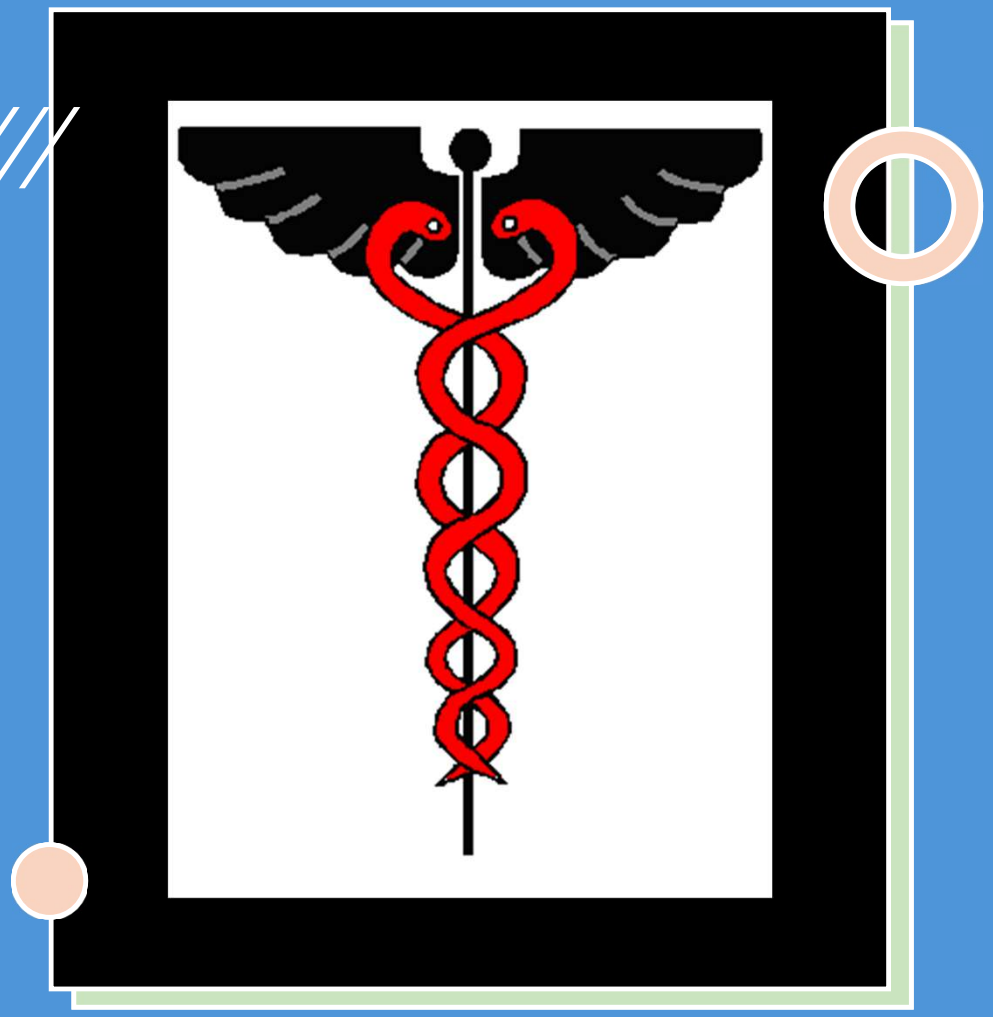
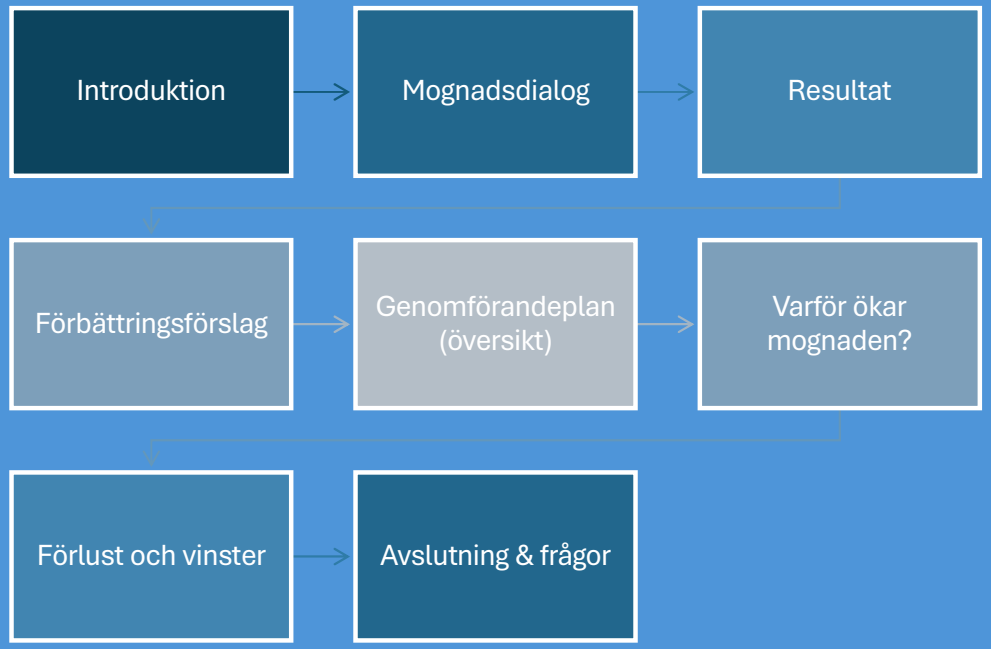
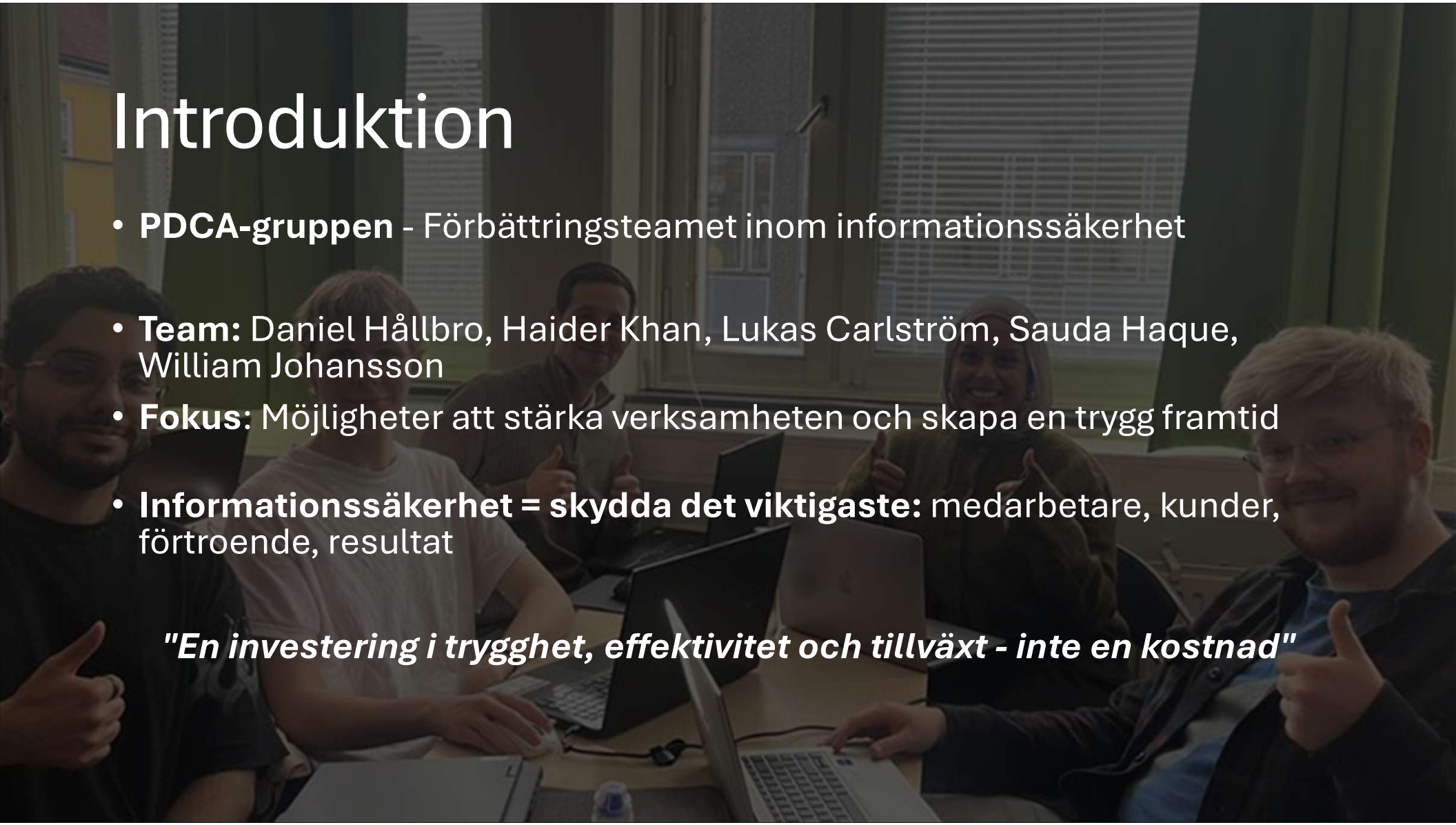
PillMedTech

