Myndigheten för samhällsskydd och beredskap

Ledningens roll inom informations- och cybersäkerhet

Stöd till dig med en ledande funktion

Ledningens roll inom informations- och cybersäkerhet
– ett stöd till dig med en ledande funktion

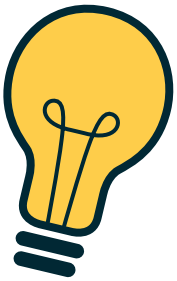
Enheten för systematisk informationssäkerhet

Kontakt: informationssakerhet@msb.se
Produktion: Advant

Publikationsnummer: MSB2532 – december 2024

Informationssäkerhet för ledningen

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



Det här stödet innehåller:

- En beskrivning av informationssäkerhet och hur du kan tänka kring informationssäkerhet i din organisation.
- Varför det är viktigt att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.
- Hur informationssäkerhet bör belysas ur ledningsperspektiv, och varför det är en viktig fråga för ledningen.
- Råd om hur du kan arbeta tillsammans med dem som arbetar med organisationens informationssäkerhet för att uppnå bästa resultat.

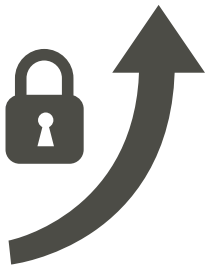
Informationssäkerhet och din organisation

Informationssäkerhet handlar om att skydda viktig information som en organisation hanterar. Det inkluderar metoder, arbetssätt och teknik för att säkerställa att informationen bara nås av behöriga, att den är korrekt samt att den kan användas som det är tänkt och är tillgänglig där och när den behövs. Informationssäkerhet handlar om just det – att införa rätt skydd för att bevara önskad nivå av konfidentialitet, riktighet och tillgänglighet.

Varför är informationssäkerhet viktigt?

Konsekvensen av bristande informationssäkerhet är ofta en ekonomisk förlust. Men brister i detta avseende kan även medföra stopp i verksamheten, att organisationens varumärke och rykte påverkas negativt, samt att information går förlorad eller rentav stjäls. Ledningen har det övergripande ansvaret för informationssäkerheten inom organisationen och är ytterst ansvarig vid incidenter.

Anpassa säkerhetsåtgärder efter era behov

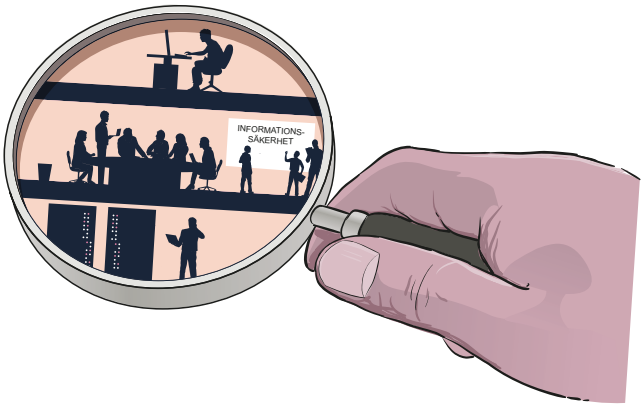


Ett väl fungerande informationssäkerhetsarbete kräver att lämpliga organisatoriska, personalrelaterade, fysiska och tekniska säkerhetsåtgärder införs och kontinuerligt anpassas, så att både information och system skyddas på ett resurseffektivt sätt utifrån aktuella och relevanta risker.

Med lämpliga säkerhetsåtgärder menas att de 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
- omvärldens förtroende för er verksamhet.

Hur arbetet med informationssäkerhet kan och bör bedrivas i just er organisation beror på en mängd faktorer. Arbetets utformning kan påverkas av exempelvis branschtillhörighet, storlek, samarbetspartner, geografisk utbredning, grad av digitalisering, verksamhetens känslighet eller samhällsnytta.



Ledningens agerande är centralt i detta arbete

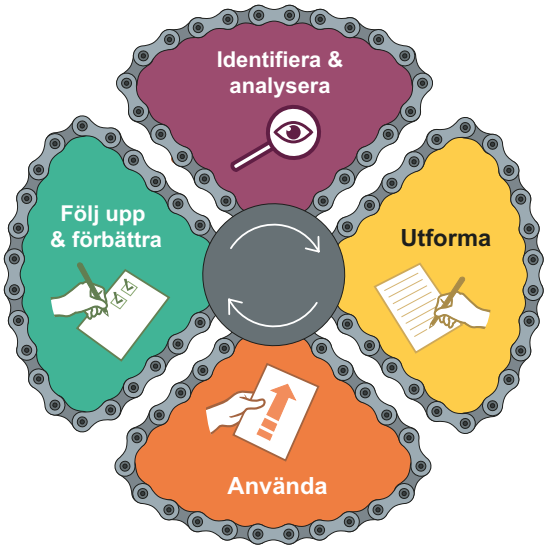
För att du som har en ledande befattning ska kunna bidra till att åstadkomma ett effektivt arbete med informationssäkerhet för just er organisation behöver du se till att informationssäkerhetsarbetet är en integrerad del av verksamhetsstyrningen och därmed bedrivs riskbaserat och systematiskt. Det innebär att du behöver kommunicera med verksamhetsansvariga och den som leder och samordnar informationssäkerhetsarbetet.

