Myndigheten för samhällsskydd och beredskap

Datum
2021-03-01

Ärendenr
MSB 2019-11710

En struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen

Redovisning av regeringens uppdrag till Myndigheten för samhällsskydd och beredskap

(Ju2019/03058/SSK, Ju2019/02421/SSK)

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

Innehåll

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984

Sammanfattning

MSB presenterar i denna redovisning en uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete. 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. Målsättningen med uppföljningsstrukturen är att statliga myndigheter, kommuner och regioner ska erbjudas stöd i sitt uppföljnings- och förbättringsarbete och att regeringen ska få en samlad nivåbedömning av det systematiska informationssäkerhetsarbetet i offentlig förvaltning.

Systematiskt informationssäkerhetsarbete innebär att organisationen arbetar medvetet och metodiskt i enlighet med ledningens mål och inriktning. Det övergripande syftet är att genom ständiga förbättringar och anpassningar till en föränderlig värld skydda informationen på ändamålsenlig nivå. Hur ett systematiskt informationssäkerhetsarbete bedrivs framgår av MSB:s föreskrifter och stöd på området, som i sin tur bygger på den internationella standardserien ISO/IEC 27000.

Med detta som utgångspunkt har MSB, i dialog och samverkan med företrädare för målgruppen, utvecklat en uppföljningsmodell. Modellen delar in det systematiska informationssäkerhetsarbetet i fyra nivåer, som är tänkta att motsvara ett stegvis utvecklingsarbete. Genom att besvara uppföljningsmodellens frågeformulär får en organisation automatisk återkoppling om sin nivå, styrkor och utvecklingsområden. Kompletterande återkoppling (benchmarking) erhålls efter inrapportering till MSB. I analysen av det samlade underlaget kan MSB dra slutsatser om vad för stöd och satsningar som är påkallade på nationell nivå. Uppföljningsstrukturen löper över två år, med lansering planerad till 2021. Därefter kommer uppföljningen att genomföras regelbundet i tvåårscykler, vilket bland annat ger möjlighet att identifiera utvecklingstrender över tid.

MSB:s uppföljningsstruktur bedöms kunna bidra till ett förbättrat och mer enhetligt arbete med informationssäkerhet inom offentlig förvaltning. Detta förutsätter dock ett brett deltagande från den offentliga förvaltningen, främjande av en positiv och bejakande uppföljningskultur, samt resurssättning av identifierade förbättringsområden.

1. Inledning

1.1 Bakgrund

Den offentliga förvaltningen digitaliseras alltmer, liksom samhället i stort. Detta medför stora möjligheter. Samtidigt har MSB återkommande pekat på en ökande säkerhetsskuld – ett gap mellan digitaliseringen och informationssäkerheten – eftersom säkerhetsarbetet generellt ofta ligger ett eller flera steg efter den nya tekniken.[1] Regeringen har framhållit att samhällets informations- och cybersäkerhet behöver stärkas, varvid en systematisk och samlad ansats i arbetet ska säkerställas.[2]

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. 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. Uppföljningsstrukturen ska även syfta till att MSB regelbundet ger regeringen en samlad bedömning om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. Regeringens beslut (Ju2019/03058/SSK, Ju2019/02421/SSK) återfinns i sin helhet som bilaga.

I ett systematiskt informationssäkerhetsarbete ingår löpande uppföljning i syfte att förbättra och anpassa arbetet utifrån organisationens behov, med målet att uppnå och bibehålla ett adekvat skydd. Uppföljning upplevs emellertid ofta som en utmaning, inklusive inom offentlig förvaltning, både avseende utformning och resurser. I värsta fall väljer organisationer helt enkelt bort att följa upp sitt arbete. Till exempel visade MSB:s enkät från 2015 att det generellt sett inte arbetades systematiskt med uppföljning av informationssäkerheten bland Sveriges kommuner.[3] I myndighetens kartläggning av regionernas (landstingens) informationssäkerhetsarbete på hälso- och sjukvårdsområdet 2018 framkom att flera regioner insåg vikten av att följa upp och utvärdera arbetet, men saknade adekvata arbetssätt.[4] Ifråga om statliga myndigheter uppgav drygt två tredjedelar i en undersökning från 2014 att informationssäkerhetsarbetet inte utvärderades alls, endast i begränsad utsträckning eller delvis.[5] Även Riksrevisionen har uppmärksammat bristen på sådan uppföljning hos statliga myndigheter.[6] MSB bedömer att ett stöd för uppföljning av

[1] Se till exempel Årsrapport statliga myndigheters it-incidentrapportering 2020 – Utmaningar för en säker och robust informationshantering (2021: MSB1692) och Nationell risk- och förmågebedömning 2019 (2019: MSB1392)
[2] Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213)
[3] Informationssäkerheten i Sveriges kommuner – Analys och rekommendationer utifrån MSB:s kommunenkät 2015 (2016: MSB1045)
[4] En bild av landstingens informationssäkerhetsarbete 2018 – Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (2018: MSB1254)
[5] En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter (2014: MSB740)
[6] Informationssäkerhetsarbete på nio myndigheter (RIR 2016:8)

det systematiska informationssäkerhetsarbetet skulle kunna lämna ett viktigt bidrag till den offentliga förvaltningens verksamhet på området.

En centralt sammanhållen uppföljning av informationssäkerheten i offentlig förvaltning skulle också kunna utgöra ett viktigt underlag för regeringens, MSB:s och andra myndigheters behovsanalys av vad för stöd och andra insatser som ska prioriteras. Även om undersökningar genomförts av informationssäkerhetsarbetet inom delar av den offentliga förvaltningen, saknas i dag en systematisk och samlad helhetsbild som också löpande uppdateras.

1.2 Disposition och avgränsningar

I denna redovisning beskrivs först vilka utgångspunkter som identifierats i utvecklingsarbetet inom ramen för uppdraget (kap. 2), följt av en presentation av resultatet: MSB:s uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete (kap. 3). Därefter lämnas en redogörelse för hur arbetet har genomförts, med tonvikt på genomförd dialog och samverkan (kap. 4). Slutligen presenteras möjlig framtida vidareutveckling (kap. 5), samt övergripande slutsatser (kap. 6).

I bilaga återfinns regeringsuppdraget till MSB, en internationell utblick, samt utdrag från den uppföljningsmodell som utvecklats.

Däremot innehåller redovisningen inte den första samlade bedömningen om nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen som ingick i uppdraget. Uppföljningen har senarelagts till 2021 på grund av den ökade belastningen på många organisationer i målgruppen, samt även MSB, i och med covid-19-pandemin. I en tid då stora delar av offentlig förvaltning behövde hantera en extraordinär situation valde MSB i samråd med regeringskansliet att avvakta med lansering av uppföljningen. Den samlade bedömningen till regeringen, jämte en bedömning av hur MSB utifrån resultatet av uppföljningen kan utveckla stödet till den offentliga förvaltningen, kommer att lämnas 2022 efter att uppföljningsstrukturen lanserats.

Det bör noteras att denna redovisning lämnas under pågående arbete. Även om uppföljningsstrukturen är konceptuellt färdigutvecklad kan exempelvis kommande pilotomgång medföra justeringar i det som här presenteras.

2. Utgångspunkter i utvecklingsarbetet

2.1 Krav och följdverkningar på utformningen

Regeringsuppdragets krav på uppföljningsstrukturen sätter inte bara de övergripande ramarna utan får också vissa direkta följdverkningar på utformningen. Därutöver har MSB identifierat vissa tillkommande krav. Kraven och följdverkningarna sammanfattas nedan.

- *En uppföljningsstruktur för hela den offentliga förvaltningen:* Uppföljningen behöver i första hand genomföras utifrån en kvantitativ metod. Frågorna som ställs behöver vara så precisa som möjligt, men samtidigt tillämpliga på olika typer av organisationer. Olika organisationers skilda utvecklingsbehov behöver beaktas.

- *En uppföljningsstruktur för systematiskt informationssäkerhetsarbete:* Det är nivån på det systematiska informationssäkerhetsarbete som står i fokus, det vill säga inte den faktiska skyddsnivån (säkerhetsåtgärder).

- *Återkoppling till medverkande organisationer om vilken nivå de befinner sig på, utifrån en skala med beskrivna nivåer för det systematiska informationssäkerhetsarbetet:* Övergripande nivåer behöver definieras och beskrivas, det vill säga det räcker inte att mäta utvecklingsnivån i enskilda delar av informationssäkerhetsarbetet. Med hänsyn till kravet på kvantitativ metod, behöver återkoppling åtminstone till del genereras automatiskt.

- *Återkoppling om förslag på åtgärder som bör vidtas för att uppnå en högre nivå på informationssäkerhetsarbetet:* Återkopplingen om den övergripande nivån behöver kunna brytas ned på enskilda arbetsområden, så att det blir tydligt var ytterligare åtgärder bör vidtas.

- *Regelbunden samlad bedömning till regeringen om nivån i den offentliga förvaltningen, med jämförbarhet över tid:* För att ge tillräckligt analysunderlag för en samlad bedömning behöver uppföljningen täcka en bredd av aspekter och med sådant djup att det går att dra meningsfulla slutsatser. Resultatet behöver vara strukturerat och jämförbart (till exempel fokus på jämförbara fakta i syfte att begränsa utrymmet för tolkningar samt tydlighet kring mätperiod).

- *Medverkan är frivillig:* Viss återkoppling behöver lämnas direkt, för att stimulera till medverkan. Samtidigt behöver kompletterande återkoppling lämnas efter att MSB tagit emot underlaget, för att stimulera till inrapportering.

- *Uppföljningsstrukturen ska vara ett stöd till medverkande organisationers eget arbete med ständiga förbättringar:* Uppföljningen behöver passa in i helheten av en organisations systematiska informationssäkerhetsarbete. Det innebär bland annat en tydlig anknytning till MSB:s befintliga föreskrifter och stöd inom informationssäkerhet (som i sin tur bygger på standardserien ISO/IEC 27000), både vad gäller vad som mäts och i den återkoppling som lämnas. Återkopplingen behöver vidare utformas så att den kan utgöra underlag till det egna uppföljningsarbetet (till exempel Ledningens genomgång[7]). Slutligen behöver arbetsinsatsen vara rimlig.

2.2 Att mäta systematiskt informationssäkerhetsarbete

2.2.1 Innebörden av systematiskt informationssäkerhetsarbete

Uppföljningsstrukturen avser den offentliga förvaltningens systematiska informationssäkerhetsarbete. På basis av *best practice* och internationell standardisering

[7] Ledningens genomgång syftar till att organisationens högsta ledning ska kunna säkerställa att ledningssystemet för informationssäkerhet är fortsatt lämpligt, tillräckligt och verkansfullt. Enligt MSB:s föreskrifter om informationssäkerhet för statliga myndigheter ska dessa minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning.

understryker MSB, i sitt arbete med att stödja och samordna samhällets informationssäkerhetsarbete, vikten av en systematisk ansats.

Att bedriva ett systematiskt arbete med informationssäkerhet betyder att det finns en tydlig och strukturerad styrning i enlighet med ledningens mål och inriktning. Det övergripande syftet med systematiskt informationssäkerhetsarbete är att genom ständiga förbättringar och anpassningar till en föränderlig värld skydda informationen på ändamålsenlig nivå. Grundläggande steg för allt systematiskt informationssäkerhetsarbete är att identifiera organisationens informationstillgångar, att värdera dem utifrån konfidentialitet, riktighet och tillgänglighet samt att bedöma de risker som kan förekomma vid hantering av informationstillgångarna. Detta ska resultera i att ändamålsenliga och proportionerliga säkerhetsåtgärder vidtas. Uppföljning och utvärdering av arbetets olika delar sker återkommande och är ett centralt underlag i styrningen.

Att arbeta systematiskt innebär alltså att organisationen arbetar medvetet och metodiskt genom stegen planera, genomföra, följa upp, utvärdera och förbättra. Konkret innebär det att organisationen, för att hantera olika uppgifter:

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.

