2003:23

STATSKONTORET

Ledningssystem för informationssäkerhet vid 24-timmarsmyndigheter

Vägledning och mallregelverk

Innehållsförteckning

Bilaga
Mallregelverket finns att ladda ner via
www.statskontoret.se/pdf/2003117.pdf

Acess-databasen finns tillgänglig via
www.statskontoret.se/publi/200323/offlismallregelverkver1.zipT

1 Bakgrund

Säkerhetsfrågor med inriktning på information och databehandling har på olika sätt uppmärksammats under de senaste 30 åren. En snabb teknisk utveckling har i hög grad bidragit. Inom näringslivet har fokus flyttats från driftsäkerhet till ett mera heltäckande synsätt på att skydda information som en kritisk resurs för affärsverksamheten. Inom den offentliga verksamheten var frågor kring personlig integritet något som tidigt debatterades. Integritetsfrågan har i viss mån hamnat i skymundan när behoven av säkerhetslösningar för att kunna utnyttja IT för att effektivisera och tillhandahålla servicetjänster dominerar. Likaså är kraven på offentlighet och sekretess en komplicerande faktor. Att både skapa öppenhet och skydd för egna resurser är en svår balansakt.

Informationssäkerhet är allomfattande och inbegriper verkligen alla delar i de flesta verksamheter. Detta ger behov av att behandla frågan både utifrån ett helhetsperspektiv och på en mycket konkret och jordnära nivå. Informationssäkerhet på en övergripande nivå uppfattas ofta som mycket abstrakt, svårfångat och inte minst tekniskt. Det bidrar ofta till att verksamhetsledningar gärna överlåter dessa frågor till andra funktionärer. Vilket i sin tur tyvärr ofta bidrar till bilden av att ledningsstöd saknas för informationssäkerhet. Informationssäkerhet på mera konkret nivå är däremot något som de flesta kommer i kontakt med och kan ha synpunkter på. På gott och på ont. På gott därför att ett personligt engagemang när det gäller säkerhet är avgörande för att skapa säkerhet. På ont därför att det är lätt att sätta säkerheten ur spel genom ett ständigt ifrågasättande som kan ha sin grund i bristande kunskap om helheten. Detta kan i sin tur naturligtvis härledas ur ett bristfälligt säkerhetsarbete.

Att arbeta med något som är så allomfattande kräver struktur och styrning. Säkerhet är inte det enda området där detta är tydligt. Kvalitetsfrågor är ett annat område som präglas av precis samma synsätt. Ett förhållande som inom i första hand näringslivet, också tidigt bidragit till utformning och tillämpning av standardiserade arbetssätt, exempelvis genom ISO-9000-standarderna.

Statskontoret har genom handböcker och rapporter av olika karaktär bidragit till offentliga förvaltningars arbete med informationssäkerhet. Både vad gäller styrning och mera process- och teknikinriktat arbete. När det nu finns en svensk och internationell standard för utformning av ledningssystem för informationssäkerhet, SS-ISO/IEC 17799 respektive SS 62 77 99-2, populärt kallad LIS, är det naturligt att bidra till spridning av användningen av denna standard. Statskontoret deltar också i detta arbete tillsammans med SIS, Swedish Institute for Standardisation. Ett primärt motiv för Statskontorets engagemang i dessa frågor är utvecklingen av ”24-timmarsmyndighe-

ten". En ansats som bygger på effektiv och säker användning av IT med Internettjänster som den allra tydligaste framgångsfaktorn. Strategin att förbättra samhällets service mot medborgarna bl.a. genom ökad interaktion mellan myndigheter. Detta skapar också behov av samordnade synsätt och teknikarkitektur etc. Det gäller också säkerhetsområdet. Samsyn när det gäller informationssäkerhetsprocesser, sekretessfrågor etc. är avgörande för att etablera och vidmakthålla allmänhetens förtroende för e-tjänster och därmed också säkra investeringarna i dessa tjänster.

