Myndigheten för samhällsskydd och beredskap

UTBILDNING I SYSTEMATISKT INFORMATIONSSÄKERHETSARBETE

# Handledning för CISO

**Titel**


Enhet: Enheten för systematisk informationssäkerhet

Produktion: Advant

Publikationsnummer: MSB1838 – september 2021
ISBN: 978-91-7927-186-2

# Innehåll

Denna handledning är för den som ska ge utbildning i systematiskt informationssäkerhetsarbete för lokala informationssäkerhetssamordnare. Dokumentet innehåller en beskrivning av utbildningsmaterialet som ingår i utbildningen, hur materialet kan användas och hur det kan anpassas till organisationens egen verksamhet. Det tar cirka åtta timmar att genomföra utbildningen fysiskt eller digitalt.

Utbildningens innehåll utgår från MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

# Inledning

## Målet med utbildningen

Målet med utbildningen är att ge grundläggande teoretiska kunskaper i informationssäkerhet. Deltagarna ska efter utbildningen ha förståelse för varför och hur informationssäkerhetsarbete bedrivs.

Ytterligare ett mål är att deltagarna ska få öva på att genomföra praktiska arbetsuppgifter som de på sikt kan komma att genomföra själva. Därför innehåller utbildningen uppgifter som är vanliga inom operativt systematiskt informationssäkerhetsarbete. Som underlag för att lösa uppgifterna kan det fiktiva företaget EL-VIS AB:s verksamhet och organisation användas.

Utbildningen är tänkt som en introduktion och kan kompletteras med hur den egna organisationen bedriver sitt informationssäkerhetsarbete. För att deltagarna självständigt ska kunna utföra arbetsuppgifter inom informationssäkerhetsarbetet kommer de att behöva mer utbildning och övning i er organisations regelverk och arbetssätt.

Utbildningen är framtagen för att fungera både när alla är fysiskt i samma rum och om utbildningen sker digitalt.

## Målgrupper för utbildningen

Materialet är utformat för dig som är CISO att använda som en introduktionsutbildning för i första hand lokala informationssäkerhetssamordnare. Lokala informationssäkerhetssamordnare är de personer som hjälper dig i det dagliga operativa informationssäkerhetsarbetet genom att stödja verksamheter i olika informationssäkerhetsfrågor och på så sätt frigöra tid för dig att arbeta strategiskt och taktiskt med informationssäkerhet.

Du som håller i utbildningen behöver ha kunskap om systematiskt informationssäkerhetsarbete och MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

Du bör också ha kunskap om den egna organisationens informationssäkerhetsarbete. Då kan du anpassa utbildningen till organisationens egna behov och förutsättningar.

## Tidsåtgång för att genomföra utbildningen

Utbildningsmaterialet är skapat för att genomföra utbildningen under en heldag (8 h) eller två halvdagar (4 h+4 h).

Om du kompletterar utbildningen med information om hur er egen organisation arbetar med informationssäkerhet kan du behöva justera utbildningstiden.

# Utbildningens innehåll och upplägg

Nedan följer en kort beskrivning av utbildningens teoretiska och praktiska delar.

## Teori

Utbildningen ger kunskap som deltagarna behöver ha för att kunna utföra uppgifter inom operativt systematiskt informationssäkerhetsarbete så som:

- Varför systematisk informationssäkerhetsarbetet behövs och hur det kan utföras.
- Viktiga begrepp inom området; bland annat konfidentialitet, riktighet och tillgänglighet.
- Skillnader mellan information och informationstillgång.
- Vikten av korrekt hantering av information och att införa olika typer av säkerhetsåtgärder.
- Vikten av att informationssäkerhetsarbetet styrs och samordnas utifrån verksamhetens behov.

Centralt i de teoretiska och praktiska delarna är de fyra metodstegen Identifiera och analysera, Utforma, Använda, samt Följa upp och förbättra som beskrivs i MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

## Uppgifter inom operativt informationssäkerhetsarbete

Utbildningsmaterialet innehåller fem praktiska uppgifter där deltagarna:

- Identifierar informationstillgångar.
- Bedömer risker.
- Klassar information.
- Föreslår lämpliga säkerhetsåtgärder.
- Presenterar resultatet av sitt arbete för en fiktiv beslutsfattare.

# Utbildningsmaterialets delar

Utbildningsmaterialet består av:

- Handledning för dig som ska hålla utbildningen (det här dokumentet).
- Powerpointpresentation som kan anpassas efter den egna organisationens informationssäkerhetsarbete och hur utbildningen läggs upp.
- Uppgiftsbeskrivning av de praktiska övningarna som innehåller sammanfattning av teori, beskriver syftet med uppgiften samt hänvisningar till stödmaterialet.
- Stödmaterial:
  - Mall med förenklade versioner av metodstödets verktyg för att lösa utbildningens uppgifter.
  - Företagsbeskrivning av det fiktiva företaget EL-VIS AB.
  - Rollkort som sammanfattar tre chefer vid EL-VIS AB syn på sin verksamhet.