Att arbeta systematiskt innebär också att organisationen medvetet kopplar ihop de olika arbetssätten till en sammanhållen process. Exempelvis bör resultatet av organisationens arbete med riskanalys användas vid valet av säkerhetsåtgärder men även som underlag vid utformning av medarbetarnas utbildning.

Systematiskt informationssäkerhetsarbete utgår från att informationssäkerhet är ett gemensamt ansvar för hela organisationen, från ledningens vision till den enskilde medarbetarens ansvarstagande i vardagen. Säkerhet ses som en förutsättning för att organisationen ska kunna använda sin information på avsett sätt och därigenom nå sina mål. Detta kan sammanfattas som säkerhetskultur – att medarbetarna delar tankemönster, värderingar och beteenden som främjar säkerheten.

MSB:s uppfattning om hur en organisation bör bedriva sitt systematiska informations-säkerhetsarbete framgår av myndighetens föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Föreskrifterna kan även användas som ett stöd av andra organisationer. Det systematiska informationssäkerhetsarbetet återspeglas även inom ramen för NIS[8] genom MSB:s föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8), vilka bland annat träffar verksamheter i kommuner och regioner, och i myndighetens olika stöd, särskilt Metodstödet på

[8] Säkerhet i nätverk och informationssystem – se Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)

informationssäkerhet.se. MSB:s föreskrifter och stöd bygger på standardserien ISO/IEC 27000 om ett ledningssystem för informationssäkerhet. ISO/IEC 27000-serien utgår från internationell *best practice* för systematiskt informationssäkerhetsarbete. Uppföljningsstrukturen har utvecklats med strävan att beskriva och mäta systematiskt informationssäkerhetsarbete så som det kommer till uttryck i dessa källor, närmast MSB:s föreskrifter om informationssäkerhet för statliga myndigheter och standarden ISO/IEC 27001[9].

2.2.2 Referenspunkter för uppföljningsstrukturens sätt att mäta

För att ge en rättvisande bild, och bidra till en positiv utveckling, måste uppföljningen mäta sådana förhållanden som faktiskt har betydelse för informationssäkerheten. Tyvärr saknas relevanta vetenskapliga studier på populationsnivå (flera organisationer) om vad för påverkan olika delar i det systematiska informationssäkerhetsarbetet har på den samlade nivån på informationssäkerheten i en organisation. Det vill säga, hur man i en uppföljning mäter vad i arbetet som leder till ett adekvat skydd är inte belagt. Därför är det viktigt att uppföljningsstrukturen innehåller en uppsättning valideringsfrågor, som tillsammans med synpunkter från medverkande organisationer, kan användas för att utveckla kunskap om dessa orsakssamband och utvärdera uppföljningen.

MSB har emellertid viss upparbetad erfarenhet på området uppföljning av informationssäkerhet, bland annat kopplat till följande arbeten:

- Bevakningsansvariga myndigheters informations- och cybersäkerhet: En sammanvägd rapport utifrån redovisningar enligt Ju2017/05787/SSK (2018)
- En bild av landstingens informationssäkerhetsarbete 2018: Kartläggning och analys av landstingens informationssäkerhetsarbete inom hälso- och sjukvårdsverksamheten (2018: MSB1254)
- Informationssäkerheten i Sveriges kommuner: Analys och rekommendationer utifrån MSB:s kommunenkät 2015 (2016: MSB1045)
- En bild av kommunernas informationssäkerhetsarbete (2015: MSB943)
- En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter (2014: MSB740)
- Årsrapporterna om statliga myndigheters it-incidentrapportering samt, från 2021, motsvarande avseende NIS-leverantörer

Dessa kartläggningar och rapporter har utgjort referenspunkter för bland annat bedömningar om vilka delar av informationssäkerhetsarbetet som bör ligga i fokus i uppföljningsstrukturen och hur frågor bör formuleras. Särskilt undersökningen av regionernas (landstingens) arbete bör nämnas, vilken byggde på SIQ:s managementmodell: Här kartlades graden av systematik och resultat inom olika områden utifrån en mognadstrappa i fyra steg (om arbetssätt finns, i vilken grad de tillämpas, vilka resultat de ger, samt hur de följs upp); uppföljningsstrukturen tar på ett liknande sätt fasta på vikten av en organisations arbetssätt, om än utifrån annorlunda metodologiska förutsättningar.

[9] SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav

Internationell utblick

Utvecklingsarbetet av uppföljningsstrukturen har vidare innefattat en genomgång av olika internationella modeller och ramverk för uppföljning och utvärdering av informationssäkerhet och informationssäkerhetsarbete (se bilagan ”Internationell utblick”). I genomgången ingick det amerikanska standardiseringsorganet NIST:s *Cybersecurity Framework*, det amerikanska energidepartementets *The Cybersecurity Capability Maturity Model* (C2M2), det amerikanska försvarsdepartementets *Cybersecurity Maturity Model Certification* (CMMC), *Cyber Assessment Framework* (CAF) från det brittiska National Cyber Security Center (NCSC), samt *Cybermätaren* som utvecklats av det finländska cybersäkerhetscentret.

Genomgången har lämnat viktiga bidrag till utvecklingsarbetet, men ingen av de studerade internationella modellerna eller ramverken har ensam kunnat ligga till grund för utvecklingen av uppföljningsstrukturen givet de krav och följdverkningar på utformningen som följer av föreliggande regeringsuppdrag. En generell reflektion är att det engelskspråkiga begreppet *cyber/cybersecurity*, som genomgående används internationellt, vanligen förstås mer i termer av it-säkerhetsåtgärder mot antagonistiska hot än systematiskt informationssäkerhetsarbete i bredare bemärkelse. De studerade modellerna tenderar i linje med detta att fokusera på implementeringen av ett antal definierade åtgärder, snarare än arbetssätt för att förstå de egna säkerhetsbehoven, välja säkerhetsåtgärder, följa upp och förbättra. Därmed bortdefinieras i stor utsträckning allriskperspektivet, som är nödvändigt för att möta hela bredden av risker kopplade till informations- och cybersäkerhet – från naturfenomen, systemfel och handhavandefel till antagonistisk verksamhet. Vidare bygger flertalet internationella modeller på det amerikanska NIST-ramverket, som tar en delvis annan ansats till informationssäkerhetsarbetet än ISO/IEC 27000-serien som MSB med flera utgår från. Slutligen är de flesta modeller som studerats inriktade på särskilda sektorer (kritisk infrastruktur eller försvar) samt kräver stora arbetsinsatser, inklusive en facilitator/tolkningsstöd för att få återkoppling, alternativt fungerar mer som checklistor än uppföljningsverktyg med inbyggd återkoppling.

3. MSB:s uppföljningsstruktur för den offentliga förvaltningens systematiska informationssäkerhetsarbete

3.1 Övergripande beskrivning

Målsättningen med uppföljningsstrukturen är, i enlighet med regeringsuppdraget, att statliga myndigheter, kommuner och regioner ska få stöd i sitt uppföljnings- och förbättringsarbete på informationssäkerhetsområdet. I det ingår bland annat återkoppling om vilken nivå organisationen befinner sig på och viktigare utvecklingsområden för framtiden. Vidare ska MSB på grundval av uppföljningen lämna en samlad nivåbedömning till regeringen. Dessutom ska myndigheten utifrån resultatet se över hur uppföljningsstrukturen och övrigt stöd på området kan utvecklas. I syfte att uppnå detta har MSB utvecklat en uppföljningsstruktur i form av en process som löper över 24

månader och som regelbundet initieras på nytt i januari månad vartannat år. Processen består av sex aktiviteter och beskriver vilka åtgärder som organisationerna i offentlig förvaltning respektive MSB vidtar i syfte att uppnå målsättningen med strukturen (se figur). En central del av strukturen utgörs av uppföljningsmodellen. Modellen består av ett formulär med 40 frågor som mäter det systematiska informationssäkerhetsarbetet och genererar automatisk återkoppling.

3.2 Närmare om uppföljningsstrukturens olika aktiviteter

Tvåårscykeln inleds internt hos MSB med förberedelser inför lanseringen av uppföljningen till den offentliga förvaltningens organisationer. I arbetet ingår att se över kontaktlistor och sambandslösningar, sluthantera eventuella behov av justeringar av uppföljningsmodellen och stödmaterialet, genomföra kommunikationsinsatser med mera. Sedan skickas uppföljningsmodellen (frågeformuläret med automatisk återkoppling) och stödmaterialet ut till organisationerna (förslagsvis i mars)[10].

En organisation har sedan en period på sju månader (fram till oktober) för att genomföra uppföljningen. Den väl tilltagna tidsrymden ger möjlighet för organisationen att arbeta med uppföljningen när det passar dess verksamhet och årscykel. När svaren är ifyllda genererar funktionaliteten i uppföljningsmodellen en automatisk återkoppling till organisationen rörande vilken nivå som det systematiska informationssäkerhetsarbetet ligger på. Återkopplingen visar också inom vilka områden som organisationen uppvisar styrkor respektive utvecklingspotential och vilka stöd som organisationen kan använda för att vidta förbättringsåtgärder som medger en höjning till nästa nivå i uppföljningsmodellen. Dessutom, vilket är av större betydelse för statliga myndigheterna än övriga organisationer, ges en indikation rörande hur väl organisationen följer kraven på systematiskt informationssäkerhetsarbete i MSB:s föreskrifter om informationssäkerhet för

[10] Tidpunkterna avser en idealbild av aktiviteternas fördelning över en tvåårscykel; se vidare kap. 4.3.2.

statliga myndigheter. Efter att ha fyllt i frågeformuläret uppmuntras organisationen att skicka underlaget till MSB för samlad analys.

När MSB får in organisationernas ifyllda frågeformulär genomför myndigheten en analys i syfte att identifiera gemensamma styrkor och brister och bygga upp en samlad bild av informationssäkerhetsarbetet i offentlig förvaltning. Analysarbetet tar inte bara sikte på den bild som ges under innevarande period utan ska även jämföra resultatet med tidigare års resultat för att identifiera trender och utveckling över tid. Det huvudsakliga syftet med analysarbetet är att tillhandahålla underlag för de återstående tre aktiviteterna i uppföljningsstrukturen. Dessa vidtas samtliga av MSB men har olika syften och stödjer samhällets informations- och cybersäkerhet på olika sätt. Arbetet med dessa tre aktiviteter löper, till skillnad från de tre tidigare, delvis parallellt:

- Göra en *samlad bedömning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen* som redovisas för regeringen. Redovisningen baseras på analysen av de inskickade frågeformulären.
- Lämna *kompletterande återkoppling till organisationerna* som lämnat in frågeformulär genom att ge möjlighet till jämförelser med olika grupper (benchmarking). MSB kan också lämna enskilt stöd i vissa fall.
- *Vidareutveckla det stöd som MSB tillhandahåller samhällets aktörer*, med särskilt fokus på offentlig förvaltning. I aktiviteten ingår även att vid behov *vidareutveckla uppföljningsstrukturen* för att förbättra uppföljningsarbetet.

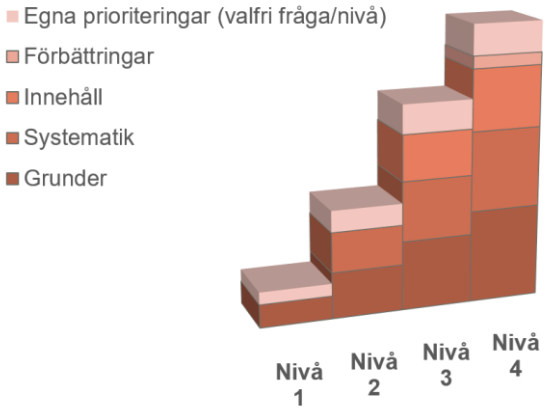
Mer information om dessa tre aktiviteter finns i avsnitt 3.4.

