Myndigheten för samhällsskydd och beredskap

Ledningens roll inom informationssäkerhet

Stöd för dig med en ledande funktion

Ledningens roll inom informationssäkerhet – ett stöd för dig med en ledande funktion

Enheten för systematisk informationssäkerhet

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

Publikationsnummer: MSB1783 - juni 2021

Förord

Du som har den här broschyren i din hand har sannolikt frågor kring din roll som ledare i din organisations arbete med informationssäkerhet.

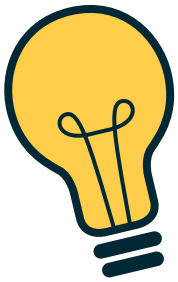
Vi hoppas att du hittar några av svaren här.

Om du sen tycker att du inte har tillräcklig med kunskap på området för att lösa alla frågor, ta din CISO (Chief Information Security Officer) till hjälp. Om din organisation inte har en CISO utser du en och krokar arm med hen. I dagens digitaliserande samhälle är det en av de viktigaste professionella relationerna du har. Klargör hur ni ska samarbeta och vad ni vill åstadkomma. Tillsammans involverar ni medarbetarna på denna spännande och värdeskapande resa till den grad av informationssäkerhet som du vill ha i organisationen.

Lycka till!

Margareta Palmqvist, enhetschef
Enheten för systematisk informationssäkerhet
Avdelningen för cybersäkerhet och säkra kommunikationer

Informationssäkerhet för ledningen



Det här stödet riktar sig till dig som leder en organisation. Du kan exempelvis vara högsta beslutande chef såsom verkställande direktör, generaldirektör eller kommundirektör, medlem i en ledningsgrupp, styrelsemedlem eller ha en annan ledande funktion.

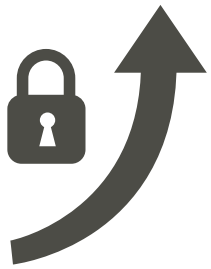
Stödet innehåller:

- En introduktion till vad informationssäkerhet är.
- Tips på hur du kan tänka kring informationssäkerhet i din organisation.
- Information om varför det är viktigt att bedriva ett systematiskt informationssäkerhetsarbete i en snabbt föränderlig värld.
- Råd för hur du behöver arbeta tillsammans med dem som arbetar med organisationens informationssäkerhet, för att uppnå bästa resultat.

Informationssäkerhet och din organisation

Information finns överallt i en organisation: inom personaladministration, ekonomistyrning, produktinformation, kunddatabaser, strategisk planering, försäljning, support och service med mera. Information kallas ibland organisationens ”blod”, eftersom den strömmar genom alla verksamheter och är livsviktig för organisationen. Det är av avgörande betydelse för alla organisationer att information är tillgänglig och korrekt, samt att känslig information inte röjs till obehöriga. Informationssäkerhet handlar om just det – att införa rätt skydd för att bevara önskad nivå av konfidentialitet, riktighet och tillgänglighet.

Att informationen hanteras säkert är avgörande när den flödar digitalt mellan myndigheter, företag och privatpersoner via olika tjänster. Digitaliseringen innebär att information hanteras på nya sätt, vilket i sin tur innebär förändrade förutsättningar för informationssäkerheten. Samtidigt som verksamheter och individer i allt större utsträckning är beroende av att de digitala systemen fungerar, digitaliseras också samhällets mörka sidor. En av följderna är en stor ökning av antalet angrepp och bedrägerier av olika slag.

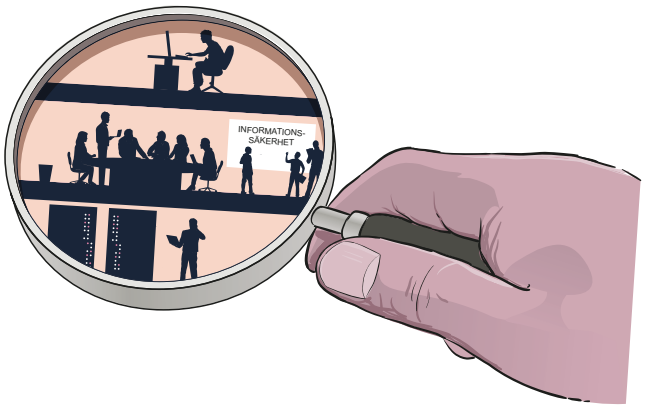


För att er organisation ska kunna utföra sitt uppdrag med hög kvalitet och nå målen och visionerna är det viktigt att ert arbete med informationssäkerhet anpassas till organisationens strategi och samhällets utveckling.

Var vill ni i ledningen att organisationen ska befinna sig om fem eller tio år?