## Handledningen till dig som ska utbilda (det här dokumentet)

Beskriver vad utbildningen innehåller och hur materialet kan användas och anpassas.

- I bilaga A hittar du en tabell med stöd för anpassning av Powerpointpresentationen. I bilaga A finns också förslag på talmanus till bilderna.
- Bilaga B innehåller exempel på hot och sårbarheter samt deras konsekvenser för ELVIS-AB.
- Bilaga C innehållet förslag till inbjudan till utbildningen.

## Powerpointpresentation

Powerpointpresentationen innehåller texter och länkar till filmer med

- Teoretisk översikt/introduktion om informationssäkerhet.
- MSB:s metodstöds fyra steg för att arbeta systematiskt med informationssäkerhet.
- Beskrivning av praktiska övningar för att:
  - identifiera informationstillgångar
  - bedöma risker
  - klassa information
  - ta fram förslag på säkerhetsåtgärder
  - presentera resultatet.

Du kan anpassa presentationen utifrån din organisations behov samt utifrån om utbildningen hålls fysiskt eller digitalt. Stöd för anpassning finns i bilaga A i detta dokument.

# Uppgiftsbeskrivning för utbildningsdeltagarna

Materialet ger deltagarna stöd i att lösa fem praktiska uppgifter. Varje uppgift inleds med en sammanfattning av teori och tips kring hur deltagarna kan tänka för att lösa uppgiften. Det finns även hänvisningar till dokumenten företagsbeskrivning, rollkort och mall för dokumentation av uppgifterna.

# Stödmaterial

## Mall för att dokumentera uppgifterna

Mallen består av för uppgifterna anpassade, förenklade verktyg från MSB:s metodstöd. Mallen används för att dokumentera resultatet av de praktiska övningarna. I mallens fem flikar finns stöd för att dokumentera resultatet av uppgifterna:

- Uppgift 1 Identifiera info
- Uppgift 2 Bedöm risk
- Uppgift 3 Klassa info
- Uppgift 4 Säkerhetsåtgärder
- Uppgift 5 Presentera

Om din organisation har egna verktyg och mallar bör du använda dem under utbildningen. Det ger deltagarna möjlighet att bekanta sig med verktyg och mallar som de senare kommer att arbeta med.

## Företagsbeskrivning EL-VIS AB

Använd det fiktiva företaget EL-VIS AB som exempel för att genomföra de praktiska uppgifterna. Dokumentet består av företagets egen beskrivning av sig själva, vad de gör, hur de är organiserade samt några förutsättningar som de identifierat för att kunna driva sin verksamhet. Du kan använda verksamheter i din organisation istället. Gör då en egen beskrivning på motsvarande sätt, och tänk på att ändra i mallar och i uppgifternas exempel.

## Rollkort EL-VIS AB

Rollkorten beskriver bakgrund om EL-VIS AB:s VD samt cheferna för avdelningarna administration, produktion och it. Där finns också sammanfattningar av de intervjuer som företagets CISO gjort med cheferna. Sammanfattningarna beskriver chefernas syn på verksamheten och dess förutsättningar.

Rollkorten kan användas på olika sätt. Kursdeltagarna kan läsa rollkorten. Ett annat alternativ är att låta deltagarna intervjua personer som fått i uppgift att spela de olika rollerna, som då har rollkorten till hjälp. Om du använder en verksamhet i din organisation istället för exempelföretaget EL-VIS AB ersätts rollkorten med att någon verksamhetsansvarig eller motsvarande kommer och presenterar sin verksamhet.

# Inför utbildningen

Du som ska leda utbildningen förbereder dig genom att:

- Läsa på utbildningsmaterialet som hänvisas till i denna handledning.
- Planera utbildningen utefter svaren på följande frågor:
  - Håller du utbildningen fysiskt eller digitalt?
  - Hur många kursdeltagare deltar?
  - Hur många grupper är lämpligt att dela upp deltagarna i?
  - Får du hjälp av någon eller några som kan spela roller eller bidra med något annat?
  - Ska du skicka ut dokumenten företagsbeskrivning och rollkort i förväg med uppmaning att läsa inför utbildningen?
- Anpassa Powerpointpresentationen utifrån Bilaga A.
- Anpassa övrigt material utifrån att du vill använda era verktyg, modeller och er verksamhet som underlag för de praktiska uppgifterna.

Förslag på inbjudan till utbildningen finns i bilaga C.

# Under utbildningen – innehåll och tidsåtgång

### Avsnitt 1: Inledning (cirka 15 minuter)

**Mål:** Deltagarna lär känna varandra genom att presentera sig. De får en överblick av innehållet i utbildningen och hur utbildningen är upplagd.