3.3 Uppföljningsmodellen

3.3.1 Nivåindelning

Uppföljningsmodellen utgör en central del i uppföljningsstrukturen och innehåller det frågeformulär som organisationerna fyller i, inklusive en funktion för automatisk återkoppling. Modellen delar in det systematiska informationssäkerhetsarbetet i fyra nivåer, som är tänkta att svara mot ett stegvis utvecklingsarbete (se figur).

Organisationer på nivå 1 har grunderna i informations-säkerhetsarbetet 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.

I frågeformuläret ställs frågor för att fånga denna nivåindelning. Gemensamt för alla nivåer är alltså att de speglar en ackumulering, till exempel att en organisation på nivå 2 inte bara måste ha viss systematik i sitt arbete utan också behöver ha kommit längre i arbetet med informationssäkerhetens grunder (än en organisation på nivå 1). Frågeområdena sammanfattas nedan.

- *Nivå 1 – organisationer som har grunderna i informationssäkerhetsarbetet*
  Frågorna mäter om de grundläggande delarna i ett informationssäkerhetsarbete är på plats. Frågorna som ställs i detta avsnitt undersöker bland annat om ledningen är engagerad i informationssäkerhetsarbetet, om en inventering av informationstillgångar har genomförts, om organisationen har arbetssätt på centrala områden (som informationsklassning och riskanalys) och om medarbetarnas kunskaper har undersökts. 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 (vilket behandlas på högre nivåer).

- *Nivå 2 – organisationer som bedriver informationssäkerhetsarbetet med viss systematik (och är bättre på grunderna)*
  Frågorna fokuserar på om informationssäkerhetsarbetet sker med viss systematik. Frågorna som ställs undersöker därför om organisationen tillämpar sina arbetssätt och om de olika delarna kopplar till varandra, till exempel om säkerhetsåtgärderna bygger på en riskanalys. En del av områdena från nivå 1 utvecklas med fördjupande frågor, till exempel om medarbetarnas kunskaper. På nivå 2 är organisationen dessutom starkare på alla tidigare frågor än på förra nivån.

- *Nivå 3 – organisationer som har ett kvalificerat innehåll i informationssäkerhetsarbetet (och är bättre på grunderna och systematiken)*
  Frågorna handlar om det systematiska informationssäkerhetsarbetet har kvalificerat innehåll (bland annat utifrån MSB:s föreskrifter om informationssäkerhet för statliga myndigheter). Frågorna som ställs i detta avsnitt undersöker därför om organisationens arbetssätt är utformade på ett sätt som kan förväntas vara ändamålsenligt. På nivå 3 är organisationen dessutom starkare på alla tidigare frågor än på förra nivån.

- *Nivå 4 – organisationer som arbetar avancerat med ständiga förbättringar (och är bättre på grunderna, systematiken och innehållet)*
  Frågorna syftar till att fånga ett avancerat ständigt förbättringsarbete, vad gäller identifiering av hinder och framgångsfaktorer samt ledningens uppföljning. På nivå 4 uppvisar organisationen mycket höga resultat på tidigare nivåers frågor. Informationssäkerhetsarbetet karaktäriseras genomgående av systematik och ändamålsenlighet.

Modellen tar hänsyn till att olika organisationer kan behöva prioritera olika delar av informationssäkerhetsarbetet. Därför kan respektive nivå uppnås på delvis olika sätt (resultat inom ”egna prioriteringar”, jämför figur). Modellen främjar dock ett helhetsgrepp på informationssäkerhetsarbetet; organisationer som satsar på spets på bekostnad av bredd når inte modellens högre nivåer.

3.3.2 Poängberäkning

Nivåbedömningen beräknas utifrån ett poängsystem där resultatet beror på de svar som lämnas i formuläret. För att klara en viss nivå måste organisationen uppnå den nivåns totalpoäng. Totalpoängen består av dels en minimipoäng för alla frågor på den nivån, dels rörliga poäng (”egna prioriteringar”) som kan samlas på olika sätt. För varje nivå måste organisationen således dels klara grundkraven för varje fråga, dels vara bättre på några områden. Minimipoängen per fråga är liktydig med nivån som ska uppnås (till exempel behöver organisationen få 1 poäng på varje fråga på nivå 1 för att uppnå denna nivå). Rörliga poäng samlas genom bättre resultat på några frågor på samma nivå eller på andra nivåer. För varje fråga måste organisationen också göra en bedömning av huruvida den är säker på svaret eller svaren som har angetts. För att kunna ange att organisationen är säker i sin bedömning måste organisationen ha dokumenterade underlag som ligger till grund för det svar som har lämnats på frågan. Ju högre nivå, desto lägre får andelen osäkra svar vara.

Beräkningsregel för modellens nivåer

Poängkraven för respektive nivå i modellen bestäms av följande ekvation, där K_n är poängkravet för att nå nivå n och F_n är antalet frågor som poäng måste erhållas från för att kunna nå n:

$$K_n = F_n(n + 0{,}5)$$

Då antalet frågor som måste besvaras på nivå 1 är 15 så blir poängkravet där, avrundat uppåt, 15*(1+0,5)=23. F_n*0,5 är den *rörliga* poäng som krävs för att nå respektive nivå. Då det är 15 frågor som måste ge poäng på nivå 1 så krävs det alltså, avrundat uppåt, 15*0,5=8 rörliga poäng för att klara nivå 1. F_n*n är därmed *minimipoängen* som krävs för att nå respektive nivå (15, på nivå 1).

3.3.3 Automatisk återkoppling

Modellen genererar en automatisk nivåbedömning av organisationens systematiska informationssäkerhetsarbete utifrån ifyllda svar, tillsammans med en beskrivning av vad det innebär. Nivåbedömningen presenteras tillsammans med ”snabba fakta”, bland annat om hur många poäng respektive säkra bedömningar som behövs för att nå nästa nivå. En indikation om hur resultatet förhåller sig till MSB:s föreskrifter för statliga myndigheters informationssäkerhet lämnas också. För organisationer som inte nått upp till nivå 1 ingår dessutom en mer framåtblickande återkoppling, baserat på svar om pågående utvecklingsarbeten som kan bidra till nivåhöjning vid nästa uppföljning.

Modellens nivåbedömning beror av svaret på alla frågor, inte av en sammanvägning av resultat på olika områden. Dock genereras en indikativ nivåbedömning för tio olika arbetsområden (se figur): 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.

I separata avsnitt lämnas mer detaljerad återkoppling om arbetet inom de olika områdena, tillsammans med hänvisningar till var det finns stöd om hur arbetet kan utvecklas (till exempel relevanta delar av Metodstödet eller enskilda vägledningar).

Slutligen ges en detaljerad sammanställning om vilka frågor som organisationen behöver få ett högre resultat på för att avancera till nästa nivå i modellen.

3.3.4 Användning av modellen

Uppföljningen lanseras i form av en excelfil tillsammans med ett brev till organisationens ledning, som förväntas fördela arbetet med att hålla ihop arbetet med svaret. MSB rekommenderar att informationssäkerhetssamordnaren eller motsvarande får uppgiften. För att svara på frågorna behövs dock underlag från olika delar av organisationen, vilket kan behöva inhämtas i exempelvis workshop-format om informationen inte redan finns samlad. Det samlade svaret bör förankras hos ledningen. Allt detta framgår av den fördjupningsinformation som följer med frågeformuläret, där uppföljningsmodellen också förklaras i mer detalj (till exempel vad som menas med systematiskt informations-säkerhetsarbete, hur nivåindelningen fungerar och hur inrapportering till MSB genomförs på ett säkert sätt).

En viktig omständighet som också lyfts fram i fördjupningsinformationen är att samtliga frågor inte behöver besvaras för att få ett resultat. Det är för att även organisationer som inte har kommit så långt i informationssäkerhetsarbetet, och därför väljer att inte svara på alla frågor, ska kunna dra nytta av uppföljningsmodellen.

Återkopplingen i modellen är grafiskt utformad så att den enkelt ska kunna användas som underlag vid exempelvis Ledningens genomgång.

3.3.5 Validering

Det är centralt att säkerställa att frågorna som ställs i modellen är rätt utformade utifrån sitt syfte, det vill säga att de ger en så korrekt bild som möjligt av på vilken nivå

organisationens informationssäkerhetsarbete befinner sig. Modellens ändamålsenlighet valideras därför genom särskilda valideringsfrågor. Dessa frågor mäter sådana faktorer som bedöms indikera att det systematiska informationssäkerhetsarbetet har givit önskat resultat. Ett exempel på en sådan fråga är: ”Hur många informationssäkerhetsincidenter, av det totala antalet som har inträffat hos er organisation de senaste två åren, hade identifierats i organisationens analys av informationssäkerhetsrisker?”. Organisationer som över tid avancerar till högre nivåer i modellen förväntas, allt annat lika, att få bättre resultat inom några eller alla av de aspekter som valideringsfrågorna handlar om. Valideringsfrågorna kan även användas av organisationen i dess eget uppföljningsarbete, genom att ge en lägesbild över säkerhetsarbetet utifrån ett antal nyckeltal. Den bild av informationssäkerheten hos organisationerna som valideringsfrågorna ger möjliggör också för MSB att ta fram bättre stöd till aktörerna. Ett exempel är att det över tid kommer att bli möjligt att se om och i så fall hur förändringen i svaren på valideringsfrågorna mellan två mättillfällen korrelerar med svaren på de nivågrundande frågorna.

3.3.6 Avgränsningar och avvägningar i utvecklingen av modellen

Som redovisades i kapitel 2 avgränsas modellen till att omfatta det systematiska arbetet med informationssäkerhet, inte den faktiska informationssäkerheten i organisationen. Avgränsningen är en direkt följd av uppdraget. Modellen mäter därmed (bland annat) hur en organisation arbetar med att bilda sig en bättre uppfattning om den egna säkerhetssituationen, hur organisationen vid behov tar vad den vet om sin säkerhetssituation och agerar för att förbättra läget – och hur organisationen sedan följer upp vad som gjorts och därmed kan dra nya slutsatser om sin säkerhetssituation. Modellen undersöker däremot inte vilket skydd som finns, såsom vilka specifika säkerhetsåtgärder som vidtagits. Detta är en viktig avgränsning.

Vidare avgränsas modellen i så måtto att det systematiska informationssäkerhetsarbetet följs upp på strategisk nivå. Modellen följer inte upp arbetet på operativ eller taktisk nivå. Med det menas att den mäter arbetet över längre perioder (två år) och att den är övergripande och holistisk i sitt innehåll, snarare än detaljerad och specifik. Modellen kan med fördel kombineras med annan uppföljning som närmare följer exempelvis det månadsvisa, veckovisa eller dagliga arbetet.

Utöver dessa principiella avgränsningar, har utvecklingsarbetet av uppföljningsmodellen inneburit några viktigare vägval. Inte sällan har synpunkterna från referensgruppen och pilotomgången fällt avgörandet (kap. 4.2). Några sådana avvägningar beskrivs här.

Fokus på jämförbara fakta

För att samla in så mycket användbar och jämförbar information som möjligt syftar frågeformuleringen i uppföljningsmodellen till att minimera inslaget av subjektivitet. Frågorna är konstruerade utifrån en strävan att så långt det är möjligt vara faktabaserade och undvika värdeomdömen. Exempelvis så undviks frågor där organisationen ska bedöma om någon åtgärd har utförts i ”tillräcklig” utsträckning. En mindre tolkningsvidd

ger mer rättvisande resultat, särskilt i bedömningen av den samlade nivån inom offentlig förvaltning.

Nackdelen med att ställa frågor på det här sättet är att de blir svårare att svara på. Det är ofta svårare att svara på hur stor andel av medarbetarna som genomgått utbildning, än om nödvändig utbildning genomförts ”i viss utsträckning, i tillräcklig utsträckning…” (eftersom man väljer själv vad det innebär). För att förenkla mätbara, kvantitativa bedömningar när osäkerhet råder, medger uppföljningsmodellen breda svarsintervall. Fokus har också lagts på att bara fråga om sådant som rimligen går att mäta.

Det ska dock noteras att en viss tolkningsvidd inte går att undvika och att detta måste beaktas i analysarbetet och jämförelser mellan olika organisationer.