Ditt och ledningens agerande har stor betydelse för hur informationssäkerhetsarbetet kommer att utvecklas i organisationen. Det är många faktorer som påverkar arbetet i organisationen, bland annat hur ni fattar beslut, hur ni sätter frågorna på agendan, hur ni själva är förebilder och hur ni legitimerar frågorna påverkar arbetet i organisationen.

Systematiskt informationssäkerhetsarbete

Systematiskt informationssäkerhetsarbete innebär att arbeta förebyggande och kontinuerligt anpassa skyddet utifrån organisationens behov och risker. Ni måste anpassa arbetet till er organisation och dess styrning, så att det blir integrerat i organisationens verksamhetsstyrning.

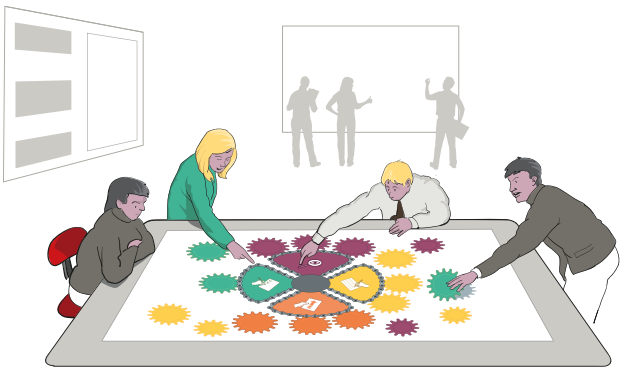
Precis som inom andra områden inom verksamhetsstyrning, till exempel ekonomi och kvalitet, behöver arbetet med informationssäkerhet vara strukturerat och systematiskt för att bli effektivt. Målet är att vid varje tillfälle har rätt nivå av säkerhet för informationen och de system som krävs för att upprätthålla en verksamhet.



Riskhantering och resurshantering i säkerhetsarbetet

Det är viktigt att komma ihåg att arbetet med informationssäkerhet berör alla i en organisation, oavsett roll. Detta gäller såväl ansvarsfördelning som riskhantering samt rutiner för planering och budgetarbete.

Genom att arbeta integrerat med säkerhetsfrågorna som en del av verksamhetens dagliga arbete ökar möjligheterna till ett väl anpassat skydd som tar hänsyn till både effekt och kostnad. Det ger också beslutsfattarna förutsättningar att göra avvägningar mellan olika risker för verksamheten.



Metodstöd för informationssäkerhet

MSB har ett metodstöd för att bedriva ett riskbaserat 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 Metodstödet**[1] som ger en snabb överblick över de bärande beståndsdelarna i arbetet, som är samma för alla organisationer. Beståndsdelarna är

- identifiera och analysera
- utforma
- använda
- följa upp och förbättra.

Ledningen och ansvar för informationssäkerhet

Ledningen har en central roll i att främja informationssäkerheten i organisationen. Alla ledningsgrupper med verksamhetsansvar behöver hålla sig informerade om aktuella risker och status i arbetet med säkerhetsåtgärder. Ledningen ansvarar för att ge nödvändig styrning och inriktning för ett ändamålsenligt arbete med informationssäkerheten.

1. Översikt av Metodstödet https://www.msb.se/sv/publikationer/metodstod-for-systematiskt-informationssakerhetsarbete--en-oversikt/.

I organisationer bör man ha strukturerat ansvaret för informationssäkerheten på ett sätt som speglar det delegerade verksamhetsansvaret. Detta innebär att varje chef, oavsett om det är en linjechef, projektägare, informationsägare eller systemägare, också ansvarar för säker hantering av den information som tillhör deras verksamhetsområde.

Den person som ansvarar för informationen inom en viss verksamhet fungerar även som **riskägare**. Riskägaren har till uppgift att identifiera, acceptera eller hantera risker, vilket ofta innebär att implementera olika säkerhetsåtgärder. Om informationsägarskapet inte har delegerats formellt är det organisationens högsta ledning som har ägarskapet.

