektion & Målbild

På fliken ”Analysstöd” ges organisationen möjlighet att redogöra för hur den ser på resultatet, samt plotta ut målbilden för de kommande två åren. Informationen här är i huvudsak till för er och den kan med fördel kopieras och användas för presentation till ledningsgruppen.

Valideringsfrågor bidrar till att förbättra modellen på sikt

Utöver ”nivåfrågorna” innehåller verktyget också valideringsfrågor (se fliken ”Analysstöd”). Syftet med valideringsfrågorna är tredelat:

- att göra det lättare för organisationer att följa upp effekterna av sitt informationssäkerhetsarbete
- att möjliggöra för MSB att ta fram bättre stöd till aktörerna, genom att kunna se samband mellan resultat på olika områden och utfallet av valideringen
- att på sikt kunna säkerställa att modellen mäter sådant som har betydelse för informationssäkerhetsarbetet, och därmed kunna utvärdera och förbättra den.

Ni behöver inte svara på valideringsfrågorna för att få ett resultat i fliken ”Återkoppling” eller kompletterande återkoppling från MSB.

Ekonomifrågor

Här ges organisationen möjlighet att följa upp hur den har understött det systematiska informationssäkerhetsarbetet med ekonomiska resurser under den senaste tvåårsperioden. Det är helt frivilligt att besvara frågorna. Frågorna bör troligen besvaras genom ett samarbete mellan informationssäkerhetssamordnaren och representanter från motsvarande en ekonomiavdelning eller en controllerfunktion.

Genom att besvara frågorna ges organisationen en möjlighet att följa om organisationen har resurssatt arbetet på ett systematiskt och tillräckligt sätt. Om organisationen rapporterar sina svar till MSB så kommer myndigheten över tid att kunna stödja organisationer med nyckeltal om hur mycket resurser som normalt sett behövs för att uppnå en viss nivå i Infosäkkollen - och därmed i organisationens eget systematiska informationssäkerhetsarbete.

Ställ frågor och lämna förbättringsförslag till MSB

Vanliga frågor och svar om uppföljningen finns på www.msb.se/infosakkollen. Infosäkkollen utvecklas kontinuerligt och MSB uppskattar alla synpunkter för framtida versioner. På hemsidan finns även verktyget publicerat, så att du kan säkerställa att du alltid använder den senaste versionen. Det går också att ställa frågor till infosakkollen@msb.se.