Informationssäkerhetsanalys



Innehåll


Introduktion
Mognadsdialog
Resultat
Förbättringsförslag
Genomförandeplan (översikt)
Varför ökar mognaden?
Förlust och vinster
Avslutning & frågor



Introduktion

- **PDCA-gruppen** - Förbättringsteamet inom informationssäkerhet

- **Team:** Daniel Hållbro, Haider Khan, Lukas Carlström, Sauda Haque, William Johansson
- **Fokus**: Möjligheter att stärka verksamheten och skapa en trygg framtid

- **Informationssäkerhet = skydda det viktigaste:** medarbetare, kunder, förtroende, resultat

"En investering i trygghet, effektivitet och tillväxt - inte en kostnad"

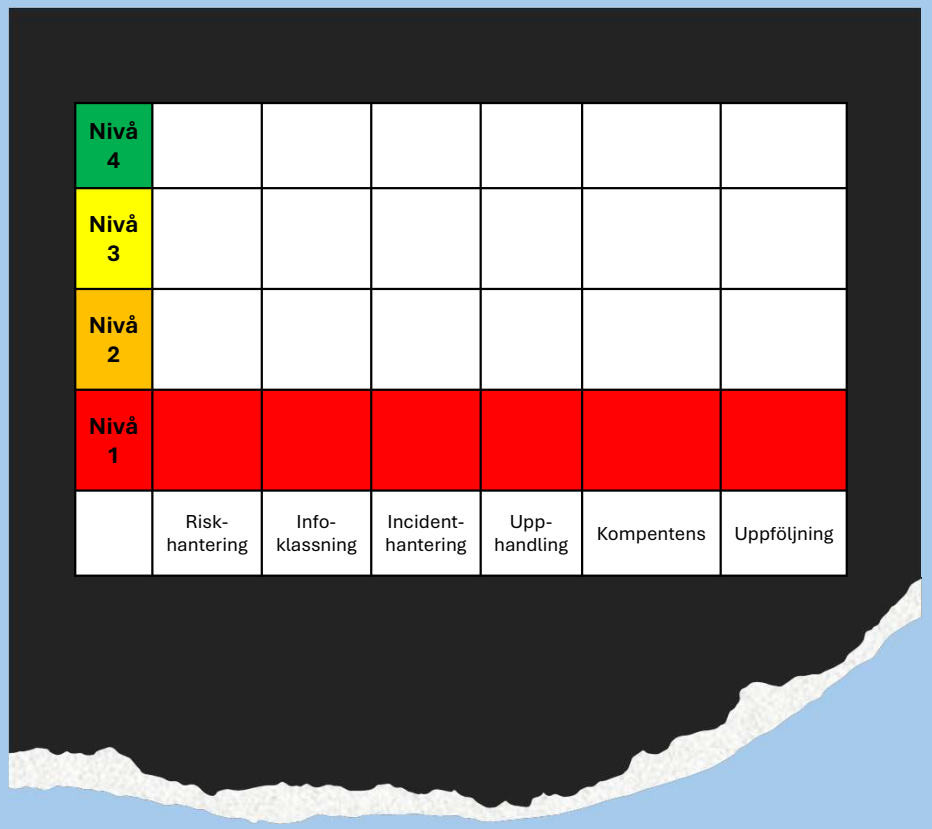
Mognadsdialogen

- MSB:s verktyg för att bedöma informationssäkerheten
- Samsyn
- Nuläge, förbättringar?
- Bygger på sex perspektiv
- Bedömning

