# Att arbeta systematiskt med informationssäkerhet

## Inledning

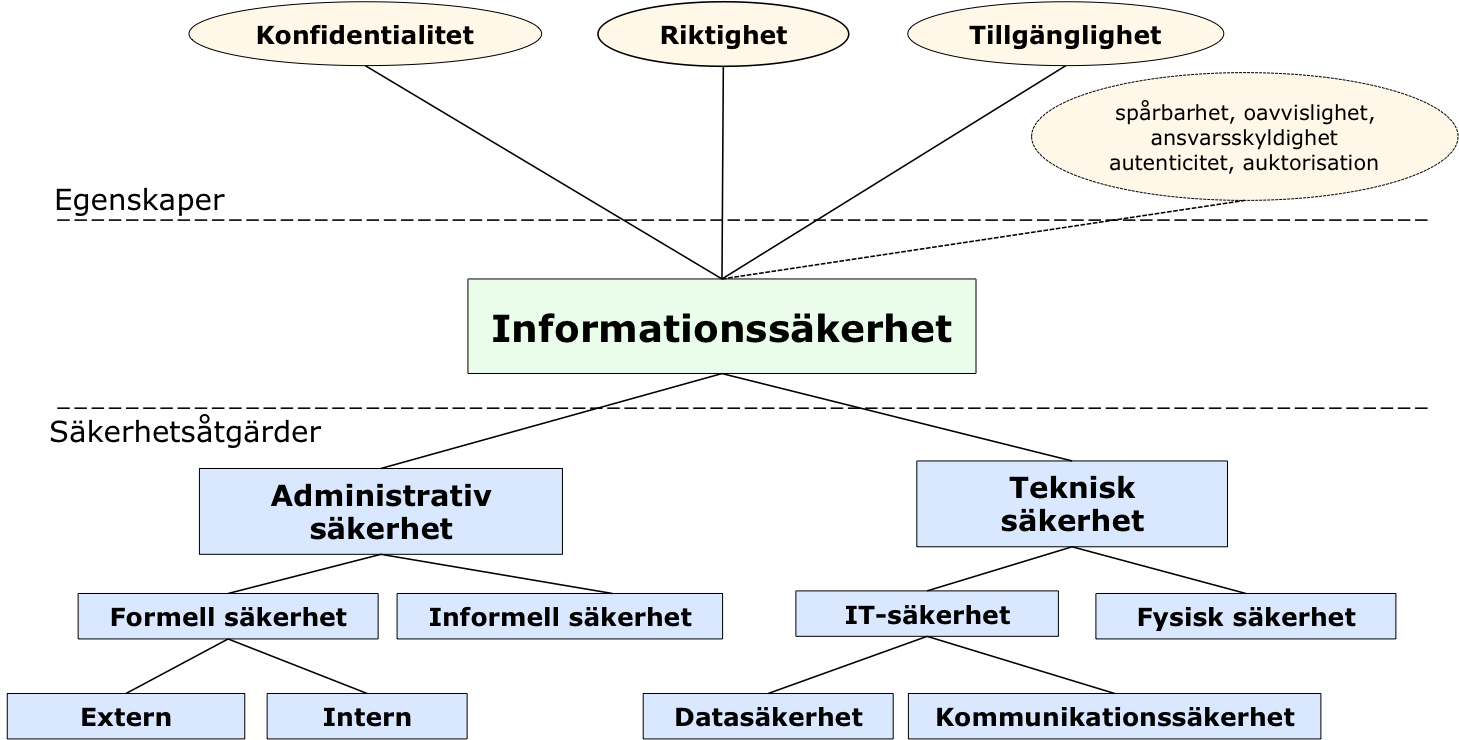
I dagens informationssamhälle är information centralt för alla typer av organisationer. Information finns i olika former såväl muntlig som skriftlig och i allt högre utsträckning digital och automatiserad. Den kan inhämtas, lagras, kommuniceras och användas i olika former av individer och organisationer och är en förutsättning för att skapa värde. Det är avgörande att skydda känslig eller värdefull information och säkra dess hantering för att undvika negativa konsekvenser för en organisation exempelvis om informationen går förlorad, inte finns till hands när den behövs eller hamnar i orätta händer. Informationssäkerhet blir därför ett grundfundament för samhällets alla aktörer.

