Myndigheten för samhällsskydd och beredskap

Metodstöd för systematiskt informationssäkerhetsarbete

En översikt

Metodstöd för systematiskt informationssäkerhetsarbete – En översikt

Enheten för systematiskt informationssäkerhetsarbete

Kontakt: informationssakerhet@informationssakerhet.se
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1365 - mars 2019
ISBN: 978-91-7383-992-1

Innehåll

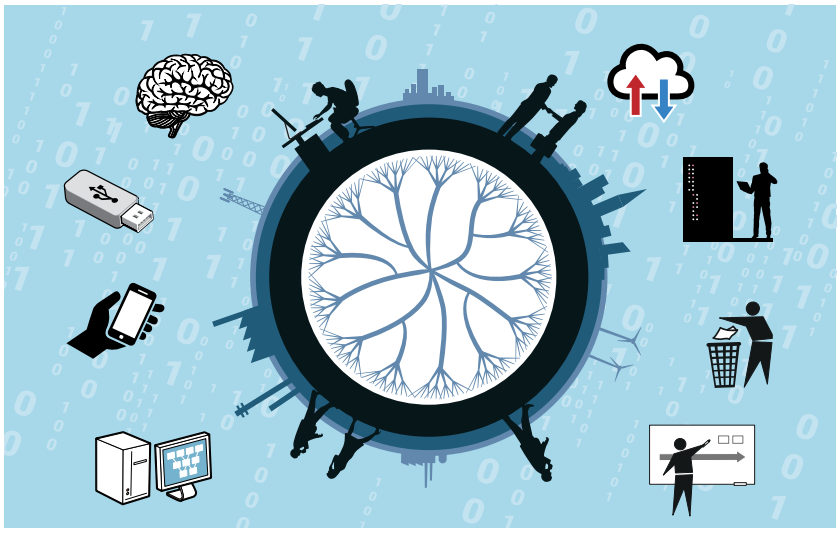
1. Inledning

1.1 Vad är informationssäkerhet?

Alla organisationer är beroende av information för att kunna utföra sina uppdrag. Vi kan kommunicera, lagra och förädla och till och med styra processer med information.

Vår information är värdefull, både för organisationer och för den enskilda individen. Ibland är informationen livsviktig om den återfinns i patientjournaler eller i styrsystemen i kärnkraftverk. Går den informationen förlorad eller är felaktig kan det få katastrofala följder.

Därför måste vi skydda vår information så att den alltid finns när vi behöver den, så att vi kan lita på att den är riktig och inte manipulerad och att endast behöriga personer får ta del av den.



Känslig information kan finnas överallt, inte enbart i elektronisk form utan även i ditt eget huvud, i papperskorgar och på många andra ställen.

Du hittar metodstödet i sin helhet och fler verktyg på: informationssakerhet.se

MSB har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete för att hjälpa organisationer att komma igång med och förbättra informationssäkerhetsarbetet. Syftet med denna översikt är att ge dig och din organisation en översiktlig bild av vad ett systematiskt informationssäkerhetsarbete innebär. Till översikten hör också en separat bilaga, **Framgångsfaktorer och exempel,** med råd och tips på hur du aktivt kan arbeta med Metodstödet i din egen verksamhet.

1.2 Metodstödet

MSB:s Metodstöd är framtaget för att stötta organisationer i att bedriva ett systematiskt informationssäkerhetsarbete. Metodstödet i sin tur bygger på de internationella standarderna i ISO/IEC 27000-serien.

ISO/IEC 27000

Metodstödet beskriver hur de komponenter som utgör ett ledningssystem för informationssäkerhet (LIS) kan utformas. Ett LIS består av alla de delar som krävs för att kunna skapa en systematik för arbetet med informationssäkerhet – allt från styrande dokument till metodik.

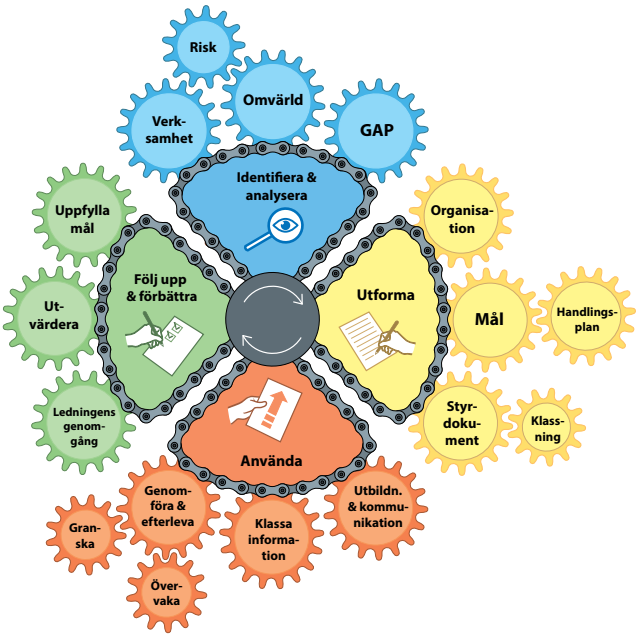
Informationssäkerhet handlar om att ge informationen rätt skydd och omfattar:

- **Konfidentialitet:** Att informationen skyddas mot obehörig insyn
- **Riktighet**: Att informationen skyddas mot oönskad förändring
- **Tillgänglighet:** Att information görs åtkomlig för behörig person vid rätt tillfälle

För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en organisation är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt.

Informationssäkerhet omfattar hela organisationens verksamhet och all information oavsett om den finns i datorer eller på ett papper. Då stora delar av informationen hanteras med hjälp av it-system handlar informationssäkerhet givetvis om teknik, men lika mycket om de rutiner som till exempel användarna behöver för att göra saker rätt.

MSB:s Metodstöd för systematiskt informationssäkerhetsarbete är utformat för att passa alla typer av organisationer. Denna översikt syftar till att ge en överblick av vad Metodstödet är och hur ett införande av ett systematiskt informationssäkerhetsarbete kan gå till.



Metodstödet och de fyra metodstegen med underliggande metoddelar.

Metodstödet är uppdelat i fyra metodsteg: identifiera och analysera, utforma, använda och följa upp samt förbättra med tillhörande metoddelar.

Metoddelarna beskrivs nedan i var sitt eget kapitel tillsammans med en ”att göra”-lista där du också har möjlighet att titta på konkreta exempel i bilagan Framgångsfaktorer och exempel.