Att etablera och genomföra ett säkerhetsarbete med den omfattning som LIS beskriver uppfattas av många som ett stort och omöjligt uppdrag. En uppfattning som dessvärre i hög grad beror på okunskap och bristande erfarenhet.

LIS innehåller inga kontroversiella eller speciellt avancerade krav utan är helt enkelt ett strukturerat sätt att bedriva normalt informationssäkerhetsarbete på.

Denna handbok har ambitionen att förenkla och avdramatisera arbetet med informationssäkerhet enligt standarden och tillhandahålla nödvändiga grunder i form av malldokument och metodstöd.

Skriften har utformats i samarbete mellan informationssäkerhets- och IT-säkerhetsexperter inom den offentliga sektorn med nätverket "SNITS", som koordineras av Statskontoret, som primär resurs. Arbetet har bedrivits inom ramen för Statskontorets projekt, INSYN. Även om samtliga medverkande idag är verksamma inom statsförvaltning och offentlig verksamhet finns också erfarenhet från informationssäkerhetsarbete i näringslivet.

Arbetsgrupp INSYN:	Wiggo Öberg, Statskontoret, projektledare
	Göran Ranlöf, Luftfartsverket
	Per Backlund, Banverket
	Bertil Regardt, RSV
	Göran Enerstål, FMV
	Lennart Castenhag, Svenska Kraftnät
	Valter Lindström, Landstinget Västra Götaland
	Göran Ribbegård, Statskontoret
	Björn Scharin, Statskontoret

Denna vägledning vänder sig i första hand till personal som har uppgifter inom informationssäkerhetsarbete vilket kan innefatta informationssäkerhetschefer, informationssäkerhetsansvariga och övrig personal med motsvarande inriktning.

2 Inledning och motiv

En vanlig fördom när det gäller säkerhetsarbete är att säkerhetsexperter och andra företrädare för sakområdet driver på utvecklingen i något slags egenintresse. Gärna genom skrämselpropaganda och påståenden om svagheter och risker som får stå oemotsagda. Självfallet kan ett dåligt genomfört säkerhetsarbete ta sig sådana uttryck. Ser man till den faktiska utvecklingen för ADB-säkerhet eller som man idag oftare kallar det, Informations- och IT-säkerhet, visar det sig att utvecklingen ändå i stor utsträckning följer verksamhetsbehoven snarare än att vara för överdrivet hög. När incidenter inträffar upplever man i många fall att säkerhetsfrågorna hamnat på efterkälken. Händelser med allvarliga konsekvenser inträffar ofta på grund av att säkerhetsåtgärderna är otillräckliga. Kanske har säkerhetsfolket inte lyckats övertyga verksamhetsledningarna om vikten av förebyggande säkerhetsåtgärder genom etablerade modeller för beslutsstöd.

Säkerhetsarbetet måste ske förebyggande, på lång sikt och för att vara effektivt och heltäckande, genomföras väl strukturerat och med tydligt stöd från verksamhetsledningen. Förankringen och medvetandet hos medarbetarna utgör själva grunden i säkerhetsarbetet. Informationssäkerhetsområdet handlar om sekretess, skydd mot obehörig åtkomst av information, tillgänglighet, åtgärder för att säkra drift och funktionalitet samt riktighet, åtgärder för att åstadkomma rätt kvalitet på information. Säkerhet åstadkommes genom många samverkande faktorer, inte en genialisk teknikkomponent eller en enstaka säkerhetsåtgärd.

Men det handlar många gånger också om nya synsätt. Inom produktionsindustrin har det länge varit naturligt att se ”produktionsapparaten” och produktionsprocessen som något mycket väsentligt för att bedriva verksamheten. Inom administrativa verksamheter, t.ex. myndigheter, där det mesta arbetet utgörs av utformning av dokument av olika slag vilket av tradition skett manuellt och med hjälp av teknik i mindre grad, har det inte varit lika enkelt att åstadkomma motsvarande synsätt på IT-stödet som den väsentliga produktionsapparat som det faktiskt är. Detta har också i många fall resulterat i bristande styrning av IT-resurser, systemutveckling och inte minst säkerhet.