Ta upp praktiska förutsättningar för utbildningen.

### Avsnitt 2: Introduktion till Informationssäkerhet (cirka 40 minuter och gruppdiskussion cirka 7 min)

**Mål:** Deltagarna får förståelse för vad informationssäkerhet är. De får kännedom om begrepp som används inom området samt förutsättningar för ett bra informationssäkerhetsarbete.

**Teori:**

- Vad informationssäkerhet är.
- Viktiga begrepp inom området så som bland annat: information, informationstillgångar, konfidentialitet, riktighet, tillgänglighet, otillåten hantering av information och säkerhetsåtgärder.
- Styrning av informationssäkerhetsarbete såsom ansvar och roller samt identifiera externa krav och interna behov.

Gruppdiskussion: Diskutera innehållet i filmen.

### Avsnitt 3: Eget informationssäkerhetsarbete (cirka 30 minuter)

Mål: Att beskriva den egna organisationens informationssäkerhetsarbete.

Passa på att marknadsföra befintliga interna regler och stöd samt pågående utveckling.

### Avsnitt 4: MSB:s metodstöd för systematiskt informationssäkerhets-arbete (cirka 10 minuter och gruppdiskussion cirka 7 minuter)

Mål: Kunskap om MSB:s metodstöd för systematiskt informationssäkerhets-arbete, hur det är uppbyggt och vilket stöd som finns att få i metodstödet.

Teori: Metodstödets fyra steg Identifiera och analysera, Utforma, Använda och Följa upp och Förbättra.

Gruppdiskussion: Diskutera innehållet i filmen.

### Avsnitt 5: Företags- eller verksamhetsbeskrivning (cirka 20 minuter)

Mål: Introducera det fiktiva företaget EL-VIS AB eller den verksamhet hos er ni valt.

Presentera företaget eller den verksamhet hos er som används i de praktiska övningarna. Låt deltagarna bekanta sig med dokumenten företagsbeskrivning och rollkort.

### Avsnitt 6: Metodstödets steg Identifiera och analysera (cirka 40 minuter teori och uppgift 20 minuter *2)

Mål: Förståelse för vad som ingår i metodstödets steg Identifiera och analysera. Introduktion till praktisk uppgift.

Teori: Beskrivning av de analyser som ingår i metodsteget. Fokus på analyserna Identifiera informationstillgångar och Bedöma risker. Hur en organisation kan använda resultatet av respektive analys.

Uppgift: Utgå från muntlig och/eller skriftlig beskrivning av en verksamhet. Identifiera informationstillgångar och bedöm risker med att hantera information på det sätt som den beskrivna verksamheten gör.

I bilaga B finns exempel på risker och sårbarheter som stöd för dig om du använder exempelföretaget ELVIS-AB.

### Avsnitt 7: Metodstödets steg Utforma (cirka 15 minuter och gruppdiskussion cirka 10 minuter)

Mål: Förståelse för arbetet med att ta fram eller anpassa interna regler och arbetssätt inom informationssäkerhet.

Teori: Arbetssätt som metodstödet föreslår för att ta fram interna regler och stöd inom informationssäkerhet.

Gruppdiskussion: Diskutera innehållet i EL-VIS AB:s informationssäkerhetspolicy.

### Avsnitt 8: Metodstödets steg Använda (cirka 15 minuter och uppgifter cirka 2x20 minuter)

Mål: Förståelse för vikten av att framtagna interna regler och arbetssätt används och efterlevs samt hur man kan främja detta.

Teori: Beskriver vikten av att utbilda och informera om framtaget informationssäkerhetsmaterial så att det används. Fokus på materialet för informationsklassning.

Uppgifter: Klassa information utifrån klassningsmatrisen och välja lämpliga säkerhetsåtgärder utifrån resultatet av riskbedömning och informationsklassning.

### Avsnitt 9: Metodstödets steg Följa upp och förbättra (cirka 15 minuter och uppgift 30 minuter)

Mål: Deltagarna förstår vikten att följa upp och förbättra interna regelverk, stöd och arbetssätt samt hur man kan arbeta med detta.

Teori: Så kan interna regelverk, informationssäkerhetsarbete och enskilda säkerhetsåtgärder i en organisation utvärderas och följas upp. Så ger du beslutsfattare underlag som de kan använda för att ta de beslut som behövs.

Uppgift: Presentera resultatet från de uppgifter som deltagarna genomfört under utbildningen för en beslutsfattare. Beslutsfattaren ska baserat på presentationen kunna förbättra informationssäkerheten inom sitt ansvarsområde genom att införa nya eller förbättrade säkerhetsåtgärder.

### Avsnitt 10: Avsluta (cirka 20 minuter)

Mål: Sammanfatta utbildningens innehåll och utvärdera utbildningen.

# Efter utbildningen

Använd utvärderingarna från Avsnitt 10. Vad kan du justera eller göra bättre inför nästa utbildningstillfälle?