Översikten utgår från att ni ska påbörja ett arbete med att implementera ett systematiskt informationssäkerhetsarbete. Metodstödet kan givetvis användas i olika skärningar beroende på hur långt ni kommit i ert arbete, den kan också användas för att introducera någon till informationssäkerhetsområdet.

I praktiken pågår ofta arbete inom flera av metodstegen samtidigt. Därför är de olika delarna i Metodstödet fristående så att organisationen kan välja de metodsteg med tillhörande vägledningar och verktyg som passar verksamhetens aktuella behov.

1.3 Målgrupp

Översikten riktar sig till dig som ansvarar för arbetet med att införa och förvalta ett systematiskt och riskbaserat informationssäkerhetsarbete.

Vanliga benämningar på rollen är informationssäkerhetssamordnare, informationssäkerhetsstrateg eller informationssäkerhetskoordinator. I MSB:s Metodstöd kallas denna person för CISO, en förkortning av den engelska titeln Chief Information Security Officer.

Arbetet med att införa eller vidareutveckla informationssäkerhet är ett lagarbete som kräver engagemang från i princip hela organisationen och särskilt ledningens uppbackning. För att lyckas behövs kunskap om bland annat verksamhetens behov, it-miljön, rättsliga aspekter, ekonomi och revision.

1.4 Nytta

Informationssäkerhet har inget egenvärde i sig utan är en stödfunktion med syftet att skydda er informationshantering som i sin tur ska bidra till att verksamheten kan utföra sitt uppdrag och uppnå sina mål. Systematiskt informationssäkerhetsarbete ger nytta på flera olika sätt, bland annat:

- **Ekonomi**: Informationssäkerhet som är anpassad efter verksamhetens förutsättningar och behov får en bra säkerhetsekonomi genom att säkerhetsincidenter kan undvikas via ett väl avpassat, ändamålsenligt och kostnadseffektivt skydd.
- **Förtroende**: Genom ett systematiskt informationssäkerhetsarbete får om världen och medarbetarna förtroende för organisationen.
- **Efterlevnad:** Ett systematiskt informationssäkerhetsarbete ger goda förutsättningar för att legala krav (till exempel dataskyddslagstiftningen och offentlighets- och sekretesslagen) efterlevs.
- **Styrning:** Ledningen får möjlighet att styra och följa upp informationssäkerheten så att man kan säkerställa dess fortsatta lämplighet, tillräcklighet och verkan.
- **Verksamhetsutveckling**: Informationssäkerhetsarbetet ska möjliggöra ett säkert informationsutbyte och utgöra stöd för utveckling och digitalisering.

2. Att införa ett systematiskt informationssäkerhetsarbete

Ett systematiskt informationssäkerhetsarbete ska vara riskbaserat. Riskanalysen är grundläggande för arbetet och risken styr vilka åtgärder vi vidtar. För detta krävs systematik i både informationssäkerhet och informationsförvaltning.

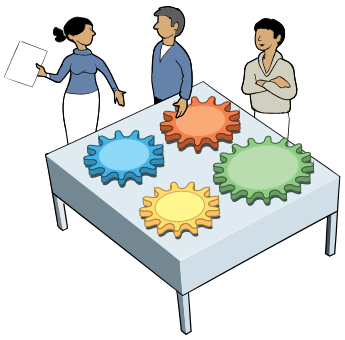
Er organisation kan välja att följa Metodstödet i sin helhet eller bara valda delar. Oavsett vilket måste insatserna anpassas till den egna organisationens specifika situation och behov. Sättet att styra och leda informationssäkerheten i er organisation måste ligga i linje med ert sätt att i övrigt styra och leda verksamheten.

Innan ni sätter igång behöver ni säkerställa att det finns förutsättningar att driva arbetet över tid. Informationssäkerhet är inte en engångsinsats utan kräver nödvändiga resurser både för införandet och efterföljande förvaltningsfas. Därför är det viktigt att ledningen alltid står bakom arbetet och att både ekonomiska och organisatoriska resurser finns tilldelade efter behov.

Ämnets natur kräver också att ett antal nyckelfunktioner knyts till arbetet. Centrala roller som behöver involveras är till exempel dataskyddsombud, it-chef, it-säkerhetsansvarig, arkivarie, säkerhetschef, jurist, kvalitetsansvarig, verksamhetsutvecklare, processägare och kommunikatör.

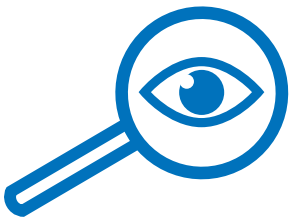
Införandet är i sig ett förändringsarbete och kommer att påverka arbetssätt och relationer mellan olika roller. Därför kan inte behovet av kommunikation och förankring under resans gång understrykas nog. En annan avgörande faktor är uthållighet – ha tålamod det är många olika trådar som ska knytas ihop.

Och kom ihåg att inget är beständigt – arbetet är en konstant process med ständiga anpassningar och förbättringar.



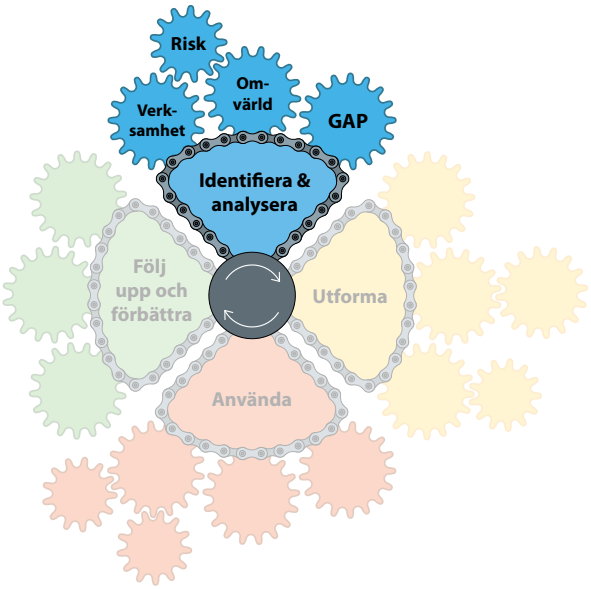
Ni kan följa metodstödet i sin helhet men också välja att enbart arbeta med de delar som känns relevanta.