Idag är IT i dess olika former var mans egendom. Alla har i princip tillgång till världsomspännande strukturer av datanät för kommunikation och tjänster genom Internet. Därmed har också säkerhetsfrågorna blivit avgörande för möjligheten att dra nytta av tekniken. De allra flesta kan säkert skriva under på att IT är en komplex teknik. Det är svårt att överblicka och utvärdera hur olika delar påverkar varandra. Användning av IT och inte minst Internet innebär också nya hot och risker kopplat till den extrema ”internationaliseringen” som tekniken innebär. En person på Filipinerna kan sprida ett data-

virus som påverkar hela världens Internettjänster och en ”hackare” i Småland kan göra intrång i Pentagons datorer. Informationssäkerhetsområdet är både på grund av teknikens möjligheter och teknikens komplexitet och risker hetare än någonsin. Bara om säkerhetsfrågorna kan hanteras på ett vettigt sätt och bara om bra säkerhetslösningar kan etableras blir investeringarna i IT lönsamma.

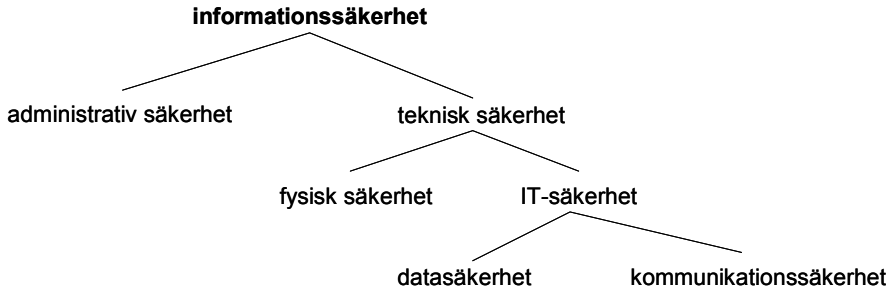
I allt större utsträckning ses säkerhet som en möjliggörare och inte som ett hinder för användning av ny teknik. Därmed finns också en acceptans för att kostnaderna för säkerhet är en given del av investerings- och driftskostnader.

2.1 Informationssäkerhet – något om teori och begrepp.

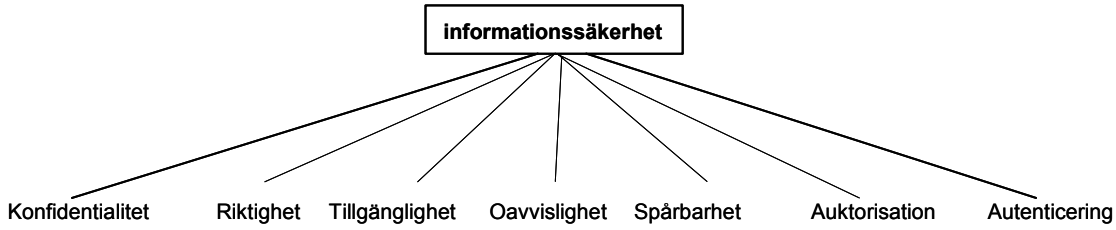
Begreppen ”informationssäkerhet” och ”IT-säkerhet” används ofta lite slarvigt. Talar vi om säkerhet för information i generella termer använder vi begreppet ”informationssäkerhet”. I detta ingår förutom säkerhet vid informationsbehandling med hjälp av IT även säkerhetsfrågor inriktade på ren dokumenthantering, arkivering, att tänka på vad som diskuteras i offentliga miljöer m.m. Begreppet innefattar också ”IT-säkerhet” med vilket vi avser säkerhet för information när den behandlas med hjälp av IT. D.v.s. den mera tekniskt inriktade säkerheten ofta relaterad till tekniska skyddsåtgärder av allehanda slag. Ofta används dock begreppet IT-säkerhet mer eller mindre synonymt med begreppet informationssäkerhet och omfattar då också administrativa skyddsåtgärder och rutiner som är tydligt kopplade till drift och användning av IT.