Mognadsdialogens nivåbeskrivning

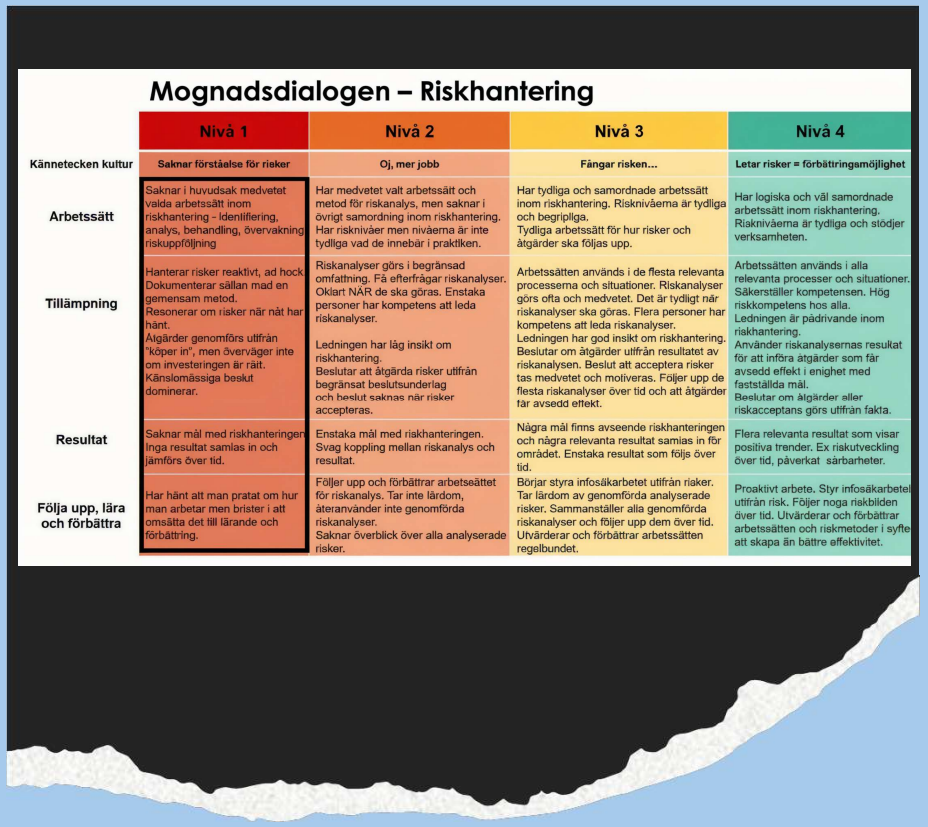
Kännetecken/kultur	Nivå 1 Reaktiva	Nivå 2 Viss systematik	Nivå 3 Förbättringsdriv	Nivå 4 Proaktiv, förutseende
Arbetssätt	Saknar i huvudsak gemensamma medvetet valda arbetssätt inom området. Lösryckte arbetssätt finns men ofta otydliga, okända eller hänger inte ihop. Låg insikt om behov av struktur inom området.	Några gemensamma, medvetet valda arbetssätt inom området. Arbetssätten hänger inte alltid ihop (samordnade). Insikt om behov av struktur och systematik finns.	Flera gemensamma, medvetet valda arbetssätt. Arbetssätten hänger ihop (samordnade). Bygger struktur och systematik. Roller och ansvar finns. Högt driv för struktur och systematik	Genomtänka, medvetet valda, väl samordnade arbetssätt inom området. Mycket systematiska och proaktiva. Arbetssätten utgår tydligt från intressenternas krav, behov och förväntningar. Roller och ansvar är adekvata och fungerar väl.
Tillämpning	Var och en arbetar efter eget huvud och situationen styr. Vissa arbetssätt tillämpas sporadiskt.	Arbetssätten används i begränsad omfattning, dvs inte i alla relevanta processer och situationer. Arbetssätt kan nyligen ha införts eller håller på att införas. Inte kända hos alla.	Arbetssätten är kända. Arbetssätten används i god omfattning i de flera relevanta processer/situationer.	Arbetssätten är välkända, används i alla relevanta processer/situationer.
Resultat	Inga långsiktiga resultat samlas in, eller jämförs över tid. Enstaka resultat och ekonomiresultat har fokus. Saknar mål.	Enstaka resultat samlas in och jämförs över tid men hänger ofta inte ihop med formulerade mål. Enstaka goda resultat. Resultaten kan sällan härledas till arbetssätten.	Flertalet resultat samlas in och jämförs över tid. Vissa uthålliga positiva resultat, vilka kan kopplas till formulerade mål. Jämför inte resultat med andra. Viss osäkerhet om resultat kan härledas till arbetssätten.	Flera relevanta resultat som visar positiva trender kopplade till formulerade mål. Positiva, uthålliga resultat, även i jämförelse med andra organisationer. Resultat kan tydligt härledas till arbetssätten. Resultatfokus
Följa upp, lära och förbättra	Reaktiv. Fokus på problemlösning och korrigerande åtgärder. Saknar insikt, men pratar OM uppföljning. Följer inte upp, utvärderar och lär inte över tid.	Enstaka arbetssätt och processer följs upp, resultat (mest tillämplighet) analyseras. Förbättringar sker ofta ad hoc eller genomförs inte systematiskt. Börjar få insikt – driver på samverkan och teamarbete.	Flera arbetssätt/processer följs upp, resultaten (mest ändamålsenlighet) analyseras och leder till förbättringar. Viss osäkerhet om orsak och verkan. Lärande börjar få fokus för förbättringar. Hög insikt, nyfikenhet och ifrågasättande.	Proaktiv. Relevanta arbetssätt/processer följs upp, analyseras och förbättringar sker, metodiskt och agilt utifrån att öka effektivitet. Högt fokus på lärande i hela organisationen.

Resultat


Nivå 4
Nivå 3
Nivå 2
Nivå 1
Risk-hantering
Info-klassning
Incident-hantering
Upp-handling
Kompentens
Uppföljning

Mognadsdialogen - Riskhantering

- **Skala:** 1
- **Varför?**
  - Riskanalyser genomförs ej
  - Virus-angrepp
  - Ledningen - Säkerhet
  - Saknar uppföljning



Mognadsdialogen – Riskhantering

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kännetecken kultur	**Saknar förståelse för risker**	**Oj, mer jobb**	**Fångar risken…**	**Letar risker = förbättringsmöjlighet**
Arbetssätt	Saknar i huvudsak medvetet valda arbetssätt inom riskhantering - identifiering, analys, behandling, övervakning riskuppföljning	Har medvetet valt arbetssätt och metod för riskanalys, men saknar i övrigt samordning inom riskhantering. Har risknivåer men nivåerna är inte tydliga vad de innebär i praktiken.	Har tydliga och samordnade arbetssätt inom riskhantering. Risknivåerna är tydliga och begripliga. Tydliga arbetssätt för hur risker och åtgärder ska följas upp.	Har logiska och väl samordnade arbetssätt inom riskhantering. Riaknivåerna är tydliga och stödjer verksamheten.
Tillämpning	Hanterar risker reaktivt, ad hock Dokumenterar sällan mad en gemensam metod. Resonerar om risker när nåt har hänt. Åtgärder genomförs utifrån "köper in", men överväger inte om invesseringen är rätt. Känslomässiga beslut dominerar.	Riskanalyser görs i begränsad omfattning. Få efterfrågar riskanalyser. Oklart NÄR de ska göras. Enstaka personer har kompetens att leda riskanalyser. Ledningen har låg insikt om riskhantering. Beslutar att åtgärda risker utifrån begränsat beslutsunderlag och beslut saknas när risker accepteras.	Arbetssätten används i de flesta relevanta processerna och situationer. Riskanalyser görs ofta och medvetet. Det är tydligt när riskanalyser ska göras. Flera personer har kompetens att leda riskanalyser. Ledningen har god insikt om riskhantering. Beslutar om åtgärder utifrån resultatet av riskanalysen. Beslut att acceptera risker tas medvetet och motiveras. Följer upp de flesta riskanalyser över tid och att åtgärder får avsedd effekt.	Arbetssätten används i alla relevanta processer och situationer. Säkerställer kompetensen. Hög riskkompetens hos alla. Ledningen är pådrivande inom riskhantering. Använder riskanalysernas resultat för att införa åtgärder som får avsedd effekt i enighet med fastställda mål. Beslutar om åtgärder eller riskacceptans görs utifrån fakta.
Resultat	Saknar mål med riskhanteringen Inga resultat samlas in och jämförs över tid.	Enstaka mål med riskhanteringen. Svag koppling mellan riskanalys och resultat.	Några mål finns avseende riskhanteringen och några relevanta resultat samias in för området. Enstaka resultat som följs över tid.	Flera relevanta resultat som visar positiva trender. Ex riskutveckling över tid, påverkat sårbarheter.
Följa upp, lära och förbättra	Har hänt att man pratat om hur man arbetar men brister i att omsätta det till lärande och förbättring.	Följer upp och förbättrar arbetseättet för riskanalys. Tar inte lärdom, återanvänder inte genomförda riskanalyser. Saknar överblick över alla analyserade risker.	Börjar styra infosäkarbetet utifrån risker. Tar lärdom av genomförda analyserade risker. Sammanställer alla genomförda riskanalyser och följer upp dem över tid. Utvärderar och förbättrar arbetssätten regelbundet.	Proaktivt arbete. Styr infosäkarbetet utifrån risk. Följer noga riskbilden över tid. Utvärderar och förbättrar arbetssätten och riskmetoder i syfte att skapa än bättre effektivitet.

