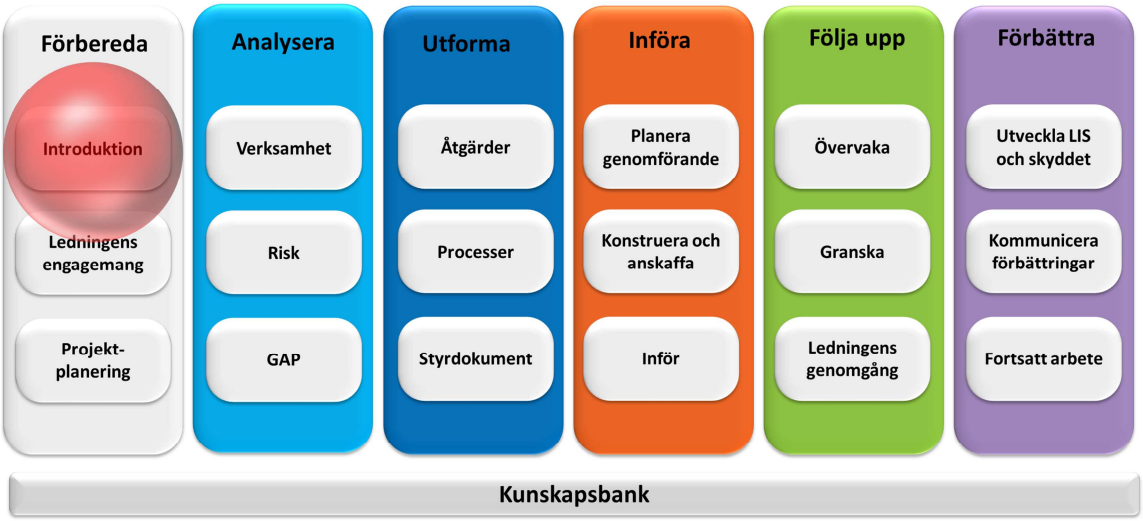
Myndigheten för samhällsskydd och beredskap

Introduktion till metodstödet



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning

1.1 Informationssäkerhet i organisationen

Alla organisationer behöver säker information. Till exempel har många organisationer omfattande och täta kundkontakter, och om kunddatabasen går förlorad kan det bli svårt eller rent av omöjligt för dem att driva en normal verksamhet. Samtidigt innebär förlusten ett brott mot reglerna i personuppgiftslagen[1] . Ett annat exempel är innovationsföretag som kan ha känsliga forskningsresultat, och om obehöriga lyckas komma åt dem drabbas företaget av stora ekonomiska förluster i form av den tid, kanske flera år, som har investerats i att utveckla nya produkter. Enligt lag måste alla myndigheter se till att allmänna handlingar hanteras på ett sådant sätt att de inte förändras eller förstörs av någon obehörig person[2].

Information i olika former är den viktigaste tillgången för de flesta organisationer. Exemplen ovan visar varför det är viktigt att i både den privata och den offentliga sektorn arbeta systematiskt och behovsanpassat med att trygga informationen så att den är konfidentiell, riktig och tillgänglig. Detta arbete är en angelägenhet för hela organisationen, inte minst ledningen.

1.2 Ledningssystem för informationssäkerhet

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

Ett ledningssystem för informationssäkerhet (LIS) är den del av ledningssystemet som styr informationssäkerheten i verksamheten[3]. Andra delar av systemet kan exempelvis hantera miljö-frågor eller kvalitet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att LIS integreras med de övriga formerna för styrning[4]. På samma sätt som inom miljö- och kvalitetsområdet finns det etablerade internationella och nationella standarder som stödjer arbetet med ledningssystem för informationssäkerhet.

---

[1] Personuppgiftslagen 1998:204.

[2] Offentlighets- och sekretesslagen (2009:400) och arkivlagen (1990:782).

[3] När det gäller statliga myndigheter har MSB föreskrivit att de ska tillämpa ett ledningssystem för informationssäkerhet, se MSBFS 2009:10. Detta innebär dock inget krav på att använda det stöd som finns på informationssäkerhet.se utan detta är helt frivilligt.

[4] I bilagorna A, B, C och D finns en utvidgad diskussion kring vad ett sådant ledningssystem är och även ett förslag på en lämplig dokumentstruktur .

Se bilaga A för en diskussion om ledningssystem i allmänhet och LIS i synnerhet.

1.3 LIS-standarder

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). I standardiserings-arbetet har man använt sig av olika organisationers samlade erfarenheter av ett systematiskt arbete med informationssäkerhet.

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

- Den som använder en LIS-standard får hjälp i sitt interna arbete men ansluter sig också till ett vedertaget sätt att arbeta med informations-säkerhet och anammar en gemensam terminologi. På så sätt blir det lättare att kommunicera och samarbeta om gemensamma informa-tionssäkerhetsfrågor med kollegor i andra organisationer, både nationellt och internationellt. SS-ISO/IEC 27001:2006 Ledningssystem för informationssäkerhet – Krav (nedan kallad 27001) är den standard som beskriver ledningssystemet och som man certifierar sig mot.
- SS-ISO/IEC 27002:2005 Ledningssystem för informationssäkerhet – Riktlinjer (nedan kallad 27002) beskriver på en generell nivå vad ledningssystemet ska innehålla. Kapitlen i 27002 omfattar allt från regelverk för informationssäkerhet (policy) och övergripande arbetssätt (riskbedömning) till de olika typer av åtgärder som behövs för att ha en god informationssäkerhet.
- SS-ISO/IEC 27003:2010 Vägledning för införande av ledningssystem för informationssäkerhet (nedan kallad 27003) ger stöd till den organisation som ska införa ett LIS.

Utöver dessa tre ”grundstandarder” innehåller 27000-serien ytterligare standarder som specifikt behandlar olika aspekter av säkerhetsarbetet, till exempel 27004 som behandlar mätning av informationssäkerhet, 27005 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.