”Andel av verksamheter”

Med hänsyn till behovet av mätbarhet används ofta andel av verksamheter i frågor som handlar om i vilken utsträckningen något tillämpas. Det är ett trubbigt mått, men har bedömts som den bästa lösningen i valet mellan att mäta något som är svårt att kontrollera för men ger en hög precision om man lyckas, eller något som är enklare att kontrollera för men som ger en lägre precision. Exempelvis vore det intressant att veta hur stor andel av alla informationstillgångar som har klassats i en organisation, men det är nästan omöjligt att svara på; därför ställs i stället frågan om informationsklassning har genomförts – med svarsalternativ som anger andel av organisationens verksamheter.

I modellen definieras verksamheter som de största organisationsindelningarna i kommuner, regioner och statliga myndigheter. Inom en kommun skulle verksamhet exempelvis kunna förstås som en förvaltning.

Tvåårsperioden

Frågan om mätperiod är viktig i alla undersökningar. Vanligtvis görs en distinktion mellan lägesbild och uppföljning. Är det förhållanden i ögonblicket som är intressant, eller förhållanden över tid? En organisations informationssäkerhet är resultatet av arbete och val under en längre tid, däribland de stöd, regelverk och övriga komponenter som organisationen har haft på plats under den tiden. Därför har det inte bedömts meningsfullt att mäta läget endast vid svarstillfället. Uppföljningen behöver också säkerställa jämförbarhet över tid och kunna visa på trender. För att medge sådan analys behöver mätperioden överensstämma med uppföljningens periodicitet. Sammantaget bedöms en tvåårsperiod vara lämplig; uppföljningen sker då tillräckligt ofta för att inte missa viktigare skiftningar mellan mättillfällena, samtidigt som hänsyn tas till resursåtgången hos medverkande organisationer och hos MSB. Genom en tvåårsperiod finns också samordningsmöjligheter med statliga myndigheters risk- och sårbarhetsanalys.

En nackdel med en utsträckt mätperiod kan vara att det blir svårare att svara på frågorna och att resultatet blir tillbakablickande (en nyutvecklad informationssäkerhetspolicy ger inte utslag i nivåbedömningen, till exempel). Det förstnämnda mildras genom att ett svar kan markeras som osäkert (om det inte går att belägga inom organisationen att ett

arbetssätt faktiskt funnits i två år). Vissa frågor är också utformade så att det räcker att en aktivitet genomförts en gång de senaste två åren. Resultatets tillbakablickande karaktär balanseras genom att det på vissa frågor går att ange att något funnits i kortare tid än två år eller håller på att utvecklas; sådana resultat visas också i den framåtblickande återkopplingen för organisationer som inte når nivå 1.

Nivåindelningen och verkligheten

Uppföljningsmodellens nivåer har som tidigare nämnts utformats för att motsvara ett stegvis utvecklingsarbete. På så sätt försöker nivåindelningen fånga verkliga förhållanden (till exempel att ett arbetssätt för informationsklassning utvecklas innan klassningen genomförs). Samtidigt är nivåerna idealistiska i så måtto att de utgår från en normerad bild av vad systematiskt informationssäkerhetsarbete bör innehålla. Enligt MSB:s bedömning är det viktigt att alla organisationer åtminstone når upp till nivå 1 – grunderna i informationssäkerhetsarbetet – samtidigt som man bör sträva högre (de som omfattas av MSB:s föreskrifter behöver åtminstone nå nivå 3). Dock bedömer MSB att en stor andel av den offentliga förvaltningens organisationer, framför allt kommuner, inte kommer att nå upp till nivå 1 i den första uppföljningen. En del av dessa organisationer bedöms hamna under nivå 1 av skäl som kan hänföras till modellens specifika normering och krav på bredd i informationssäkerhetsarbetet (till exempel kanske en undersökning av medarbetarnas kunskaper är det enda som saknas); här kan alltså en nivåhöjning ske till nästa tvåårscykel. Organisationer som har valt att satsa på några områden kan få höga resultat på dessa samtidigt som låga resultat på ett eller flera andra områden gör att nivån i modellen anges som låg. Ett stort antal organisationer bedöms dock ha ett mer omfattande utvecklingsarbete framför sig innan de når nivå 1, givet vad tidigare undersökningar visat.

Ett problem med ett sådant utfall – utöver den låga nivån i sig – är att den som arbetar med informationssäkerhet i organisationen kan bli modfälld. Snarare än att sänka ambitionen och justera modellen, är det viktigt att MSB och övriga berörda myndigheter främjar en positiv och bejakande uppföljningskultur. Kommunikationen kring uppföljningen, liksom användningen av resultaten, bör präglas av en framåtblickande ansats, där det ses som positivt att organisationer medverkar och på så sätt stärker sitt förbättringsarbete.

Det bör noteras att värdet av återkopplingen för organisationen inte blir mindre av en låg nivåbedömning. Indikativ nivå inom enskilda arbetsområden, liksom den mer detaljerade återkopplingen, genereras på samma sätt även om en organisation till exempel inte når nivå 1.

3.4 Analysarbetet

MSB:s analys av de inrapporterade underlagen vidtar efter att tidsfristen för svar löpt ut (oktober).

Den *kompletterande återkopplingen till medverkande organisationer* bör idealt inte dröja mer än ett par månader (december). Tidsåtgången beror på antalet organisationer som har rapporterat till MSB, hur individuellt anpassad återkopplingen ska vara, hur mycket material den ska

omfatta, samt MSB:s resurser. Hur detaljerad benchmarking som kan tas fram beror också på antalet organisationer som har rapporterat till MSB. Om det exempelvis bara är enstaka kommuner som rapporterar till MSB så kanske benchmarking för de organisationerna bara kan göras gentemot hela den inrapporterande mängden kommuner. Om det är många kommuner som har rapporterat till MSB så kan benchmarking bland kommuner också göras mellan kommuner som liknar varandra på olika sätt. Till exempel kan medelstora svenska kommuner, eller kommuner i Småland, eller storstadsnära kommuner benchmarkas om mängden inrapporterande kommuner är stor.

Utöver en kompletterande återkoppling enligt ovan, kan det också finnas skäl för MSB att lämna mer individualiserat stöd i undantagsfall. Om till exempel stora utmaningar påvisas hos en myndighet med nationellt samhällsviktig verksamhet kan MSB välja att stödja den myndigheten enskilt.

Den *samlade bedömningen till regeringen* bedöms kunna lämnas efter ytterligare ett par månader (i mars månad det andra året i tvåårscykeln). I framtagningsarbetet ingår analys, rapportskrivning, kvalitetssäkring och beredning.

I analysen av sammanställningen av svaren kommer MSB att kunna redovisa på vilken nivå de rapporterande organisationerna befinner sig och vilka som är de vanligaste utmaningarna och styrkorna i deras systematiska informationssäkerhetsarbete. Det bör därutöver vara möjligt att finna kopplingar mellan olika områden där typiska brister finns, och som kanske inte har noterats av de inrapporterande organisationerna själva.

MSB bör utifrån den samlade analysen även kunna redogöra för ett antal av datan motiverade åtgärder som myndigheten själv kan genomföra för att hjälpa organisationer att förebygga eller hantera vanliga problem och brister. Vidare bör MSB kunna lämna rekommendationer till regeringen om satsningar som skulle kunna göras för att stärka det systematiska informationssäkerhetsarbetet på olika sätt.

Det kan noteras att även värdet av analysen är helt avhängigt hur stor del av den offentliga förvaltningens organisationer som medverkar och rapporterar in sina resultat till MSB.

Under återstoden av tvåårscykeln arbetar MSB med *utveckling av myndighetens stöd* på grundval av dragna slutsatser, samt med eventuella *justeringar av uppföljningsstrukturen, eller specifikt uppföljningsmodellen,* utifrån behov som har identifierats under analysfasen och i återkoppling från medverkande organisationer. Ändringar i modellen måste övervägas noggrant då de kan försvåra jämförelser med resultat från tidigare mättillfällen och därmed måste kvalitetssäkras och beredas noga. Ändringar måste också införas på ett väl genomtänkt sätt för att ge de medverkande organisationerna rättvisa förutsättningar både i uppföljningen och i sitt utvecklingsarbete över tid.

4. Beskrivning av uppdragets genomförande

4.1 Ändrade förutsättningar – ändrad tidsplan

Enligt regeringsuppdraget skulle uppföljningen genomföras under 2020 och en första samlad bedömning lämnas till regeringen i samband med uppdragets redovisning i mars 2021.

På grund av covid-19-pandemins belastning på den offentliga förvaltningen och delvis på MSB bedömdes det inte lämpligt att lansera uppföljningen som planerat, varför tidsplanen justerades och lanseringen sköts upp till 2021. Förseningen medförde dock några fördelar för uppdragets genomförande: uppföljningsmodellen som utvecklats är väsentligt mer genomarbetad och bättre rustad att fungera över tid, och den praktiska hanteringen runt den storskaliga uppföljningen kan planeras och lösas på ett mer hållbart sätt. Vidare kan modellen verifieras och förbättras genom två pilotomgångar.

En samlad bedömning av nivån på den offentliga förvaltningens systematiska informationssäkerhetsarbete, jämte en bedömning av hur MSB:s stöd kan utvecklas, kommer att lämnas 2022 efter att lanseringen genomförts som del av uppföljningsstrukturens första tvåårscykel.

4.2 Dialog och samverkan

När en produkt som träffar en så stor och mångfacetterad målgrupp som hela den offentliga förvaltningen ska tas fram, måste den vara väl förankrad. Det gäller särskilt som ämnesområdet informationssäkerhetsarbete i sig är komplext.

Därför har MSB i utvecklingsarbetets olika faser haft dialog med företrädare för statliga myndigheter, kommuner och regioner samt flera andra relevanta aktörer. Dels har en referensgrupp lämnat synpunkter på förslaget till uppföljningsstruktur, dels har modellen verklighetstestats inom ramen för en pilotomgång.

Referensgruppen bidrog med mycket värdefull återkoppling på olika aspekter av det dåvarande förslaget till uppföljningsstruktur. Utöver ett stort antal mindre justeringar ledde granskningen bland annat till att innehållet i nivå 4 ändrades (från totalförsvar till avancerat arbete med ständiga förbättringar) och att nivåbeskrivningarna/avancemangsordningen förtydligades. I referensgruppen ingick företrädare från Pensionsmyndigheten, Skolverket, Ekonomistyrningsverket, Säkerhetspolisen, Länsstyrelsen i Uppsala län, Huddinge kommun, Simrishamn kommun, Region Västerbotten och Region Östergötland.

Pilotomgången gav bekräftelse på att upplägget och utformningen i stort fungerar även för en organisation som inte har bakgrundsinformation om regeringsuppdraget eller uppföljningsstrukturen. Några av deltagarna noterade att de hamnat lågt i nivåbedömningen jämfört med sin egen bild. Det var i grunden väntat att många organisationer inte kommer att nå särskilt högt (jämför kap. 3.3.6). För att ge medverkande organisationer realistiska förväntningar och ett konstruktivt intryck även vid lägre resultat justerades vissa beskrivningar i stödmaterialet. Dessutom kompletterades återkopplingen i

modellen med en framåtblickande komponent för organisationer som inte nått nivå 1. I pilotomgången deltog företrädare från Stockholms universitet, Upphandlingsmyndigheten, Region Halland, Västra Götalandsregionen, kommunerna Mariestad/Töreboda/Gullspång och Skellefteå kommun.

Utöver referensgruppen och pilotomgången har löpande dialog förts med Sveriges Kommuner och Regioner samt samverkan genomförts med Myndigheten för digital förvaltning. En auktoriserad certifieringsrevisor för standardserien ISO/IEC 27000 har också lämnat synpunkter på förslaget till uppföljningsstruktur.