Förbättringsförslag - Riskhantering

Vad?

- Inför & dokumentera system
- Åsidosätt tid
- Utbilda personal
- Revidera ledningsmötena

Hur?

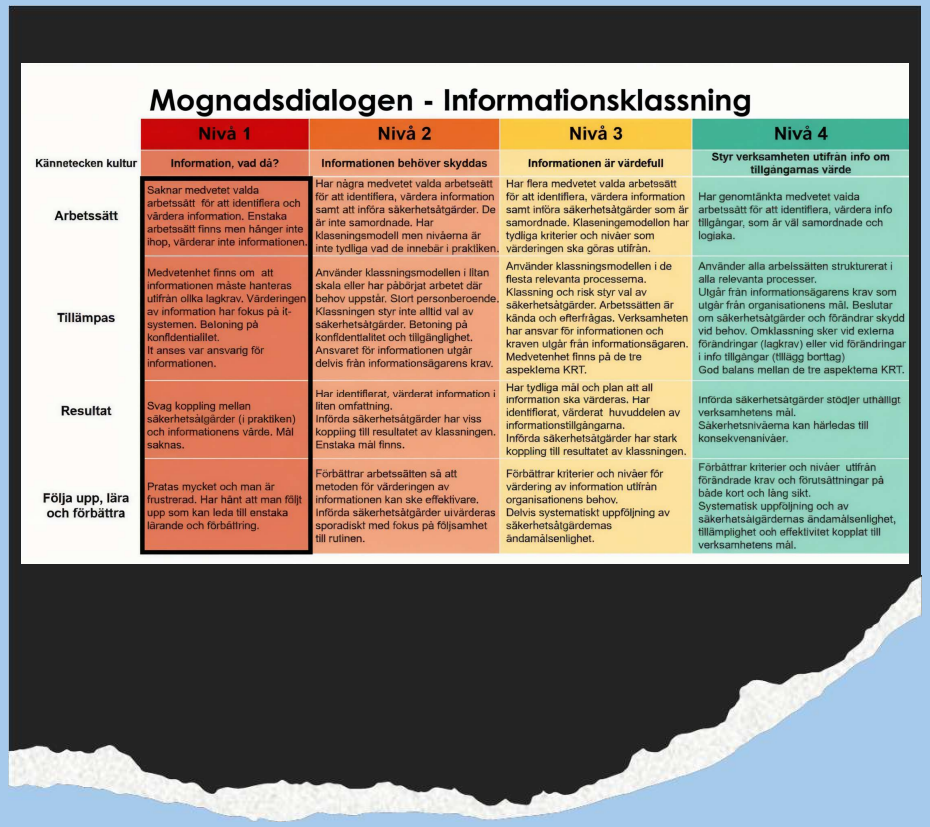
- Säkerhet som stående punkt vid möten
- Genomför riskanalyser
- Phishing-mejl

Vem?

- VD/Ledningen: Planerar, tid/möten
- IT: Skickar ut fake phishing-mejl
- Säkerhetschef: Genomför riskanalys

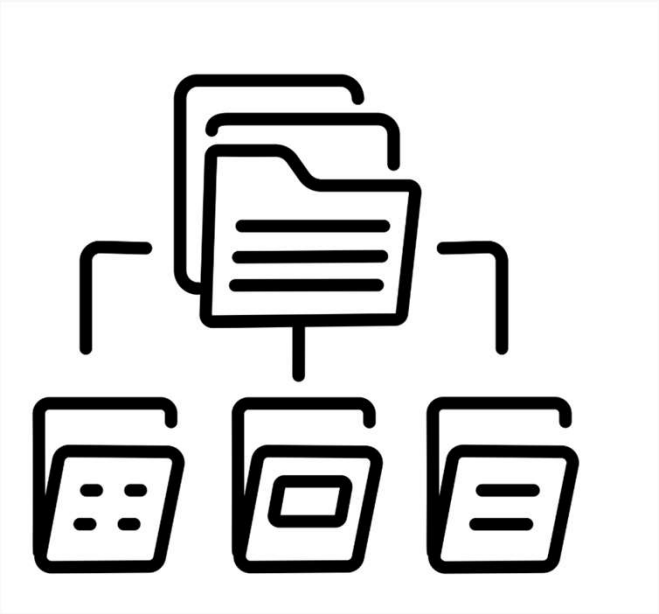
Mognadsdialogen - Informationsklassning

- **Skala**: 1
- **Varför?**
  - Ingen modell eller styrdokument
  - All information behandlas likadant
  - Inbrott: Svårt att veta om känslig info förlorades
  - Ingen uppföljning eller förbättring