1.4 Stöd för verksamhetens arbete

På www.informationssäkerhet.se finns stöd för organisationer som ska införa eller förbättra sitt ledningssystem för informationssäkerhet med utgångspunkt i standarderna. Stödet är utformat som ett metodstöd. På webbplatsen finns

även annan information som stödjer ett systematiskt informationssäkerhetsarbete: information om strategier på området, rättsliga regelverk, utbildningsmaterial med mera.

Detta metodstöd riktar sig i huvudsak till dem som ska arbeta systematiskt med informationssäkerhet i en verksamhet, exempelvis verksamhetschefer, säkerhetschefer och informationssäkerhetsansvariga. I arbetet med att införa eller vidareutveckla ett sådant ledningssystem är det dock viktigt att engagera representanter från i princip hela organisationen. Exempelvis behövs kunskap om verksamhetens behov, IT-miljön, rättsliga aspekter, ekonomi och revision.

Dessutom måste metodstödet på informationssäkerhet.se och standarderna 27001 och 27002 anpassas till den aktuella verksamhetens behov. Metodstödet kan närmast beskrivas som ett ”smörgåsbord”. Vissa organisationer behöver ett omfattande ledningssystem – andra ett betydligt enklare. Ledningssystemet ska dock vara utformat efter verksamheten och på en sådan nivå att det ger

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

Ett ledningssystem kan utformas på lite olika sätt men vissa delar är grundläggande. Myndigheten för samhällsskydd och beredskap (MSB) har givit ut föreskrifter om statliga myndigheters informationssäkerhet[5] och där står det att myndigheterna ska

1. upprätta en informationssäkerhetspolicy och andra styrande dokument
2. utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet
3. klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet
4. använda riskanalyser för att bestämma hur risker ska hanteras samt vilka åtgärder som ska vidtas
5. dokumentera viktiga granskningar och säkerhetsåtgärder.

Dessutom ska myndighetens ledning hålla sig informerad om arbetet och minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet.

Detta arbete ska enligt föreskrifterna följa standarderna 27001 och 27002. Dessa föreskrifter är bara bindande för statliga myndigheter men uppräkningen visar ändå vad ett ledningssystem bör innehålla även i andra organisationer.

[5] MSBFS 2009:10 Myndigheten för samhällskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

2. Framgångsfaktorer

Erfarenheter från Sverige och andra länder visar att det finns ett antal viktiga framgångsfaktorer för att lyckas bra med att införa ett ledningssystem för informationssäkerhet.

2.1 Ledningens engagemang

Det är ytterst viktigt att ledningen formellt beslutar att införa ett LIS. Beslutet bör bygga på att ledningen är engagerad och förstår vilken nytta verksamheten har av informationssäkerhetsarbetet. Ledningen måste också aktivt stödja arbetet med informationssäkerhet genom att föra upp frågorna på agendan i olika sammanhang, kontinuerligt följa arbetet och ge det tillräckliga resurser samt ge ansvar och befogenheter till de berörda parterna. Ledningens beslut bör spridas i organisationen i syfte att förankra intentionerna.

2.2 Förankring i och kunskap om organisationen

Med ledningens engagemang och uttalade mandat kan ledningssystemet förankras i organisationen, men det räcker inte. Informationssäkerhetsarbetet kommer att innebära förändringar och nya arbetsuppgifter, och därför måste alla delar av den verksamhet som ingår vara villiga att ta emot, använda och efterleva det nya. Ett sätt är att tidigt i processen identifiera de aktörer som påverkar eller påverkas av arbetet på något sätt, och bjuda in alla relevanta parter som deltagare i processen. Det kan exempelvis vara lämpligt med en referensgrupp med personer från olika delar av verksamheten som kan ge råd och tips om hur de planerade åtgärderna skulle tas emot i den egna verksamhetsdelen eller som kan tänka på frågor ur olika perspektiv (till exempel juridiska, ekonomiska och sociala perspektiv).

De personer som ska hålla samman arbetet med att införa LIS ska naturligtvis ha god kunskap om LIS, men de måste också ha förankring i och kunskap om organisationen. Att införa LIS är ett förändringsarbete och det kan underlätta mycket om de drivande personerna är väl kända och har förtroende i organisationen.

2.3 Tillräckliga resurser

En annan viktig faktor är att det finns tillräckligt med resurser för att genomföra arbetet, i form av relevant kompetens, tid, bemanning och pengar. En del gör misstaget att avsätta för lite pengar som bara räcker fram till dess att

ledningssystemet finns som en serie dokument på intranätet. Då kvarstår ändå arbetet med att få verksamhetens olika delar att följa de fastslagna åtgärderna och säkerhetsprocesserna. Det är en stor fördel om någon av de centrala deltagarna har genomgått en liknande process tidigare.

Eftersom ett LIS-införande är ett förändringsarbete är det viktigt att tänka igenom vilka krav det ställer på de personer som ska arbeta med införandet. Det är också viktigt att de som ingår i projektgruppen får möjlighet att lära sig och förstå de standarder som ska införas. I projektgruppen måste det även finnas personer med kompetens inom IT-säkerhetsområdet eftersom många av de säkerhetshöjande åtgärder som ska övervägas, förbättras, utformas och införas är av teknisk karaktär, framför allt när det gäller att utforma och införa LIS.

2.4 Verksamhetsanpassning

Både själva införandet av ett LIS och allt informationssäkerhetsarbete ska verksamhetsanpassas. Denna verksamhetsanpassning innebär olika saker för varje organisation, men i det stora handlar det om organisationens storlek och verksamhet. Organisationskulturen är också viktig, liksom organisationens utseende och de styrformer som finns. Dessutom måste införandet anpassas till det säkerhetsmässiga utgångsläget.

Verksamhetsanpassningen bygger alltså på det utgångsläge som finns när LIS-införandet börjar. I praktiken kan verksamhetsanpassning handla om att förankringsprocessen måste ta lång tid eller att man måste börja med snabba problemlösningar som kan ge en acceptabel säkerhetsnivå eller snabba resultat för att senare jobba mot ett fullskaligt LIS-införande. Det kan också hända att LIS-projektet i början måste begränsas till en del av verksamheten.