Slutligen har MSB i olika sammanhang informerat om utvecklingsarbetet i nätverken Snits, HoSIS och KIS (informationssäkerhetssamordnare vid statliga myndigheter, inom hälso- och sjukvården respektive i kommunerna), i Samfi (Samverkansgruppen för informationssäkerhet, myndigheter med av regeringen särskilt utpekat ansvar för informationssäkerhetsfrågor i samhället) samt i Informations- och cybersäkerhetsrådet (med representation från både offentlig förvaltning, akademi och näringsliv).

Genom hela processen har initiativet som sådant fått mycket positiv respons. Behovet av denna typ av stöd har framgått tydligt. MSB:s förslag till uppföljningsstruktur har också bemötts övervägande positivt. Både synpunkter som har inneburit en förfining av MSB:s förslag och sådana som pekat delvis i annan riktning (till exempel en mer säkerhetsåtgärdsnära uppföljning) har varit mycket värdefulla i utvecklingsarbetet.

4.3 Kommande arbete

4.3.1 Pilotomgång 2

En andra pilotomgång är planerad till våren 2021, då uppföljningen kommer att genomföras på samma sätt som vid lansering men i mindre skala. Utöver själva uppföljningsmodellen omfattar detta bland annat test av en sambandslösning för säker kommunikation med de medverkande, samt test av MSB:s analysupplägg.

Till denna pilotomgång kommer ytterligare representanter för statliga myndigheter, kommuner och regioner att bjudas in. Syftet är att öva hela förfarandet samt att identifiera och lösa eventuella problem inför det första fullskaliga genomförandet.

4.3.2 Lansering och efterarbete

Lansering till hela den offentliga förvaltningen planeras preliminärt till början av sommaren 2021, med svarstid ca fyra månader. Kommunikationen om uppföljningen kommer att utvecklas inför lanseringen, för att stimulera till medverkan och stödja organisationernas arbete med att använda uppföljningsmodellen. När medverkande organisationer lämnat sina underlag vidtar analysen av svaren, vilken ligger till grund för den kompletterande återkopplingen till organisationerna, den samlade bedömningen till regeringen, samt till förslag om vidareutveckling av uppföljningsstrukturen och MSB:s övriga stöd på området (se vidare kap. 3.2).

Som nämnts ovan kommer utskick av kommande versioner av uppföljningen troligen att genomföras något tidigare på året. På så sätt kan de organisationer som inleder sin verksamhetsplanering under våren, om de så önskar, slutföra uppföljningen innan planeringsarbetet vidtar. MSB:s ambition är att så långt som möjligt ge organisationerna utrymme att genomföra uppföljningen vid den tidpunkt de själva finner bäst, utifrån egen bedömning om när verksamhetsnyttan blir som störst. Samtidigt behöver MSB få in rapporteringen på ett sammanhållet sätt för att kunna göra en meningsfull analys. Sammantaget bedöms det därför lämpligt att lansera uppföljningen tidigt på året (förslagsvis i mars), med svarsfrist satt till en bit in på hösten (oktober).

5. Möjlig vidareutveckling av uppföljningsstrukturen

I regeringsuppdraget ingår att beskriva hur uppföljningsstrukturen kan vidareutvecklas. Även om det ännu saknas ett resultat att reflektera utifrån, har ett inledande analysarbete genomförts kring potentiella utvecklingsområden som skulle kunna övervägas i framtiden:

- Hur en hög inrapporteringsfrekvens kan säkerställas.
- Automatisk återkoppling om hur en enskild organisations resultat förhåller sig till organisationens resultat från tidigare mättillfällen.
- Andra nya funktioner i modellen (till exempel filtrering, mer granulära råd, stöd för riskanalys).
- Bilagefunktion avseende säker bedömning.
- Teknisk plattform för uppföljningen.
- Uppföljning av budgetering, kostnader och investeringar
- Uppföljning av it-säkerhet.

När det gäller *inrapporteringsfrekvensen*, det vill säga att organisationerna inte bara använder uppföljningsmodellen utan även skickar in sina svar till MSB, är det centralt att säkerställa en hög andel. Ett fullödigt underlag för MSB:s analysarbete möjliggör mer välgrundade bedömningar och åtgärdsförslag till regeringen samt ger bättre förutsättningar för utveckling av stöd till målgruppen. Bland de vägar till ökad inrapportering som har analyserats kan nämnas införande av rättslig reglering som gör det obligatoriskt för organisationer att rapportera in svar. Eftersom konsekvenserna av låg inrapporterings-frekvens blir påtagliga för möjligheten att få en rättvisande bild av informations-säkerhetsarbetet i offentlig förvaltning kan det finnas anledning till sådan formell kravställning. Detta skulle exempelvis kunna ske i form av att krav på att redovisa sin informationssäkerhet med stöd av uppföljningsmodellen införs i statliga myndigheters regleringsbrev. Ett annat sätt som kan övervägas är att knyta uppföljningsstrukturen närmare redan etablerade uppföljningsprocesser. Det handlar exempelvis om att utreda möjligheten att låta uppföljningsstrukturen utgöra ett verktyg i processen att rapportera om informationssäkerhet i risk- och sårbarhetsanalyser i enlighet med förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Om krav på inrapportering ska övervägas så bör det beaktas att MSB inte har någon tillsynsuppgift kopplad till vare sig föreskrifterna för statliga myndigheter eller NIS-föreskrifterna.

I dagsläget är modellens implementation kapabel att omedelbart och automatiskt återkoppla vilken nivå i modellen en organisation befinner sig på, huruvida de lämnade svaren indikerar att organisationen klarar kraven i MSB:s föreskrifter om informationssäkerhet hos statliga myndigheter, samt hur långt organisationen har kommit inom tio delområden i det systematiska arbetet, med mera. Den återkopplingen baseras dock enbart på de svar som har lämnats vid det aktuella mättillfället. Medverkande organisationer kan också antas ha ett intresse av att kunna få en *automatiskt genererad jämförelse som visar vilken utveckling som har skett från ett mättillfälle till ett annat*.

Bland *övriga funktioner* som MSB har identifierat som intressanta ingår att kunna filtrera de nivågrundande frågorna så att organisationer snabbt kan titta på alla och enbart de frågor (och eventuellt även enskilda svarsalternativ) som kopplar till ett visst arbetsområde (exempelvis informationsklassning). En annan funktion som skulle kunna utvecklas är mer detaljerad återkoppling om hur organisationen på ett resurseffektivt sätt kan uppnå högre nivåer i modellen. En tredje identifierad funktion, eller snarare grupp av funktioner, är automatiserade stöd med koppling till företeelser som modellen berör. Det kan handla om automatiserat stöd för riskanalys (som innehåller sådant som en organisation kan få poäng för i de nivågrundande frågorna) eller automatiserat stöd för att samla risker och incidenter på ett översiktligt sätt (så att det blir lätt att kontrollera hur många inträffade incidenter som faktiskt hade förutsetts i organisationens riskanalys).

Uppföljningsmodellen skulle på sikt även kunna kompletteras med en *bilagefunktion* kopplat till angivandet av säker bedömning. Om en organisation till exempel har fyllt i att den har en informationssäkerhetspolicy på plats med visst innehåll, och att bedömningen är säker, skulle den kunna ombedjas att bilägga dokumentet. Det skulle bland annat bidra till valideringen av modellens träffsäkerhet.

Utöver uppföljningens innehåll och utformning skulle möjligheten att använda en anpassad *teknisk plattform* för arbetet kunna göra stor skillnad för insamling, analys av resultat och återkoppling.

Det skulle kunna övervägas att inkludera *budgetering, kostnader och investeringar* i uppföljningen. Genom att mäta vilka resurser organisationer lägger på informationssäkerhetsarbetet, och på vilket sätt, skulle det gå att undersöka samband med nivån på arbetet och även dess effekter. På sikt skulle det kunna ge en indikation om hur olika budgeterings- och investeringsstrategier leder till olika resultat i modellens uppföljning.

Slutligen skulle det även kunna övervägas att inkludera *it-säkerhet* på ett mer genomgripande sätt i uppföljningsmodellen, eller att skapa en ny modell i detta syfte. Som redovisats avser uppföljningen inom ramen för detta uppdrag det systematiska informationssäkerhetsarbetet på en strategisk nivå. Denna systematik ska, genom resultat i organisationens riskbedömning och informationsklassning, resultera i att tekniska säkerhetsåtgärder införs i it-miljön. Samtidigt lägger MSB och andra myndigheter ökat fokus på normering och stöd avseende säkerhetsåtgärder, utifrån en bedömning om att tillräckliga tekniska säkerhetsåtgärder inte vidtas och att enskilda organisationer har svårt

att omsätta identifierade globala och nationella risker till faktiska säkerhetsåtgärder. MSB har föreskrivit om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7) samt tagit fram en stödjande vägledning. Dessutom har deltagande myndigheter[11] i etableringen av det nationella cybersäkerhetscentret tillsammans tagit fram rapporten Cybersäkerhet i Sverige – Rekommenderade säkerhetsåtgärder (2020). Värdet av ett uppföljningsstöd avseende säkerhetsåtgärder har lyfts av en del organisationer i kontakt med MSB.

6. Slutsatser

Utvecklingsarbetet inom ramen för det här uppdraget har bekräftat den bredd, och ibland brokighet, som kännetecknar informationssäkerhetsarbetet inom offentlig förvaltning. Att olika organisationer har olika förutsättningar och behov är inte oväntat. Men även bortsett från sådana faktorer, har det blivit tydligt att arbetet inom det offentliga Sverige är långt ifrån är enhetligt. Centrala begrepp som systematik, risk, hot och sårbarhet förstås ofta olika, vilket naturligen medför utmaningar på samhällsnivå.

MSB:s uppföljningsstruktur har fördelen att den kan vara lite mer handfast än en föreskrift och samtidigt mer normsättande än en enskild vägledning. Den ska omfatta alla kommuner, regioner och statliga myndigheter samlat. En nationell uppföljning av detta slag, som genomförs återkommande, har potential att fungera som styrning, utöver som stöd och mätning. På sikt kan uppföljningsstrukturen därmed bidra inte bara till förbättring, utan även bringa mer enhetlighet i hur vi gemensamt bedriver ett systematiskt informationssäkerhetsarbete. Ytterst gagnar detta såväl skyddet av medborgarnas information som den offentliga förvaltningens funktion, vilket även är av värde ur ett totalförsvarsperspektiv.

En sådan positiv utveckling förutsätter dock tre saker:

- *Ett brett deltagande av den offentliga förvaltningens organisationer*. Uppföljningsstrukturen bygger på samskapande, där den enskilda organisationen får ett underlag till förbättringar och även bidrar till utveckling på nationell nivå. Om uppföljningen ska fungera som normsättande och generera ett tillräckligt analysunderlag för den samlade bedömningen, behöver en stor del av den offentliga förvaltningen medverka. En grundförutsättning är att uppföljningsstrukturen skapar mervärde för medverkande organisationer (användarvänlighet, relevans, återkoppling med mera). Men det är inte nödvändigtvis tillräckligt för att uppnå ett brett deltagande. En ambitiös informations-säkerhetssamordnare kan hållas tillbaka av bristande förutsättningar, författningskrav och annan viktig verksamhet kan behöva gå före, eller insikten om mervärdet kan av olika skäl saknas. Därför bör andra incitament också övervägas för att signalera vikten av att genomföra uppföljningen och rapportera in svaren (jämför kap. 5).

[11] Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen.

- *En positiv och bejakande uppföljningskultur.* Förbättring på informationssäkerhetsområdet kan ta tid, kräva genomgripande åtgärder i verksamheten och medföra obehagliga insikter längs vägen. På samma sätt som en välfungerande incidentrapportering bygger på att anmälning premieras, bör resultaten i uppföljningsstrukturen bemötas positivt från MSB och övriga berörda myndigheter. MSB bedömer att en stor andel av den offentliga förvaltningen inte kommer att nå upp till modellens nivå för grundläggande informationssäkerhetsarbete. Både i kommunikationen kring uppföljningen och hur resultaten faktiskt används bör perspektivet vara att bidra till ständiga förbättringar snarare än att döma svaga resultat.