Mognadsdialogen - Informationsklassning

Kännetecken kultur	Nivå 1 Information, vad då?	Nivå 2 Informationen behöver skyddas	Nivå 3 Informationen är värdefull	Nivå 4 Styr verksamheten utifrån info om tillgångarnas värde
Arbetssätt	Saknar medvetet valda arbetssätt för att identifiera och värdera information. Enstaka arbetssätt finns men hänger inte ihop, värderar inte informationen.	Har några medvetet valda arbetssätt för att identifiera, värdera information samt att införa säkerhetsåtgärder. De är inte samordnade. Har klasningsmodell men nivåerna är inte tydliga vad de innebär i praktiken.	Har flera medvetet valda arbetssätt för att identifiera, värdera information samt införa säkerhetsåtgärder som är samordnade. Klaseningemodellon har tydliga kriterier och nivåer som värderingen ska göras utifrån.	Har genomtänkta medvetet vaida arbetssätt för att identifiera, värdera info tillgångar, som är väl samordnade och logiaka.
Tillämpas	Medvetenhet finns om att informationen måste hanteras utifrån ollka lagkrav. Värderingen av information har fokus på it-systemen. Beloning på konfidentiallitet. It anses var ansvarig för informationen.	Använder klassningsmodellen i liten skala eller har påbörjat arbetet där behov uppstår. Stort personberoende. Klassningen styr inte alltid val av säkerhetsåtgärder. Betoning på konfidentialitet och tillgänglighet. Ansvaret för informationen utgår delvis från informationsägarens krav.	Använder klassningsmodellen i de flesta relevanta processerna. Klassning och risk styr val av säkerhetsåtgärder. Arbetssätten är kända och efterfrågas. Verksamheten har ansvar för informationen och kraven utgår från informationsägaren. Medvetenhet finns på de tre aspektema KRT.	Använder alla arbelssätten strukturerat i alla relevanta processer. Utgår från informationsägarens krav som utgår från organisationens mål. Beslutar om säkerhetsåtgärder och förändrar skydd vid behov. Omklassning sker vid exlerna förändringar (lagkrav) eller vid förändringar i info tillgångar (tillägg borttag) God balans mellan de tre aspektema KRT.
Resultat	Svag koppling mellan säkerhetsåtgärder (i praktiken) och informationens värde. Mål saknas.	Har identifierat, värderat information i liten omfattning. Införda säkerhetsåtgärder har viss koppiing till resultatet av klassningen. Enstaka mål finns.	Har tydliga mål och plan att all information ska värderas. Har identifiorat, värderat huvuddelen av informationstillgängarna. Införda säkerhetsåtgärder har stark koppling till resultatet av klassningen.	Införda säkerhetsåtgärder stödjer uthålligt verksamhetens mål. Säkerhetsniväema kan härledas till konsekvenaniväer.
Följa upp, lära och förbättra	Pratas mycket och man är frustrerad. Har hänt att man följt upp som kan leda till enstaka lärande och förbättring.	Förbättrar arbetssätten så att metoden för värderingen av informationen kan ske effektivare. Införda säkerhetsåtgärder uivärderas sporadiskt med fokus på följsamhet till rutinen.	Förbättrar kriterier och nivåer för värdering av information utifrån organisationens behov. Delvis systematiskt uppföljning av säkerhetsåtgärdernas ändamålsenlighet.	Förbättrar kriterier och nivåer utifrån förändrade krav och förutsättningar på både kort och lång sikt. Systematisk uppföljning och av säkerhetsåtgärdernas ändamålsenlighet, tillämplighet och effektivitet kopplat till verksamhetens mål.



Förbättringsförslag - Informationsklassning

Vad?

- Införa klassningsmodell
- Koppla till lagkrav och skydd
- Utbilda VD/IT

Hur?

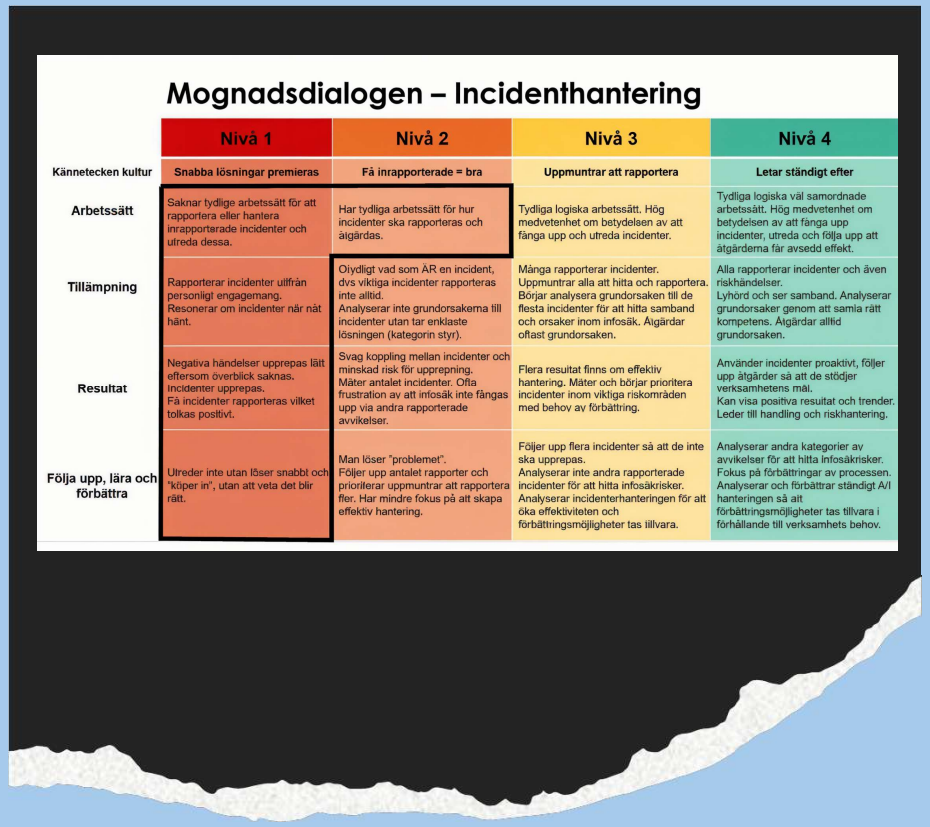
- Besluta modell
- Testa på viktig info
- Utbilda personal
- Koppla till behörighet, backup, kryptering

Vem?

- VD: beslutar
- CISO: leder
- IT: tekniska skydd
- Chefer: klassar sin info

Mognadsdialogen - Incidenthantering

- **Skala**: 1
- **Varför?**
  - Policy finns, övriga styrdokument saknas.
  - Bristande analys av grundorsaker.
  - Upprepning av incidenter.
  - Förbättra uppföljning och motverkan.



Mognadsdialogen – Incidenthantering

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kännetecken kultur	**Snabba lösningar premieras**	**Få inrapporterade = bra**	**Uppmuntrar att rapportera**	**Letar ständigt efter**
Arbetssätt	Saknar tydlige arbetssätt för att rapportera eller hantera inrapporterade incidenter och utreda dessa.	Har tydliga arbetssätt för hur incidenter ska rapporteras och åtgärdas.	Tydliga logiska arbetssätt. Hög medvetenhet om betydelsen av att fånga upp och utreda incidenter.	Tydliga logiska väl samordnade arbetssätt. Hög medvetenhet om betydelsen av att fånga upp incidenter, utreda och följa upp att åtgärderna får avsedd effekt.
Tillämpning	Rapporterar incidenter utifrån personligt engagemang. Resonerar om incidenter när nåt hänt.	Oiydligt vad som ÄR en incident, dvs viktiga incidenter rapporteras inte alltid. Analyserar inte grundorsakerna till incidenter utan tar enklaste lösningen (kategorin styr).	Många rapporterar incidenter. Uppmuntrar alla att hitta och rapportera. Börjar analysera grundorsaken till de flesta incidenter för att hitta samband och orsaker inom infosäk. Åtgärdar oftast grundorsaken.	Alla rapporterar incidenter och även riskhändelser. Lyhörd och ser samband. Analyserar grundorsaker genom att samla rätt kompetens. Åtgärdar alltid grundorsaken.
Resultat	Negativa händelser upprepas lätt eftersom överblick saknas. Incidenter upprepas. Få incidenter rapporteras vilket tolkas positivt.	Svag koppling mellan incidenter och minskad risk för upprepning. Mäter antalet incidenter. Ofta frustration av att infosäk inte fångas upp via andra rapporterade avvikelser.	Flera resultat finns om effektiv hantering. Mäter och börjar prioritera incidenter inom viktiga riskområden med behov av förbättring.	Använder incidenter proaktivt, följer upp åtgärder så att de stödjer verksamhetens mål. Kan visa positiva resultat och trender. Leder till handling och riskhantering.
Följa upp, lära och förbättra	Utreder inte utan löser snabbt och "köper in", utan att veta det blir rätt.	Man löser "problemet". Följer upp antalet rapporter och prioriterar uppmuntrar att rapportera fler. Har mindre fokus på att skapa effektiv hantering.	Följer upp flera incidenter så att de inte ska upprepas. Analyserar inte andra rapporterade incidenter för att hitta infosäkrisker. Analyserar incidenterhanteringen för att öka effektiviteten och förbättringsmöjligheter tas tillvara.	Analyserar andra kategorier av avvikelser för att hitta Infosäkrisker. Fokus på förbättringar av processen. Analyserar och förbättrar ständigt A/I hanteringen så att förbättringsmöjligheter tas tillvara i förhållande till verksamhets behov.