2.1.1 Grundläggande begrepp

Begreppet informationssäkerhet kan beskrivas på flera olika sätt, beroende på ändamål. En vanlig uppdelning enligt figuren nedan ingår i SIS Handbok 550, Terminologi för Informationssäkerhet, där man utgår från skyddsåtgärdernas miljö, teknisk respektive administrativ etc.



En annan uppdelning kan göras utifrån infologiska skyddsmål enligt den välbekanta amerikanska bokstavsserien C-I-A (*confidentiality-integrity-availability*), ibland kompletterad med ett eller flera andra begrepp, t.ex. *accountability, authentication, authorazation, assurance, audit och non repudiation*. En vanlig uppdelning kan vara följande.



2.2 Standardisering ett sätt att konkretisera, styra och kvalitetssäkra.

Byggnader, vägar och broar konstrueras med ett stort mått av säkerhetstänkande som en av de allra viktigaste förutsättningarna. En självklarhet tycker vi, att hus byggs så att de inte utgör en fara för dem som bebor eller vistas i dem, att vägarna medger den trafik de är avsedda för utan att innebära ökade risker för trafikanterna, att broar inte faller samman vid normal användning etc. Normerna för dessa konstruktioner är så väl förankrade att vi känner oss mycket trygga när vi använder dem.

Att vi nått den nivån av tillit har i stor utsträckning sin grund i lång tradition av att utnyttja beslutade standarder för byggnation och kontroll av att dessa följs.

På samma sätt tillämpas väl utvecklade normer i form av ISO-standarder för kvalitet, både inom offentlig sektor och näringslivet som en naturlig och självklar komponent för att nå och vidmakthålla nödvändig konkurrenskraft. I många fall certifieras verksamheter som ser ett värde i att inför omvärlden verifiera att man tar kvalitetsaspekterna på allvar och är en trovärdig part, leverantör etc.

I ett samhälle där användning av IT är en del av infrastrukturen för medborgarnas kontakter med offentliga organ borde det vara lika viktigt att utveckling och användning av tjänster med hjälp av IT har en motsvarighet när det gäller normer för säkerhet.

Den svenska och internationella standarden SS-ISO/IEC 17799 ”Ledningssystem för informationssäkerhet” från 1999 har sitt ursprung i den brittiska standarden BS 7799 som i sin första version utkom 1995. Standarden står för ett affärsmässigt synsätt för att styra informationssäkerheten i en verk-

samhet. Begreppet informationssäkerhet har sin grund i att information betraktas som en tillgång som, liksom andra viktiga tillgångar i en organisation, har ett värde och följaktligen måste få ett lämpligt skydd med utgångspunkt från verksamhetskraven.

Information om standarden kan man få hos SIS. Genom projektet TK318 bedriver SIS ett omfattande arbete för att sprida och underlätta tillämpningen av standarden.

2.3 24-timmarsmyndigheten – kräver bra informationssäkerhet för att få allmänhetens förtroende

24-timmarsmyndigheten som idé innebär bl.a. att myndigheter med serviceskyldigheter mot allmänheten eller näringslivet skall tillhandahålla tjänster över Internet. Detta innebär också att personliga integritetskänsliga uppgifter skall kunna hanteras inom ramen för Internettjänsterna. Dokument med rättsverkan skall kunna undertecknas med elektroniska underskrifter och myndigheterna skall inhämta information från andra myndigheter och organisationer av betydelse för effektivisering av tjänsteutövningen. Självfallet kommer medborgarna att ta för givet att detta sker med tillräcklig säkerhet. Det kommer att anses som oacceptabelt att privat information om en individ är tillgänglig för obehöriga, att tjänsterna inte är tillgängliga när de behövs och att tvivel finns huruvida information och resultat är korrekta. Samverkan mellan myndigheter och andra offentliga organisationer kommer att vara en väsentlig del av infrastrukturen. Det är då rimligt att det finns en djupt gående samsyn när det gäller informationssäkerhet. Om en part behandlar en informationsmängd som hemlig och en annan part hanterar den som helt öppen information är det lätt att inse att det kan medföra skador för de inblandade. Ett förtroende som fläckas i dessa avseenden kommer kraftigt att motverka den effektivisering som 24-timmarsmyndighetens förväntas ge. Kanske vänds givna succéer till kostsamma fiaskon.