En viktig del i verksamhetsanpassningen är att integrera LIS med de befintliga verksamhetsprocesserna. LIS ska integreras med verksamhetsstyrningen i stort, till exempel befintliga ledningssystem inom miljö eller kvalitet. Det kan också handla om att integrera med till exempel COSO[6] som är en övergripande modell för verksamhetsstyrning med fokus på intern styrning och kontroll, eller med ITIL[7] som är ett metodstöd för styrning av driften.

För att verksamhetsanpassa och integrera systemet med den övriga verksamheten kan man göra organisationsövergripande riskanalyser med fokus på organisationen som helhet och de hot, oönskade händelser och tillstånd[8] som kan hindra organisationen från att uppnå sina övergripande mål. I en sådan övergripande riskanalys hanteras alla typer av hot, inte enbart de som är

[6] COSO, The COmmittee of the Sponsoring Organizations of the Treadway Commission, är ett metodstöd för intern styrning och kontroll.
[7] ITIL, IT Infrastructure Library, är en sammanställd praxis för IT-service management.
[8] Det är bäst att inte enbart analysera rena hot utan även oönskade händelser och oönskade tillstånd eftersom de också kan hota verksamheten.

riktade mot informationstillgångarna. För offentlig verksamhet finns dessutom flera regelverk som *kräver eller förutsätter att riskanalyser genomförs*.[9] Det mest effektiva är då att möta kraven genom att göra en riskanalys som beaktar alla dessa olika regleringar. Dessutom är flera hot gemensamma för hela organisationen och det är praktiskt att ta hand om dem på en övergripande nivå. När det senare gäller riskanalyser på lägre hierarkisk nivå kan man bortse ifrån dessa hot eller hänvisa till en övergripande analys.

Det går att använda samma metod oavsett vad riskanalysen fokuserar på: en organisationsövergripande analys eller en analys som fokuserar på en enstaka verksamhetsprocess eller ett IT-system.

Informationssäkerhet är inget som existerar självständigt från de befintliga verksamhetsprocesserna – tvärtom. Informationssäkerheten är en egenskap som andra processer och system får genom att säkerheten integreras i dem. Därför är det viktigt att undersöka hur alla befintliga processer ser ut och hur de kan bli informationssäkra på ett lämpligt sätt. Det gäller att se hur ett LIS ska utformas så att det fungerar med och blir en del av verksamhetens totala sätt att styra arbetet.

Alla organisationer är olika och därför är det svårt att ge fler konkreta råd för hur verksamhetsanpassningen ska gå till. Det viktiga är dock att både ledningen och projektgruppen hela tiden är medveten om vikten av denna anpassning.

[9] MSBFS 2009:10, förordning om intern styrning och kontroll i staten (2007:603), förordning om statliga myndigheters riskhantering (1995:1300), arbetsmiljölagen (1977:1166), förordning om internrevision vid statlig myndighet (2006:1228), förordning om krisberedskap och höjd beredskap (2006:942) och säkerhetsskyddsförordningen (1996:633).

3. Organisation för LIS-införande

Utgångspunkten är att metodstödet ska vara förhållandevis enkelt att använda, även för dem som inte har arbetat med systematiskt informationssäkerhetsarbete på det här sättet tidigare. Innan arbetet börjar är det dock viktigt att göra vissa förberedelser och se till att de som ska arbeta med införandet av LIS har relevant kompetens.

1. *Mandat*: Den som får i uppdrag att införa eller utveckla organisationens LIS ska ha tillräckligt och tydligt mandat från ledningen att genomföra arbetet.

2. *Långsiktighet och konsultstöd*: Arbetet med ett LIS är i princip ständigt pågående och kan beskrivas som en uppåtgående spiral. När man har genomfört de sista punkterna i processen är det dags att börja om för att ytterligare utveckla och förfina informationssäkerhetsarbetet. Det är därför viktigt att långsiktigt och metodiskt bygga upp intern kompetens i organisationen. Ofta är det bra med konsultstöd men organisationen bör vara aktiv och engagerad så att inte kompetensen försvinner när konsulten har genomfört sitt uppdrag.

3. *Organisationskunskap*: För att få ett fungerande ledningssystem för informationssäkerhet är det nödvändigt att anpassa införandet till den egna organisationen. Detta förutsätter att den eller de som arbetar med detta har eller kan få god insikt i organisationen och dess verksamhet.

4. *Olika discipliner*: Informationssäkerhet berör flera olika discipliner och det kan bli aktuellt med frågor inom teknik, ekonomi, organisation och juridik. Vissa saker är betydligt lättare att lösa i början av arbetet än senare när ledningssystemet är på plats. För att tidigt uppmärksamma sådana frågor är det lämpligt att involvera organisationens jurister, IT-ansvariga och ekonomer redan från början.

Det är en fördel om arbetet kan bedrivas i projektform eftersom det innefattar ramar i form av pengar, kalendertid, bemanning och så vidare. Många organisationer har dessutom redan en beslutad modell för projektstyrning som man bör följa. Sådana projektstyrmodeller anger ofta att projektet ska ha en sponsor i verksamhetens ledning som sitter med i projektstyrgruppen, att man bemannar projektet på ett rimligt sätt för att kunna lösa uppgiften samt att man sätter upp milstolpar för vad som ska vara uppnått och när. I projektets startfas är det bra att upprätta en projektplan, och metodstödet med processmodellens steg kan vara en utgångspunkt för de olika stegen och beslutspunkterna i projektet.

4. Metodstödet

4.1 Metodstödets syfte

Det krävs olika insatser för att informationssäkerhetsarbetet ska följa verksamhetens övergripande strategi och styrning, och metodstödet och dess olika delar är ett frivilligt metodstöd som underlättar arbetet med dessa insatser. Metodstödet avser informationssäkerhet för verksamheten i stort och är inte fokuserat på informationssäkerhet i enskilda system.