Har du förbättringsförslag på utbildningsmaterialet? Mejla till informationssakerhet@informationssakerhet.se

# Bilaga A

## – Talmanus och stöd för att anpassa Powerpointpresentationen

Utgå från förslagen och prata fritt från bilderna eller skriv ett eget talmanus i Powerpointpresentationens anteckningsdel. Det senare är särskilt bra om olika personer genomför utbildningen vid olika tillfällen.

Tabellen ger en överblick av Powerpointpresentationens innehåll och har följande kolumner

- Bild – numret på bilden i Powerpointpresentationen (observera att om du lägger till egna bilder kommer numreringen att förskjutas).
- Avsnitt –beskriver vilka bilder som hör ihop genom att ta upp ett specifikt ämne.
- Anpassning – Markeringarna nedan står också på Powerpoint-bilderna och beskriver hur du anpassar presentationen.
  - Anpassa ( ) – behöver anpassas eller kan behöva anpassas.
  - Fysiskt möte ( ) – om utbildningen sker fysiskt.
    Dölj de bilder som är märkta
  - Digitalt möte ( ) – om utbildningen sker digitalt.
    Dölj de bilder som är märkta
- Talmanus – Förslag på talmanus finns till de flesta bilder. Du är fri att justera detta. ”[bildtext]” betyder att du kan tala från texten på den aktuella Powerpoint-bilden.
- Tips och referenser – Tips och referenser till mer information.