Fundamentet är gemensamma normer och synsätt. Genom det bygger vi förtroende!

Säkerhet för privatpersoner och andra aktörer på Internet skapas i hög grad genom god identifiering av både individer som utnyttjar tillgängliga tjänster och organisationer som tillhandahåller dessa eller utbyter information sinsemellan. Ramavtal har tecknats om tjänster för identifiering av privatpersoner och offentliganställda i sin tjänsteutövning. Möjligheten att utnyttja dessa tjänster ger möjlighet till korrekt identifiering och tillämpning av elektronisk signering över Internet.

SHS (Spridning och Hämtnings System) är ett av Statskontoret upphandlat konceptet som bidrar med att skapa säkerhet och funktionalitet vid datakommunikation mellan myndigheter och andra parter.

Befintlig lagstiftning med inriktning på personlig integritet, offentlighet och sekretess, säkerhetsskydd och elektroniska underskrifter täcker naturligtvis stora delar av informationssäkerhetsområdet.

För att effektivisera handläggning och i högre grad kunna möta medborgarnas krav på ökad tillgänglighet ökar också kraven på elektronisk ärendehantering internt inom myndigheterna. Det innebär att metoder, verktyg och rutiner måste finnas för att på elektronisk väg kunna signera, verifiera, hantera och distribuera handlingar säkert.

Men! Säkerhetsteknik och lagar räcker inte för att åstadkomma och vidmakthålla nödvändig säkerhet för statsförvaltningens informationsbehandling relaterat till "24-timmarsmyndigheten".

Säkerhet måste byggas inom varje organisation genom väl utformade policies och regler för informationssäkerhet. Regelverk som omfattar hela informationssäkerhetsområdet och anger ramar för och inriktning för ett långsiktigt och förebyggande säkerhetsarbete. Även inkluderande regler för samverkan med andra, leverantörer och samverkanspartner.

Bara genom att bedriva ett heltäckande och effektivt säkerhetsarbete som omfattar hela verksamheten skapas nödvändigt förtroende för organisationernas IT-behandling och informationssäkerhet. Informationssäkerhet handlar om ett kontinuerligt arbete snarare än stora projekt som startas upp med pompa och ståt. Och som alltför ofta tappar luften efter alltför kort tid.

Att tillämpa SS-ISO/IEC 17799 som utgångspunkt för detta ger goda möjligheter. Standardens syfte och omfattning ger nödvändig struktur för ett väl genomfört IT-säkerhetsarbete som förutsättning för en nödvändig säkerhetsnivå.

Denna handbok över tillämpning av LIS bygger på att någorlunda enkelt åstadkomma grundläggande motiv och riktlinjer för ett kontinuerligt informationssäkerhetsarbete. Det vill säga beskrivning av informationssäkerhetsarbetet ingående processer och övergripande säkerhetskrav.

3 Informationssäkerhet enligt svensk standard (LIS) – syfte och principer

Den svenska standarden kallas oftast i dagligt tal för ”LIS” vilket är en något missvisande benämning. LIS är en förkortning av Ledningssystem för Informationssäkerhet. Standarden är en anvisning för hur man åstadkommer ett sådant, inte ledningssystemet i sig.