4.2 Målsättningar med metodstödet

Standarderna 27001 och 27002 visar hur ett ledningssystem för informationssäkerhet kan se ut. Standarderna ger god ledning när det gäller *vad* som kan och bör ingå i organisationens LIS. För att lättare kunna införa och vidareutveckla systemet behöver dock många organisationer mer praktiskt stöd för att veta *hur* de olika delarna ska utformas och införas.

I 27003 finns en modell när det gäller att införa ledningssystem för informationssäkerhet i verksamheter. För att bli praktiskt användbar måste dock 27003 tolkas och specificeras ytterligare. Metodstödets syfte är att göra just detta genom att erbjuda konkreta metodsteg och mallar för arbetet med LIS.

För att metodstödet ska vara så praktiskt och användbart som möjligt är följande egenskaper prioriterade:

- *Verksamhetsinriktat*. Det är i verksamheten som riskerna finns och ska hanteras. Informationssäkerhetsarbetet ska vara anpassat till och integrerat med verksamheten.
- *Pedagogiskt och konkret*. Det ska vara enkelt att ta till sig och använda metodstödet.
- *Vedertaget*. Metodstödet bygger på internationellt vedertagna standarder för informationssäkerhet (27000-familjen).
- *Komplett*. Metodstödet ska täcka in informationssäkerhetens alla aspekter. Genom att tillämpa metodstödet ska organisationen kunna få ett ändamålsenligt ledningssystem för informationssäkerhet.
- *Generiskt*. Metodstödet ska kunna användas av organisationer av alla typer och storlekar, både företag och myndigheter.
- *Pragmatiskt*. Metodstödet ska gå att använda i praktiken, och detta är viktigare än att det är helt och hållet akademiskt stringent.

4.3 Metodstödets relation till BITS

Krisberedskapsmyndigheten gav ut rekommendationerna och verktygen BITS och BITS Plus (BITS = Basnivå för informationssäkerhet)[10] som har haft en relativt tydlig inriktning på IT- och systemsäkerhet, medan 27000-serien av standarder och detta metodstöd fokuserar på informationssäkerhet i relation till hela organisationen eller verksamheten. BITS stöds inte längre av MSB, men den som tidigare har arbetat enligt BITS kan oftast använda det befintliga arbetet som en viktig utgångspunkt i det fortsatta arbetet, speciellt när det gäller utformningen av skydd för specifika informationssystem. Den senaste versionen av BITS har anpassats till ledningssystem för informationssäkerhet och har samma kapitelindelning och upplägg som 27002.

4.4 Att använda metodstödet

Metodstödet beskriver en process och riktar sig till den som ska arbeta med informationssäkerhet i en verksamhet. Metodstödet bygger på standarderna i 27000-serien. Som nämnts tidigare går det också att kombinera Metodstödet med andra standarder, till exempel ITIL och COSO.

Man kan antingen använda hela metodstödet med tillhörande vägledningar eller välja de delar som passar verksamhetens aktuella behov. Det är dock viktigt att anpassa hela eller delar av metodstödet så att det passar den egna verksamheten.

Metodstödet kan ses som en ”idealiserad” bild av hur arbetet kan bedrivas, i tydliga steg som logiskt följer på varandra.

Metodstödet är uppbyggt så att det ska kunna användas av en organisation som ännu inte har gjort några anpassningar av sitt befintliga informations-säkerhetsarbete till standarden för LIS. Det finns en logisk följd i de olika processtegen, delprocesserna och dessas aktiviteter.

I praktiken lär det i de flesta fall inte vara möjligt att följa metodstödet från A till Ö. Det är snarare så att metodstödet kan ses som ett smörgåsbord från vilket man plockar och anpassar de bitar som behövs i den egna organisationen. Det innebär att man i praktiken inte bör se de olika proces-stegen och delprocesserna som sekventiella utan snarare att dessa tidsmässigt kan genomföras i olika ordning eller samtidigt beroende på det utgångsläge och de behov som den egna organisationen har. Ett exempel är att framtagandet av informationssäkerhetspolicyn behandlas i processteget *Utforma* medan det i själva verket kan vara mer relevant att ta fram denna redan i ett inledande skede som ett bevis för ledningens engagemang och en signal till organisationen att ta det påbörjade LIS-arbetet på allvar. Ett annat exempel på hur metodstödet kan användas i praktiken är att det här dokumentet, tillsammans med dokumentet om ledningens engagemang kan användas för att klippa och klistra ihop en egen introduktion, anpassad efter den egna

[10] Mer om BITS, se http://www.msb.se/RibData/Filer/pdf/24855.pdf

organisationens behov av introducerande information. Kom dock ihåg att respektera de upphovsrättsliga villkoren enligt creative commons presenterade inledningsvis i varje dokument.

För att på bästa sätt tillämpa metodstödet är rekommendationen att bedriva arbetet i projektform. På det viset tvingas man att arbeta strukturerat genom att skapa en projektorganisation och en plan för hur arbetet ska bedrivas resurs- och tidsmässigt. I projekttänken finns också inbyggt att ledningen engageras i form av styrgrupper och förutbestämda beslutspunkter. För mer information om projektarbete se dokumentet *Projektplanering*.

Metodstödets olika delar går lika bra att använda om arbetet bedrivs i linjen. I det kontinuerliga informationssäkerhetsarbetet kan man använda valda delar av metodstödet för att stärka och anpassa informationssäkerhetsarbetet till LIS.