Förbättringsförslag - Incidenthantering

Vad?

- Införa ett tydligare och konkret arbetssätt för att rapportera, samordna och följa upp incidenter.

Hur?

- Se över riktlinjer och rutiner samt hur dessa kommuniceras.
- Formulär för incidentrapportering.
- Utbilda och följ upp.

Vem?

- Säkerhetschef och CISO med stöd av ledningsgruppen

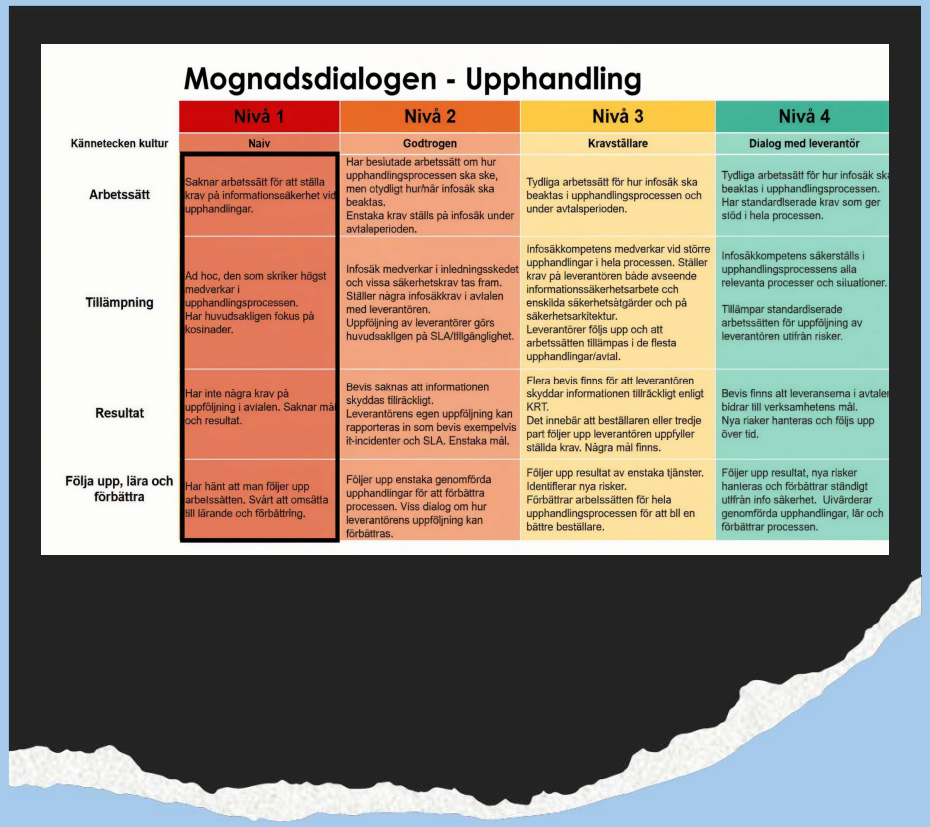
Tips! Ta hjälp av

SS-EN ISO/IEC 27002:2022: Kapitel 5.24-27

MSB's Metodstöd - Incidenthantering

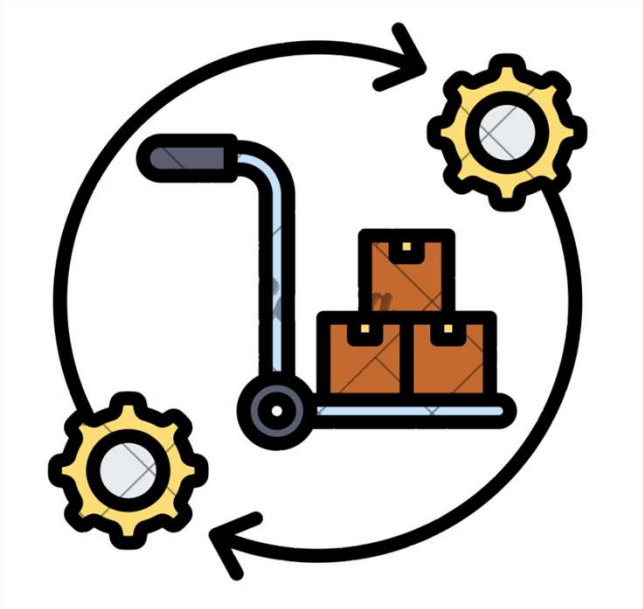
Mognadsdialogen - Upphandling

- **Skala: 1**
- **Varför?**
  - Säkerhetskrav i upphandlingar & avtal är ej definierade.
  - Leverantörsstyrning saknar systematik.
  - Saknar systematisk uppföljning av avtal & leveranser.



Mognadsdialogen - Upphandling

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kännetecken kultur	Naiv	Godtrogen	Kravställare	Dialog med leverantör
Arbetssätt	Saknar arbetssätt för att ställa krav på informationssäkerhet vid upphandlingar.	Har beslutade arbetssätt om hur upphandlingsprocessen ska ske, men otydligt hur/när infosäk ska beaktas. Enstaka krav ställs på infosäk under avtalsperioden.	Tydliga arbetssätt för hur infosäk ska beaktas i upphandlingsprocessen och under avtalsperioden.	Tydliga arbetssätt för hur infosäk ska beaktas i upphandlingsprocessen. Har standardiserade krav som ger stöd i hela processen.
Tillämpning	Ad hoc, den som skriker högst medverkar i upphandlingsprocessen. Har huvudsakligen fokus på kosinader.	Infosäk medverkar i inledningsskedet och vissa säkerhetskrav tas fram. Ställer några infosäkkrav i avtalen med leverantören. Uppföljning av leverantörer görs huvudsakligen på SLA/tillgänglighet.	Infosäkkompetens medverkar vid större upphandlingar i hela processen. Ställer krav på leverantören både avseende informationssäkerhetsarbete cch enskilda säkerhetsåtgärder och på säkerhetsarkitektur. Leverantörer följs upp och att arbetssätten tillämpas i de flesta upphandlingar/avtal.	Infosäkkompetens säkerställs i upphandlingsprocessens alla relevanta processer och situationer. Tillämpar standardiserade arbetssätten för uppföljning av leverantören utifrån risker.
Resultat	Har inte några krav på uppföljning i avialen. Saknar mål och resultat.	Bevis saknas att informationen skyddas tillräckligt. Leverantörens egen uppföljning kan rapporteras in som bevis exempelvis it-incidenter och SLA. Enstaka mål.	Flera bevis finns för att leverantören skyddar informationen tillräckligt enligt KRT. Det innebär att beställaren eller tredje part följer upp leverantören uppfyller ställda krav. Några mål finns.	Bevis finns att leveransema i avtalen bidrar till verksamhetens mål. Nya risker hanteras och följs upp över tid.
Följa upp, lära och förbättra	Har hänt att man följer upp arbelssätten. Svårt att omsätta till lärande och förbättring.	Följer upp enstaka genomförda upphandlingar för att förbättra processen. Viss dialog om hur leverantörens uppföljning kan förbättras.	Följer upp resultat av enstaka tjänster. Identifierar nya risker. Förbättrar arbelssätten för hela upphandlingsprocessen för att bli en bättre beställare.	Följer upp resultat, nya risker hanteras och förbättrar ständigt utifrån info säkerhet. Utvärderar genomförda upphandlingar, lär och förbättrar processen.