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 1 | 1 Inledning | | Välkommen till dagens utbildning i systematiskt informationssäkerhetsarbete! | |
| 2 | 1 Inledning |  | Dagens agenda: [läs från bildtext]. | Ändra agendan om du ändrat innehållet i och/eller upplägget för utbildningen. |
| 3 | 1 Inledning |  | [läs från bildtext] | Presentera dig, deltagarna och grupperna. Gå igenom information som är viktig. |
| 4 | 1 Inledning |  | [läs från bildtext] | Presentera dig, deltagarna och grupperna. Gå igenom information som är viktig. |
| 5 | 1 Inledning | | [läs från bildtext] | Om utbildningen är en av flera i en serie utbildningar ni lagt upp för att utbilda era informationssäkerhetssamordnare informera om det här. |
| 6 | 2 Informations-säkerhet | | Nu går vi in på vad systematisk informationssäkerhet är. | Fråga gärna vad deltagarna känner till om informationssäkerhet. |
| 7 | 2 Informations-säkerhet | | Vi ska titta på en film som visar varför informationssäkerhet är viktigt. | Diskutera filmens budskap med deltagarna efter filmen. |
| 8 | 2 Informations-säkerhet | | Information är det som ska skyddas. Information kan vara av olika värde i olika situationer och kan om den hanteras fel ge problem för en organisation själv eller andra.<br>[läs om olika information på bilden]<br>På nästa bild pratar vi mer om begreppen konfidentialitet, riktighet och tillgänglighet. | Prata om närliggande begrepp så som data, informationstillgångar och kunskap.<br>Diskutera gärna de olika typerna av information som finns på bilden utifrån när de behövs och för vem de är viktiga. Till exempel: priset på korv – olika för konsument respektive konkurrent? |
| 9 | 2 Informations-säkerhet | | De här tre begreppen, konfidentialitet, riktighet och tillgänglighet är viktiga inom informationssäkerhet. [läs bildtext] | |
| 10 | 2 Informations-säkerhet | | Vad som är felaktig hantering varierar. Hur man ska hantera olika information beskrivs i organisationens regler. Det är viktigt att förstå att felaktig hantering kan ge konsekvenser för enskilda personer i organisationen, och ibland för samhället. | Diskutera påståendena på bilden. Vad vill de visa på för problem? Använd gärna begreppen konfidentialitet, riktighet, tillgänglighet. |
| 11 | 2 Informations-säkerhet | | Vi skyddar informationen mot felaktig hantering genom att införa olika säkerhetsåtgärder. [bildtext]<br>Under dagen kommer vi att prata mer om att arbeta systematiskt med informationssäkerhet, risker och hur man skyddar information tillräckligt. | Både ett arbetssätt som hjälper till att välja tillräckliga säkerhetsåtgärder och att införa och förvalta enskilda säkerhetsåtgärder (organisatoriska, administrativa, tekniska och fysiska). |
| 12 | 2 Informations-säkerhet | | Systematiskt informationssäkerhetsarbete kännetecknas bland annat av: [läs från bildtext]. | |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 13 | 2 Informations-säkerhet | | Strategisk, taktisk och operativ beskriver informationssäkerhetsarbetets olika nivåer. På varje nivå leds arbetet, beslut fattas och arbete utförs och följs upp. Hur detta görs kan variera beroende på verksamhet och på vilken nivå man avser. | Strategisk, taktisk och operativ kommer från management-teori och är ett sätt att tänka på styrning. |
| 14 | 2 Informations-säkerhet | | Ledningens ansvar är att sätta mål och ge inriktning åt verksamheternas arbete. Det inkluderar informations-säkerhetsarbetet.<br>CISO står för Chief Information Security Officer och är den som leder och samordnar informationssäkerhets-arbetet i en organisation.<br>Chefers ansvar är att leda sin verksam-het och att ge information som hanteras i verksamheten tillräckligt skydd.<br>Medarbetare med särskilt utpekade roller inom informationssäkerhetsarbetet hjälper till att stötta verksamheten uti-från sin kompetens och ansvarsområde tex it-chef (it-miljön), personalchef (per-sonalsäkerhet), ekonomichef (upphand-ling), fastighetschef (lokaler) osv.<br>Alla medarbetare har ett ansvar för att hantera den information de arbetar med säkert genom att följa interna regler. | Diskutera gärna vad ansvar betyder i er organisation och hur rollerna ser ut hos er. |
| 15 | 2 Informations-säkerhet |  | [läs från bildtext]<br>Beroende på vilken roll en person har ser ansvaret för informationssäkerhet olika ut. Ansvaret kan tex innebära att ta fram underlag och stödja i olika situationer eller fatta beslut (chefer). | Har CISO annat ansvar i er organisa-tion? Uppdatera i så fall texten. |
| 16 | 2 Informations-säkerhet |  | [bildtext] | Uppdatera om er organisation berörs av annan reglering som är särskilt viktig för er. |
| 17 | | | PAUS | |
| 18 | 3 Eget informations-säkerhetsarbete |  | | |
| 19 | 3 Eget informations-säkerhetsarbete |  | | Anpassa efter vad ni i organisationen gjort och planerar att göra i ert infor-mationssäkerhetsarbete. |
| 20 | 3 Eget informations-säkerhetsarbete |  | | Beskriv din roll närmare och vilket ansvar du har. |
| 21 | 3 Eget informations-säkerhetsarbete |  | | Justera utifrån vad deltagarna ska göra i organisationens informations-säkerhetsarbete framöver. |
| 22 | 3 Eget informations-säkerhetsarbete |  | | Justera utifrån det ansvar deltagarna kommer att ha och vilka uppgifter de kommer att utföra. |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 23 | 4 Metodstödet | | Nu går vi vidare med att titta på MSB:s metodstöd för informationssäker och dess delar. Metodstödet [läs bildtext]. | Mer information: https://www.informationssakerhet.se/metodstodet/metodstodet/ |
| 24 | 4 Metodstödet | | | Diskutera filmens budskap med deltagarna efter filmen. |
| 25 | 5 Företags-beskrivning |  | Fram tills nu har vi pratat om grunderna i informationssäkerhet. Som utgångspunkt för de övningar ni kommer att göra ska vi nu presentera ett företag. [bildtext] | Antingen presenterar du företaget eller så görs presentationen av någon som spelar en av företagets roller t.ex. VD. Deltagarna kan också själva läsa på materialen Företagsbeskrivning EL-VIS AB och Rollkortet för den verksamhet de ska analysera. |
| 26 | 5 Företags-beskrivning |  | Hej! Jag arbetar på ett modernt och miljövänligt företag. Mitt namn är [rollkort] och jag är [rollkort] på EL-VIS AB [bildtext]. | Kan bytas mot eget exempel. Tänk då på att ändra i mallar och i uppgifternas exempel.<br>Mer tips om vad du kan berätta om finns i företagsbeskrivningen för EL-VIS AB och på rollkorten för den roll du representerar. |
| 27 | 5 Företags-beskrivning |  | Vi driver ett vattenkraftverk, vi ansvarar också för en damm och att dammvallen är säker. Vårt kraftverk kan producera en effekt på upp till 50 MW. | |
| 28 | 5 Företags-beskrivning |  | Vi är ett aktiebolag. Våra ägarförhållanden: Elvis G.P. Karlsson äger 20 % av aktierna, medarbetare och släkt ytterligare 25 %. Vår organisation [läs bildtext].<br>Vi har en extern it-leverantör som heter ExtremIT. De hanterar en hel del av vår it-miljö men inte allt. | |
| 29 | 5 Företags-beskrivning |  | Gällande informationssäkerhetsarbetet, som vi förstår ni är särskilt intresserade av, [läs bildtext]<br>Vi är ganska bra på informationssäkerhet tycker vi själva. Tack för mig! | |
| 30 | 6 Metodstöd Analysera | | | |
| 31 | 6 Metodstöd Analysera | | Det här stegets syfte är att förstå verksamhetens behov och förutsättningar genom att genomföra olika analyser: [läs bildtext]. | Mer information: https://www.informationssakerhet.se/metodstodet/analysera/ |