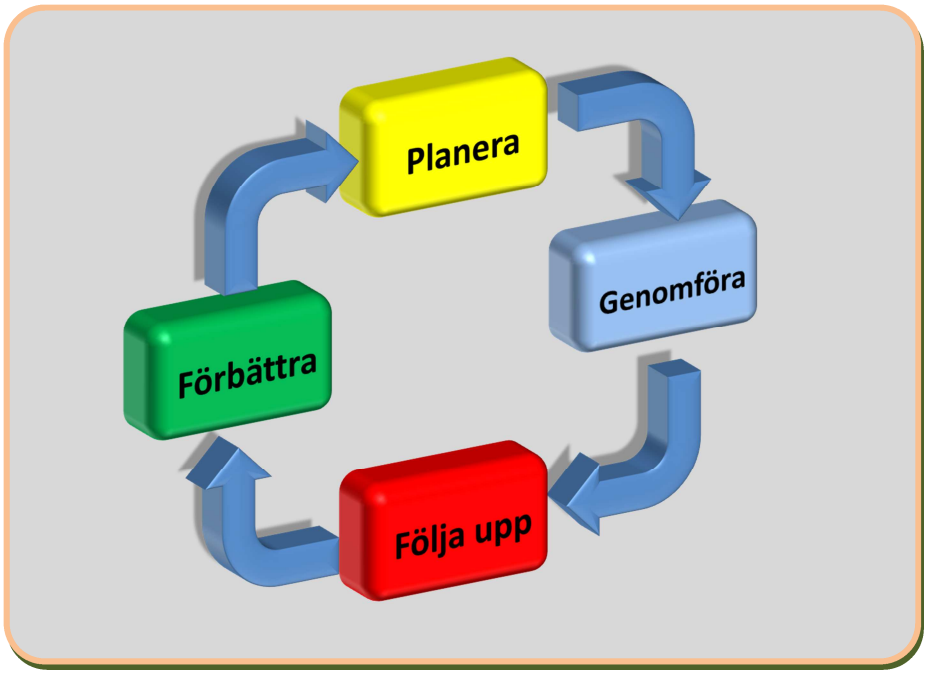
5. Metodstödets delar

Här följer en kort genomgång av hur man arbetar enligt den så kallade PDCA-metoden[11] (”plan, do, check, act”), och därefter en snabb genomgång av de olika aktiviteterna för varje processteg. Samtliga processteg förklaras ingående i separata dokument som finns på informationssäkerhet.se.

5.1 Planera, genomföra, följa upp och förbättra

När det gäller informationssäkerhet går PDCA-metoden ut på att ständigt förbättra arbetssätt och säkerhetslösningar. Detta görs genom att hela tiden låta PDCA-cykeln snurra runt (figur 1).

Figur 1. PDCA-cykeln



På detta sätt får man ett strukturerat arbete som går ut på att analysera och mäta både nya och gamla företeelser, planera åtgärder som sedan införs, och som i sin tur granskas och leder till nya förbättringar. Metodiken i PDCA är

[11] PDCA introducerades av den amerikanske statistikern William Edwards Deming, en förgrundsgestalt inom kvalitetstekniken.

alltså användbar när man börjar från noll men också när man redan har något som ska förbättras och anpassas till LIS.

Metodstödets tre första processteg förbereda, analysera och utforma motsvarar PDCA-cykelns första fas, *planera*. Den som redan har ett LIS på plats behöver förmodligen inte göra en fullständig verksamhetsanalys, men om man har nya informationstillgångar behöver de klassificeras. Det är viktigt att göra om eller komplettera riskanalyser med viss regelbundenhet och när omständigheterna förändras. Nya informationstillgångar behöver också gapanalyseras.

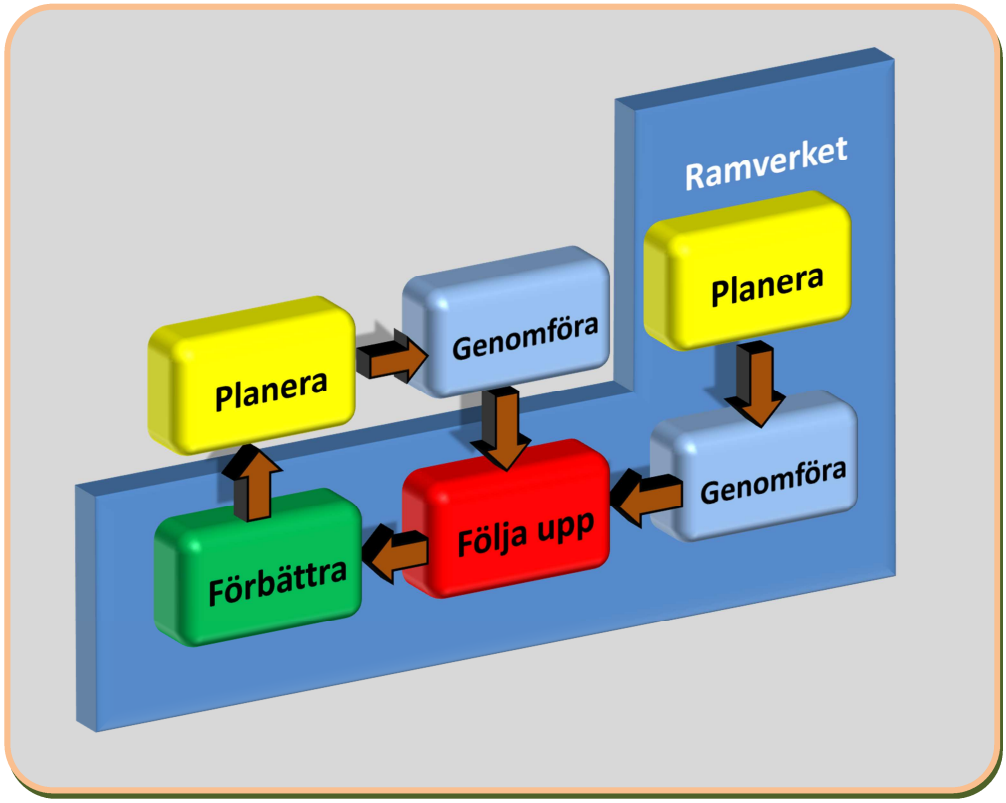
Metodstödets processteg införa motsvarar PDCA-cykelns andra fas, *genomföra*. Om ledningssystemet redan finns på plats innebär det här processteget att man genomför de förbättringar och inför de åtgärder som behövs enligt analyserna i planerafasen.

