Myndigheten för
samhällsskydd
och beredskap

Mognadsdialogen

Mognadsdialogen

Enhet: Enheten för systematisk informationssäkerhet (SI)

Text: MSB
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1996 – juni 2022
ISBN: 978-91-7927-280-7

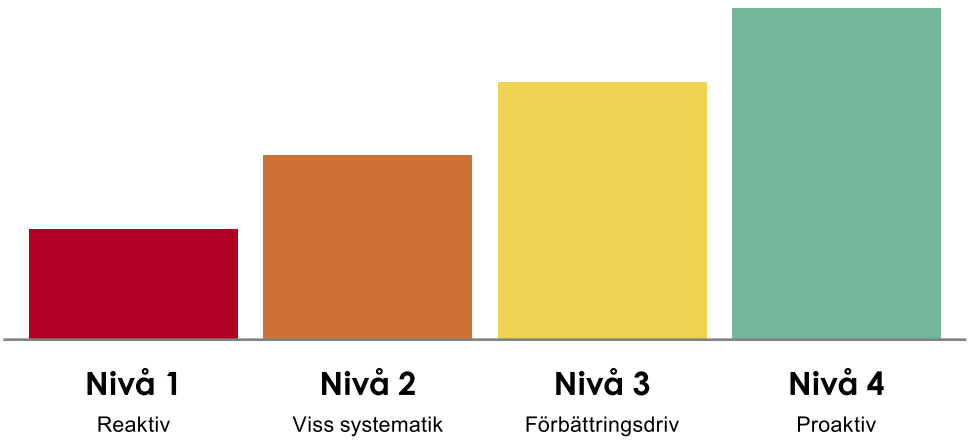
Mognadsdialogen

Mognadsdialogen är ett pedagogiskt verktyg för uppföljning av organisationens systematiska informationssäkerhetsarbete. Genom dialog skapas förståelse och samsyn om organisationens nuläge och viktiga utvecklings- och förbättringsområden.

Verktyget ger en bild av nuläget i relation till framgångsrika organisationer och hur effektivt organisationen arbetar med att skydda sin information utifrån dess behov, krav och förutsättningar. Organisationens ledning och CISO ges härigenom bättre förutsättningar att förstå varandras roller, ansvar och möjligheter att tillsammans ”göra rätt saker på rätt sätt”.

Mognadsdialogen passar de flesta organisationer och visar hur systematiskt och resultatinriktat informationssäkerhetsarbetet är utifrån fyra mognadsnivåer. Ju mer effektivt det systematiska informationssäkerhetsarbetet bedrivs desto högre mognadsresultat.

Figur 1. Fyra mognadsnivåer



Innehåll

Uppföljning med Mognads-dialogen

En förutsättning för ett framgångsrikt informationssäkerhetsarbete är att ledningen, CISO och andra berörda har samsyn om nuläget och vad som behöver prioriteras. Då finns förutsättningar för att dra åt samma håll, att informationssäkerhetsarbetet blir effektivt och medvetna beslut kan fattas för att ge informationen rätt skydd.

Mognadsdialogen syftar till att genom dialog skapa en gemensam bild av och förståelse för organisationens nuläge i det systematiska informationssäkerhetsarbetet. Att genomföra en mognadsdialog går relativt snabbt.

Mognadsdialogen bidrar till att

- skapa samsyn och enas om organisationens nuläge
- identifiera och prioritera områden för utvecklings- och förbättringsarbetet
- öka insikten om vad ett systematiskt arbetssätt innebär
- öka förståelsen för vad som ingår i informationssäkerhetsarbetet
- öka insikten om vad som krävs för att öka mognaden
- öka ledningens engagemang och förmåga att leda och styra.

Vad är Mognadsdialogen?

Mognadsdialogen är ett pedagogiskt verktyg för att utarbeta en gemensam syn på nuläget. Nuläget skapas genom att i dialog jämföra sig med fördefinierade mognadsbeskrivningar enligt fyra olika mognadsnivåer. Nivåerna utgår från vad som kännetecknar organisationer som bedriver ett framgångsrikt informationssäkerhetsarbete.

Mognadsdialogen bygger på SIQ:s managementmodell[1]. Modellen är en etablerad forskningsbaserad så kallad excellencemodell inom kvalitet. I Mognadsdialogen har SIQ:s managementmodell förenklats.