Förbättringsförslag - Upphandling

Vad?

- Fixa ett styrdokument för upphandling med upphandlingsprocesser.

Hur?

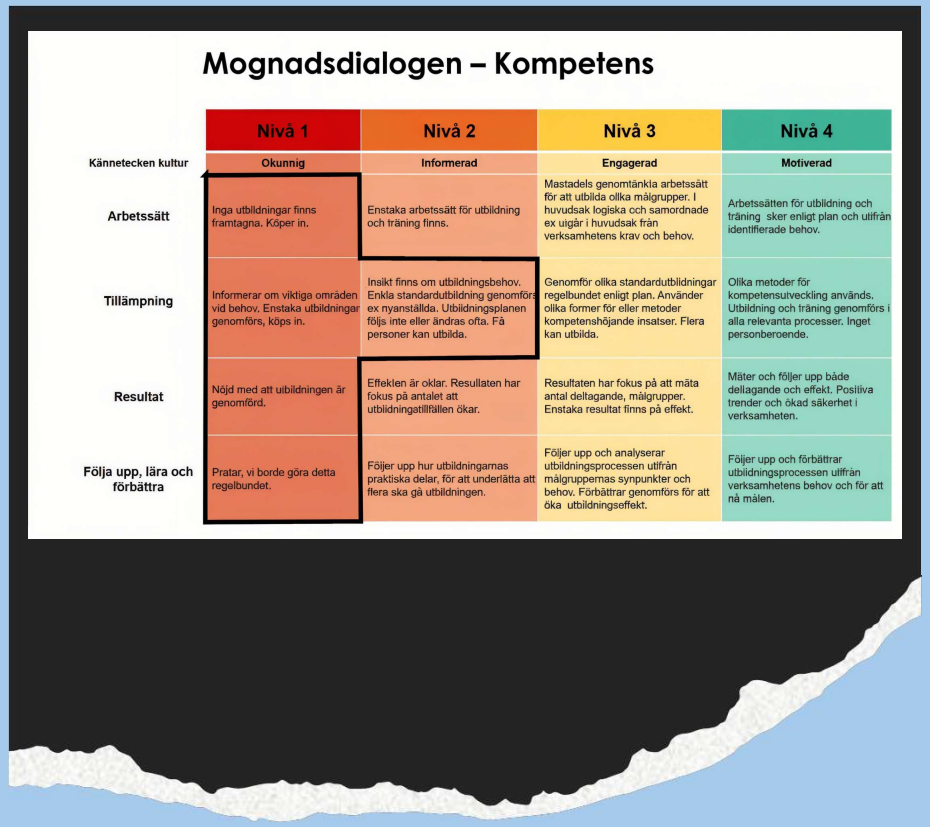
- Inför mall-bilagor med: Säkerhetskrav. Leverantörsbedömning innan avtal. Grundlig bakgrundskontroll av leverantör. Årlig uppföljning av leverantörer.
- Få in rutinen!

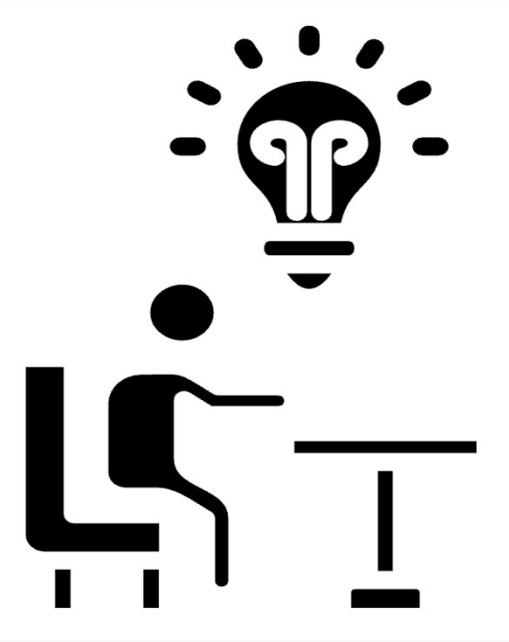
Vem?

- CISO sätter krav på leverantörer, jurist för legalitet.
- Avdelningschef.

Mognadsdialogen - Kompetens

- **Skala: 1**
- **Varför?**
  - Avsaknad av säkerhetsutbildning vid anställning.
  - Har förståelse för att utökad utbildning skulle förbättra verksamheten.





Förbättringsförslag - Kompetens

Vad?

- Öka förståelsen och medvetenheten av informationssäkerhet i arbetet.

Hur?

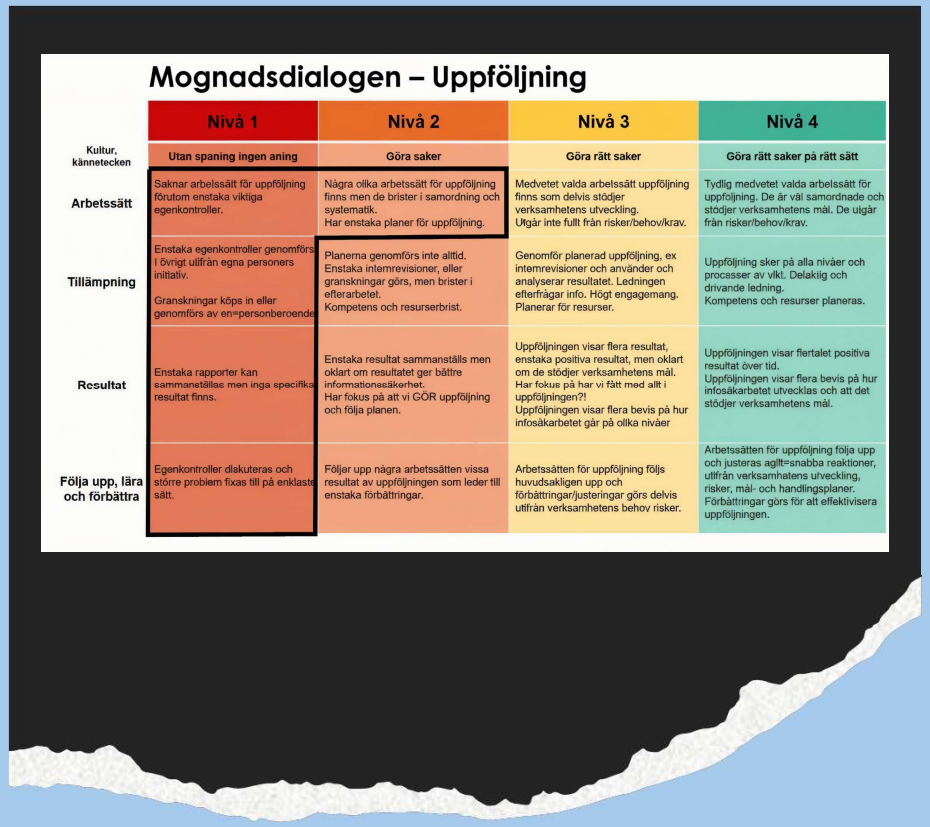
- Anordna workshops.
- Minute learning.
- Kompetens-tester
- Ge Säkerhetschefen en formell säkerhetsutbildning.