En god informationssäkerhet innebär att informationssäkerheten är anpassad för verksamhetens förutsättningar och behov. Ledningen får möjlighet att styra och följa upp informations­säker­hets­arbetet, det vill säga att säkerheten är effektiv och ändamålsenlig. Det innebär att verksamheten kan få en bra säkerhetsekonomi där nyttan överväger kostnaderna. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge verksamhetens kritiska information det skydd den behöver. Ett väl fungerande informationssäkerhetsarbete stödjer därmed verksamheten så att den kan nå sina långsiktiga mål.

All informationssäkerhet tar sin utgångspunkt i tre centrala egenskaper som ska upprätthållas;

* konfidentialitet – att information skyddas så att obehöriga inte får åtkomst
* riktighet – att informationen skyddas mot oönskad förändring
* tillgänglighet - att informationen ska vara tillgänglig när den behövs av behöriga användare

Dessa egenskaper kompletteras ibland även med en eller flera andra egenskaper, såsom spårbarhet, oavvislighet, ansvarighet, autentisering och auktorisation (se figur 1).



**Figur 1. Informationssäkerhetens egenskaper och typer av säkerhetsåtgärder**

Informationssäkerhet omfattas av både administrativ och teknisk säkerhet vilket innebär att fokus behöver vara på både människor och it (se figur 1). Teknisk säkerhet omfattar förutom hantering av it-system även hantering av lokaler, larm, inpasseringssystem och datautrustning. Administrativ säkerhet inkluderar bland annat rutiner för behörigheter, utbildning av medarbetare, riskmodell och informationsklassning. Detta bidrar till en medveten säkerhetskultur.

## Systematiskt informationssäkerhetsarbete

Att arbeta systematiskt innebär att utifrån vision, mål och policy utforma och etablera effektiva arbetssätt som ständigt utvärderas och förbättras. En organisation som bedriver sin verksamhet på ett genomtänkt och strukturerat sätt uppnår lättare effektivitet, såväl i produktion som kostnadsmässigt. Detta gäller även inom informationssäkerhetsområdet. Att bedriva ett systematiskt arbete med informationssäkerhet betyder att det finns en tydlig styrning som på ett strukturerat och förutsägbart sätt leder arbetet i enlighet med policy. Det övergripande syftet med systematiskt informationssäkerhetsarbete är därmed att genom ständiga förbättringar och anpassningar till en föränderlig värld skydda informationen på önskad nivå.

## Krav och riskbaserad informationssäkerhet

Krav på informationssäkerhet baseras dels på interna verksamhetskrav men även rättsliga och avtalsmässiga krav, branschkrav och krav från intressenter. Informationssäkerhetsarbetet är därför inte isolerat utan bör integreras i alla verksamhetsprocesser och samordnas med ledningsarbetet. Kraven på alla verksamheter och komplexiteten ökar dessutom i takt med digitaliseringen. Detta medför ett ökat behov av systematik kring informationssäkerhetsarbetet för att kunna stödja organisationens mål och verksamhet.

Allt informationssäkerhetsarbete har sin grund i de risker som organisationer identifierar. Detta är specifikt och centralt i 27000-serien. Arbetet är därför riskbaserat och organisationen ska ta hänsyn till de risker som finns och genomföra bedömningar om hur dessa ska hanteras för att undvika negativa konsekvenser. Detta är särskilt viktigt eftersom det sker ständig nya förändringar i verksamheten och i informationsflöden. Att tänka i risker gör att alla beslut som fattas i verksamheten blir väl balanserade och organisationen får ett medvetet risktagande. Systematiskt informationssäkerhetsarbete, är genom systematiken i arbetssättet, processtyrt och innebär ett ständigt pågående arbete. Därmed får även verksamheten en process till ständiga förbättringar.

## Ledningens ansvar och betydelse

Ledningen har det övergripande ansvaret för informationssäkerheten inom sin organisation. Den är ytterst ansvarig och behöver fatta nödvändiga beslut om inriktning och resurser. En ledning som är engagerad och införstådd med verksamhetsnyttan med informationssäkerhetsarbetet skapar förutsättningar för en hög säkerhetsmedvetenhet i hela organisationen. Ledningens beslut bör spridas i organisationen i syfte att förankra intentionerna. En viktig del av informationssäkerhetssamordnarens uppdrag är därför att skapa arbetssätt som involverar och engagerar ledningen.

Informationssäkerhetsarbetet är en stödprocess som behöver vara väl förankrad och ska bidra till kund- och verksamhetsnyttan, vilket inkluderar att skydda verksamheten och det egna varumärket, upprätthålla kontinuitet och undvika informationsläckage med mera.