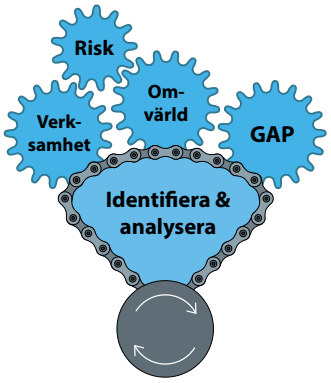
3. Identifiera och analysera



Ett systematiskt informationssäkerhetsarbete måste alltid anpassas efter en organisations specifika omständigheter. Därför är det viktigt att analysera både omvärlden och den egna verksamheten för att känna till nuläget och vad som sätter ramarna för er. Analyserna lägger grunden för utformningen av organisation och arbetet med informationssäkerhet samt styrdokument som policy, riktlinjer och instruktioner. Resultatet av analyserna ska alltså styra vilka säkerhetsåtgärder som ska införas och hur det systematiska informationssäkerhets arbetet bör utformas och bedrivas. I detta metodsteg bör följande analyser genomföras:

- Verksamhetsanalys
- Omvärldsanalys
- Riskanalys
- Gapanalys





Utgå alltid från redan genomförda analyser, strategier och kartläggningar från olika delar av organisationen.

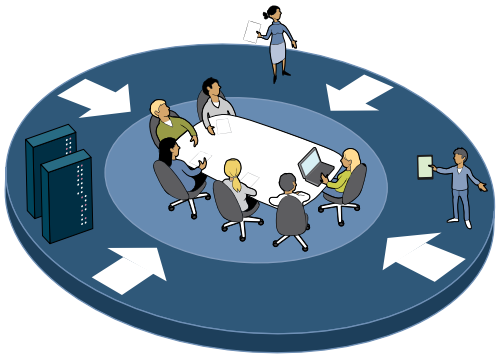
Analysera övergripande första gången – fastna inte i detaljerna, ni kan alltid utveckla underlaget successivt. Avgränsa er så långt som möjligt till det som påverkar informationshanteringen. Det gör ingenting ifall analyserna överlappar varandra, det viktigaste är att ni inte råkar utelämna något väsentligt.

Resultatet av analyserna är en lista på interna och externa förutsättningar och aktörer samt hur de påverkar informationssäkerhetsarbetets utformning i nästa steg. Dessutom upprättas en lista på informationstillgångar som ska skyddas, vilka övergripande risker de ska skyddas mot, samt valda säkerhetsåtgärderoch status på dessa.

3.1 Verksamhetsanalys

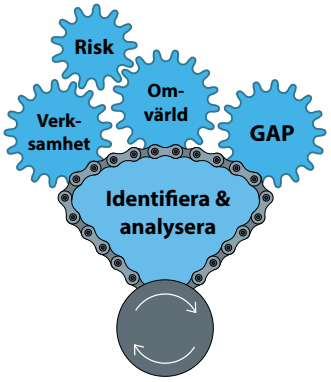
I verksamhetsanalysen ska informationstillgångarna identifieras samt interna intressenters behov, förväntningar och förutsättningar kartläggas. Eftersom det systematiska informationssäkerhetsarbetet omfattar hela organisationen behöver ni veta hur den styrs, vilka målsättningarna är, hur infrastrukturen är uppbyggd, vilka drivkrafter som finns, vilka resurser och kompetenser som finns samt hur kulturen ser ut.

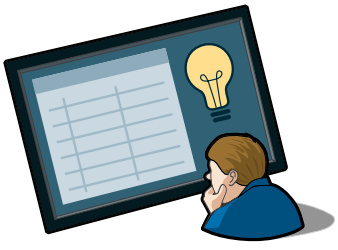
Verksamhetsanalysen är central för er anpassning av styrning och arbetssätt. Ju bättre förståelse ni har av organisationens processer och inre liv – desto bättre förutsättningar har ni för att införa och förvalta arbetssättet.



Att göra:

- Analysera era interna intressenter – det vill säga roller och organisatoriska enheter inom er organisation som påverkar eller påverkas av informationssäkerheten och hur den styrs.
- Analysera era interna förutsättningar. Lägg särskilt fokus på hur informationshanteringen styrs och vilka resurser och kompetenser som finns tillgängliga.
- Analysera era informationstillgångar – det vill säga information som verksamheten hanterar och som ni därmed ska skydda, inklusive de resurser som behandlar informationen (exempelvis it-system). Definiera begreppen och vad ni vill analysera. Det är viktigt att alla använder samma terminologi till exempel informationstillgång kontra informationsmängd eller system kontra tjänst. Inventeringen utgör underlaget för informationsklassning (se kapitel 4.4 och 5.1). Utgå från organisationens olika processer och kom ihåg att förteckningen är en nulägesbild och därmed färskvara.
- Ni kan också välja att identifiera de huvudsakliga informationstillgångarna på rubriknivå i detta skede för att få en överblick, det vill säga dokumentera huvudtyperna av information i huvud- och stödprocesserna. Notera också om känsliga personuppgifter eller annan särskilt känslig eller kritisk information hanteras. En detaljerad inventering kan göras senare med respektive informationsägare i samband med informationsklassning (se kapitel 5.1).
- Dokumentera resultatet från varje del på ett sätt som stödjer ert fortsatta arbete med uppbyggnad av styrande dokument och andra aktiviteter. Resultatet av analysen kan ge behov av återkoppling till projektägare eller ledningen – till exempel om det visar sig att det saknas vissa kritiska förutsättningar för att åstadkomma ett systematiskt informationssäkerhetsarbete.

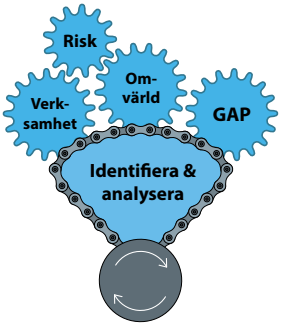




I bilagan **Framgångsfaktorer och exempel** kan du få tips och råd om hur du arbetar med samtliga analysmetoder.

3.2 Omvärldsanalys

Omvärldsanalysen innefattar identifiering av rättsliga krav samt kartläggning av externa intressenters (som kunder, leverantörer, medborgare och granskare) behov, förväntningar och förutsättningar (som tekniska, sociala, miljömässiga, politiska) vilka ni behöver ta ställning till.



Se bilagan **Framgångsfaktorer och exempel**.