Vem?

- HR, CISO och Chefer.
- Göran Rubens.

Mognadsdialogen - Uppföljning

- **Skala: 1**
- **Varför?**
  - Ingen systematisk uppföljning, arbetet sker ad hoc och ej enligt policy
  - Backup tas, men återställning testas inte och incidenter dokumenteras inte
  - Säkerhetsarbetet är personberoende, saknar gemensamma rutiner
  - Data riskeras, katastrofplaner saknas och inga mätbara förbättringar finns
  - Följa upp, lära och förbättra innebär att vi kontrollerar om åtgärder fungerar i praktiken, drar lärdomar av incidenter och använder erfarenheterna för att införa konkreta förbättringar.



Mognadsdialogen – Uppföljning

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kultur, kännetecken	Utan spaning ingen aning	Göra saker	Göra rätt saker	Göra rätt saker på rätt sätt
Arbetssätt	Saknar arbetssätt för uppföljning förutom enstaka viktiga egenkontroller.	Några olika arbetssätt för uppföljning finns men de brister i samordning och systematik. Har enstaka planer för uppföljning.	Medvetet valda arbetssätt uppföljning finns som delvis stödjer verksamhetens utveckling. Utgår inte fullt från risker/behov/krav.	Tydlig medvetet valda arbetssätt för uppföljning. De är väl samordnade och stödjer verksamhetens mål. De utgår från risker/behov/krav.
Tillämpning	Enstaka egenkontroller genomförs i övrigt utifrån egna personers inittiativ. Granskningar köps in eller genomförs av en=personberoende	Planerna genomförs inte alltid. Enstaka internrevisioner, eller granskningar görs, men brister i efterarbetet. Kompetens och resurserbrist.	Genomför planerad uppföljning, ex internrevisioner och använder och analyserar resultatet. Ledningen efterfrågar info. Högt engagemang. Planerar för resurser.	Uppföljning sker på alla nivåer och processer av vlkt. Delaktig och drivande ledning. Kompetens och resurser planeras.
Resultat	Enstaka rapporter kan sammanställas men inga specifika resultat finns.	Enstaka resultat sammanställs men oklart om resultatet ger bättre informationssäkerhet. Har fokus på att vi GÖR uppföljning och följa planen.	Uppföljningen visar flera resultat, enstaka positiva resultat, men oklart om de stödjer verksamhetens mål. Har fokus på har vi fått med allt i uppföljningen?! Uppföljningen visar flera bevis på hur infosäkarbetet går på olika nivåer	Uppföljningen visar flertalet positiva resultat över tid. Uppföljningen visar flera bevis på hur infosäkarbetet utvecklas och att det stödjer verksamhetens mål.
Följa upp, lära och förbättra	Egenkontroller diskuteras och större problem fixas till på enklaste sätt.	Följer upp några arbetssätten vissa resultat av uppföljningen som leder till enstaka förbättringar.	Arbetssätten för uppföljning följs huvudsakligen upp och förbättringar/justeringar görs delvis utifrån verksamhetens behov risker.	Arbetssätten för uppföljning följs upp och justeras agilt=snabba reaktioner, utifrån verksamhetens utveckling, risker, mål- och handlingsplaner. Förbättringar görs för att effektivisera uppföljningen.

Förbättringsförslag - Uppföljning

Vad?

- Införa tydlig uppföljningsprocess
- KPI:er för incidenter, backup & utbildning
- Stickprov & interna revisioner

Hur?

- Kvartalsvisa möten per avdelning
- Använd mallar för rapportering
- Säkerhetschef samordnar

Vem?

- Säkerhetschef: rapporterar till ledning
- Avdelningschefer: följer upp kvartalsvis
- IT: testar backuper
- Ledning: granskar årligen enligt ISO 27001

Tidsplan: 0-6 månader

Vad ska vi börja med?

- **Styrdokument – Riktlinjer och rutiner**
  - Se över befintliga riktlinjer och rutiner
    - Behöver de uppdateras?
    - Behövs det fler?
- **Se över och utöka utbildning i organisationen**
  - Utbilda medarbetare i nya riktlinjer och rutiner
- **Informationsklassningsmodell**
  - Börja med att klassa information
    - Klassa.skr.se
    - Pocketsafe.se
    - MSB's metodstöd - Klassningsmodell

…Och vidare framöver

Förslagsvis

- **6-12 månader**
  - Hur har det gått?
  - Gör Mognadsdialogen igen
    - Uppnår vi nivå 2?
  - Börja arbeta mot nivå 3

- **Långsiktigt mål**
  - Isocertifiering
    - Stärker organisation och varumärke
    - Lönsamhet och bra kultur

Således ökar mognaden

- Från ad hoc → systematiskt och enhetligt arbete
- Tydliga rutiner för risker, incidenter och information
- Roller och ansvar gör att rutinerna följs
- Mätbara resultat och uppföljning
- Ständig förbättring genom lärande (PDCA)
- Höjer mognaden från nivå 1 till nivå 3

Förlust och vinster

Förlust:

- Projekt som har gått förlorade
- Produktivitet och tid
- Otrygghet
- Risk för framtiden

Vinster:

- Effektivitet och trygghet
- Kundförtroende
- Attraktiv arbetsgivare
- Långsiktig stabilitet
- Konkurrensfördel

Avslutning

- Informationssäkerhet är en möjlighet att bygga styrka och förtroende
- PillMedTech har många styrkor: vi kan tillsammans höja mognaden
- Rekommendation: steg-för-steg med ledningens stöd
- Skapar arbetssätt som möter krav och ger försprång framåt
- Ledningens engagemang är nyckeln till framgång
- Informationssäkerhet kan bli en av PillMedTechs största styrkor

- **Frågor/funderingar?**

Tack för oss!

Daniel Hållbro
Haider Khan
Lukas Carlström
Sauda Haque
William Johansson

Källor

- 2-1 PillMedTech_Version_1-4
- Policy för informationssäkerhet PillMedTech version 2
- SKRs informationssäkerhetsarbetets grunder
- MSBs mognadsdialogen
- Metodstöd för informationssäkerhetsarbete | MSB