Genom att följa denna struktur säkerställs att informationssäkerheten är integrerad i alla delar av verksamheten och att alla nivåer av ledningen är medvetna om och engagerade i säkerhetsarbetet.

Säkerhetsåtgärder kan variera i sin karaktär och kan behöva införas av olika interna eller externa funktioner eller individer. Den chef som är riskägare och ansvarig för informationen ansvarar för att ställa krav på och följa upp att interna och externa tjänster upprätthåller rätt nivå av informationssäkerhet, oavsett vem som implementerar säkerhetsåtgärderna. Det är viktigt att den som har informationssäkerhetsansvaret för en verksamhet får tillräckliga resurser, beslutsmandat och delaktighet i centrala beslut som påverkar verksamhetens informationssäkerhet, till exempel när det gäller säkerhetsåtgärder.

Den som **leder och samordnar en organisations informationssäkerhetsarbete** kallas här för Chief Information Security Officer (**CISO**), precis som i MSB:s metodstöd. Denna roll kan också kallas informationssäkerhetschef, informationssäkerhetssamordnare eller informationssäkerhetsstrateg. CISO är beroende av att du som ingår i ledningen 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 stötta ledningen och övriga roller som har ett informationssäkerhetsansvar i operativa, taktiska och strategiska frågor.

Ett riskbaserat systematiskt informationssäkerhetsarbete är ett förändringsarbete som påverkar organisationen på många sätt, vilket kräver ett samarbete och mellan ledningen och CISO.

Frågor att ställa

Följande frågor – utan inbördes prioritetsordning – kan vara till hjälp för att få en övergripande bild av hur informationssäkerhetsarbetet fungerar i organisationen.

Informationssäkerhetsarbetet: Har ledningen beslutat om en tydlig inriktning med utsedda roller och mandat? Finns det ett systematiskt arbete? Är det känt i organisationen och fungerar det som det är tänkt?

Säkerhetsmedvetande: Hur ser säkerhetskulturen i organisationen ut? Hur främjar vi informationssäkra beteenden?

Hinder: Finns det några hinder för att föra informationssäkerhetsarbetet framåt?

Informationstillgångar: Vet vi vilken vår mest kritiska information är? Vet vi vilka system som hanterar vår kritiska information? Hur jobbar vi systematiskt med detta?

Verksamhet: Vet vi vilken del av verksamheten som är mest kritisk, där organisationen har ett stort beroende av att informationshanteringen fungerar?

Krav: Hur säkerställer vi att vi lever upp till lagkrav som ställs på vår informationssäkerhet? Finns det interna krav? Finns det andra krav?

Risker: Är arbetet riskbaserat? Hur ser processen för riskanalys och riskhantering ut? Finns det några allvarliga identifierade risker som ledningen borde känna till?

Skydd: Hur vet vi om våra säkerhetsåtgärder motsvarar behoven, med hänsyn till skyddsvärden, risker och kostnader?

Incidenter: Har vi en process för incidenthantering? Innehåller den rutiner för när och hur ledningen bör informeras?

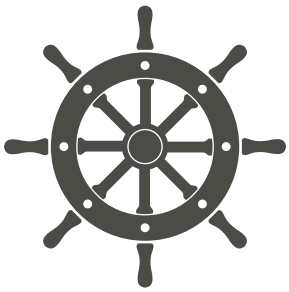
Revisioner: Har organisationen genomfört informationssäkerhetsrelaterade revisioner? Vilka resultat har de gett, positivt och negativt? Hur har ledningen hanterat resultaten?

Uppföljning: Följer vi upp informationssäkerhetsarbetet? Ingår informationssäkerhet i den ordinarie verksamhetsstyrningen (årshjul)?

Kontinuitetshantering: Har vi en plan B? Vem jobbar med den?

Underleverantörer: Hur säkerställer vi styrning och uppföljning för tillräcklig informationssäkerhet hos våra leverantörer?

En ledning som gör skillnad



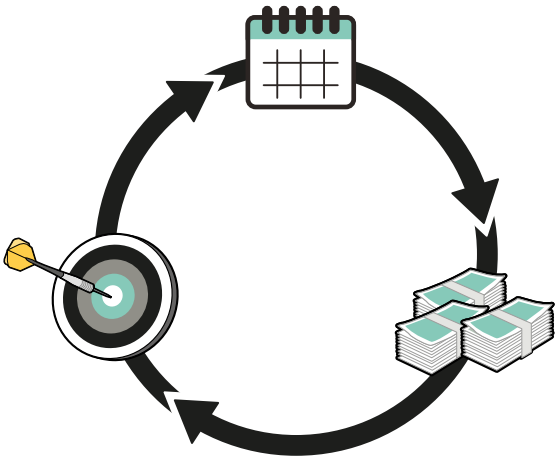
Du som har en ledande position behöver inte vara expert på informationssäkerhet, men du behöver precis som på andra områden ha tillräcklig kunskap för att kunna fatta lämpliga beslut.