Att göra:

- Analysera organisationens externa intressenter och hur relationen påverkar er informationshantering och i förlängningen informationssäkerheten. Håll er på en generell nivå och definiera principiella krav och behov som ni behöver förhålla er till. Detaljering av krav och vilka åtgärder som ska vidtas görs i metodsteget Använda (se kapitel 5).
- Analysera organisationens externa förutsättningar, till exempel politiska och tekniska förutsättningar och trender.
- Analysera rättsliga krav i olika författningar, det vill säga krav som är kopplade till er organisations informationshantering eller direkt till informationssäkerhet, till exempel dataskyddsförordningen, säkerhetsskyddslagen, bokföringslagen, MSB:s och andra myndigheters föreskrifter och NIS-regleringen. Kraven kan handla om informationssäkerhet i sin helhet eller om vilket skydd vissa specifika informationsmängder behöver. Ta hjälp av juridisk expertis.

3.3 Riskanalys

Genom en riskanalys identifierar ni de hot och oönskade händelser som kan leda till negativa konsekvenser för er organisation. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Riskerna tas fram genom en kreativ men strukturerad process, där riskerna och potentiella händelser som kan leda till negativa konsekvenser beskrivs. Dessa bedöms sedan med avseende på sannolikheten att de inträffar samt potentiella konsekvenser.

Viktigt att tänka på när man gör en riskanalys är att resultatet är en uppskattning och inte en exakt bild av verkligheten. Det är inte heller syftet, utan riskanalysen ska ge underlag för beslut om vilka säkerhetsåtgärder som ska införas men också höja medvetenheten om hot, sårbarheter och risker hos de som deltar i analysen. Riskanalysen hjälper till med prioriteringen av åtgärder eftersom allt inte kan genomföras samtidigt.

Riskanalyser ska göras återkommande i förvaltningsfasen. Den initiala i implementeringsfasen bör göras med ledningen för att identifiera sådana prioriterade risker som påverkar utformningen av arbetet och särskilt vilka delar som behöver fås på plats omgående – till exempel styrning av åtkomst eller kravställning i upphandlingar.

Att göra:

- Anpassa metod för riskhantering till organisationens befintliga eller besluta om gemensam metod så att alla delar av organisationen som arbetar med riskhantering använder samma begrepp, konsekvensskala, principer för riskvärdering och riskacceptans så långt som möjligt.
- Definiera omfånget av riskanalysen samt deltagare. Starta om möjligt med ledningsgruppen i införandefasen.
- Genomför riskanalysen i workshop. Låt deltagarna vara kreativa – få alla att föreställa sig risker, inträffade eller potentiella. Försök att analysera riskerna utan att beakta befintliga säkerhetsåtgärder.
- Dokumentera och återkoppla resultatet inklusive förslag på hantering. Kommunicera även till berörda riskägare – det vill säga de som är ansvariga för de verksamhetsområden inom vilka riskerna ska hanteras. Resultatet ska också ligga till grund för val av säkerhetsåtgärder.

Se bilagan **Framgångsfaktorer och exempel**.

3.4 Gapanalys

Syftet med en gapanalys är att identifiera skillnaden mellan den önskade informationssäkerhetsnivå som ni vill uppnå och den befintliga nivån på er informationssäkerhet vid analystillfället. Med hjälp av en gapanalys synliggör ni en eventuell skillnad mellan nuläget och önskat läge, som ni behöver överbrygga genom att utforma och införa ett antal olika säkerhetsåtgärder för informationssäkerhet.

Resultatet av gapanalysen är en lista över vilka säkerhetsåtgärder som ni ska tillämpa, samt en beskrivning av åtgärdernas aktuella status. Listan beskriver om dessa åtgärder redan existerar eller inte, samt om de fungerar på ett tillfredsställande sätt eller inte.

Se bilagan **Framgångsfaktorer och exempel**.

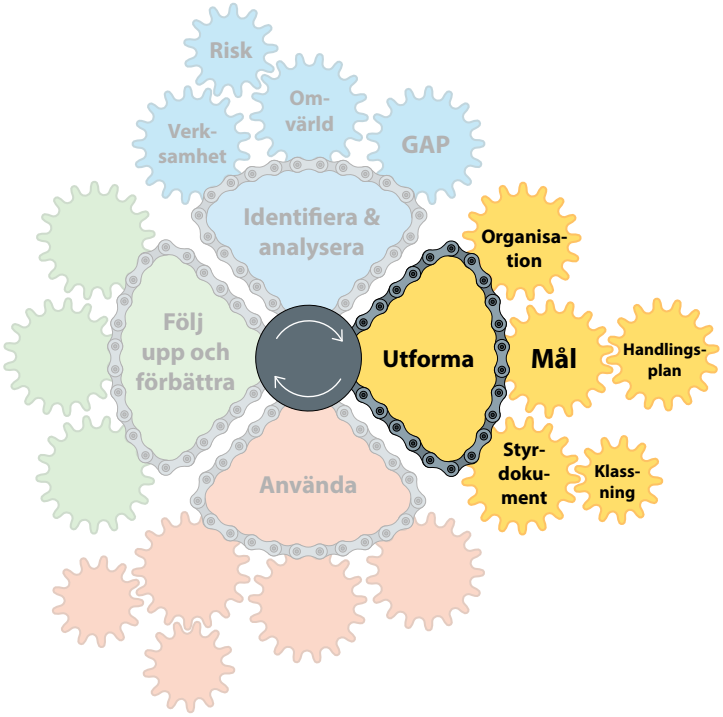
Att göra:

- Fastställ vilka säkerhetsåtgärder som ska ingå i gapanalysen.
- För varje säkerhetsåtgärd som ni har beskrivit behöver ni nu avgöra om åtgärden existerar eller inte, samt om den fungerar tillfredsställande.

4. Utforma

I metodsteget Utforma skapas de huvudsakliga delar som behövs för verksamhetens systematiska informationssäkerhetsarbete. I detta metodsteg bör följande analyser genomföras:

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan



4.1 Organisation

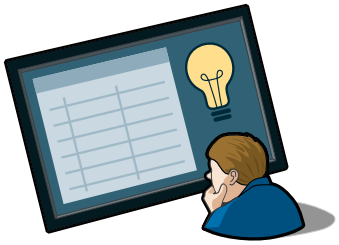
På basis av de analyser ni har gjort ska ni nu utforma er organisation för informationssäkerhet. Viktigt är att utgå ifrån er verksamhet, roller, ansvarsområden, mandat och beslutsvägar.

Grundprincipen är att ansvaret för själva informationssäkerheten ska följa det ordinarie verksamhetsansvaret. Detta gäller hela vägen från ledning till enskilda medarbetare. Det yttersta ansvaret ligger därmed på högsta ledningen.