| 32 | 6 Metodstöd Analysera | | Följande analyser ingår i metodsteget. Vi ska gå igenom verksamhetsanalys och riskanalys mer noggrant snart men innan dess en kort beskrivning av syftet med de övriga analyserna:<br>Omvärldsanalys – här identifierar vi externa krav och förutsättningar inklusive rättsliga krav samt våra externa intressenter.<br>Gapanalysen – här jämför vi den nivå av säkerhet som vi ser att vi har med den vi borde ha.<br>Under verksamhetsanalysen identifierar vi [läs bildtext i höger spalt]. | |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 33 | 6 Metodstöd Analysera Tillgångar | | [bildtext] | Mer information: https://www.informationssakerhet.se/metodstodet/analysera/#verksamhetsanalys<br>Resurser som behandlar information: genom att ta emot, lagra, bearbeta, visa eller kommunicera den. |
| 34 | 6 Metodstöd Analysera Tillgångar |  | Nu ska vi gå till den mall som vi ska använda för att göra första uppgiften. | Gå igenom hur deltagarna kan tänka och vad de olika kolumnerna i verktyget betyder. |
| 35 | 6 Metodstöd Analysera Tillgångar |  | Uppgift 1 Identifiera informations-tillgångar | Fråga gärna efter att uppgiften är genomförd hur det gått. |
| 36 | 6 Metodstöd Analysera Tillgångar |  | Uppgift 1 Identifiera informations-tillgångar | Fråga gärna efter att uppgiften är genomförd hur det gått. |
| 37 | 6 Metodstöd Analysera Risk | | Nu går vi över till att titta på hur vi kan förstå mer om risker med hur vi hanterar vår information: [bildtext]. | Mer information: https://www.informationssakerhet.se/metodstodet/analysera/#riskanalys<br>Arbetet med att införa åtgärderna i planen görs under ”Använda”. |
| 38 | 6 Metodstöd Analysera Risk | | [bildtext] | |
| 39 | 6 Metodstöd Analysera Risk |  | [bildtext] | |
| 40 | 6 Metodstöd Analysera Risk |  | Det här är exempel på kriterier och nivåer för att bedöma konsekvenser. De kommer vi att använda i uppgiften. | Gå övergripande igenom kriterierna och nivåerna. |
| 41 | 6 Metodstöd Analysera Risk |  | Vi kommer också att använda de här nivåerna för att bedöma sannolikhet. Till höger ett exempel på riskmatris som är markerad i fyra färger – risknivåer. | Gå igenom vad de olika kolumnerna betyder. |
| 42 | 6 Metodstöd Analysera Risk |  | Exempel | Gå igenom hur deltagarna kan tänka och vad de olika kolumnerna i verktyget betyder. S = sannolikhetsnivå och K = konsekvensnivå. |
| 43 | 6 Metodstöd Analysera Risk |  | Uppgift 2 Bedöma risker | |
| 44 | 6 Metodstöd Analysera Risk |  | Uppgift 2 Bedöma risker | |
| 45 | | | LUNCH | |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 46 | 7 Metodstöd Utforma | | | |
| 47 | 7 Metodstöd Utforma | | [bildtext] | |
| 48 | 7 Metodstöd Utforma | | För att förstå hur vi ska utforma olika material utgår vi från behovet. Material som behövs på de olika nivåerna strategisk, taktisk och operativ nivå behöver förändras utifrån nya förut-sättningar. Utformningen i de olika nivåerna behöver samverka för att få en helhet som inte är överlappande eller har glapp.<br>Sammanfattningsvis [läs bildtext]. | Mer information: https://www.infor-mationssakerhet.se/metodstodet/utforma/ |
| 49 | 7 Metodstöd Utforma |  | Här är exempel på en struktur för hur en organisation kan utforma sitt interna regelverk för informationssäkerhet. Strukturen ger styrning på de tre nivå-erna, strategisk, taktisk och operativ [bildtext]. | Tänk på att även strategisk nivå behöver och berörs av dokument på operativ nivå.<br>Prata om hur strukturen ser ut i er organisation. Peka särskilt på styr-dokument för informationsklassning och riskbedömning. [viktigt för att hela kedjan ska bli tydlig, från Identi-fiera till Utforma till Använda!] |
| 50 | 7 Metodstöd Utforma | | Här har vi vårt exempelföretags infor-mationssäkerhetspolicy: [bildtext]<br>Vad tycker ni är bra respektive mindre bra med den? | Tips: Bra att skydda det viktigaste men de andra it-systemen då?<br>Bra att inte ändra information i styr- och reglersystem (viktig verksamhet) men de andra it-systemen då?<br>Bra att ledningen ska få stöd men övriga medarbetare då? |
| 51 | 8 Metodstöd Använda | | | |
| 52 | 8 Metodstöd Använda | | [Bildtext] | Mer information: https://www.infor-mationssakerhet.se/metodstodet/anvanda/ |
| 53 | 8 Metodstöd Använda Utbildning | | Att utbilda och kommunicera är viktigt och kan göras på olika sätt. Olika mål-grupper kan behöva olika information och vi behöver vara medvetna om att det finns olika sätt att lära sig saker på t.ex. genom att läsa, lyssna eller prova på och öva.<br>När vi stödjer verksamheter [läs bildtext]. | |
| 54 | 8 Metodstöd Använda Klassa | | Att hjälpa verksamheter att klassa information är nästa uppgift vi stödjer verksamheter med. Att klassa informa-tion är att [läs bildtext]. | Mer information:<br>https://www.informationssakerhet.se/metodstodet/utforma/<br>https://www.informationssakerhet.se/metodstodet/anvanda/#klass-ning-av-information<br>Tänk på att värde för organisationen inkluderar organisationen själv och de kunder, samarbetspartner och andra som är beroende av organisa-tionens informationshantering. |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 55 | 8 Metodstöd Använda Klassa | | Klassning är en värdering av informationens betydelse för verksamheten och dess intressenter. [bildtext] | |
| 56 | 8 Metodstöd Använda Klassa |  | Bedömningarna utgår från organisationens klassningsmatris. | Gå igenom klassningsmatrisen och hur deltagarna ska använda den. |
| 57 | 8 Metodstöd Använda Klassa | | | Gå igenom hur deltagarna kan tänka och vad de olika kolumnerna i verktyget betyder. |
| 58 | 8 Metodstöd Använda Klassa |  | Uppgift 3 Klassa information | |
| 59 | 8 Metodstöd Använda Klassa |  | Uppgift 3 Klassa information | |
| 60 | 8 Metodstöd Använda Säkåtgärd | | Att välja säkerhetsåtgärder är att välja sätt att skydda informationen. Välja säkerhetsåtgärder behöver göras utifrån verksamhetens behov. [läs bildtext] | Organisationens egna säkerhetskrav är sådana krav som kommer tillkommer utifrån den verksamhet (t ex speciella lagkrav) som organisationen bedriver och andra förutsättningar (tex ägarförhållanden, lokalisering). |
| 61 | 8 Metodstöd Använda Säkåtgärd | | De säkerhetsåtgärder vi väljer kan vara [bildtext]. | Mer information: https://www.informationssakerhet.se/metodstodet/utforma/#vad-är-en-säkerhetsåtgärd?-anchor |
| 62 | 8 Metodstöd Använda Säkåtgärd | | En handlingsplan eller åtgärdsplan som vissa säger är [bildtext]. | I metodstödet finns Handlingsplanen under steget identifiera och analysera. Det är för den tas fram där första gången. Här ska säkerhetsåtgärder väljas för att skydda en avgränsad del av organisationens information. Vi använder en handlingsplansmall för att utföra uppgiften |
| 63 | 8 Metodstöd Använda Säkåtgärd |  | Säkerhetsåtgärderna är på övergripande nivå. Om ni får tid, fördjupa gärna säkerhetsåtgärderna utifrån resultatet av era analyser. | Gå igenom hur deltagarna kan tänka och vad de olika kolumnerna i verktyget betyder. |
| 64 | 8 Metodstöd Använda Säkåtgärd |  | Uppgift 4 Ta fram förslag på säkerhetsåtgärder | I det här fallet tar vi fram förslag på säkerhetsåtgärder men det är beslutsfattaren som utifrån sitt ansvar beslutar vilka som ska införas. Detta kan förstås se olika ut i olika organisationer. |
| 65 | 8 Metodstöd Använda Säkåtgärd |  | Uppgift 4 Ta fram förslag på säkerhetsåtgärder | I det här fallet tar vi fram förslag på säkerhetsåtgärder men det är beslutsfattaren som utifrån sitt ansvar beslutar vilka som ska införas. Detta kan förstås se olika ut i olika organisationer. |
| 66 | | | PAUS | |