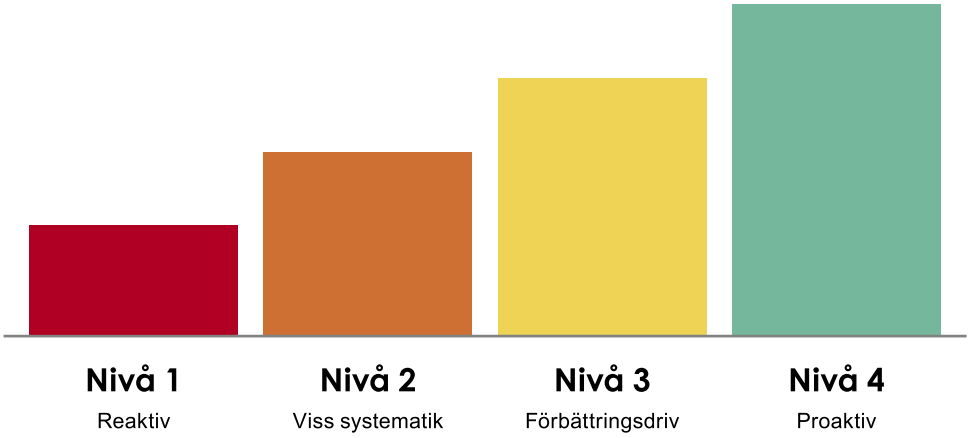
Resultatet placerar organisationen på en av fyra mognadsnivåer där

- **nivå 4** kännetecknas av hög medvetenhet, proaktivitet och enastående resultat – den här nivån uppnås av mycket få organisationer
- **nivå 3** kännetecknas av hög medvetenhet, systematik och ständiga förbättringar
- **nivå 2** kännetecknas av att viss medvetenhet och viss systematik börjar etableras
- **nivå 1** kännetecknas av låg medvetenhet och avgörande brister i arbetssätt och systematik. Kan ha påbörjat arbetet, men det är inte etablerat.

De allra flesta organisationer bedöms vara på nivå 1 eller 2.

1. https://www.siq.se/vara-tjanster/siq-managementmodell/

Figur 2. Fyra mognadsnivåer

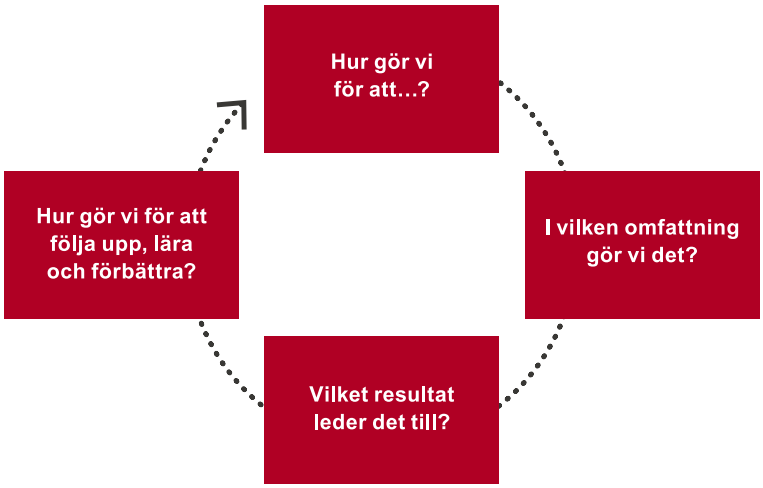


Vad utvärderas i Mognadsdialogen och hur?

För att komma fram till sin mognadsnivå har man fokus på några få frågor som fångar hur systematiskt man arbetar. Under utvärderingen för man dialog kring:

- Arbetssätt – Hur gör vi, har vi etablerade och medvetet valda arbetssätt?
- Tillämpning – I vilken omfattning använder vi arbetssätten, gör vi som vi säger att vi ska göra?
- Resultat – Vilka resultat leder våra arbetssätt till? Kan resultaten härledas till arbetssätten?
- Följa upp, lära och förbättra – Hur utvärderar vi arbetssätten och hur förbättrar vi dem?

Figur 3. Systematiken fångas i frågorna



I Mognadsdialogen utvärderas centrala delar av organisationens informationssäkerhetsarbete, här kallat perspektiv, baserat på ISO/IEC 27000-serien. Mognadsbedömning görs för varje perspektiv.