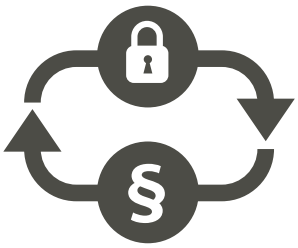
- På vilka marknader, och i vilken grad av digitalisering?
- På vilket sätt skulle problem med informationssäkerheten kunna äventyra en sådan utveckling?
- På vilket sätt kan god informationssäkerhet stödja eller möjliggöra den utveckling ni önskar?

Informationssäkerheten behöver anpassas till er organisation på ett sätt som ger er nytta i form av ökad kvalitet och konkurrensförmåga, minskade risker och kostnader för incidenter, säkerställd efterlevnad av rättsliga krav och i slutänden omvärldens förtroende. Hur arbetet med informationssäkerhet kan och bör bedrivas i just er organisation beror på en mängd faktorer som exempelvis branschtillhörighet, storlek, samarbetspartner, geografisk utbredning och grad av digitalisering. Det är ni som leder organisationen som kan detta bäst och som behöver fatta nödvändiga beslut för att åstadkomma ett effektivt arbete med informationssäkerhet för just er organisation.



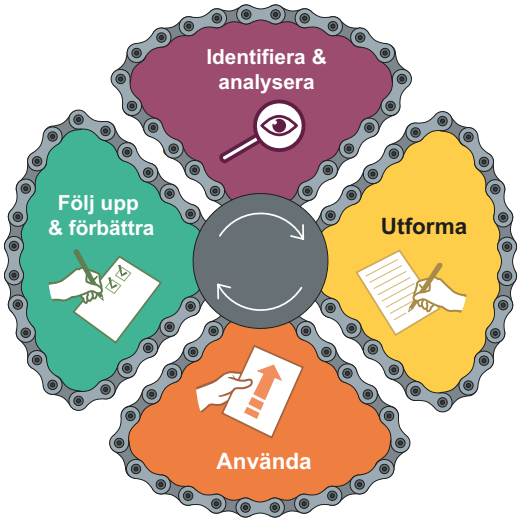
För att säkerställa att informationssäkerheten anpassas till er organisations specifika förutsättningar och mål, och över tid möter förändringar i och utanför organisationen, behöver ni arbeta systematiskt.

Systematiskt informations-säkerhetsarbete

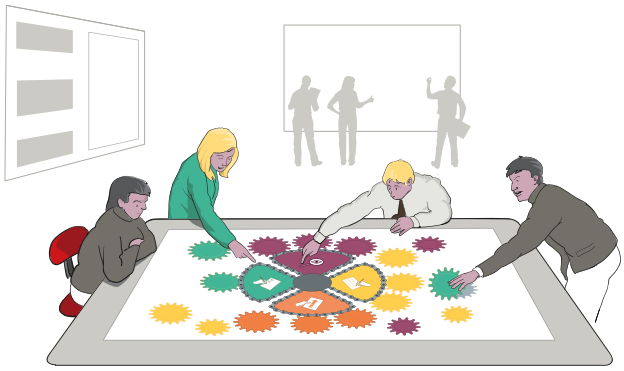


Precis som inom andra områden, till exempel ekonomi- och kvalitetsstyrning, behöver arbetet med informationssäkerhet vara strukturerat och systematiskt för att bli effektivt. Den snabba utvecklingen inom informationshantering motiverar detta ytterligare, eftersom det ständigt kommer nya hot, nya tekniska möjligheter och förändrade lagkrav. Det räcker inte att införa ett antal säkerhetsåtgärder och sedan slå sig till ro, utan säkerhetsåtgärdernas effektivitet måste ses över regelbundet så att säkerheten över tid är anpassad till organisationens utveckling och förändringar i omvärlden.

MSB har tillsammans med experter tagit fram ett metodstöd för att bedriva ett systematiskt informationssäkerhetsarbete. Det baseras på standardserien ISO/IEC 27000, som är etablerad i Sverige och internationellt. För dig som ledare finns också en översikt av stödet som ger en snabb överblick över de bärande beståndsdelarna i arbetet, som är samma för alla organisationer. Delarna är Identifiera och analysera, Utforma, Använda samt Följa upp och förbättra.



Det systematiska informationssäkerhetsarbetet måste anpassas till er organisation och dess styrning, så att arbetet blir integrerat i organisationens verksamhetsstyrning. Det gäller såväl ansvarsfördelning som riskhantering samt rutiner för planering och budgetarbete. Genom att informationssäkerhetsarbetet blir en del av den löpande verksamheten istället för något utanför den, ökar förutsättningarna för ett effektivt arbete. Förutsättningarna ökar också för ett väl anpassat skydd som inte kostar för mycket eller stör verksamheterna i onödan.



