Fördjupningsinformation om Cybersäkerhetskollen

Beskrivning och bakgrund till Cybersäkerhetskollen,
MSB:s uppföljningsstrukturer för systematiskt cybersäkerhetsarbete

Innehåll

Varför Cybersäkerhetskollen?

MSB har tagit fram uppföljningsmodellen Cybersäkerhetskollen[1] för att stödja organisationer, särskilt i den offentliga förvaltningen och NIS-leverantörer, i deras förbättringsarbete på cybersäkerhetsområdet. I det ingår bland annat automatisk återkoppling om vilken nivå organisationen befinner sig på och om vilka utvecklingsområden som för organisationen är särskilt viktiga att se över inför framtiden.

När underlaget rapporteras in till MSB får organisationen också kompletterande återkoppling. Möjlighet ges då att jämföra sitt resultat med andra organisationers. MSB kommer att använda inrapporterat underlag för att lämna en samlad lägesbedömning till regeringen samt för att utveckla myndighetens stöd. Resultatet kommer endast att redogöras för på aggregerad nivå. Svaren från de samlade kollarna bidrar till MSB:s bedömning av nivån på cybersäkerhetsarbetet i det civila försvaret.

Infosäkkollen

Under 2019 fick MSB ett regeringsuppdrag[2] att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet, utifrån detta togs Infosäkkollen fram. Infosäkkollen undersöker organisationens arbete med systematisk informationssäkerhet.

It-säkkollen

Den 29 mars 2023 mottog MSB ett regeringsuppdrag[3] om att Infosäkkollen ska erbjudas privata företag, särskilt NIS-leverantörer, men också om att ta fram en uppföljningsstruktur av it-säkerhetsåtgärder, It-säkkollen. It-säkkollen genomförs i full skala för första gången 2025 och har tidigare genomförts som en självskattningsundersökning av en organisations it-säkerhetsåtgärder. It-säkkollen undersöker organisationens arbete med it-säkerhetsåtgärder på såväl översiktlig som mer detaljerad nivå. It-säkkollen genomförs 2025 som en pilot och kommer därefter att utvärderas.

Ot-säkkollen

MSB kommer 2025 för första gången att genomföra Ot-säkkollen. Ot-säkkollen är framtagen utifrån uppdraget i budgetpropositionen för 2025 (2024/25:1) om att vidareutveckla Cybersäkerhetskollen. Ot-säkkollen undersöker organisationens ot-säkerhetsarbete.

Ot-säkkollen riktar sig i huvudsak till de organisationer som innehar eller vars verksamhet är beroende av industriella informations- och styrsystem (ICS). Dessa organisationer finns ofta, men inte enbart, inom de samhällsviktiga sektorerna energiförsörjning, dricksvattenförsörjning samt transporter och kan vara såväl offentliga som privata organisationer.

Leveranskedjekollen

Den 27 februari 2025 mottog MSB ett regeringsuppdrag[4] om att genomföra en kartläggning av digitala leveranskedjor och att ta fram en modell för uppföljning av digitala leveranskedjor. Utifrån detta uppdrag har MSB tagit fram Leveranskedjekollen. Leveranskedjekollen undersöker organisationens arbete med säkra leveranskedjor, samt kartlägger system där incidenter kan orsaka stora konsekvenser för samhället.

---

[1] Cybersäkerhetskollen är samlingsnamn för Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen.
[2] Ju2019/03058/SSK, Ju2019/02421/SSK
[3] Fö2023/00697
[4] Fö2025/00390

Infosäkkollen och it-säkkollen utgår från föreskrifter, stöd och ISO-standard

Uppföljningsmodellen utgår från det systematiska cybersäkerhetsarbetet som det beskrivs i MSB:s föreskrifter och stödmaterial, som i sin tur är förenligt med säkerhetsstandardserien ISO/IEC 27000.

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

Ot-säkkollen utgår från standarden IEC 62443

Uppföljningsmodellen för ot-säkerhet utgår från serien av standarder IEC 62443.

Modellen ger stöd till uppföljning på en strategisk nivå. Resultatet visar i vilken utsträckning organisationen bedriver ett systematiskt arbete för ot-säkerhet, det vill säga har förutsättningar för att upprätta en god ot-säkerhet. Modellen mäter inte om den enskilda organisationens skydd är tillräckligt. Ot-säkkollen genomförs 2025 som en pilot och kommer sedan att utvärderas.

Leveranskedjekollen är en fördjupning

Uppföljningsmodellen för säkra digitala leveranskedjor stödjer organisationer att säkra sina leverantörskedjor. Leveranskedjekollen mäter inte mot föreskrifter eller en standard. Frågorna baseras istället på den strategiska analys inom området som MSB tagit fram samt utifrån underlag i inkommen incidentrapportering till myndigheten.