Att införa ett systematiskt informationssäkerhetsarbete är att leda förändringsarbete vilket kräver ett samarbete och stöd mellan ledning och CISO. För att nå framgång behövs förståelse om organisationskulturen och hur denna kan tas tillvara på i arbetet.

För att ett systematiskt informationssäkerhetsarbete inte ska stanna upp är det viktigt att ledningen kontinuerligt följer och kommunicerar arbetet. CISO bör löpande få möjlighet att redovisa hur arbetet fortskrider för ledningen. Ledningens ansvar är också aktivt stödja arbetet med informationssäkerhet genom att föra upp frågorna på agendan i olika sammanhang, se till att informationssäkerhetsarbetet har tillräckligt med resurser samt ge ansvar och befogenheter till berörda parter.

## Organisation, ansvar och roller

För att kunna utveckla och erhålla kontinuitet i informationssäkerhetsarbetet är det väsentligt att roller och ansvar är definierade och kända inom hela organisationen.

Informationssäkerhetsansvaret bör följa verksamhetsansvaret. Avdelningar/enheter ska verka operativt i säkerhetsarbetet inom respektive verksamhetsområde. Enhetscheferna ansvarar för fortlöpande analys, kontroll och uppföljning av informationssäkerheten samt fastställande av rätt nivå för informationsskyddet.

Alla medarbetare har ansvar att känna till och efterleva styrande dokument inom informationssäkerhet. För att medarbetare ska förstå betydelsen av informationssäkerhet i sitt arbete behövs olika kompetensutvecklingsinsatser.

Organisationens informationssäkerhetsfunktion, CISO är en stödfunktion vars uppgift är att utveckla, samordna och följa upp informationssäkerhetsarbetet i organisation. Funktionen kan vid behov stödja med metod- och expertkompetens i enheternas löpande operativa informationssäkerhetsarbete.

Mer information om hur informationssäkerhetsarbetet kan organiseras och vilka roller som bör ingå finns att läsa i metodstödets delområde *Utforma Organisation*.

## Integrera informationssäkerhet i styrningen

På övergripande nivå bör informationssäkerhet integreras med organisationens verksam­hets­styrning. Mål, aktiviteter och handlingsplan inom informationssäkerheten bör följa samma planeringsrutiner och tidsramar som övrig verksamhetsplanering, inklusive budgetarbete. Likaså bör informationssäkerheten följas upp enligt samma rutiner och tidsramar som övrig verksamhet.

För att uppnå rätt nivå av informationssäkerhet är det centralt att arbetet med informationssäkerhet genomsyrar verksamhetens löpande verksamhet. Det ska leda till att det blir en naturlig del i den ordinarie verksamheten och kulturen.

För att lyckas med integrering krävs att organisationens chefer och medarbetare förstår och accepterar sitt ansvar inom informationssäkerhet. Informationssäkerhetsfunktionen stödjer genom sin expertkompetens på informationssäkerhetsområdet.

Arbetar organisationen i enlighet med flera ledningssystemstandarder, till exempel kvalitet och miljö, kan dessa med fördel integreras till ett ledningssystem (kallas då ibland för ett verksamhets­system). Detta är tämligen enkelt sedan alla ledningssystemstandarder numera är harmoni­serade, det vill säga är strukturerade på samma sätt. Det enda som skiljer dem åt är områdesspecifika tillägg.

Om organisationen även arbetar efter andra för området närliggande standarder som till exempel COSO[[1]](#footnote-1) eller ITIL[[2]](#footnote-2) bör även dessa integreras med informationssäkerhet.

När ett ledningssystem enligt standarden 27001 byggs upp är det viktigt att det utformas efter verksamheten och på ett sådant sätt att det ger

* tillräckligt stöd till hela verksamheten när det gäller att arbeta strukturerat och systematiskt med att skydda information och
* tillräckligt stöd till ledningen så att den kan styra informationssäkerhetsarbetet.

### Sammanfattning

En verksamhet som har ett effektivt informationssäkerhetsarbete kännetecknas av

* **Ledningens vilja att styra verksamhetens informationssäkerhet**
* **Informationssäkerhetsarbete som skapar ett värde för verksamheten**
* **Riskbaserat informationssäkerhetsarbete som leder till ständiga förbättringar**
* **Verksamhetsstyrning där informationssäkerhetsarbetet följer den årliga planerings- och uppföljningscykeln.**

1. COSO – The Committee of the Sponsoring Organizations of the Treadway Commission är ett metodstöd för intern styrning och kontroll [↑](#footnote-ref-1)
2. ITIL – IT Infrastructure Library är en sammanställd praxis för it service management [↑](#footnote-ref-2)