MSB:s metodstöd hjälper er att ta fram underlag för att kunna anpassa informationssäkerhetsarbetet. Resultaten från analyssteget ger en förståelse för era interna och externa förutsättningar, övergripande risker och informationssäkerhetens nulägesnivå. Utifrån resultatet kan informationssäkerhetsarbetet utformas så att det anpassas till och kan användas av er organisation, och så att organisationen inför säkerhetsåtgärder som möter de risker ni inte accepterar. Allteftersom arbetet med informationssäkerhet växer fram följs det upp och förbättras så att säkerheten hela tiden anpassas till organisationens mål på bästa sätt.

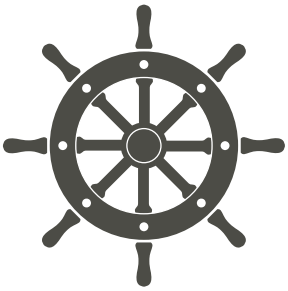
Arbete kan pågå i alla metodstödets delar samtidigt, och efter hand passerar ni alla metodsteg om och om igen. När det systematiska informationssäkerhetsarbetet har genomförts i ”flera varv” räcker det ofta att göra mindre justeringar regelbundet och vid behov, för att över tid anpassa arbetet till förändringar i organisationen och dess omvärld.

Ledningen och ansvar för informationssäkerhet

Hur har ni delegerat **ansvaret för informationssäkerhet** i organisationen? Som grundregel bör informationssäkerhetsansvaret följa det delegerade verksamhetsansvaret, så att chefer för verksamheter också ansvarar för säker hantering av verksamhetens information. Det kan vara till exempel linjechefer, projektägare, informationsägare eller systemägare. Den som ansvarar för informationssäkerheten i en verksamhet kan också sägas vara *riskägare* för verksamheten. Riskägaren ansvarar för att risker identifieras och accepteras eller hanteras, exempelvis med säkerhetsåtgärder. Om informationsägarskapet eller riskägarskapet inte har delegerats formellt är det organisationens högsta ledning som har ägarskapet.

Eftersom säkerhetsåtgärder kan ha olika karaktär kan de behöva införas av olika interna eller externa funktioner eller individer. Ansvaret för att ställa krav på och följa upp att interna och externa tjänster bibehåller rätt nivå av informationssäkerhet ligger dock kvar på den

chef som är riskägare och ansvarig för informationen – oavsett vem som ska införa säkerhetsåtgärderna. Därför är det av avgörande betydelse att den som får informationssäkerhetsansvaret för en verksamhet också får tillräckliga resurser, beslutsmandat och delaktighet i centrala beslut som påverkar verksamhetens informationssäkerhet, till exempel i fråga om säkerhetsåtgärder.



Den som **driver en organisations informationssäkerhetsarbete** kallas här, precis som i MSB:s metodstöd, för *CISO – Chief Information Security Officer*. Andra benämningar på rollen är informationssäkerhetschef, informationssäkerhetssamordnare eller informationssäkerhetsstrateg. CISO är beroende av att du ger ramar och förutsättningar att utforma och driva organisationens informationssäkerhetsarbete.

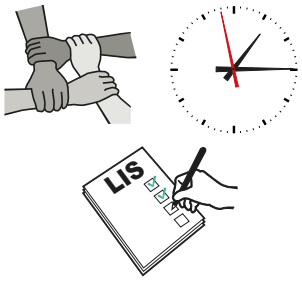
CISO:s uppdrag spänner över hela organisationen och innefattar allt ifrån att planera och anpassa informationssäkerhetsarbetet till att utifrån behov stötta ledningen och alla övriga roller som har ett informationssäkerhetsansvar i operativa, taktiska och strategiska frågor.

En ledning som gör skillnad

Du som är i en ledande position behöver inte vara expert på informationssäkerhet, även om du precis som på andra områden ändå behöver ha viss kunskap för att kunna fatta lämpliga beslut.

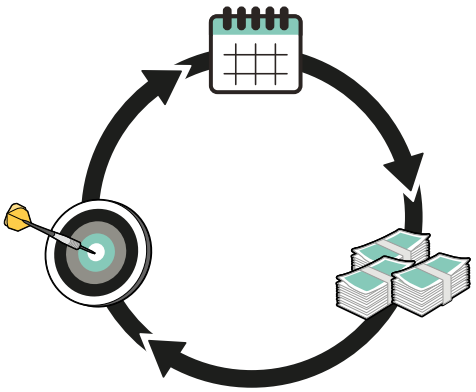
För att bidra till informationssäkerhetsarbetet på bästa sätt är det extra viktigt att du själv är en förebild i organisationen genom att följa de interna reglerna, håller dig informerad om hur informationssäkerhetsarbetet går genom att vara lyssnande och nyfiken, fattar de beslut som behövs samt tilldelar resurser som motsvarar era målsättningar och ambitioner.