MSB:s analys visar att allt fler incidenter påverkar digitala leveranskedjor och att just dessa incidenter riskerar att få störst samhällskonsekvenser. Modellen innehåller en kartläggning av digitala leveranskedjor. Med hjälp av kartläggningen kan MSB stötta organisationer och samhället bättre.

Modellen ger stöd till uppföljning på en strategisk nivå av leverantörskedjor. Resultatet visar i vilken utsträckning organisationen bedriver ett systematiskt arbete med säkra leveranskedjor. Modellen mäter inte om den enskilda organisationens arbete är tillräckligt. Leveranskedjekollen kan stötta organisationer i att förbereda inför det ökade fokuset på säkra leveranskedjor som kommer med NIS2. Leveranskedjekollen genomförs 2025 som en pilot och kommer sedan att utvärderas.

Så kan ni arbeta med Cybersäkerhetskollen

Uppföljningsmodellen är omsatt i ett verktyg i Excel. Kärnan i verktyget är formulär med frågor om centrala delar av det systematiska cybersäkerhetsarbetet (se flikarna ”Infosäkkollen”, ”It-säkkollen”, ”Ot-säkkollen” och ”Leveranskedjekollen”).

- Infosäkkollen består av 40 frågor och följer upp säkerhetsarbetet inom tio centrala områden.
- It-säkkollen består av 53 frågor och följer upp säkerhetsarbetet inom sex centrala områden.
- Ot-säkkollen består av 54 frågor och följer upp säkerhetsarbetet inom åtta centrala områden.
- Leveranskedjekollen består av 15 frågor och följer upp säkerhetsarbetet inom fyra centrala områden.

Samla in underlag från olika delar av organisationen

Eftersom era svar avser organisationen i sin helhet behövs underlag från olika delar av verksamheten. Ett bra sätt att samla in den nödvändiga informationen är att anordna en eller flera workshops där medarbetare med olika funktioner och roller deltar. Organisationens CISO kan med fördel hålla ihop arbetet (alternativt någon i stabsfunktion). Det samlade svaret bör förankras hos ledningen. För att alla delar ska få ett bra och realistiskt svar som speglar organisationen är det viktigt att relevanta roller deltar. Till exempel bör it-säkerhetsansvarig eller it-chef medverka vid it-säkkollen, vid ot-säkkollen bör lämplig driftspersonal eller driftschef delta och leveranskedjekollen bör ansvarig personal för upphandling och inköp delta.

Hur lång tid tar det att svara på frågorna?

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

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

Svaren måste fyllas i och lämnas in säkert

Svaren som lämnas i verktyget behöver hanteras och rapporteras in till MSB på ett säkert sätt. Följ de anvisningar som finns i under fliken ”Säker hantering”, samt på www.msb.se/cybersakerhetskollen eller https://etjanst.msb.se/sv/e-tjanster. MSB kommer av säkerhetsskäl inte ta emot informationen på andra sätt än de som anges där.

Skicka in svaren senast den 12 september 2025

Era svar behöver komma in till MSB senast den 12 september 2025 för att er organisation ska kunna få kompletterande återkoppling från MSB och bidra till den samlade bedömningen på nationell nivå.

Ni får återkoppling när ni har fyllt i svaren

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

Underlag för att arbeta med förbättringar

Tänk på att nyligen genomförda förbättringar inte kommer att få fullt genomslag i den återkoppling ni får, eftersom uppföljningen utreder om ett arbetssätt eller en teknisk åtgärd funnits på plats och tillämpats under hela den senaste tvåårsperioden. Uppföljningen tittar bakåt i tiden, men själva nyttan med resultatet handlar om att se framåt. Tanken är att få fram ett underlag till arbetet med ständiga förbättringar, och att främja en positiv uppföljningskultur över tid, snarare än att fokusera på resultatet i sig.

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

Rapportera in svaren och få mer återkoppling

När svaren rapporteras in till MSB kommer er organisation att få kompletterande återkoppling. I den ingår en jämförelse med snittet för andra, liknande organisationer. Jämförelsen utgår från det samlade underlaget och från 2025 gäller det för hela Cybersäkerhetskollen.

Vad är ett systematiskt cybersäkerhetsarbete?

Arbetet med cybersäkerhet är ett gemensamt ansvar för hela organisationen. Vidtagande av säkerhetsåtgärder är en förutsättning för att organisationen ska kunna använda sin information på avsett sätt och leverera sina samhällsviktiga tjänster. Att bedriva ett systematiskt arbete med cybersäkerhet betyder att det finns en tydlig och strukturerad styrning i enlighet med ledningens uppsatta vision och mål.