- *Resurssättning av identifierade förbättringsområden.* Utifrån uppföljningen kommer brister och utmaningar i informationssäkerhetsarbetet att kunna identifieras, både i den enskilda organisationen och inom den offentliga förvaltningen som helhet. En del kan troligen åtgärdas utan särskilda kostnader. Men många förbättringar torde förutsätta investeringar i kompetenshöjande åtgärder, utvecklade stöd, nya system och så vidare. Effekten av uppföljningsstrukturen är således även avhängig att förbättringsarbetet resurssätts, inklusive på central nivå.

Bilaga 1: Regeringens uppdrag till MSB

Regeringen

Kopia
Regeringsbeslut **II:11**

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

Justitiedepartementet

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad

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.

Telefonväxel: 08-405 10 00
Fax: 08-20 27 34
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Rosenbad 4
E-post: ju.registrator@regeringskansliet.se

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).

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984

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.

På regeringens vägnar

Mikael Damberg

Joel Mård Larsson

Kopia till

Myndigheten för digital förvaltning
Sveriges kommuner och landsting (SKL)
Statsrådsberedningen/SAM
Justitiedepartementet/L4, PO
Försvarsdepartementet/SUND, MFI
Socialdepartementet/FS, FST
Finansdepartementet/BA, OFA K, OFA SFÖ
Infrastrukturdepartementet/D, DF

3 (3)

Bilaga 2: Internationell utblick

Internationell utblick – internationella modeller och ramverk för uppföljning och utvärdering av informations- och cybersäkerhet

I arbetet med att utveckla en struktur för uppföljning av den offentliga förvaltningens systematiska informationssäkerhetsarbete har befintliga internationella modeller och ramverk på området studerats. Syftet har varit att utnyttja internationella erfarenheter om hur organisationer kan använda sig av mätverktyg och modeller för att utvärdera och öka sin informations- och cybersäkerhet. Internationellt finns ett stort antal modeller och ramverk på området. För att begränsa studieområdet har modeller, utvärderingsverktyg och ramverk valts som riktar sig till organisationer och mindre aktörer, vilket utesluter modeller som används i utvärderandet av ett lands eller en regions cybersäkerhetsförmåga. Avsnittet ger inledningsvis en övergripande beskrivning av de standarder som ligger till grund för flertalet modeller. Vidare beskrivs ett antal utvalda modeller/ramverk från olika länder för att visa på deras olika inriktningar och utformningar.

Standarder

Det amerikanska standardiseringsorganet *National Institute of Standards and Technology* (NIST), däribland säkerhetsåtgärderna i NIST SP 800-53, och den fristående organisationen *International Organization for Standardization* (ISO), där specifikt 27000-serien berör informationssäkerhet, ligger ofta till grund för utformandet av modeller och ramverk på området. De behöver inte vara ömsesidigt uteslutande, utan kan fungera som komplement till varandra. Förenklat kan sägas att NIST utgår mer från säkerhetsåtgärder, medan ISO fokuserar mer på risk och systematiskt arbete, från ledningen ut i organisationen. Båda är tongivande inom informationssäkerhet, men med olika geografisk spridning. ISO-standarden är redan etablerad i svensk offentlig förvaltning sedan länge. En anledning är att MSB:s föreskrifter om informationssäkerhet för statliga myndigheter pekar på standarden.

NIST har även utvecklat ett cybersäkerhetsramverk för självutvärdering, *NIST Cybersecurity Framework* med syftet att användas av organisationer som vill hantera och reducera effekterna av cybersäkerhetsrisker. Ramverket skapades initialt för aktörer inom kritisk infrastruktur, men kan användas av både privata och offentliga aktörer inom varierande sektorer. Till skillnad från ISO/IEC 27000-serien är *NIST Cybersecurity Framework* en gratistjänst.[12]

I ISO/IEC 27000-serien ingår också en standard för mätning av informationssäkerhet (27004), som stödjer den utvärdering av ett ledningssystem för informationssäkerhet som ska göras enligt kraven i 27001. Detta omfattar mätning och övervakning av informationssäkerheten såväl som informationssäkerhetsarbetet, samt analys och utvärdering av resultaten. I standarden beskrivs hur en organisation kan planera och utforma sin utvärdering: vad, hur och när övervakning/mätning kan ske samt hur processer för detta kan tas fram. En mätningsstandard i NIST-serien återfinns i 800-55.

Modeller och ramverk

De modeller och ramverk som redovisas nedan är utvalda för att kunna appliceras på mikronivå, såsom inom organisationer eller avgränsade branscher. De är antingen utvecklade på departements- eller myndighetsnivå och har således fått stor spridning både nationellt och internationellt. *NIST Cybersecurity Framework* beskrivs förhållandevis ingående då det ligger till grund för majoriteten av de modeller som utvecklas under senare tid.

[12] MSB tillhandahåller ISO/IEC 27001 och 27002 till kommuner och länsstyrelser utan kostnad.

NIST Cybersecurity Framework

Detta ramverk utvecklat av det amerikanska standardiseringsorganet NIST är ett riskbaserat sätt för organisationer att själva utvärdera och hantera cybersäkerhetsrisker. Ramverket bör inte ses som strikta riktlinjer, utan snarare som en guide som anpassas efter varje organisations behov och förutsättningar. Målet med modellen är att underlätta för organisationer att:

1. Beskriva sin nuvarande cybersäkerhetsstatus
2. Beskriva sina mål inom cybersäkerhet
3. Identifiera och prioritera bland förbättringsmöjligheter inom ramen för en kontinuerlig och systematisk process
4. Utvärdera framstegen mot att nå målen
5. Kommunicera mellan interna och externa intressenter gällande cyberrisker [13]

Ramverket består av tre delar: *Framework Core* (kärnan), *Framework Implementation Tiers* (implementeringsnivåerna) och *Framework Profiles* (profilerna).

Kärnan består i sin tur av fem funktioner som illustrerar en organisations cykel gällande hantering av cyberrisker: *Identify, Protect, Detect, Respond and Recover*. Funktionerna behöver inte följas i en specifik ordning utan ska snarare ses som övergripande områden som formar ett systematiskt arbete med cybersäkerhet. Under de fem funktionerna finns kategorier som utgör delområden för varje funktion. Efter kategorierna följer ett antal underkategorier som ger exempel på konkreta säkerhetsåtgärder en organisation kan vidta. Den sista delen av ramverket är den informativa referensen som ger exempel på stöd i existerande standarder (best practice) för att fördjupa kunskapen inom varje underkategori där bland annat ISO-serien och NIST:s standarder rekommenderas.

Ramverket fokuserar på externa cybersäkerhetshot och de medföljande risker detta innebär: det vill säga, det är huvudsakligen antagonistiska cyberrisker som avses.[14] Cybersäkerhet beskrivs som en viktig del av organisationens övergripande riskarbete. Syftet är att på ett kostnadseffektivt sätt hantera de cyberrelaterade risker som kan uppstå och det rekommenderas att följa redan existerande standarder och rutiner för att ha ett robust system. Dock bör modellen anpassas efter en organisations individuella risker och således inte ses som en generell checklista.

Ramverkets andra del, implementeringsnivåerna, skapar en möjlighet för organisationer att avgöra hur de ser på cybersäkerhetsrisker samt en utvärdering av de existerande processerna för att hantera dessa risker. Graderna delas in i fyra nivåer från Delvis (nivå 1) till Adaptiv (nivå 4) och är ramverkets mätningsdel. Organisationen bör utgå från existerande processer gällande bland annat riskhantering, juridik och hotbild för att kartlägga hur förmågan kan höjas. Nivåerna innebär inte mognadsgrad, utan snarare ett tydliggörande av vilka områden som prioriteras, vilket i sin tur kan bidra till förmågehöjning. Att nå en högre nivå uppmuntras om det anses kostnadseffektivt för den enskilda organisationen och om det i sin tur bidrar till en minskning av cybersäkerhetsrisker.

Den sista delen av ramverket, profilerna, beskriver inriktningen som organisationen valt från ramverkets kategorier och underkategorier. Profilen kan användas som ett sätt att se hur väl organisationen följer de standarder och riktlinjer som presenteras under ramverkets kärna (Core). Profilen kan även användas för att ge organisationen en överblick över hur nuvarande läge ser ut och då även visa på hur organisationen kan förbättras och nå sin ”målprofil”. Att skapa en profil görs genom att välja ut vilja underkategorier i kärnan (Core) som är mest relevanta för organisationen att följa. Den nuvarande profilen ger således en bild av organisationens utgångsläge och nuvarande kapacitet. Organisationen kan således använda

[13] https://www.nist.gov/cyberframework/online-learning/components-framework

[14] NIST definierar övergripande cybersäkerhet som: ”The ability to protect or defend the use of cyberspace from cyber attacks”.

profilen till att jämföra det aktuella tillståndet med den målbild som vill nås. Profilen bidrar till att skapa en vägledning (roadmap) som följer organisationens egna mål och visioner. Givet organisationers komplexitet finns möjligheten att använda sig av flertalet profiler som riktar sig till olika delar av organisationen. Vidare kan kategorier och underkategorier adderas efter behov för att hantera och studera organisationens risker, och de har således inte krav på att implementeras i sin helhet. Den nuvarande profilen kan sedan användas för att stödja prioritering och mätning av framsteg mot målprofilen, samtidigt som man tar hänsyn till andra behov såsom kostnadseffektivitet och innovation. Profilernas funktion kan användas för att göra självutvärderingar och kommunicera behov inom eller mellan organisationer.

Modellen används genom att 1) prioritera omfattningen, 2) välja inriktning (orient) 3) skapa en nuvarande organisationsprofil 4) genomföra en riskbedömning 5) skapa en målprofil av organisationen 6) bestämma, analysera och prioritera brister samt att 7) implementera en handlingsplan.

Framgångsrik implementering av ramverket mäts i huruvida organisationen når de mål som beskrivs i målprofilen, vilket inte nödvändigtvis korrelerar med höga värden på samtliga implementeringsnivåer. Ledningens engagemang är centralt inom ramverket (vilket även ISO-serien betonar).

Flertalet modeller använder *NIST Cybersecurity Framework* som stöd i sin utformning. Två amerikanska departement, *Department of Defence* och *Department of Energy* har båda utvecklat utvärderingsmodeller som baseras på, och kan användas med, ramverket.

The Cybersecurity Capability Maturity Model (C2M2)

Den amerikanska modellen *Cybersecurity Capability Maturity Model* (C2M2), som är utformad av det amerikanska energidepartementet, fokuserar på att mäta och förbättra en organisations cybersäkerhetsprocesser.[15] I likhet med NIST:s ramverk är C2M2 ett verktyg för självutvärdering som utvecklades för organisationer inom kritisk infrastruktur, främst inom energisektorn, men kan även användas inom ett flertal sektorer och branscher.

Med cybersäkerhetsrisk avses primärt risker av antagonistisk karaktär såsom intrång och angrepp. Ramverket beskriver att cybersäkerhetsrisker visserligen är en del av organisationens generella riskmiljö men modellen inriktar sig främst mot att säkerställa att antagonistiska risker minimeras. Syftet med modellen är att underlätta en organisations löpande utvärdering av sina cybersäkerhetsförmågor, att kunna kommunicera behov efter utvärderingen samt att tydliggöra en prioritering av cybersäkerhetsinvesteringar. Till skillnad från NIST:s ramverk beskrivs C2M2 som en modell som ingående beskriver de åtgärder en organisation behöver vidta för att nå en högre cybersäkerhetsmognad. Fördelen med en mognadsmodell som används av flera aktörer inom samma bransch är skapandet av en måttstock (benchmark) vilket innebär att en organisation kan jämföra sina resultat med andra inom samma område eller få en övergripande bild av branschen i stort.