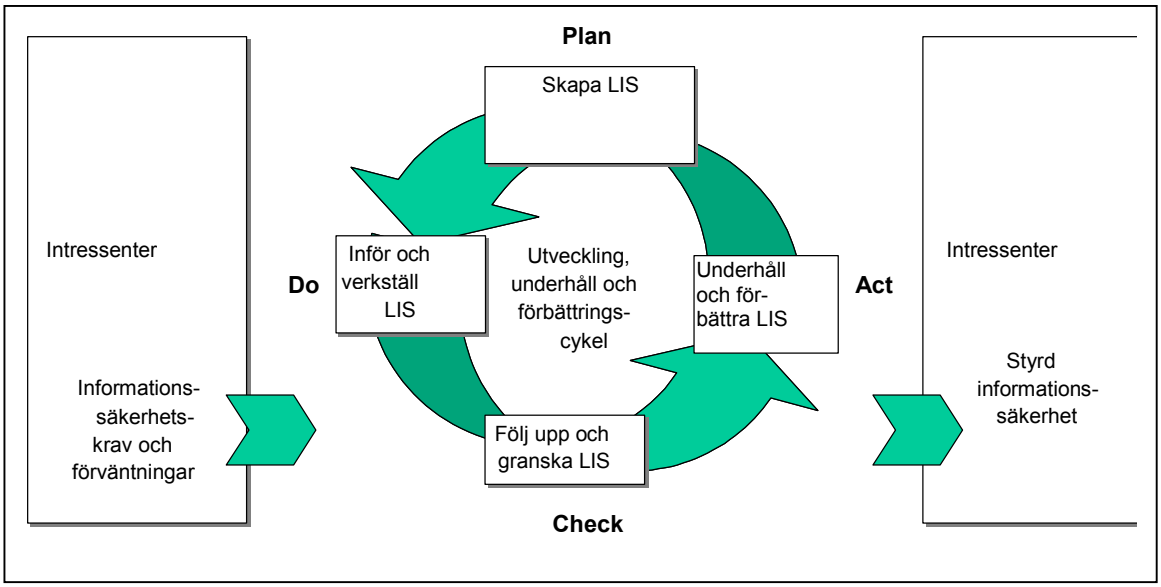
Ett sätt att beskriva vad ett ledningssystem för informationssäkerhet (LIS) omfattar, är följande:

- Dokumenterad informationssäkerhetspolicy på en övergripande nivå med verksamhetskraven som utgångspunkt som beskriver ledningens viljeinriktning.
- Riktlinjer för informationssäkerhet som pekar ut ansvar, säkerhetsprocesser och mål.
- Anvisningar och regler på lämpliga nivåer som anger hur och vilka säkerhetsåtgärder som skall vidtas.
- Definierad modell för riskanalys och riskhantering.
- Definierad modell för uppföljning och förbättring av säkerheten.
- Införda säkerhetsåtgärder och rutiner för riskhantering och uppföljning.
- Personal som är medveten om och följer gällande regler.

Viktiga utgångspunkter är att LIS utgår ifrån verksamhetens behov av skydd baserat på genomförda riskanalyser. Vidare att hänsyn tas till intressenters behov och att verksamhetens ledning tar ett tydligt ansvar för informationssäkerheten.

En förutsättning för ett väl fungerande LIS är att det inte blir ett regelverk ”vid sidan om” utan integreras med verksamhetens processer och arbetssätt.

Arbetet med LIS beskrivs i standarden som en s k PDCA-cykel enligt nedan.



De olika delarna omfattar:

Plan (skapa och förvalta LIS)	Fastställ säkerhetspolicy, syfte, mål, processer och rutiner som är relevanta för riskhantering och förbättring av informationssäkerhet i enlighet med organisationens övergripande policy och mål.
Do (inför & verkställ LIS)	Inför och verkställ säkerhetspolicy, kontroller, processer och rutiner.
Check (övervaka & granska LIS)	Fastställ och, där så är tillämpbart, mät processens prestanda mot säkerhetspolicy, mål och praktisk erfarenhet och rapportera resultaten till ledningen för granskning.
Act (underhålla och förbättra LIS)	Vidta korrigerande och förebyggande åtgärder baserade på resultatet av ledningens granskning, för att uppnå ständig förbättring av LIS.