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 och hålla dig informerad om hur informationssäkerhetsarbetet går. Du behöver lyssna in, vara nyfiken, fatta de beslut som behövs samt tilldela resurser som motsvarar era målsättningar och ambitioner.

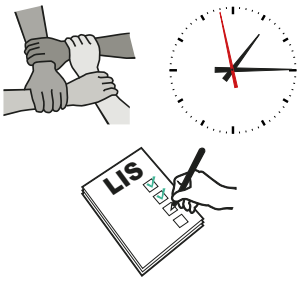
En god relation och kommunikation mellan ledningen och den som ansvarar för att leda och samordna informationssäkerhetsarbetet i organisationen är viktig, eftersom ni är ömsesidigt beroende av varandra:

- För dig som sitter i ledningen är CISO central för att förverkliga ledningens beslut och för att vara den främsta källan till kunskap och information om informationssäkerhetsarbetet i organisationen.
- För CISO är det viktigt att ledningen fattar informerade beslut för att informationssäkerhetsarbetet ska kunna drivas framåt i organisationen.

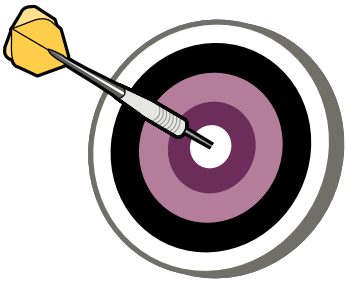
En förutsättning för informationssäkerhetsarbetet är att båda parter har samma förväntningar och mål. Tillsammans bör ni komma överens om en strategisk målbild för organisationens informationssäkerhet och vara överens om principiella tillvägagångssätt för att nå denna målbild. Viktigt är att CISO har mandat som möjliggör uppdraget. Även rapporteringsvägar och samarbetsformer med andra roller i organisationen behöver klargöras. Det är viktigt att du som ledare ger de förutsättningar som krävs, så att CISO kan ge stöd till de ansvariga i verksamheten.



Genom att du som beslutsfattare regelbundet håller dig uppdaterad om status för informations- och cybersäkerhetsarbetet, intern mognad och utveckling samt måluppfyllelse och risker ni lever med, kan du följa upp och fatta relevanta beslut, till exempel om resurser eller riskacceptans. De tillfällen ni som ledning får information om status för arbetet kallas **ledningens genomgång**. Ärendet samordnas och bereds normalt av CISO. Kom överens i förväg om frekvens för genomgången och hur underlaget utformas vad gäller omfattning och nivå, för att möta era behov. Vad som är ändamålsenligt beror på din roll och på organisationens struktur och storlek.



Inför ett årligt möte (ledningens genomgång) kan någon ur ledningen ha ett förmöte tillsammans med CISO för att bestämma mötets omfattning, form, inriktning med mera.



Hur ser man ledningens engagemang?

Avslutningsvis: Hur kan man se att ledningen är engagerad i styrningen av informationssäkerhetsarbetet? Det varierar förstås, men här är några exempel:

Indikation på engagerad ledning	Hur detta kan uttryckas
Det finns en uttalad viljeriktning från ledningen.	I policy-dokument.
Ledningen informerar sig löpande om status på informationssäkerhetsarbete.	Ledningens genomgång.
Pågående satsningar/fokusområden inom informationssäkerhet drivs framåt genom ledningsbeslut.	Genomförda internutbildningar.
Hinder och behov av stöd för bättre informationssäkerhet är identifierade och adresserade.	Eventuella konflikter, interna mandat.
Kommunikation om behovet och nyttan med informationssäkerhet för verksamheten sker löpande.	Interna nyhetsbrev.

Sammanfattning

- Håll dig informerad om informationssäkerhetsläget, både löpande och vid särskilda genomgångar med CISO.
- Du behöver inte vara expert, men du behöver tillräcklig kunskap inom området för att förstå informationen, kunna ställa rätt frågor och fatta väl underbyggda beslut.
- Se till att du har experter och använd dem.
- Var tydlig med förväntningar.
- Får du inte information, fråga efter den.
- Var aktiv.
- Be din CISO om utbildning och stöd.
- Uppmuntra till incidentrapportering – avvikelser är viktiga för lärande och förbättringar.
- Välkomna revision på området.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2532 – december 2024