C2M2 riktar sig främst mot områden inom information, informationsteknologi och driftsteknologi (operations technology) samt de miljöer de verkar inom. Modellen används främst i utvärderandet av informationstillgångar inom it och drift. Modellen består av tio domäner som i sin tur mynnar ut i ett antal mål. Inom dessa mål finns flertalet mognadsindikatorer, MIL (Maturity Indicator Level). Mognadsindikatorerna finns i fyra nivåer, från MIL0 till MIL3, och är specifika för varje domän. För att nå en högre mognadsnivå måste organisationen nå de mål som finns inom domänen samt genomföra samtliga aktiviteter på nivån under. Exempelvis måste alla aktiviteter inom MIL1 och MIL2 slutföras för att nå till MIL3. I likhet med NIST:s ramverk är målet inte nödvändigtvis att nå högsta möjliga MIL

15 https://www.energy.gov/sites/prod/files/2019/08/f65/C2M2%20v2.0%2006202019%20DOE%20for%20Comment.pdf

inom varje domän utan organisationen bör själv avgöra vilka domäner som är kostnadseffektiva och relevanta att prioritera. Både C2M2 och NIST:s cybersäkerhetsramverk kan med fördel användas tillsammans då C2M2 ger en fördjupad beskrivning av de aktiviteter som behöver nås.

Energidepartementet förespråkar att organisationen använder modellen med stöd av en facilitator, men kan förmedla ett arbetsverktyg (toolkit) som underlättar en egen utvärdering. Modellen genomförs genom samma sju steg som beskrivs i NIST:s ramverk men med en specificerad matris för ingångsvärden, aktiviteter och förväntade mål.[16]

Cybersecurity Maturity Model Certification (CMMC)

Det amerikanska försvarsdepartementet har tillsammans med ett flertal aktörer utvecklat en modell för certifiering av cybersäkerhetsmognad, *Cybersecurity Maturity Model Certification* (CMMC). Syftet med modellen är bland annat att ställa krav på, och få en översikt över, de underleverantörer som är verksamma inom försvarsindustrin Detta ställer krav på informationssäkerheten i hela leverantörskedjan. För att få leverera produkter och materiel till försvarsindustrin behöver samtliga underleverantörer således certifiera sig mot CMMC. Riskbegreppet beskrivs i en kontext av antagonistiska hot, exempelvis ”malicious cyber activity”. Vidare läggs stor vikt vid tekniska aspekter av säkerhet hos leverantörerna såsom att ha rätt konfigureringar och uppdateringar av programvara. Ett mer omfattande allriskperspektiv anläggs inte inom modellen. Modellen är uppbyggd utifrån ett antal modeller och standarder, däribland NIST:s standarder, ISO 27001 och *CERT Resilience Management Model*.[17] CMMC mäter cybersäkerhetsmognad genom fem nivåer, från nivån Grundläggande cyberhygien till nivån Avancerad. Modellen utgår från 17 domäner, till skillnad från C2M2:s tio. Varje domän innehåller ett antal processer och rutiner (practices) som sträcker sig över fem nivåer. Modellen riktar sig främst mot försvarsindustrisektorn, *Defense Industrial Base* (DIB), för att öka säkerheten och resiliensen. Syftet med modellen är att skapa en enhetlig standard för cybersäkerhet samt att ge möjligheten att underlätta skydd av känslig information.

För varje nivå i skalan måste både processerna och rutinerna tillgodoses. Utöver det mäter CMMC även mognaden för en organisations institutionalisering av processer och rutiner (practices). I likhet med C2M2 måste en organisation nå samtliga grundläggande nivåer för att tillgodoräkna sig en högre nivå. Modellen skiljer sig åt från andra modeller genom dess certifiering, som måste ske av extern part, vilket verifierar att implementering av både processer och rutiner genomförts. Modellen utgår inte från NIST:s cybersäkerhetsramverk men använder dess standarder, exempelvis NIST SP 800-171 och NIST SP 800-53. För att bli certifierad måste alla de krav som modellen specificerar följas, vilket är en skillnad mot de andra modellerna som inte har samma certifieringsmål. Det finns inget explicit krav på att en facilitator bör medverka men å andra sidan måste en extern part certifiera organisationen.

Cyber Assessment Framework (CAF)

Även i Storbritannien finns ett antal utvärderingsmodeller för cybersäkerhet. *National Cyber Security Center* (NCSC) har tagit fram 14 cybersäkerhets- och resiliensprinciper, en vägledning kring principerna samt ett ramverk, *Cyber Assessment Framework* (CAF), som tillsammans skapar CAF-samlingen. Samlingen syftar till att skapa en systematisk och genomgripande metod för att bedöma hur cyberrisker hanteras inom organisationer.[18] Till skillnad från de amerikanska modellerna, C2M2 och CMMC, riktar sig ramverket främst till organisationer och myndigheter som omfattas NIS-regleringen, är del av Storbritanniens kritiska infrastruktur eller hanterar cyberrelaterade risker för allmän säkerhet. Då

[16] https://www.energy.gov/sites/prod/files/2019/08/f65/C2M2%20v2.0%2006202019%20DOE%20for%20Comment.pdf
[17] https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf
[18] https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog

ramverket bland annat riktar sig till NIS-leverantörer och verksamheter inom kritisk infrastruktur avgränsas ramverket inte endast till antagonistiska cyberhot, utan nämner också andra störningar som risker. Dock läggs en större tonvikt på attacker med antagonistiskt ursprung och det betonas att organisationer behöver utveckla en förmåga att hantera sådana risker. Bland annat används ramverket som en vägledning till de tillsynsmyndigheter som är verksamma inom NIS-regleringen, med syfte att mäta mognaden inom respektive sektor. Ramverket utgår från de 14 principerna som NCSC specificerat. Varje princip följs av en fördjupning, exempelvis ”Governance”, där fördjupningen är ”Board direction”. Därefter kan organisationen avgöra huruvida den uppnått beskrivningen i fördjupningen. Vidare använder modellen *Indicators of good practice* (IGP), vilket ger en fingervisning om hur väl organisationen når målen. Klassningsnivån sträcker sig från ”Not achieved” till ”Partly Achieved” och slutligen ”Achieved”. Det finns dock inga krav på organisationer att följa CAF. I likhet med de andra modellerna kan CAF genomföras som ett självskattningstest eller med hjälp av en extern enhet såsom exempelvis en tillsynsmyndighet. CAF ställer inget krav på att en extern facilitator bör hålla utvärderingen, utan bör användas som ett självutvärderingsverktyg eller av relevant myndighet (exempelvis en tillsynsmyndighet inom ramen för NIS-direktivet). Dock är mätskalan relativt övergripande vilket kan skapa rum för tolkningsproblematik. NCSC:s syfte med modellen är inte att skapa en heltäckande checklista över cyberrisker utan snarare att förstå och använda de framtagna principerna, jämföra resultaten med organisationens nuvarande situation, identifiera brister, samt implementera nya processer. Då det finns ett antal olika sätt att uppnå CAF-resultaten på, kan en viss osäkerhet om huruvida resultaten kan mätas och göras allmängiltiga finnas. Detta kan i sin tur försvåra tolkningen av i vilken utsträckning en organisation har infört en lämplig nivå av cyberresiliens. Dock beskriver NCSC att införandet av IGP ger en guide till vilken typ av åtgärder som normalt skulle finnas i en organisation med hög cyberresiliens.

Cybermätaren

Under hösten 2020 lanserade Finlands nationella cybersäkerhetscenter (NCSC-FI) ”Cybermätaren”[19], som hjälper företagsledningar och organisationer att bättre hantera cyberrisker och trygga verksamhetens kontinuitet. Verktyget syftar till att hjälpa organisationer att hantera cyberhot och bedöma kritiska funktioner, processer och beroenden.

NCSC-FI genomförde 2019-2020 en pilotstudie av cybermognadsnivån hos företag som är kritiska för försörjningsberedskapen. Det är den huvudsakliga målgruppen för modellen, men den lämpar sig för bedömning av alla slags företag, organisationer och offentliga aktörer oberoende av bransch.

Modellen baseras i huvudsak på NIST:s ramverk och C2M2 – och i likhet med dem ligger huvudfokus på förmågor och åtgärder. Valet av de två modellerna motiveras av NIST:s internationella gångbarhet samt C2M2:s initiala inriktning mot energisektorn, och därigenom, kritisk infrastruktur. Modellen syftar till att på ett enkelt sätt möjliggöra för organisationer inom kritisk infrastruktur att bedöma de viktigaste cybersäkerhetsriskerna, stärka cyberförmågan samt kartlägga de resurser som går till cyberriskhantering. Genom att skapa en förståelse för en organisations befintliga förmågor och hur pass känslig den är för cyberrisker, kan modellen anpassas efter organisationen. Modellen hjälper organisationer att kartlägga inom vilka områden de behöver utvecklas för att stärka mognadsnivån.

Modellens genomförande består av fem steg som inleds med att ledningen utser en sponsor för bedömningen samt en projektledare (som tillsammans med övriga deltagare genomför bedömningen med stöd av Cybermätaren). Det rekommenderas att ta stöd av en facilitator (extern expert). I Cybermätaren ställs ett större antal frågor uppdelat på elva avsnitt, med utgångspunkt i modellen, där svaren graderas mellan 0-4. Graderingen består av en bedömning om i vilken utsträckning något implementeras (ej, partiellt, mestadels, helt). Det specificeras inte under vilken period förmågor och

[19] https://www.kyberturvallisuuskeskus.fi/sv/cybermataren

åtgärder ska ha funnits på plats, varför modellen ger mer av en ögonblicksbild än en uppföljning av arbete över tid. Inom varje avsnitt kan mognadsnivåerna 0-3 nås. En uppdaterad bedömning bör göras med 1-2 års intervall.

Resultatet av formuläret ger organisationer en mognadsindikation, vilket skapar en överskådlighet av organisationens position i förhållande till andra inom samma bransch. Organisationer kan på frivillig basis dela sina resultat med NCSC-FI vilket öppnar upp för kartläggning och framtagning av rekommendations- och referensnivåer på nationell nivå. Rapporteras resultatet in till NCSC-FI kan upplägget därmed ge en möjlighet att se både trender och skillnader mellan branscher och även skapa underlag för organisationer att arbeta med att stärka sin cybersäkerhetsförmåga.

Bilaga 3: Uppföljningsmodellen – exempel på frågor och återkoppling

- Introduktion till nivå 1 och exempel på fråga

Nivå 1: Informationssäkerhetsarbetets grunder

Organisationer på nivå 1 har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad utsträckning. Något resultat behöver uppvisas på varje fråga, men det finns inga krav på särskild systematik eller innehåll i arbetet (vilket behandlas på högre nivåer).

Frågorna som ställs undersöker bland annat om ledningen är engagerad i informationssäkerhetsarbetet, om en inventering av informationstillgångar har genomförts, om organisationen har arbetssätt på centrala områden (som informationsklassning och riskanalys) och om medarbetarnas kunskaper har undersökts.

Har ledningen styrt organisationens informationssäkerhetsarbete de senaste två åren?

Flera val kan kryssas i

Ja, under den perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om…		
Målsättning och inriktning	Ansvar och befogenheter för informations-säkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informations-säkerhetsarbetet	Resurser som informations-säkerhetsarbetet kräver
Regler för informations-säkerhetsarbetet (alternativt att beslut/översyn delegerats)	Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande	Ja, men ledningen har inte beslutat om eller sett över någon av de nämnda aspekterna under hela den perioden
Nej		

Säker bedömning (dokumenterat underlag finns)	Osäker bedömning (dokumenterat underlag saknas)

MSB:s kommentar

Med ”ledningen” menas organisationens högsta ledning:
- Hos myndigheter kan det handla om en myndighetschef, en styrelse eller en nämnd.
- Hos en kommun kan det handla om kommundirektören och den politiska ledningen, beroende på frågan.
- Hos regioner kan det på motsvarande sätt handla om regiondirektören och den politiska ledningen, beroende på frågan.

I de fall styrningen är uppdelad mellan tjänstemannanivån och den politiska ledningen så behöver båda ha deltagit i styrningen i enlighet med den uppdelning man har.

Med "sett över" avses inte nödvändigtvis att ändringar har gjorts. Att ledningen har haft en genomgång och diskussion om respektive svarsalternativ kan räcka.