Standarden består av två delar där den första delen utgörs av anvisningar och ”bör”-krav och den andra delen utgörs av målformuleringar och ”skall”-krav för att bli certifierad mot standarden. Standarden är strukturerad enligt följande områden, där 3 – 12 är obligatoriska:

1 Omfattning
2 Termer och definitioner
3 Säkerhetspolicy
4 Organisatorisk säkerhet
5 Klassificering och styrning av tillgångar
6 Personal och säkerhet
7 Fysisk och miljörelaterad säkerhet
8 Styrning av kommunikation och drift
9 Styrning av åtkomst
10 Systemutveckling och systemunderhåll
11 Kontinuitetsplanering för verksamheten
12 Efterlevnad

Standarden är samordnad med ISO 9001:2000 och ISO 14001:1996 i syfte att stödja införande och genomförande som är enhetligt och integrerat med relaterade ledningssystemstandarder.

Fördelar med ett LIS:

- Ger en bra och beprövad struktur för kontinuerligt säkerhetsarbete.
- Ger förutsättningar för önskad skyddsnivå.
- Beslutsmodell som bygger på verksamhetssituationen.
- Tydlighet mot anställda.
- Skapar trovärdighet i omvärlden.
- Skapar möjlighet till informations- och processamband med omvärlden.
- Ger möjlighet till uppföljning av rådande säkerhetsnivå.

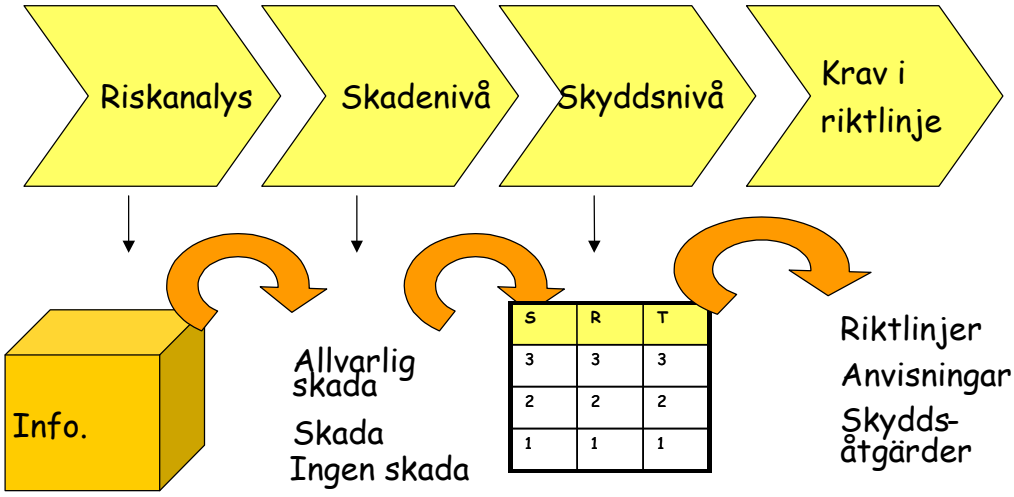
3.1 Säkerhetsprocessen som helhet

Ett ledningssystem för informationssäkerhet är en grundläggande framgångsfaktor för det kontinuerliga säkerhetsarbete som ska bedrivas i en verksamhet där informationsbehandling är en viktig del. Regelverket som utgör stommen i systemet ställer krav på hur verksamheten ska skydda sin information och andra värdefulla tillgångar.

Riskhantering är processen som styr att tillgångarna får rätt nivå på skyddet och att risker kontinuerligt bedöms och tas om hand. En viktig del av ledningssystemet är därför att skapa en process för kontinuerlig riskhantering. Incidenthantering och kontinuitetsplanering är två andra processer som måste etableras för att kontinuerligt kunna ta omhand incidenter och säkerställa verksamhetens kontinuitet och informationstillgångarnas säkerhet.

En viktig komponent i processen att uppnå en god säkerhet är informationsklassificering. Värdet på informationen är utgångspunkt för vilket skydd som krävs. Att hitta en gemensam modell för att klassificera information i ett givet antal klasser ger förutsättningar för ett väl utformat skydd och ett enhetligt sätt att hantera informationen på inom en verksamhet och vid utbyte av information med andra organisationer.