Metodstödets processteg följa upp motsvarar PDCA-cykelns tredje fas, *följa upp*. Detta steg är alltid lika aktuellt hur bra organisationens LIS än fungerar. Det är viktigt att ständigt fråga sig om de införda åtgärderna fungerar och om man använder arbetssätt och metoder som är funktionella och aktuella.

Metodstödets sista processteg förbättra motsvarar PDCA-cykelns fjärde fas, *förbättra*. Här genomförs de förbättringar som identifierades i processteget följa upp. Det som kräver ytterligare analys går in i planerafasen och så fortsätter cykeln.

Bilden i figur 2 visar att metodstödets processteg förbereda, analysera och utforma samt införa, det vill säga PDCA-cykelns planera och genomföra är infartsvägen till PDCA-cykeln som sedan snurrar vidare. Efter det första varvet innehåller planera och genomföra sedan de kompletterande analyser och klassificeringar som ständigt behövs, liksom arbetet med att införa nya och bättre åtgärder.

Figur 2. Stegen planera och genomföra ändrar karaktär efter PDCA-cykelns första varv.



5.2 Ständiga förbättringar

PDCA-metoden bygger på ständiga förbättringar i form av nya analyser, åtgärder och uppföljningar, och ser på så sätt till att säkerhetsåtgärderna alltid är anpassade till den rådande risksituationen och verksamheten.

Ständiga förbättringar har inget egenvärde i sig utan syftet är att göra förbättringar där det behövs och när det behövs. Sådana förbättringar kan handla om att stärka skyddet om det visar sig att risksituationen har ändrats. Förbättringarna kan även handla om att anpassa olika metoder så att de blir mer användarvänliga eller att ytterligare integrera LIS med andra styrmedel och verksamhetsprocesser.

6. Processtegen

Innan det går att börja arbetet med att införa ett LIS i en organisation måste ledningen besluta att det ska göras. Detta är den första beslutspunkten i processmodellen. Ledningens beslut bör grundas på kunskap om och förståelse för vad det innebär att införa ett LIS. Informationen i kapitel 2 om framgångsfaktorer går att använda för att ta fram ett beslutsunderlag.

I det följande beskrivs Metodstödets olika delar kortfattat. För ingående beskrivningar, se respektive metoddokument på www.informationssäkerhet.se.

Introduktion	
Ledningens engagemang	För att få ett fungerande LIS måste ledningen vara motiverad att avsätta resurser för arbetet. Alla inblandade måste också förstå att LIS-arbetet är en investering som på kort sikt innebär stora kostnader.
Projekt-planering	När ledningen beslutat att införa ett LIS måste projektet planeras. Resurser måste säkras och tidsplanen måste synkas med organisationens normala verksamhet.

Analysera	
Verksamhet	Det första steget är att identifiera verksamhetens informationstillgångar samt verksamhetens interna och externa krav på informationssäkerhet. Därefter klassificeras informationen, som tillsammans med riskanalysen definierar verksamhetens skyddsbehov.
Risk	Med kunskap om informationstillgångarna och verksamhetens krav gör man en riskanalys för att se vilka risker som kan påverka informationssäkerheten. Hotens sannolikhet och konsekvens bedöms av nyckelpersoner från verksamheten. Riskanalysen och verksamhetsanalysen definierar tillsammans verksamhetens skyddsbehov.
GAP	I gapanalysen jämförs verksamhetens existerande skydd med de säkerhetsåtgärder som föreslås i standarden 27001. Bedömningen görs för varje föreslagen åtgärd, med utgångspunkt i det skydds-behov som verksamhetsanalysen och riskanalysen visade.

Utforma	
Åtgärder	Med utgångspunkt i skyddsbehovet fastställs de mål och säkerhetsåtgärder som krävs för en balanserad informationssäkerhet. Grunden är åtgärderna i standarden (27002), vilka kompletteras vid behov.
Processer	I detta läge är det dags att utforma de processer för informationssäkerheten som krävs för att tillgodose de fastställda säkerhetsåtgärderna. Det kan till exempel gälla incidenthantering och behörighetsadministration.
Styrdokument	Policy och styrdokument för informationssäkerheten tas fram. Genom policyn anger ledningen sin inriktning för informationssäkerheten med tydliga mål, krav och ansvar. De andra styrdokumenten anger regler och rutiner för informationssäkerheten inom olika områden.

Införa	
Planera genomförande	Nästa steg är att ta fram en förbättringsplan som bygger på vad som måste göras för att omvandla verksamhetens informationssäkerhet från nuläget (se gapanalys) till det beslutade läget (se fastställda säkerhetsåtgärder).
Konstruera och anskaffa	Införandeplanen identifierar de olika insatser som krävs för att alla beslutade säkerhetsåtgärder ska följas av de relevanta medarbetarna och få praktisk nytta i verksamheten.
Inför	Planerna sätts i verket. Bland annat ska processer initieras, medarbetare ska utbildas och tekniska och administrativa säkerhetsåtgärder ska införas.

Följa upp	
Övervaka	Alla avvikelser från den beslutade informationssäkerhetsnivån identifieras genom de införda rutinerna för att rapportera incidenter, övervaka och logga. Avvikelserna åtgärdas och dokumenteras.
Granska	Detta moment går ut på att följa upp de säkerhetsåtgärder som specificeras av ledningssystemet, det vill säga de åtgärder och metoder som har valts ut och införts. Den interna granskningen fokuserar på om åtgärderna existerar och fungerar tillfredsställande.
Ledningens genomgång	Uppföljningens syfte är att informera verksamhetens ledning om vilka ytterligare åtgärder som ska genomföras och hur utformningen av skyddet ska ändras för att passa den förändrade situationen.

Förbättra	
Utveckla LIS och skyddet	Resultatet av uppföljningen används nu för att justera policyn och styrdokumenten. Skyddsbehovet kan ha förändrats på grund av nya omständigheter.
Kommunicera förbättringar	För att utveckla skyddet är det viktigt att kommunicera förbättringsåtgärder till alla relevanta parter i organisationen så att de är medvetna om de åtgärder och förändringar som görs.
Fortsatt arbete	Nu är ledningssystemet infört och funktionaliteten har verifierats under en längre tid. Ledningssystemet har blivit en integrerad del av verksamheten. Nu gäller det att fortsätta på samma sätt.