- Introduktion till nivå 2 och exempel på fråga

Nivå 2: Systematik i informationssäkerhetsarbetet

Organisationer på nivå 2 bedriver informationssäkerhetsarbetet med viss systematik och är dessutom bättre på grunderna (frågorna under nivå 1).

Frågorna som ställs undersöker om organisationen tillämpar sina arbetssätt och om de olika delarna kopplar till varandra, till exempel om säkerhetsåtgärderna bygger på en riskanalys. En del av områdena från nivå 1 utvecklas med fördjupande frågor, till exempel om medarbetarnas kunskaper.

Har organisationen, de senaste två åren, infört de säkerhetsåtgärder som beslutats?

Flera angränsande val kan kryssas i för att få ett bredare intervall

MSB:s kommentar

Ja, under den perioden har organisationen infört…		
Alla de beslutade säkerhets-åtgärderna	75% till mindre än 100% av de beslutade säkerhetsåtgärderna	50% till mindre än 75% av de beslutade säkerhets-åtgärderna
25% till mindre än 50% av de beslutade säkerhets-åtgärderna	Mer än 0% till mindre än 25% av de beslutade säkerhetsåtgärderna	Nej

Frågan avser säkerhetsåtgärder som organisationen har fattat beslut om de senaste två åren.

Svara nej om inga beslut har fattats om säkerhetsåtgärder. Svara ja (alla) om beslut har fattats om att inte införa några säkerhetsåtgärder alls.

Säker bedömning (dokumenterat underlag finns)	Osäker bedömning (dokumenterat underlag saknas)

- Introduktion till nivå 3 och exempel på fråga

Nivå 3: Kvalificerat innehåll i det systematiska informationssäkerhetsarbetet

Organisationer på nivå 3 uppvisar ett kvalificerat innehåll i informationssäkerhetsarbetet och är dessutom bättre på grunderna och det systematiska arbetet (frågorna under nivå 1-2).

Frågorna handlar om det systematiska informationssäkerhetsarbetet har kvalificerat innehåll (bland annat utifrån MSB:s föreskrifter om informationssäkerhet för statliga myndigheter). Frågorna som ställs undersöker därför om organisationens arbetssätt är utformade på ett sätt som kan förväntas vara ändamålsenligt.

Har organisationen i sin undersökning av medarbetarnas kunskaper, de senaste två åren, undersökt deras kunskaper inom följande grundläggande områden?

Flera val kan kryssas i

MSB:s kommentar

Ja, organisationen har undersökt medarbetarnas kunskaper om…		
Vad som menas med informations-säkerhet och informations-säkerhetsarbete, samt varför det är viktigt för organisationen	Gällande regler och krav som styr informations-säkerhetsarbetet inom organisationen	Vilka stöd och verktyg som medarbetarna har tillgång till för att kunna arbeta på ett informationssäkert sätt
Informations-säkerhetsrelaterade hot, sårbarheter och risker	Vad medarbetarna ska göra om en informations-säkerhetsincident inträffar	Nej, men undersökningen har omfattat andra grundläggande områden
Nej		

Med ”medarbetare” menas anställda såväl som annan personal som arbetat i organisationen i minst sex månader.

Med "undersökt" avses här intervjuer, enkäter, tester eller andra förfrågningar.

Undersökningen möjliggör för organisationen att veta vad medarbetarna vet och förstår, så att utbildningsinsatser kan designas och inriktas mot områden där kunskapen är låg.

Säker bedömning (dokumenterat underlag finns)	Osäker bedömning (dokumenterat underlag saknas)

- Introduktion till nivå 4 och exempel på fråga

Nivå 4: Ständiga förbättringar av det systematiska informationssäkerhetsarbetet

Organisationer på nivå 4 arbetar avancerat med ständiga förbättringar och är dessutom bättre på grunderna, systematiken och innehållet (frågorna under nivå 1-3). Informationssäkerhetsarbetet karaktäriseras genomgående av systematik och ändamålsenlighet.

Frågorna som ställs undersöker hur organisationen arbetar med identifiering av hinder och framgångsfaktorer samt ledningens uppföljning.

Har organisationens ledning, de senaste två åren, arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?

MSB:s kommentar

Flera val kan kryssas i

Ja, under den perioden har organisationens ledning minst en gång per år 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 säkerhets-åtgärderna 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 (exempelvis sådana som finns i fliken Valideringsfrågor)	Integrera informations-säkerhetsarbetet med befintliga sätt att leda och styra organisationen	Ja, men ingen av de nämnda aktiviteterna har genomförts

Säker bedömning (dokumenterat underlag finns)	Osäker bedömning (dokumenterat underlag saknas)

- Exempel på återkoppling om organisationens nivå/inledning

Sammanställning

Organisationens nivå

Organisationen är på nivå 1. Det innebär att den har grunderna i informationssäkerhetsarbetet på plats, åtminstone i begränsad omfattning. Organisationen uppvisar resultat i grundläggande delar som att ledningen är engagerad, att inventering av informationstillgångar har gjorts, att det finns arbetssätt för centrala områden och att medarbetarnas kunskaper har undersökts.

Nivå 1

Sammanställningens innehåll

Snabba fakta om poängresultatet
Översiktsbild med indikativ nivå per arbetsområde
Resultat per arbetsområde
Indikation i förhållande till MSBs föreskrifter för statliga myndigheter
Detaljerad sammanställning av resultat

Tänk på att...
Den övergripande nivåbedömningen tar sikte på bredd i informationssäkerhetsarbetet. Resultat måste uppnås på alla frågor på respektive nivå. För att nå en högre nivå måste bättre resultat uppnås på alla tidigare nivåers frågor (se vidare i Fördjupningsinformation).

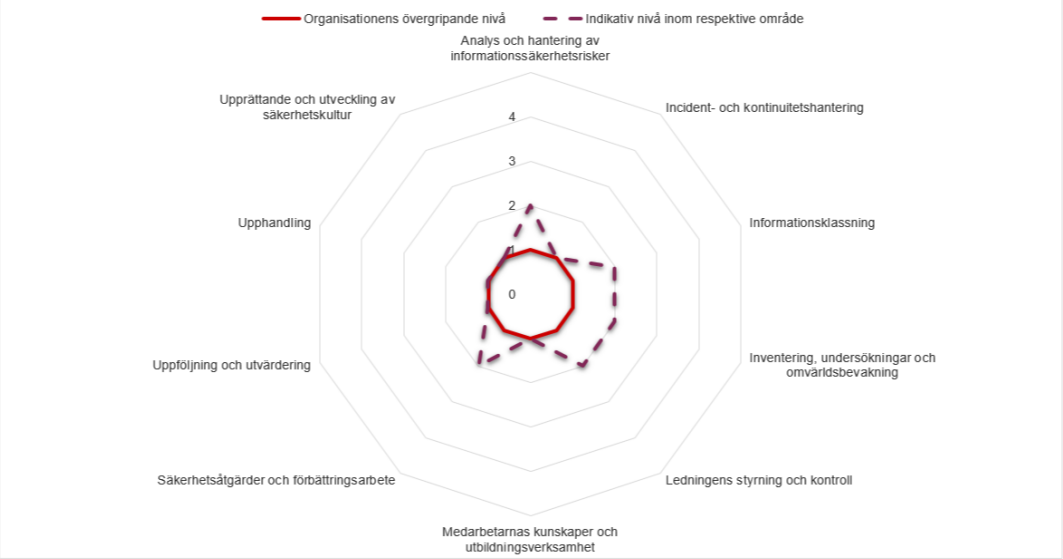
Snabba fakta

- 123 poäng har samlats in totalt.
- 39 av 40 frågor har fyllts i på ett giltigt sätt.
- 34 säkra bedömningar har angetts i de giltigt ifyllda frågorna.
- 0 poäng till krävs för att nå nästa nivå.
- 3 frågor måste ge mer poäng för att nästa nivå ska kunna nås.
- 60% av alla bedömningar måste vara säkra för att nå nästa nivå.

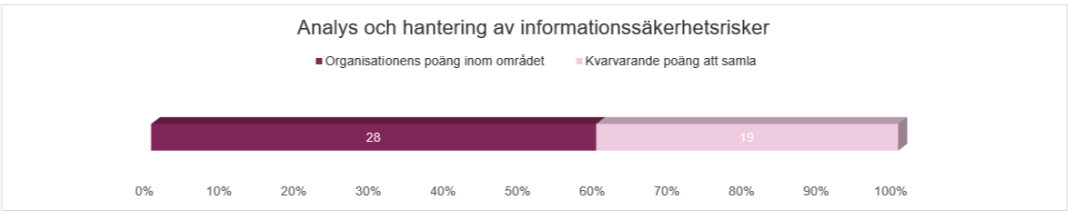
- Exempel på återkoppling om övergripande nivå i förhållande till arbetsområden

Översiktsbild med indikativ nivå per arbetsområde

Diagrammet visar organisationens övergripande nivå (i rött) samt en indikation på nivån för olika arbetsområden (lilastreckat). Områdesnivåerna är indikativa eftersom de bygger på minimikraven för respektive nivå. För mer information om hur niváerna beräknas, se Fördjupningsinformationen. En yttre cirkel har lagts till för att diagrammet ska kunna visa om en organisation har nått maxpoäng i sitt arbete med något område.



- Exempel på återkoppling om arbetsområde



Arbetet inom det här området har legat före organisationens samlade systematiska informationssäkerhetsarbete under den senaste tvåårsperioden. Om arbetet håller samma nivå under den kommande tvåårsperioden så behövs inga mer satsningar inom ämnet för att nå en högre samlad nivå i modellen.

Resultatet inom området beror på vad organisationen lämnat för svar om sitt arbete med analys och hantering av informationssäkerhetsrisker (exempelvis om ett arbetssätt finns, hur det tillämpas och vad det innehåller) samt om hur arbetet med analys av informationssäkerhetsrisker kopplar till andra delar av informationssäkerhetsarbetet (exempelvis om underlag från omvärldsbevakningen används vid riskanalys och om säkerhetsåtgärder väljs på grundval av riskanalys).

Stödmaterial för att komma vidare i arbetet (finns på MSB.se):
- Metodstödet analysera risker
- Rapporten Cybersäkerhet i Sverige 2020 – hot, metoder, brister och beroenden

- Exempel på återkoppling avseende MSB:s föreskrifter för statliga myndigheters informationssäkerhet

Indikation i förhållande till MSB:s föreskrifter om statliga myndigheters informationssäkerhet

Alla organisationer kan använda MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2020:6) som ett stöd i att sätta målsättningar för arbetet. Statliga myndigheter ska efterleva dem.

I detta avsnitt indikeras i vilken utsträckning föreskrifterna uppfylls. Det är viktigt att komma ihåg att det endast handlar om en indikation utifrån lämnade svar; modellen syftar inte till att omfatta hela författningen eller alla sätt som kraven kan uppnås på. På MSB.se finns underlag om hur indikationen har tagits fram.

OBS: MSB använder inte svaren för att kontrollera enskilda myndigheters regelefterlevnad. Det är inte syftet med modellen och MSB har inte någon tillsynsuppgift kopplad till föreskrifterna.

Systematiskt och riskbaserat informationssäkerhetsarbete

4 § Myndigheten ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande.

Hur informationssäkerhetsarbetet ska utformas

5 § Informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation.

När myndigheten utformar informationssäkerhetsarbetet ska den

1. säkerställa att det finns en informationssäkerhetspolicy där ledningens målsättning med och inriktning för informationssäkerhetsarbetet framgår,
2. tydliggöra myndighetsledningens och den övriga organisationens ansvar, inklusive den eller de som utses att leda och samordna informationssäkerhetsarbetet, och ge dessa befattningar de befogenheter som behövs,
3. säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser,
4. upprätta de interna regler, arbetssätt och stöd som behövs, och
5. säkerställa att innehållet i myndighetens interna regler, arbetssätt och stöd utvärderas samt vid behov anpassas.

Utformningen av informationssäkerhetsarbetet ska dokumenteras.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984