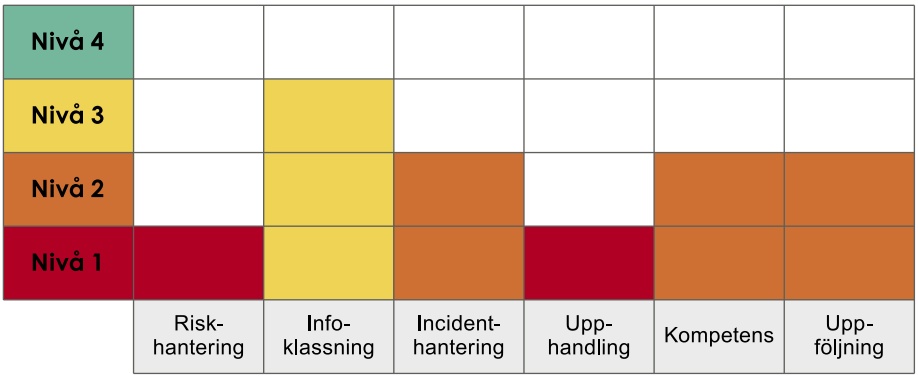
Varje perspektiv har fördefinierade mognadsbeskrivningar för respektive mognadsnivå avseende arbetssätt, tillämpning, resultat samt arbetet med att följa upp, lära och förbättra arbetssätten. Beskrivningarna används för att kunna enas kring organisationens mognadsnivå.

De perspektiv som ingår är:

- Riskhantering
- Informationsklassning
- Incidenthantering
- Upphandling
- Kompetens
- Uppföljning

Mognadsdialogen ska ge en övergripande insikt om verksamhetens mognad inom informationssäkerhetsarbetets olika perspektiv. Perspektivens resultat summeras inte till ett sammanfattande resultat. Det innebär att det blir mer synligt var styrkor och svagheter finns utifrån verksamhetens mål.

Figur 4. Exempelbild av hur resultatet kan se ut för respektive perspektiv.



När kan Mognadsdialogen användas?

Mognadsdialogen kan användas när ni vill och passar de flesta organisationer. Det passar bra att göra Mognadsdialogen i samband med organisationens verksamhetsplanering. Det lättöverskådliga resultatet kan med fördel användas vid ledningens genomgång[2].

Mognadsdialogen kan göras vid ett enstaka tillfälle men kan också ske återkommande, som ett arbetssätt i organisationens uppföljningsarbete, då för att följa utvecklingen över tid. Verktyget är i första hand inte tänkt för att jämföra sig med andra organisationer, men om man gör det är det viktigt att inte bara jämföra mognadsnivåer utan att det också ges utrymme för dialog om hur man resonerat och kommit fram till resultatet. Mognadsdialogen blir då ett stöd för att jämföra och lära av andra organisationer.

Mognadsdialogen kompletterar andra typer av uppföljningar genom att ge en övergripande bild av hur effektivt organisationen arbetar för att skydda sin information. Verktyget ger återkoppling på förmågan att arbeta systematiskt och resultatinriktat utifrån organisationens behov, krav och förutsättningar. Fokus är inte huvudsakligen att man gör något utan snarare hur effektivt man gör det. Detta leder till en ökad förmåga hos organisationen att anpassa skyddet av sin information, vilket i sin tur leder till minskade risker och ökad sannolikhet att organisationen når sina övergripande mål.

Hur går Mognadsdialogen till?

För att Mognadsdialogen ska stödja och ge nytta är det som alltid viktigt att arbetet planeras noga. Arbetet kan delas upp i tre faser: förberedelser, själva genomförandet av mognadsbedömningen och efterarbetet.

Läs vidare nedan om hur man håller en Mognadsdialog.

Bakgrund – SIQ:s managementmodell

SIQ:s managementmodel[3] är en etablerad forskningsbaserad så kallad excellence-modell inom kvalitet med fokus på ledning och styrning utifrån klart identifierade framgångsfaktorer. Jämförbara modeller finns utanför Sverige, exempelvis EFQM[4] som är den europeiska modellen.