För att arbetet med informationssäkerhet ska bli bra behöver ledningen stöd av en CISO, som har till uppgift att driva arbetet i organisationen och vara ledningens kontaktpunkt i dessa frågor. CISO behöver rapportera direkt till och ha en god dialog med ledningen för att kunna göra ett bra jobb.



En god relation och kommunikation mellan ledning och CISO är viktig eftersom ni är ömsesidigt beroende av varandra. För ledningen är CISO central för att förverkliga ledningens beslut och för att vara den främsta källan till kunskap och information om informationssäkerheten. För CISO är ledningens informerade beslut avgörande för att informationssäkerhetsarbetet ska kunna drivas framåt i organisationen. Att införa ett systematiskt informationssäkerhetsarbete är att genomföra ett förändringsarbete som påverkar organisationen på många sätt. Hur väl detta lyckas är helt beroende av samarbetet mellan ledningen och CISO.

En förutsättning för arbetet är att ledningen och CISO har gemensamma förväntningar och mål. Ledningen och CISO bör därför tillsammans komma överens om en strategisk målbild för organisationens informationssäkerhet. Ledningen och CISO bör också komma överens om principiella tillvägagångssätt för att nå denna målbild, till exempel genom att tillämpa en viss standard.

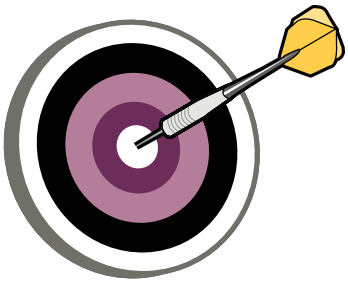


Ledningen behöver tillsammans med CISO bestämma hur, när och vem som ska informeras om informationssäkerheten. Följ organisationens årshjul även när det kommer till informationssäkerhet, så att till exempel planering, statusavstämningar, resursbehov och uppföljningsresultat för informationssäkerheten hanteras samtidigt som för organisationens verksamheter. Det kan också finnas skäl att ha ett lite mer omfattande möte en gång per år, som kompletteras med kortare möten däremellan. Ett sådant årligt möte bör ligga lämpligt i tid i förhållande till organisationens verksamhets- och budgetplanering.

Inför ett möte med CISO kan någon ur ledningen som ska delta ha ett *förmöte* tillsammans med CISO för att bestämma mötets omfattning, form, inriktning med mera. Om ni inte redan har utsett en kontaktperson för CISO i ledningen är det en god idé att göra det. Det hjälper er att ha effektiva möten tillsammans och att ha en löpande dialog.

Det finns ett antal områden där ledningen har anledning att hålla sig informerad och ställa frågor till CISO:

- **Informationstillgångar.** Vilka är de mest kritiska och känsliga informationstillgångarna i organisationen?
- **Externa krav.** Vilka lagkrav finns på organisationens informationssäkerhet? Vilka andra externa krav finns? Hur väl efterlever organisationen dem?
- **Risker.** Vilka är de allvarligaste informationssäkerhetsriskerna? Vilka risker är specifika för organisationen, och vilka delas med samhället i stort samt med vår bransch eller sektor?
- **Skydd.** Hur ser organisationens skydd ut? Är det tillräckligt, eller finns det allvarliga brister och sårbarheter? Vilka säkerhetsåtgärder bedöms vara otillräckliga? Har organisationen genomfört gapanalyser gentemot etablerade ramverk eller standarder som exempelvis ISO/IEC 27000?
- **Incidenter.** Har allvarliga incidenter inträffat, eller återkommer vissa incidenter ofta? Har incidenter inträffat hos samarbetspartner som till exempel it-leverantörer? Hur har incidenterna hanterats?
- **Revisioner.** Har organisationen genomfört informationssäkerhetsrelaterade revisioner? Vilka resultat har de gett, positivt och negativt?
- **Säkerhetsmedvetenhet.** Hur är medvetenheten om informationssäkerhet och risker med digitalisering och it-användning i organisationen? Finns tillräcklig kompetens i säker hantering av information hos medarbetare eller chefer generellt, och inom särskilt viktiga funktioner som it-funktionen?
- **Informationssäkerhetsarbetet.** Hur arbetar organisationen idag med informationssäkerhet? Hur planerar och arbetar CISO för att organisationen ska arbeta systematiskt med informationssäkerhet?



Du som leder organisationen bör hålla dig informerad om informationssäkerhetsläget, både löpande och vid särskilda genomgångar med CISO. Du behöver som sagt inte vara expert, men du behöver viss grundkunskap för att förstå informationen, kunna ställa rätt frågor och fatta underbyggda beslut. Be din CISO om utbildning och stöd vid behov!

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 *www.msb.se*
Publ.nr MSB1783 - juni 2021