| PPT-bild | Avsnitt | Anpass-ning | Talmanus | Tips och referenser |
|---|---|---|---|---|
| 67 | 9 Metodstödet Följa upp och förbättra | | | |
| 68 | 9 Metodstödet Följa upp och förbättra | | [bildtext] | |
| 69 | 9 Metodstödet Följa upp och förbättra | | Man följer upp för att förstå hur väl informationssäkerhetsarbetet fungerar och om säkerhetsåtgärder ger det skydd som det är tänkt. [bildtext] | Mer information: https://www.informationssakerhet.se/metodstodet/folja-upp-och-forbattra/<br>Exempel på verktyg som kan ger stöd för att följa upp är Uppföljningsverktyget och MSB:s infosäkkollen https://www.msb.se/infosakkollen |
| 70 | 9 Metodstödet Följa upp och förbättra | | Hur något ska följas upp behöver anpassas. Man kan t.ex. följa upp [läs bildtext]. | |
| 71 | 9 Metodstödet Följa upp och förbättra |  | | Gå igenom hur deltagarna kan tänka inför sin presentation.<br>Har er organisation ett sätt som beslutsunderlag ska skrivas på använd det sättet. |
| 72 | 9 Metodstödet Följa upp och förbättra |  | Uppgift 5 Presentera resultatet för beslutsfattare | |
| 73 | 9 Metodstödet Följa upp och förbättra |  | Uppgift 5 Presentera resultatet för beslutsfattare | |
| 74 | 10 Avsluta | | Idag har vi: [bildtext] … | |
| 75 | 10 Avsluta | | | Fråga deltagarna vad de tänker om informationssäkerhet nu efter dagen. |
| 76 | 10 Avsluta | | Utvärdering | Individuellt eller i arbetsgrupper.<br>Skicka på e-post till dig eller samla in. |
| 77 | 10 Avsluta | | | |