Modellen har stora likheter med ISO-standarder avseende det systematiska arbetssättet och metodiken i hur revisioner genomförs. Modellen bygger på en 1 000-poängsskala som bedöms utifrån ett systematiskt sätt att ställa frågor. Systematiken att ställa frågor leder till en insikt om hur väl verksamheten är strukturerad och fungerar. Detta är utgångspunkten för hur Mognadsdialogen har utvecklats.

2. https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra
3. https://www.siq.se/
4. https://www.siq.se/vara-tjanster/efqm-model/

Att hålla Mognadsdialogen

En bra planering är avgörande för att få ett bra resultat. Eftersom alla organisationer har olika behov så är det viktigt att ta hänsyn och anpassa upplägget till era förutsättningar. Här är råd och stöd för vad man bör tänka på.

Processen följer tre steg: förberedelse, genomförande och efterarbete.

Figur 5. Planeringsstegen

Förberedelser

För att få ut mesta möjliga av Mognadsdialogen är det viktigt att planera hur den ska genomföras utifrån din organisations förutsättningar. En bra start är att fundera igenom syftet. Finns det fler syften än att identifiera ett gemensamt nuläge? I så fall påverkar det vad ni behöver förbereda och var ni lägger tyngdpunkten när ni genomför dialogen.

Mognadsdialogen genomförs i workshopformat. Personen som leder workshoppen kan vara organisationens CISO eller någon annan som har erfarenhet av att leda samtal och workshoppar.

Workshopledaren behöver i god tid sätta sig in i Mognadsdialogen, förstå modellen och dess innebörd av arbetssätt, tillämpning, resultat och förbättringar för att kunna leda samtalet och mötet smidigt, ställa följdfrågor med mera.

Att föra en dialog som ska leda till att deltagarna känner medägarskap tar tid. Avsätt därför minst 3–4 timmar för att hinna gå igenom alla perspektiv tillsammans. Man kan också dela upp det i två tillfällen om 2 timmar. En fördel kan då vara att arbetet hinner mogna och nya reflektioner kommer fram. Om ni har möjlighet att avsätta en hel dag för att också arbeta vidare med resultatet, kan ni komma riktigt långt.

Omfattning

Mognadsdialogen består av sex delar som är centrala för informationssäkerhet. Självklart kan man prioritera bort någon del som man bedömer vara mindre relevant för organisationen eller på grund av tidsbrist.

Vilka bör vara med vid Mognadsdialogen?

För att resultatet ska vara väl förankrat och inte bestå av en persons åsikt, är det viktigt att olika roller som berörs av informationssäkerhetsarbetet är med på workshoppen. Förutom ledare och verksamhetsrepresentanter bör olika specialistroller vara med. Nedan följer ett antal förslag på sammansättningar som kan tjäna som utgångspunkt för vilka roller som är aktuella att ha med från er organisation.

Förslag 1: Ledningsgrupp. Genom att ledningen aktivt medverkar i Mognadsdialogen kan förståelsen och engagemanget för att bedriva ett systematiskt informationssäkerhetsarbete öka. Det är en fördel genom att resultatet, nuläget och vägen framåt blir väl förankrat i hela ledningen, vilket spar tid och kan snabba upp utvecklingstakten. En avgörande förutsättning är att ledningen har tid.

Förslag 2: En mindre och väl sammansatt grupp som kan bidra till att ge en helhetsbild av organisationen. Det kan vara ledare och specialister som berörs av informationshanteringen, till exempel funktioner inom säkerhet, it och dataskydd samt gärna personer från kärnverksamheten. Gruppens sammansättning gör att resultatet blir brett förankrat i organisationen. Nästa steg blir här att presentera resultatet för ledningen som underlag för en dialog om det fortsatta arbetet. Genom detta blir ledningen engagerad på ett för dem kanske mer tidseffektivt sätt.

Förslag 3: En eller ett par personer kan också genomföra Mognadsdialogen. Det är viktigt att tänka på att värderingen då riskerar att bli subjektiv och kanske inte kan få samma tyngd när den presenteras för förankring hos ledningen. Vid det här arbetssättet blir det än mer viktigt att tydligt dokumentera hur man resonerat sig fram till resultatet.

Praktiska frågor

Boka en bra lokal och möblera så att alla deltagare kan se och höra varandra. Deltagarna behöver enkelt kunna följa med i dialogen och samtidigt kunna se presentationer och blädderblock.