En verksamhet kan bedrivas i en organisatorisk del (till exempel avdelning, sektion eller enhet), ett löpande arbetsflöde (till exempel process) eller ett tidsbegränsat arbete (till exempel projekt). Ansvar i alla olika former behöver definieras. Här är det särskilt viktigt att beakta hur styrningen av informationshanteringen sker i övrigt.

Den eller de som arbetar med informationssäkerhet utgör en viktig stödfunktion för verksamhetsansvariga – ungefär på samma sätt som det finns stödfunktioner inom ekonomi, personal eller kommunikation. CISO har det övergripande ansvaret att leda och samordna arbetet med informationssäkerhet. CISO ska alltid ha det strategiska perspektivet – oavsett storlek på organisationen. Skillnaden är att CISO i stora organisationer kanske enbart arbetar strategiskt, medan rollen i mindre organisationer arbetar operativt i större utsträckning.

Råd och forum kan fungera som bra komplement till linjearbetet och underlätta samordning och kommunikation kring informationssäkerhet i organisationen. De ger möjlighet att ta upp aktuella frågor och diskutera strategiska val med andra viktiga roller och involvera dem som ambassadörer för området.

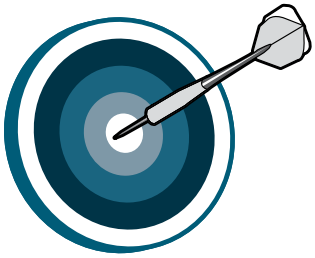


I bilagan **Framgångsfaktorer och exempel** kan du få mer tips och råd.

Att göra:

- Tydliggör och fastställ i styrdokument ansvaret för olika roller (VD/GD, övriga chefer, medarbetare m.m.) inklusive särskilt utpekade funktioner som till exempel it, personal och ekonomi.
- Tydliggör och fastställ CISO:s roll i styrdokument. Observera att CISO inte är liktydigt med it-säkerhetsansvarig.
- Fastslå hur och när CISO ska rapportera till ledningen.
- Skapa vid behov ett informationssäkerhetsråd eller forum med bred representation från organisationen.

4.2 Informationssäkerhetsmål



Informationssäkerhetsmålen är grundläggande för att ni internt ska kunna kommunicera, prioritera och genomföra sådana aktiviteter som leder till ett systematiskt och förbättrat informationssäkerhetsarbete. Målen kan delas in i två typer: långsiktiga mål och kortsiktiga mål.

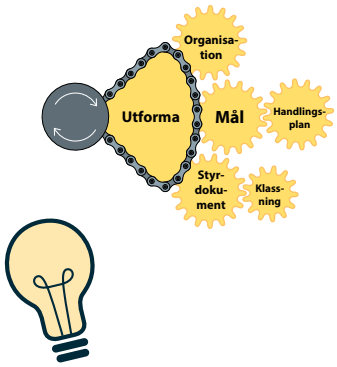
Utgå från de analyser som ni har gjort i analysfasen och harmonisera med befintliga visioner, målsättningar eller strategier som har bäring på informationssäkerhet, till exempel rörande annan säkerhet, kvalitet och it eller digitalisering.

Såväl era långsiktiga som kortsiktiga informationssäkerhetsmål bör överensstämma med sättet som ni vanligtvis arbetar med mål i er organisation, till exempel strategier och verksamhetsplaner. Det är också viktigt att beakta nationella och bransch- eller sektorspecifika visioner, strategier, mål och handlingsplaner.

Informationssäkerhetsmålen ska i förlängningen bidra till att uppnå verksamhetsmålen.

Att göra:

- Ta fram långsiktiga informationssäkerhetsmål som ger uttryck för er viljeinriktning på lite längre sikt (cirka 3–5 år) och som stödjer verksamhetsmålen. De långsiktiga målen behöver inte vara mätbara, utan kan vara övergripande. Skriv in målen i informationssäkerhetspolicyn (se kapitel 5.3).
- Ta fram kortsiktiga informationssäkerhetsmål som uttrycker hur ni på cirka 1–2 år, ska arbeta för att uppnå era långsiktiga strategiska mål. De kortsiktiga målen ska vara konkreta och ha en tydlig koppling till de analyser som ni har gjort. Använd som underlag för aktiviteterna i handlingsplanen (se kapitel 4.5).



Se bilagan **Framgångsfaktorer och exempel**.

4.3 Styrdokument

Styrdokumenten är det formella ramverket för ert informationssäkerhetsarbete. I styrdokumenten ska ni ange vad som ska finnas och göras samt hur det ska gå till. Dokumenten kan även sammanställa vilka krav som är obligatoriska och vilka som är rekommenderande (ska- och börkrav).

Styrdokument reglerar området på olika nivåer: från ledningens övergripande viljeinriktning i en informationssäkerhetspolicy, via organisationens övergripande regelverk, till mer detaljerade instruktioner som rör specifika säkerhetsåtgärder (till exempel fysisk åtkomst till en viss lokal, eller hantering av en viss brandvägg).

Dokumenthierarkier ser olika ut i olika organisationer – använd er befintliga dokumenthierarki med tillhörande beslutsstrukturer. I detta exempel används följande uppställning:

- Policy
- Riktlinjer
- Instruktioner

En informationssäkerhetspolicy beslutas av ledningen (VD, GD, eller styrelse) och avser ledningens viljeinriktning med informationssäkerheten. Allt informationssäkerhetsarbete i en organisation ska utgå ifrån en informationssäkerhetspolicy.

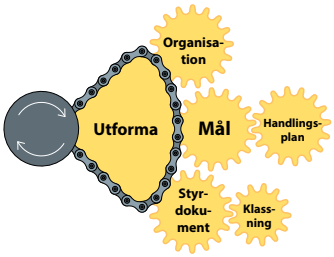
Riktlinjer beskriver vad som ska och bör finnas – det vill säga ska- och börkrav. I de fall riktlinjer och instruktioner illustrerar det önskade tillståndet för informationssäkerhetsarbetet och inte nuläget, bör samtidigt beslutas om en handlingsplan för att nå upp till kraven. Lämpligt är att beslut kring riktlinjer som ska gälla för hela organisationen fattas av ledningen, medan specifika instruktioner kan beslutas av chefer vars verksamhet de berör.

Se bilagan **Framgångsfaktorer och exempel**.

Att göra:

- Ta fram, besluta och kommunicera informationssäkerhetspolicy.
- Ta fram, besluta och kommunicera riktlinjer med avstamp i valda säkerhetsåtgärder samt tillhörande handlingsplan.
- Ta fram verksamhetsnära instruktioner som anger hur arbetet ska utföras så att riktlinjerna uppfylls.