Det övergripande syftet med ett systematiskt cybersäkerhetsarbete är att skydda information, it-system, industriella kontroll- och styrsystem samt leveranskedjor hos samhällsviktiga verksamheter på rätt nivå genom ständiga förbättringar och anpassningar till en föränderlig värld.

De grundläggande stegen vid allt systematiskt cybersäkerhetsarbete är att:

- identifiera organisationens informationstillgångar, it-system, ot-system, digitala leveranskedjor
- värdera informationstillgångarna utifrån konfidentialitet, riktighet och tillgänglighet
- bedöma de risker som kan förekomma mot informationstillgångar, it-system, ot-system, digitala leveranskedjor
- införa ändamålsenliga och proportionerliga säkerhetsåtgärder.

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

Planera, genomför, följ upp, utvärdera och förbättra

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

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. över tid följer vilka resultat tillämpningen av arbetssätten leder till,
4. utvärderar och förbättrar arbetssätten.

Koppla ihop arbetssätten till en sammanhållen process

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

Främja en god säkerhetskultur

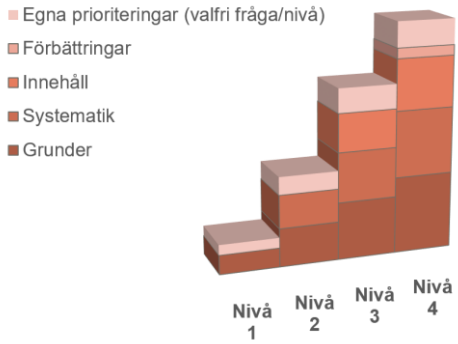
Cybersäkerheten i organisationen påverkas inte bara av de olika arbetsmomenten i cybersäkerhets-arbetet och de tekniska eller administrativa säkerhetsåtgärder som införs. Också säkerhetskulturen i organisationen spelar en avgörande roll för att både det systematiska arbetet och skyddet ska fungera.

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

Cybersäkerhetskollen visar nivån på cybersäkerhetsarbetet

Uppföljningsmodellen delar in det systematiska cybersäkerhetsarbetet i fyra nivåer, som är tänkta att motsvara ett stegvis utvecklingsarbete:

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



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

Nivåbedömningen i Cybersäkerhetskollen utgår från svar på frågorna i flikarna ”Infosäkkollen”, ”It-säkkollen”, ”Ot-säkkollen” och ”Leveranskedjekollen”.

Nivå 1: Grunderna i cybersäkerhetsarbetet

Frågorna i nivå 1 mäter om organisationen har de grundläggande delarna i cybersäkerhetsarbetet på plats. Frågorna undersöker bland annat:

- om ledningen är engagerad i cybersäkerhetsarbetet,
- om organisationen har arbetssätt på centrala områden,
- om organisationen följer upp och utvärderar.

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

För att uppnå en nivå inom varje ”koll” måste alla nivå 1 frågor ha besvarats.

Nivå 2: Cybersäkerhetsarbetet bedrivs med viss systematik

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

Nivå 3: Kvalificerat innehåll i cybersäkerhetsarbetet

Frågorna i avsnittet handlar om huruvida det systematiska cybersäkerhetsarbetet har ett kvalificerat innehåll. För Infosäkkollen och It-säkkollen betyder detta att de organisationer som klarar nivå 3 lever upp till stora delar av MSB:s föreskrifter för statliga myndigheter, MSBFS 2020:6 och MSBFS 2020:7, medan för Ot-säkkollen utgår det kvalificerade innehållet från standarden IEC 62443. Leveranskedjekollens kvalificerade innehåll utgår till viss del från MSBFS 2020:6 men främst från

MSB:s analyser. Frågorna undersöker om organisationens arbetssätt är utformade på ett sätt som kan förväntas vara ändamålsenligt.

Nivå 4: Ständiga förbättringar

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

Olika organisationer kan behöva prioritera olika delar av arbetet

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

Nivån räknas fram genom poäng och andel säkra bedömningar

Det krävs ett visst antal poäng för att uppnå varje nivå. Poängen beräknas utifrån svar på frågorna som grupperats i avsnitt för respektive nivå. För att nå en viss nivå behövs en totalpoäng, som består av två delar: lägstapoäng per fråga och rörliga poäng (egna prioriteringar). Dessutom krävs säkra bedömningar för en viss andel av de frågor som har besvarats.