Workshopledaren ansvarar för helheten, att se till att alla deltagare kommer till tals och att deltagarna lyssnar uppmärksamt på varandra. Detta är centralt för att verkligen enas om ett nuläge. Optimalt är om workshopledaren enbart har ledar-rollen och inte samtidigt är en av gruppdeltagarna. Har ledaren båda rollerna är det extra viktigt att vara uppmärksam på sin förmåga att växla mellan rollerna – att vara neutral och leda gruppen och att samtidigt framföra sina synpunkter.

Kalla deltagarna i god tid och se till att de är införstådda med varför det är viktigt att de deltar, övergripande vad som kommer att hända och vad deras roll är.

Workshopmaterial

Förbered hur workshoppen ska genomföras. Till hjälp finns ett workshopmaterial i powerpoint-format så att man smidigt kan ta sig igenom hela Mognadsdialogen. Här är några exempel på innehåll:

- Beskrivning av relationen – arbetssätt, tillämpning, resultat och förbättring.
- En generiskt bild med kännetecken för de fyra mognadsnivåerna.
- Alla de sex perspektivens olika nivåbeskrivningar med tillhörande processbild.
- En mall för dokumentation av resultatet.
- I Metodstödet finns en mall[5] för handlingsplan för att dokumentera och prioritera förbättringsområden.

5. https://www.informationssakerhet.se/metodstodet/utforma/

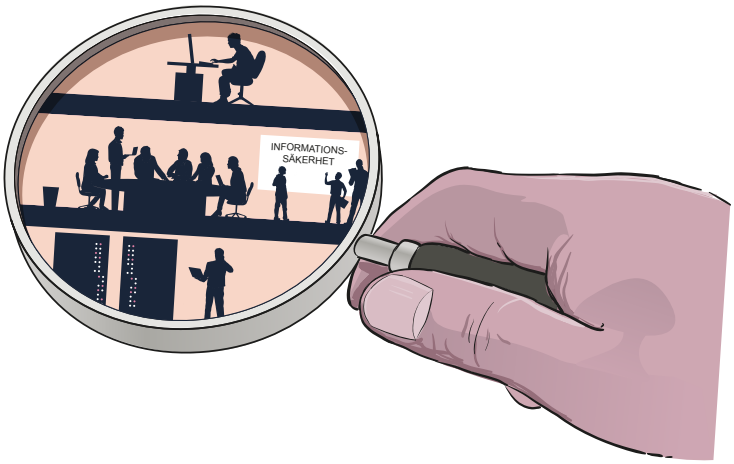
Genomförande

Alla deltagare ska vara införstådda med varför workshoppen äger rum, vad arbetet innebär, hur modellen fungerar samt hur resultatet är tänkt att användas.

Förslag till inledning av workshoppen:

- Agenda för dagen.
- Syftet med dagen och förväntningar.
- Ordningsregler (lyssna aktivt, låta alla komma till tals, ha ett öppet sinne).
- Kort introduktion till Mognadsdialogen och hur resultatet ska användas.
- Upplägg för mognadsbedömningen och hur arbetet ska dokumenteras. Utse vem som ska ansvara för att dokumentera under workshoppen.

Börja med att gå igenom vad Mognadsdialogen är och hur den är uppbyggd, säkerställ att alla har förstått innan arbetet påbörjas.



Följ sedan arbetsflödet genom att:

1. Arbeta med ett perspektiv i taget. Bekanta er med respektive perspektiv och processen, det som ingår i perspektivet.
2. Samtala och enas om vilken nivå som bäst överensstämmer med er organisations mognadsnivå.
3. Inventera och resonera kring förbättringsförslag som skulle kunna öka mognaden.
4. När alla perspektiv är klara, gå igenom hela resultatet. Känns resultatet rimligt och rätt? Prioritera förbättringsförslag.
5. Dokumentera vad ni kommit fram till på ett övergripande men begripligt sätt.

Efterarbete och användning av resultatet

Efter mötet sammanställs resultatet på detaljnivå så att underlaget blir lätt att använda och förstå senare. Förankra den bearbetade versionen med workshoppens deltagare. Resultatet används för att prioritera vilka åtgärder som behöver införas för att föra organisationens informationssäkerhetsarbete framåt.