4.4 Klassningsmodell



Klassning är en förutsättning för att skapa rätt skydd för informationen och undvika överskydd med onödigt höga kostnader och krångliga rutiner som följd. Klassning ska ske på ett enhetligt sätt i hela organisationen så att likvärdig information får samma skyddsnivå.

Att klassa information innebär att man gör en konsekvensbedömning för vad som kan hända om informationens konfidentialitet, riktighet och tillgänglighet inte upprätthålls i den utsträckning verksamheten behöver.

Klassningsmodellen används för att värdera informationstillgångar. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas på ett enhetligt sätt utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

För att få enhetligt skydd för olika information som klassats lika behövs skyddsnivåer som speglar konsekvensnivåerna. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver.

Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. Klassningsmodellen kan på så sätt fungera som ett gemensamt ramverk för att underlätta kommunikationen mellan beställare och leverantörer av olika tjänster.

Se bilagan **Framgångsfaktorer och exempel**.

Att göra:

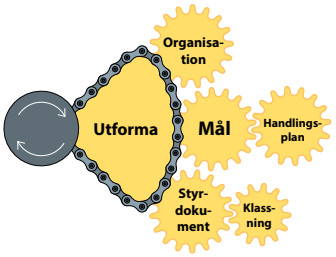
- Skapa en klassningsmodell med konkreta beskrivningar och värden för de olika nivåerna. Harmonisera med konsekvensskalan för riskanalyser. Vid avsaknad av en modell kan MSB:s klassningsmatris vara till ett bra stöd.
- Ta fram skyddsnivåer med graderade säkerhetsåtgärder som kan mappas mot klassningsmodellen.
- Dokumentera klassningsmodellen i en riktlinje.
- Ta fram stödmaterial som kan användas av organisationen vid genomförandet av informationsklassningar.

4.5 Handlingsplan

För att få struktur för det fortsatta arbetet är det lämpligt att ta fram en årlig handlingsplan. Syftet är att tydliggöra hur organisationen ska gå från behov till faktisk åtgärd i enlighet med slutsatserna i analyserna i kapitel 3. Handlingsplanen kan också innehålla mål och aktiviteter som är kopplade till delar av det systematiska arbetet med informationssäkerhet, exempelvis att se över roller och ansvar eller ta fram en process för riskhantering. I handlingsplanen befäster ni prioriteringen för era insatser.

Anpassa processen för och innehållet i den årliga handlingsplanen till organisationens övriga verksamhetsplanering och måluppföljning.

Aktiviteter kan ingå i planer inom andra områden, som exempelvis generell säkerhet, kvalitetsstyrning och it eller digitalisering. Integrera informationssäkerheten i andra områden och processer i så stor utsträckning som möjligt.



För it finns ofta en förvaltningsmodell med årliga förvaltningsplaner för it-systemen. Dessa innehåller i regel aktiviteter och budgetar som beslutas av objektägare. Använd förvaltningsplanerna för att få in relevanta säkerhetsåtgärder och andra informationssäkerhetsrelaterade aktiviteter på ett integrerat sätt i organisationens it-styrning.

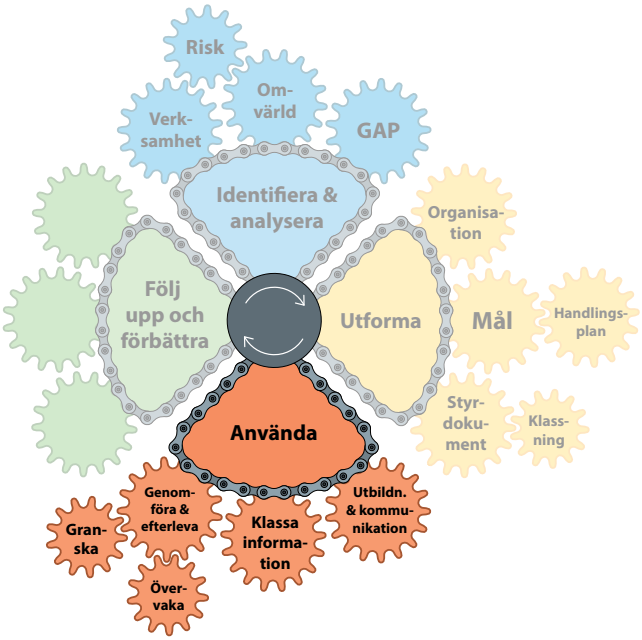
Att göra:

- Ta fram en årlig handlingsplan och prioritera de aktiviteter som har bäst effekt.
- Sträva efter en balans mellan följande två typer:
  - Aktiviteter som minskar eller eliminerar de mest kritiska (det vill säga mest allvarliga och betydande) bristerna enligt er gapanalys.
  - Aktiviteter som är resursmässigt genomförbara enligt de förutsättningar som ni beskriver i handlingsplanen.

5. Använda

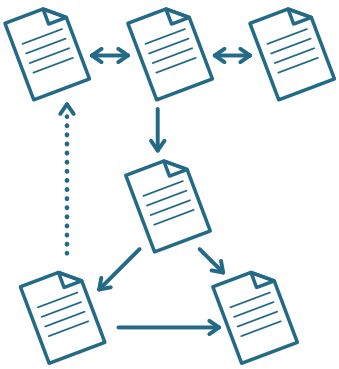
I metodsteget Använda tillämpar organisationen den utformade styrningen. Detta beskrivs nedan i tre avsnitt:

- Klassningsmodell
- Genomföra och efterleva
- Utbilda och kommunicera



När styrning och metodik är på plats är det dags att tillämpa ledningssystemet. Aktiviteter som ingår i handlingsplanen ska genomföras och styrdokument ska efterlevas enligt utpekat ansvar. Incidenter, oförutsedda händelser och förändringar behöver hanteras. Medarbetare ska utbildas och klassningar ska genomföras och dokumenteras. Med andra ord ska ni få det systematiska informationssäkerhetsarbetet att fungera i vardagen.