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

Tabellen visar översiktligt hur upplägget fungerar:

Nivå	Frågorna på nivå 1	Frågorna på nivå 2	Frågorna på nivå 3	Frågorna på nivå 4	Krav
1	**Behöver besvaras**	Behöver inte besvaras	Behöver inte besvaras	Behöver inte besvaras	Alla frågorna i avsnittet för nivå 1 behöver besvaras med minst 1 poäng. Högst 50 % av svaren får vara osäkra bedömningar.
2	**Behöver besvaras**	**Behöver besvaras**	Behöver inte besvaras	Behöver inte besvaras	Alla frågorna i avsnitten för nivå 1 och 2 behöver besvaras med minst 2 poäng. Högst 40 % av svaren får vara osäkra bedömningar.
3	**Behöver besvaras**	**Behöver besvaras**	**Behöver besvaras**	Behöver inte besvaras	Alla frågorna i avsnitten för nivå 1, 2 och 3 behöver besvaras med minst 3 poäng. Högst 30 % av svaren får vara osäkra bedömningar.
4	**Behöver besvaras**	**Behöver besvaras**	**Behöver besvaras**	**Behöver besvaras**	Alla frågorna i avsnitten för alla nivåer behöver besvaras med minst 4 poäng. Högst 20 % av svaren får vara osäkra bedömningar.

Ekvation för poängkraven

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

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

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

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

Hur Cybersäkerhetskollens frågor besvaras

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

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

Två typer av frågor

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

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

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

Säker och osäker bedömning

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

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

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

Cybersäkerhetskollen följer upp de senaste två åren

Alla frågor i Cybersäkerhetskollen handlar om en säkerhetsåtgärd (arbetssätt eller teknisk åtgärd) har funnits på plats under hela den senaste tvåårsperioden och inte bara någon gång under denna period, eftersom nivån på organisationens cybersäkerhetsarbete är resultatet av arbete och val som har gjorts över tid. Då både förändringar och uppföljning tar tid att genomföra blir det inte effektivt att mäta för ofta. Det är också en fördel att mätperioden sammanfaller med hur ofta uppföljningen genomförs. Vartannat år kommer MSB erbjuda undersökningen till offentlig förvaltning och NIS-leverantörer och be att resultaten rapporteras in.

Cybersäkerhetskollen använder måttet ”andel av verksamheter”

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

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

Infosäkkollen och It-säkkollen stödjer tillämpning av MSB:s föreskrifter

Statliga myndigheter är skyldiga att bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete i enlighet med MSB:s föreskrifter om statliga myndigheters informations- och cybersäkerhet (MSBFS 2020:6) och MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7). Även organisationer som inte omfattas av föreskrifterna, exempelvis NIS-leverantörer, kan använda dem som stöd för sitt arbete och för att hitta rätt ambitionsnivå. Infosäkkollen och It-säkkollen är utformade så att de kan indikera i vilken utsträckning organisationen uppfyller olika krav i föreskrifterna. Tanken med det är att stödja tillämpningen av föreskrifterna.

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

Det är viktigt att komma ihåg att modellen bara kan ge en indikation, den är inte tänkt att omfatta hela författningen eller alla sätt som kraven kan uppnås på. Till exempel berör modellen inte fysiskt skydd.

Modellen mäter inte hur organisationens arbete förhåller sig till specifika krav i andra författningar, exempelvis dataskyddsförordningen och säkerhetsskyddslagen. Vid lanseringen av Cybersäkerhetskollen 2025 finns varken en proposition eller cybersäkerhetslagen på plats i Sverige. Mot denna bakgrund är Cybersäkerhetskollen inte fullt ut anpassad till NIS2-regleringen. Samtidigt bedöms att de som klarar av MSB:s föreskriftskrav står väl rustade för att klara NIS2 och övrig kommande EU-reglering.

MSB använder inte svaren för att kontrollera om föreskrifterna följs

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

Reflektion & Målbild

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

Valideringsfrågor

Under fliken ”Analysstöd” återfinns valideringsfrågorna. Syftet med valideringsfrågorna är tredelat:

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

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

Ekonomifrågor

Här ges organisationen möjlighet att följa upp hur den har understött det systematiska cybersäkerhetsarbetet med ekonomiska resurser under den senaste tvåårsperioden. Frågorna bör troligen besvaras genom ett samarbete mellan CISO och representanter från motsvarande en ekonomiavdelning eller en controllerfunktion.

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

Ställ frågor och lämna förbättringsförslag till MSB

Vanliga frågor och svar om uppföljningen finns på www.msb.se/cybersakerhetskollen. Om frågan inte besvaras i vår FAQ går det också att ställa frågor till cybersakerhetskollen@msb.se. Cybersäkerhetskollen utvecklas kontinuerligt och MSB uppskattar alla synpunkter för framtida versioner.