# Ledningssystem

Alla organisationer har ett ledningssystem, eller ett ”system” för att leda verksamheten. Det handlar helt enkelt om hur ledningen styr sin verksamhet. Detta ledningssystem kan vara mer eller mindre strukturerat och mer eller mindre konkret. Det kan kalla styrsystem eller styrmodell eller ingenting alls, men det finns där.

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är därmed den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning.

Ledningssystemet bygger därmed på organisationens planerings- och uppföljningscykler. Dessa cykler innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och -kontroller samt ser över styrdokumenten med jämna mellanrum.

## ISO-standarder för ledningssystem för informationssäkerhet

Hur informations­säkerhetsarbetet kan bedrivas på ett systematiskt sätt och i enlighet med ”best practice” finns beskrivet i standarderna för ledningssystem för informationssäkerhet. Metodstödet bygger på dessa standarder och utgör ett stöd i hur man omsätter standarderna i praktiken. Metodstödet kan till stora delar användas utan att ha tillgång till standard­dokumenten men vi rekommenderar användarna av Metodstödet att även inskaffa åtminstone 27000, 27001 och 27002. Se nedan för en närmare beskrivning.

Standarder kring informationssäkerhet har samlats i standardserien 27000. Den har tagits fram inom ramen för samarbetet i de internationella standardiseringsorganen ISO (International Organization for Standardization) och IEC (International Electrotechnical Commission). Standarderna arbetas fram mot bakgrund av de deltagande internationella experternas samlade erfarenheter av ett systematiskt arbete med informationssäkerhet. Från svensk sida deltar SIS (Swedish Standards Institute) med experter från de organisationer som valt att delta i SIS arbete på nationell nivå. [[1]](#footnote-1)

Standarderna är strukturerade i tre nivåer: krav, riktlinjer och stöd. Dessa olika nivåer visar vad (krav) en organisation bör göra när det gäller informationssäkerhet samt hur (riktlinjer och stöd) man kan arbeta.

Den som använder en LIS-standard får hjälp i sitt interna arbete men ansluter sig också till ett vedertaget sätt att arbeta med informations­säkerhet och anammar en gemensam terminologi. På så sätt blir det lättare att kommunicera och samarbeta om gemensamma informa­tions­säkerhets­frågor med kollegor i andra organisationer, både nationellt och internationellt.

De grundläggande standarderna i 27000-serien är:

* SS ISO/IEC 27000 Översikt och terminologi beskriver de standarder som ingår i 27000-serien. Här finns också de termer som används i de övergripande standarderna på informationssäkerhetsområdet samlade.[[2]](#footnote-2) Förutom översikt och terminologi förs även ett resonemang kring betydelsen av att arbeta strukturerat med informationssäkerhet och vilken nytta en organisation har av att ta stöd i 27000-standarderna.
* SS-EN ISO/IEC 27001:2017 Ledningssystem för informationssäkerhet – Krav är den standard som beskriver ledningssystemet och som man kan certifiera sig mot.
* SS-EN ISO/IEC 27002:2017 Ledningssystem för informationssäkerhet – Riktlinjer beskriver vilka säkerhetsåtgärder ledningssystemet generellt ska innehålla. Kapitlen i 27002 har fokus på säkerhetsåtgärder men omfattar även frågor om styrning av informationssäkerhet såsom regelverk för informationssäkerhet (policy), organisation och efterlevnad.
* ISO/IEC 27003:2017 Information Technology – Security Techniques – Information Security Management Systems – Guidance[[3]](#footnote-3) ger vägledning i hur en organisation kan uppfylla kraven i 27001.

Utöver dessa fyra ”grundstandarder” innehåller 27000-serien ytterligare standarder som specifikt behandlar olika aspekter av säkerhetsarbetet, till exempel 27004[[4]](#footnote-4) som behandlar mätning av informationssäkerhet, 27005[[5]](#footnote-5) som ger stöd för riskhantering och 27006 som ställer krav på de organisationer som reviderar och certifierar ledningssystem för informationssäkerhet. En komplett förteckning över de ingående dokumenten finns på [www.sis.se](http://www.sis.se).

När det gäller terminologi på svenska så finns Teknisk rapport SIS-TR 50:2015.

1. Samtliga informationssäkerhetsstandarder är framtagna i samarbete mellan ISO och IEC. När en standard dessutom benämns SS-ISO/IEC innebär det att den antagits som svensk standard. Om det förutom SS även står EN (SS-EN ISO/IEC) innebär det att standarden är antagen som europeisk standard av den europeiska standardiseringsorganisationen CEN (European Committee for Standardization).

   För standarder som inte anges med årtal hänvisas till den senaste utgåvan. SS ISO/IEC 27000 utkommer med kortare intervaller än de andra standarderna för att vid varje tidpunkt vara så aktuell som möjligt. [↑](#footnote-ref-1)
2. Termer och definitioner finns inte i de standarder vi hänvisar till i metodstödet utan endast samlade i SS-ISO/IEC 27000. [↑](#footnote-ref-2)
3. 27003:2017 kommer att översättas till svenska och antas som svensk standard. [↑](#footnote-ref-3)
4. SS ISO/IEC 27004:2017 kom ut i ny reviderad form 2017, revideringen innebär en förenkling av innehållet. SS-ISO/IEC 27004:2010 håller en hög teoretisk nivå som kan vara svår att omsätta i praktik. [↑](#footnote-ref-4)
5. 27005 är under revidering. Vad detta kommer att innebära innehållsmässigt är i nuläget (våren 2018) svårt att säga. [↑](#footnote-ref-5)