5.1 Klassa information

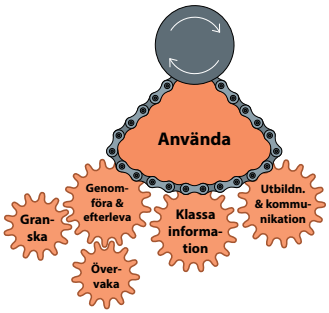


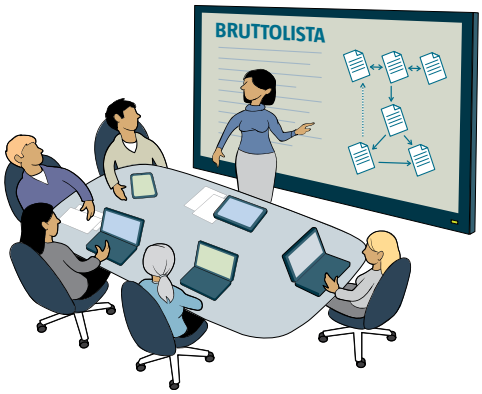
Informationstillgångar består av information och resurser som används för att hantera information, exempelvis it-system, it-infrastruktur och fysiska tillgångar. Själva informationen är den primära tillgången som ni ska klassa. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

Om ni har kopplat säkerhetsåtgärder till klassningsmodellen (se kapitel 4.4), avgör klassningen vilka säkerhetsåtgärder som ska finnas för respektive informationstillgång, något som skulle kunna kallas för en bruttolista av säkerhetsåtgärder.

Bruttolistan behöver justeras utifrån specifika förutsättningar för det sammanhang som just den informationen eller det systemet används i. Genom att göra en kompletterande riskanalys kan ni identifiera om säkerhetsåtgärderna är otillräckliga eller överskyddanden samt om ackumulerade eller aggregerade informationsmängder ställer andra krav på skydd än vad en enskild informationstyp gör.

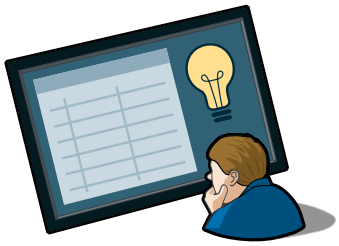
Det är informationsägarnas ansvar att se till att klassning av deras information genomförs. CISO stödjer med metodik.





Att göra:

- Klassa identifierad information enligt klassningsmodellen i en workshop med informationsägaren och sakkunniga deltagare.
- Mappa resultatet mot skyddsnivåerna och bedöm säkerhets-åtgärderna.
- Genomför kompletterande riskanalys för att se om det behövs särskilda justeringar i det enskilda fallet.
- Repetera regelbundet och vid förändringar som påverkar informationshanteringen.



I bilagan **Framgångsfaktorer och exempel** kan du få mer tips och råd.

5.2 Genomföra och efterleva

Handlingsplanen och styrdokumenten genererar ett ständigt pågående arbete i organisationen, av en mängd olika roller. I det dagliga arbetet är det viktigt att hitta balans mellan planerade aktiviteter och frågor som dyker upp löpande. Samtidigt behöver verksamheten stöd med efterlevnaden av styrdokumenten. Därför är det mycket viktigt att CISO:s roll och ansvar är tydligt fastställda i styrdokumenten och i handlingsplanen samt accepterade i organisationen.

Vissa aktiviteter kan CISO ansvara för och genomföra, men huvud-ansvaret för de flesta aktiviteter bör ligga hos andra roller i organisa-tionen. I stället behöver CISO ägna tid åt att koordinera och styra det löpande arbetet med organisationens informationssäkerhet och kommunicera med andra, särskilt i syfte att förklara och inspirera för att lyckas få hela organisationen att arbeta i samma riktning. Det är viktigt med ständig omvärldsbevakning och kontinuerlig kontakt med verksamheten. Särskilt i början innan rutinerna har satt sig.

Se bilagan **Framgångsfaktorer och exempel**.

Att göra:

- Genomför handlingsplanens aktiviteter. Var beredd att ompröva aktiviteterna, till exempel till ändrade verksamhetsmål.
- Utbilda verksamheten och stötta i efterlevnad av styrdokument. Analysera anledning till brister och för in i förbättringsarbetet (se kapitel 6).
- Hantera större händelser och förändringar som incidenter, upphandlingar, nya lagar, omorganisationer och ändrade hotbilder. Klassa informationstillgångar, analysera risker och utforma skydd fortlöpande.
- CISO ska styra och stödja arbetet, men se upp för att bli översköljd av operativa frågor som kan genomföras av andra. Om CISO lägger ned för mycket av sin arbetstid i ett eller ett fåtal projekt, så blir rollen tyvärr osynlig för den övriga organisationen.
- Dokumentera kontinuerligt för att kunna förfina styrning och metodik – informationssäkerhetsarbetet är en process i ständig rörelse.

5.3 Utbilda och kommunicera

För att höja medvetenheten och kunskapen om informationssäkerhet krävs ständig utbildning och kommunikation. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som ni har valt att implementera.

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärlig för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

Samtidigt behöver alla medarbetare engageras i olika mån i informationssäkerhetsarbetet för att skapa en god säkerhetskultur.

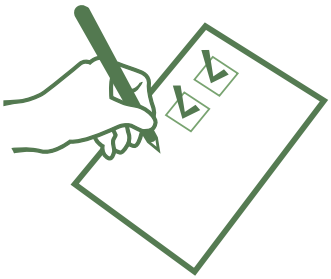
Om informationssäkerhet är ett nytt begrepp för organisationen behöver ni ägna tid åt att motivera nyttan och fördelarna med arbetet. Ett grundläggande argument är att informationssäkerhet förbättrar kvalitet och effektivitet i informationshanteringen och bidrar till verksamhetens målsättningar. Informationssäkerhet är också en förutsättning för att lyckas väl med annat förändringsarbete exempelvis satsningar på digitalisering.

Se bilagan **Framgångsfaktorer och exempel**.