Nu är det dags att använda resultatet, och det är viktigt att det fattas beslut om vad som ska prioriteras för att öka mognaden och vad som tillfälligt nedprioriteras. Om mognadsbedömningen gjordes med ledningen kan de ge CISO i uppdrag att utarbeta ett förslag till handlingsplan som innehåller tydliga åtgärder och prioriteringar, som de senare kan fatta beslut om.

Om resultatet ska presenteras för ledningen i efterhand, är det viktigt att tänka på att resonemanget presenteras tydligt så att ledningen kan känna igen sig i beskrivningen av nuläget och ta till sig resultatet. Kom ihåg att inleda med att gå igenom Mognadsdialogens övergripande uppbyggnad.

Tips på vägen

Mognadsdialogen är ett arbetssätt för att komma vidare i ert systematiska informationssäkerhetsarbete genom att få förståelse för nuläget och öka engagemanget för informationssäkerhet. Vid nästa mognadsdialog kan jämförelse göras mot tidigare genomförda dialoger och organisationens utveckling blir tydlig.

Mognadsdialogen kan anpassas för att fungera bättre i just din organisation, så prova er fram vad som passar er. Lycka till i förbättringsarbetet med er informationssäkerhet.

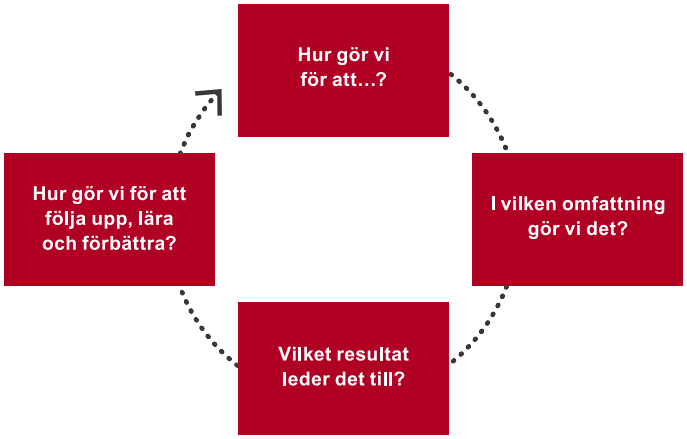
Att leda gruppen genom Mognadsdialogens arbetssteg

Här är några tips och råd för dig som ska leda workshoppen, exempelvis hur du använder bilder och mallar, samt andra praktiska tips.

Förståelse för modellen

Börja med att gå igenom modellen och använd illustrationerna markerade med 1-3 i worshopmaterialet. Skriv gärna ut illustration 2 och eventuellt perspektivbilderna till deltagarna, så att de kan gå tillbaka och läsa när de behöver.

Illustration 1. Säkerställ att alla förstår skillnaden mellan arbetssätt, tillämpning, resultat samt följa upp, lära och förbättra.



Arbetssätt – Hur säger vi att vi ska göra? Har vi etablerade och medvetet valda arbetssätt? Är de kända? Är arbetssätten nya? Hur väl är de integrerade och samverkar med andra arbetssätt? Stödjer arbetssätten våra mål och planer? (Med arbetssätt avses vanligtvis dokumenterade riktlinjer, rutiner, metoder och organisation.)

Tillämpning – I vilken omfattning använder vi arbetssätten, gör vi som vi säger att vi ska göra?

Resultat – Vilka resultat leder våra arbetssätt till? Vilka bevis finns? Finns koppling till våra strategier och mål? Kan resultaten härledas till arbetssätten? Hur är resultatens nivåer i förhållande till målen, i jämförelse med andra? Är resultaten uthålliga, har de förbättrats över tid?

Följa upp, lära och förbättra – Hur följer vi upp arbetssättens ändamåls-enlighet, tillämpning och effektivitet? Hur leder uppföljningen till lärande och till förbättringar av arbetssätten?

Tips! Resonera gärna lite extra kring skillnaden mellan resultat och följa upp, lära, förbättra. Notera särskilt att ordet *hur* betonas, exempelvis *hur* ni gör när ni följer upp.

Illustration 2. Gå igenom den generiska nivåbeskrivningen som beskriver *hur* en organisation i allmänhet fungerar på de fyra olika nivåerna.