Bilaga A: Ledningssystem för informationssäkerhet

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 kallas för ett styrsystem eller en styrmodell eller ingenting alls, men det finns där.

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

För att en organisations ledningssystem ska fungera är det nödvändigt att samla in kritisk information från verksamheten, filtrera den och sedan presentera den på ett sätt som är begripligt för beslutsfattaren. På samma sätt måste övergripande policydokument från ledningen tolkas och införas på detaljnivå längre ner i verksamheten. Den som är ansvarig för en viss del av verksamheten måste tolka ledningens styrdokument och anpassa dem till sin del av verksamheten, och även dokumentera hur han eller hon väljer att göra detta för att på så sätt åstadkomma spårbarhet. En tumregel är att alla säkerhetslösningar på detaljnivå ska gå att härleda uppåt i beslutshierarkin. På samma sätt ska man kunna vandra nedåt i hierarkin för att se hur varje organisationsdel, ned till grupp och individ har valt att införa de övergripande styrningar som ledningen har gått ut med.

Ledningssystemet bygger 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.

LIS består av

- styrdokument för informationssäkerhet
- modeller och metoder för riskhantering och klassning
- system för incidenthantering och kontinuitetsplanering
- beslut om och åtgärder för att uppnå eller upprätthålla den beslutade säkerhetsnivån.

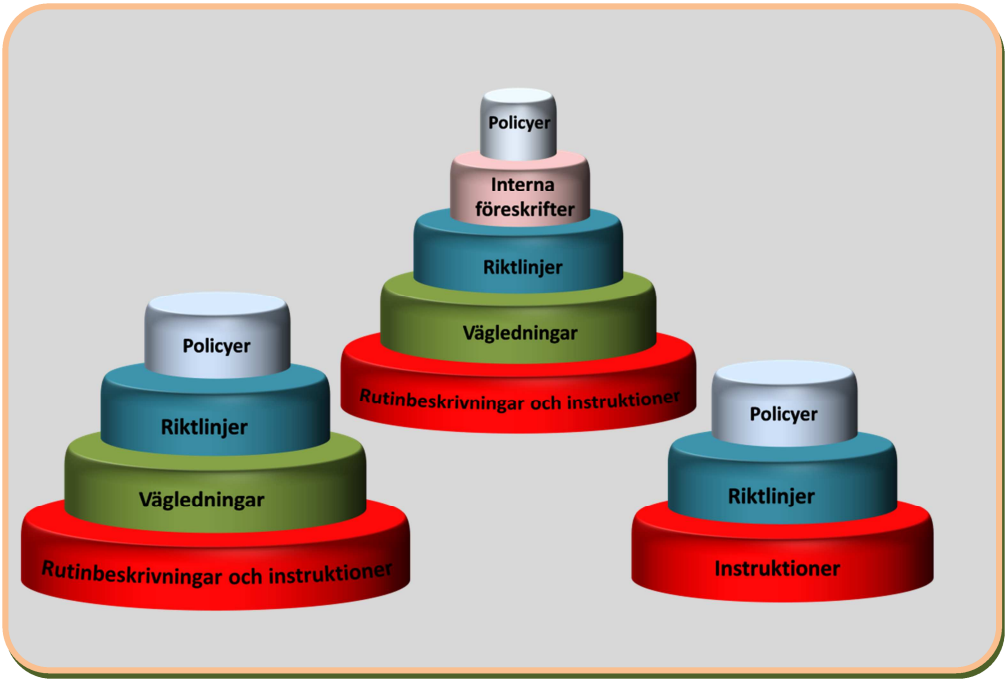
Förenklat kan man säga att LIS går ut på att hålla ordning i informationssäkerhetsarbetet, och det innefattar då också *hur* man håller ordning, det vill säga de metoder och arbetssätt som behövs. För att kunna arbeta så här strukturerat krävs dokumentation och att all dokumentation är spårbar.

Bilaga B: Styrdokument i ett ledningssystem

En viktig del av ledningssystemet är de interna styrdokument som reglerar informationssäkerhetsområdet. Dessa dokument bör följa den struktur som organisationen har för andra styrdokument. Det finns många olika benämningar på interna styrdokument, till exempel riktlinjer, anvisningar, allmänna råd, vägledningar, handböcker och instruktioner. Det viktiga är dock inte vad de kallas utan att benämningarna är konsekvent använda och att de olika dokumenttyperna följer en given hierarki så att läsaren känner igen sig och förstår vilken vikt de olika dokumenten har, eller vilken grad av styrning de anger, samt hur dokumenten förhåller sig till varandra. Styrdokumentshierarkin avspeglar graden av styrning, se bilaga D för exempel på hur olika dokumenttyper kan användas för att tydliggöra graden av styrning i varje dokument.

I en logisk och tydlig styrdokumentstruktur passar varje dokumenttyp in på en viss nivå i hierarkin. Antalet nivåer kan givetvis variera, se figur B1 för några olika tänkbara dokumenthierarkier.

Figur B1. Exempel på dokumenthierarkier



Dessa styrdokument kompletteras med, eller kompletterar, andra styrmedel som ekonomisk styrning och beslut i enskilda frågor. Gemensamt för alla policydokument, föreskrifter, riktlinjer och vägledningar är att de reglerar generella förhållanden som troligen inte förändras särskilt ofta. Det är dock viktigt att styrdokumenten hålls aktuella och de behöver därmed ses över med jämna mellanrum. När det gäller reglering av unika och mer tillfälliga förhållanden är det bättre med beslut i dessa enskilda frågor.

Samtliga styrdokument bör ha en tydlig ägare, och det bör också tydligt stå vem som ansvarar för att styrdokumentet hålls aktuellt och revideras vid behov. Styrdokument på lägre hierarkisk nivå behöver normalt sett revideras oftare än styrdokument på högre nivå.