Att göra:

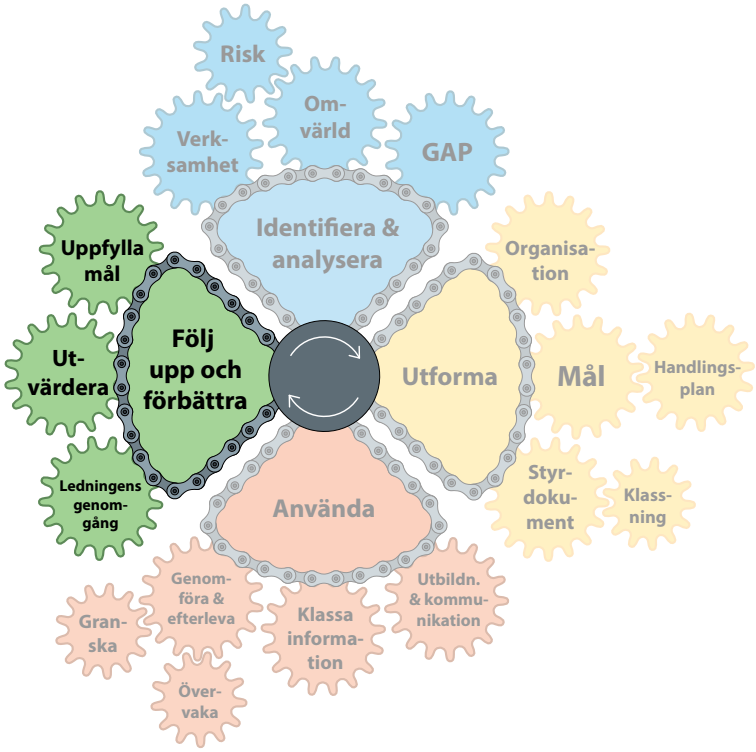
- Genomför handlingsplanens aktiviteter. Var beredd att ompröva Engagera ledningen och be dem att uttrycka sitt stöd – både formellt och informellt. Förädla era argument för organisationens olika nivåer.
- Skapa en målgruppsanpassad utbildnings- och kommunikationsplan för informationssäkerhet med olika aktiviteter över en längre tid.
- Synliggör vad som är på gång. Skapa en särskild sida för informationssäkerhet på intranätet.

6. Följa upp och förbättra



Detta metodsteg vägleder om utformning av arbetssätt för uppföljning och förbättring av informationssäkerhetsarbetet och dess styrning. Avsnittet består av:

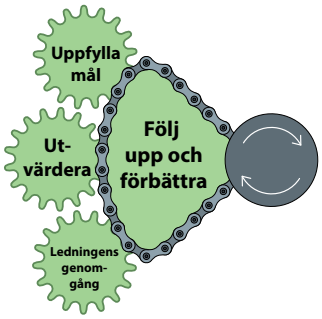
- Utvärdera och följa upp
- Ledningens genomgång



Informationshanteringen förändras konstant. Organisatoriska förändringar, teknisk utveckling eller förändrade hotbilder ställer också krav på ständig anpassning och förbättring av det systematiska informationssäkerhetsarbetet.

Genom en strukturerad övervakning och mätning ges förutsättningar för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande.

Resultatet från detta metodsteg kan användas som grund för interna revisioner och ledningens genomgång samt som ingångsvärde till förnyade analyser när nästa cykel i det systematiska informationssäkerhetsarbetet börjar.



6.1 Utvärdera och följa upp

Syftet med att övervaka (även kallat monitorera) och mäta är att få reda på om ert systematiska informationssäkerhetsarbete, riskhanteringsarbete samt alla beslutade säkerhetsåtgärder är:

- ändamålsenligt utformande
- har avsedd verkan
- existerar och fungerar tillfredsställande.

Genom att kontrollera efterlevnaden kan organisationen få bättre kunskap om informationssäkerhetsläget och upptäcka brister som behöver korrigeras. Efterlevnadskontroll kan ske exempelvis genom övervakning eller mätning.

Övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras.

Mätning anger ett värde. Exempelvis kan man mäta nyckeltal för att se progress eller brist på progress. Mätning sker ofta i planerade intervaller i form av mognadsmätning eller benchmarking.

Att göra:

- Definiera hur kontrollen av efterlevnaden ska ske, vad som ska övervakas eller mätas och hur. Utveckla omfånget i takt med att det systematiska informationssäkerhetsarbetet växer fram och att det blir mera etablerat.
- Nedan exempel på olika nivåer för utvärdering. Utgå från hur stora resurser ni har beslutat er för att avsätta för själva utvärderingen.

Liten – börja med:

- Uppfyllnad av informationssäkerhetsmål
- Bedömning av ledningssystemets lämplighet, tillräcklighet och verkan

Mellan – lägg till:

- Förnyad gapanalys mot till exempel standard
- Efterlevnad av internt styrande dokument
- Mognadsmätning

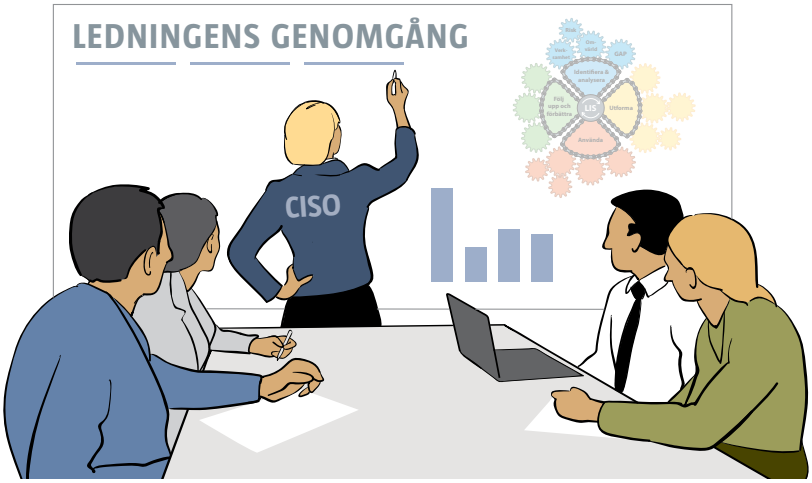
Stor – lägg till:

- Extern revision av det systematiska informationssäkerhetsarbetet

I bilagan **Framgångsfaktorer och exempel** kan du få mer tips och råd.

6.2 Ledningens genomgång av informationssäkerhetsläget

Vid ledningens genomgång tar ledningen ställning till om verksamhetens systematiska informationssäkerhetsarbete och dess styrning är fortsatt lämpliga, tillräckliga och har avsedd verkan. Genomgången bör göras vid ett fysiskt möte där informationssäkerhetsläget i verksamheten redovisas av CISO och där ledningen beslutar om arbetets inriktning och resurser baserat på en utvärdering av uppföljningen. Beslutet kan gälla förbättringar av informationssäkerheten, förändringar i sättet att leda och styra informationssäkerheten samt resurstilldelning. Beslutet blir ledningens inriktning för det fortsatta systematiska informationssäkerhetsarbetet.



Att göra:

- Fastställa när och vid vilka intervall ledningens genomgång ska ske.
- Planera inför ledningens genomgång.
- Genomföra ledningens genomgång.
- Hantera resultat av ledningens genomgång.

Se bilagan **Framgångsfaktorer och exempel**.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer: MSB1365 - mars 2019 ISBN: 978-91-7383-992-1