# Bilaga B

## – Exempel på hot, sårbarheter och konsekvenser

Förslag att utgå ifrån om deltagarna har svårt att genomföra uppgiften att bedöma risk. Förslagen är på en övergripande nivå och kan detaljeras.

**Tabell 1.** Exempel på hot, sårbarheter och konsekvenser

| Hot | Sårbarhet | Konsekvenser |
|---|---|---|
| Obehöriga kan ta sig in i företagets lokaler. | Det fysiska skyddet är inte tillräckligt. | Skador på lokalerna.<br>Skador på utrustning.<br>Stulen eller ändrad information. |
| Företagets information skyddas inte tillräckligt. | Företaget vet inte informationens värde och skyddar den därför inte tillräckligt. | Onödigt mycket tid läggs på att diskutera hur informationen ska skyddas.<br>Vilket skydd information får varierar från gång till gång. |
| Information kommer obehörig till del eftersom personalen inte vet hur de ska göra. | Personal vet inte hur de ska hantera viss information | Information lämnas ut eller läcker för att den inte skyddas tillräckligt. |
| Information kommer obehörig till del via it-system. | Ansvarig för it-driften vet inte vilket skydd informationen behöver. | It-system har brister så att informationen inte skyddas tillräcklig. |
| Personalen kommer inte åt information. | Avbrott i it-system är längre än vad verksamheten accepterar. | Företaget förlorar pengar och förtroende hos kunderna. |
| Problem och incidenter hanteras inte tillräckligt snabbt. | Företaget saknar arbetssätt för att hantera incidenter. | Det tar lång tid att få tillbaka verksamheten i normalt läge.<br>Företaget förlorar pengar och förtroende hos kunderna. |
| Privat utrustning med dålig säkerhet kopplas till företagets nät. | Det finns ingen spärr på företagets nät mot annan utrustning än företagets. Det saknas ett ”gästnätverk” där extern utrustning får kopplas in. | Skadlig kod kommer in i företagets nätverk och ställer till stora problem. |
| It-driften från extern leverantör uppfyller inte företagets behov. | Otydliga avtal gällande ansvar och leveranser när det gäller säkerheten. | Otillräckliga it-tjänster, längre avbrott vid incidenter, it-systemen är inte skyddade i den omfattning företaget tror. |
| Dammluckorna öppnas och stängs inte som avsett då den automatiska styrningen inte fungerar. | Oskyddad kommunikation mellan kontorets övervaknings-styrsystem och kraftverkets utrustning. | Personal behöver åka ut till kraftverket för att kontrollera/öppna och stänga manuellt.<br>Översvämning i och ovanför dammen om luckorna inte kan öppnas vid stora vattenflöden.<br>Störningar i kraftproduktionen. |

# Bilaga C

## – Förslag till inbjudan till utbildningen

Välkommen på utbildning i systematiskt informationssäkerhetsarbete!

Utbildningen ger teoretisk kunskap om vad informationssäkerhet är och varför det är viktigt. Du får också öva på att genomföra några arbetsuppgifter som är vanliga inom operativt systematiskt informationssäkerhetsarbete det vill säga för att stödja verksamheter i det dagliga informationssäkerhetsarbetet.

Utbildningen sker ”digitalt”/”fysiskt” den ”datum”. Vi börjar kl ”X” och slutar kl ” Y”. Förutom föreläsningar och övningar kommer vi att ha lunch som ”ingår” (meddela ev allergier) /”du ta med dig” och två pauser.

Den här utbildningen är ”en introduktion till bli lokal informationssäkerhetssamordnare” .

Jag ser fram emot en dag där vi lär känna varandra och kan lära av varandras erfarenheter.

”XXXX”
CISO


Myndigheten för
samhällsskydd
och beredskap


651 81 Karlstad  Tel 0771-240 240  **www.msb.se**
Publ.nr MSB1838 – september 2021  ISBN 978-91-7927-186-2