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kännetecken	Reaktiv	Viss systematik	Förbättringsdriv	Proaktiv
Arbetssätt				
Tillämpning				
Resultat				
Följa upp, lära och förbättra				

Tips! Jämför med arbetet inom ett helt annat område, exempelvis miljö.

Illustration 3. Gå igenom vilka perspektiv i det systematiska informationssäkerhetsarbetet som kommer att bedömas på workshoppen och i vilken ordning.

Nivå 4						
Nivå 3						
Nivå 2						
Nivå 1						
	Risk-hantering	Info-klassning	Incident-hantering	Upp-handling	Kompetens	Upp-följning

Mognadsbedömningen

Använd process- och perspektivbilder. Arbeta med ett perspektiv i taget.

Börja med processbilden så att alla har klart för sig vad som ingår exempelvis i riskhanteringsprocessen. Därefter går ni igenom det aktuella perspektivet. Låt var och en läsa igenom först, och ett tips är att de skriver ner sin egen bedömning innan ni samtalar gemensamt.

Figur 6. Exempel riskhanteringens ingående delar

Resonera om skillnaderna mellan de olika nivåerna. Diskutera och reflektera över hur det ser ut i er organisation för att komma fram till vilken mognadsnivå som bäst beskriver organisationens nuläge. Här följer några ytterligare frågor att ta stöd av:

- **Arbetssätt.** Är de dokumenterade och beslutade? Finns det områden där var och en har sitt eget arbetssätt, jobbar efter ”eget huvud”? Är de relevanta, hänger arbetssätten ihop, vad saknas?
- **Tillämpning.** Fortsätt med att reflektera över huruvida arbetssätten används, följs och tillämpas. I vilken omfattning används arbetssätten – av alla i organisationen, vissa enheter eller personer, eller inte någon dvs. arbetssättet är en hyllvärmare? Hur etablerade är arbetssätten, har de just börjat användas?
- **Resultat.** Vilka bevis finns för att arbetssätten ger den effekt det är tänkt? Finns mål och nås målen? Vilka resultat finns sammanställda? Finns trender? Är de positiva? Görs jämförelser med andra organisationer?
- **Följa upp, lära och förbättra.** Diskutera kring hur arbetssätten följs upp och analyseras, och hur arbetssätten förbättras. Hur skapas ett lärande när vi följer upp?

Var lyhörd för om gruppen har helt eller delvis olika uppfattningar om en bedömning. Det behöver inte vara negativt, utan kan istället vara en möjlighet att skapa ny insikt och förståelse om organisationen. Kom ihåg att ställa öppna frågor (vad- och hur-frågor). Låt var och en beskriva vad de ser utifrån sin horisont.

När ni börjar bli klara, sammanfatta diskussionen med att komma överens om mognadsnivån. Dokumentera vilken nivå ni enas om i mallen. Dokumentera också löpande för varje perspektiv vad som fungerar bra, styrkor samt brister och förbättringsområden. Dokumentera åskådligt så att alla kan hänga med, när ni skapar den gemensamma bilden av nuläget.

Tips! Använd whiteboard eller blädderblock med – och + och skriv ner det som framkommer. Eller jobba direkt i ett dokument på datorn så att alla kan se.

Resonera kring vad som bäst skulle kunna öka mognaden eller möjliga/viktiga prioriteringar eller nedprioriteringar.

Avslutning

När alla perspektiv bedömts, sammanfatta och reflektera över resultatet. Stämmer bilden av nuläget? Är det något ni vill justera, något som missats eller glömts bort?

Gå igenom vilka förslag på förbättringar som dokumenterats. Kom överens om nästa steg och hur resultatet ska tas vidare.

Några frågor att diskutera och fatta beslut om:

Vilka arbetssätt eller satsningar skulle få oss att stärka vårt systematiska arbete, dvs. öka mognaden?

- Vilka förbättringsområden bör prioriteras närmaste tiden?
- Vilka förbättringsområden bör tillfälligt nedprioriteras närmaste tiden?
- När och hur bör åtgärderna följas upp? Ansvar?
- Hur ska vi följa upp bedömningen i Mognadsdialogen?

Slutligen utvärderas mötet. Har förväntningarna infriats eller inte? Hur har dialogen fungerat, har alla kommit till tals? Vad tar vi med oss?

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1996 – juni 2022 ISBN 978-91-7927-280-7