Bilaga C: Dokument i standarden

Bilaga D i standarden för införande av LIS (27003) handlar om strukturen för policydokument. Där finns en svensk kommentar om att begreppet policy i internationella sammanhang används för fler typer av dokument än vad som är normalt i svenska språket. I svenska språket, och den rekommendation som ges i metodstödet är att policy används för ett övergripande dokument som anger ledningens viljeinriktning. Policydokument i standarden avser snarare alla typer av styrdokument, även av typen rutinbeskrivningar.

I 27001 och 27002 nämns policyer i flera olika sammanhang. På den högsta hierarkiska nivån finns en säkerhetspolicy och en informationssäkerhetspolicy, och enligt standarden 27001 bör det även finnas en policy för LIS. Därutöver finns policyer på en lägre hierarkisk nivå, till exempel en åtkomstpolicy och krypteringspolicy. I kapitel 15 i 27002, Efterlevnad, används ”säkerhets-policyer” som ett samlingsbegrepp för de interna regler som styr säkerhets-arbetet. En säkerhetspolicy och en informationssäkerhetspolicy är dokument på en övergripande nivå och behandlas i bilaga D. Den policy för LIS som nämns är i princip en beskrivning av ledningssystemet och därmed inte en policy enligt svenskt språkbruk. Åtkomstpolicy, krypteringspolicy och liknande är snarare rutinbeskrivningar enligt den exemplifierade styrdokuments-hierarkin i det här dokumentet.

Man kan säga att LIS-standarden förutsätter att det finns ett regelverk med styrdokument under nivån säkerhetspolicy och informationssäkerhetspolicy men över nivån åtkomstpolicy. Detta regelverk kallas alltså för ”säkerhets-policyer” i standarden, men det står inget om hur regelverket bör utformas.

Bilaga D: Beskrivning av styrdokumentshierarki

Avsikten med beskrivningen nedan är att belysa vad man bör tänka på när man skriver styrdokument. Det finns ofta behov av att reglera olika saker olika mycket. Detta görs enklast genom att ha olika typer av styrdokument med olika hög grad av styrning. Det kan också vara bra att ha särskilda dokumenttyper i vilka man ger stöd för hur styrdokumenten ska tolkas och användas.

Policyer. Med policy menas här ett styrdokument som uttrycker ledningens övergripande viljeinriktning. En policy innehåller normalt inga handlingsregler utan de finns främst i styrdokument av typen interna föreskrifter och riktlinjer. Policyn har trots detta en styrande effekt eftersom den anger att alla i organisationen ska ha ett enhetligt förhållningssätt eller agera enhetligt. Eftersom policyn uttrycker ledningens viljeinriktning är det naturligt att bara den högsta ledningen kan besluta om en sådan.

Ska-regler, till exempel kallade interna föreskrifter. En organisation kan välja att utfärda interna föreskrifter med bindande regler som därmed alltid ska följas. Det är viktigt att föreskriften bara innehåller de regler som verkligen behöver vara bindande. I de interna föreskrifterna är det viktigt att även peka ut vem som har ansvaret för att de olika reglerna följs. Interna föreskrifter kan gälla för hela organisationen och bör då beslutas av den högsta ledningen. De kan också gälla för en del av organisationen eller för en tydligt definierad typ av verksamhet och kan då beslutas av någon som har en hög befattning i denna del av verksamheten.

Bör-regler, till exempel kallade riktlinjer. En riktlinje innehåller handlingsregler som inte utesluter andra handlingssätt även om det är troligt att reglerna ska följas. Detta innebär att det inte finns några bindande regler i en riktlinje. Den ska inte heller innehålla något material av informationskaraktär, till exempel hänvisningar till andra regler, såvida det inte är nödvändigt för att förstå riktlinjen. Riktlinjer kan gälla för hela organisationen och bör då beslutas av en befattningshavare på tillräckligt hög nivå för att få rätt tyngd i organisationen. Andra riktlinjer gäller för bara en del av organisationen eller för en tydligt definierad typ av verksamhet, och de kan beslutas av någon som har en hög befattning i denna del av verksamheten.

Vägledningar. En vägledning kan redovisa praxis och de gällande reglerna samt ge exempel på bra arbetssätt. Den kan redogöra för reglerna inom ett visst område på ett så klart och enkelt sätt som möjligt. I en vägledning ska det bara finnas handlingsregler som också finns i styrdokument med ska- och bör-regler. Vägledningar kan även innehålla konkreta och handgripliga råd och rekommendationer, gärna med en förklaring till varför det är lämpligt att agera på ett visst sätt. Dessutom kan de innehålla mallar, exempelsamlingar med mera. Vägledningar kan beslutas av någon som har en lämplig befattning med tanke på vägledningens innehåll.

Rutinbeskrivningar. Inom informationssäkerhetsområdet finns det ofta behov av att i detalj reglera hur arbetet ska bedrivas. Det kan till exempel

handla om hur och när man ska göra säkerhetskopior eller hur man övervakar och hanterar händelseloggar. Denna hantering är ofta viktig för säkerheten och bör kontrolleras genom bindande regler. Ofta handlar det om detaljer som kan behöva ändras när man till exempel inför ny teknik, och sådant passar inte att reglera i interna föreskrifter. Det är dock viktigt att beslutsfattaren har fått mandat att ta fram sådana rutinbeskrivningar. Det kan finnas juridiska komplikationer med bindande beslut på denna nivå, och därför kan man behöva rådfråga någon med juridisk kompetens.

De styrande dokumentens relation till varandra

Under säkerhetspolicyn och/eller informationssäkerhetspolicyn kan det finnas en eller flera interna föreskrifter, riktlinjer och vägledningar. Typen av styrdokument beror på hur stark styrning som behövs på området och hur viktigt det är att tydliggöra handlingsreglerna. Inom ett område kan det alltså mycket väl finnas en riktlinje men ingen föreskrift. Ibland kan det vara nödvändigt att målgruppsanpassa vägledningar inom samma sakområde och därmed ha flera vägledningar som i sak behandlar samma verksamhet.