Bilden nedan visar på den grundläggande säkerhetsprocessen där riskanalys utgör basen utifrån vilken man kan bedöma skadenivå för informationen. Därefter definieras korrekt skyddsnivå och rätt krav kan identifieras i verksamhetens regelverk.



Med utgångspunkt från den aktuella skyddsnivån, hotbilder, riskbedömning och regelverkets krav vidtas skyddsåtgärder. Först då kommer informationen att erhålla sin faktiska skyddsnivå.

3.2 Riskhantering

Att skapa en process för riskhantering är en förutsättning för att hålla sitt ledningssystem uppdaterat och skyddet på rätt nivå. Genom att inkludera riskanalys som en del i projekt, systemutvecklings- och förändringsprocesser ges ett naturligt sätt att arbeta aktivt med riskhantering.

En metod för riskanalys ska fastställas som är lämplig med hänsyn till LIS och den för verksamheten identifierade informationssäkerheten samt de legala och författningsreglerade kraven.

Riskanalysen har till syfte att på ett systematiskt sätt granska och identifiera risker i en verksamhet. Vad som är viktigt vid en riskanalys är att kunna

värdera konsekvenserna och vilka följder dessa kommer att få för verksamheten. Av denna anledning är det inte själva metoden för riskanalys som är det viktigaste utan verksamhetskunnandet hos de som deltar i analysarbetet. Riskanalysen ska alltid utgå ifrån informationstillgångarna i verksamheten, då det är den som innehåller ett värde, både ekonomiskt och ur andra hänseenden, vilket medför att det är den som ska ges ett anpassat skydd.

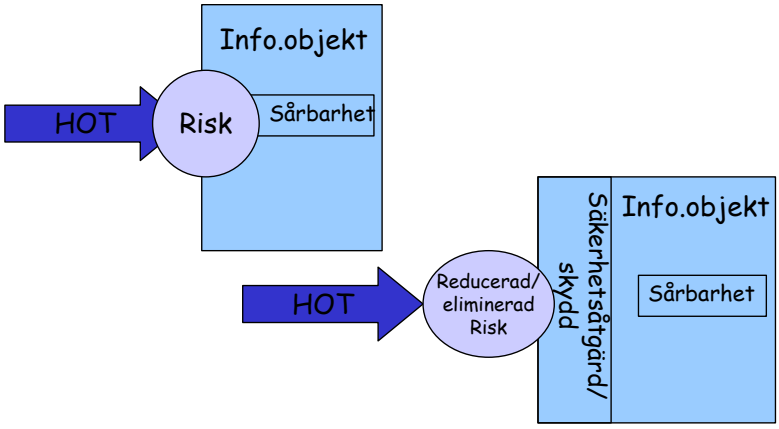
Informationstillgångar kan utsättas för olika typer av hot. Ett hot är en oönskad handling eller händelse som antas kunna riktas mot aktuella informationstillgångar i framtiden. Att något är oönskat innebär att man antar att sekretessen, riktigheten eller tillgängligheten hos de aktuella informationsresurserna kan försämras.

Informationstillgångar som ska analyseras kan vara allt ifrån en verksamhet eller process till ett eller flera system eller en specifik informationsmängd, ett register eller en databas.

Det finns ett antal grundläggande moment som bör utföras i en riskanalys. De är:

1. Identifiera tillgångar som ingår i analysobjektet och dess ägare.
2. Identifiera hot och risker.
3. Bedöm konsekvenserna av hot och risker som därmed anger sårbarheten hos de aktuella tillgångarna.
4. Värdera riskerna och den skada konsekvenserna kan medföra för verksamheten.
5. Bedöm sannolikheten för att identifierade hot skall bli verklighet.
6. Avgör om risken överstiger den acceptabla nivån och därmed måste tas om hand.

Efter att dessa grundläggande moment utförts är det sedan möjligt att definiera vilka styrmedel och åtgärder som ska användas.



Analysresultatet bör sedan presenteras på ett enkelt och överskådligt sätt, gärna grafiskt.

En riskanalys bör konkret resultera i följande:

- En kartläggning av brister och hotbild.
- En strukturerad spegling av verksamhetens nuläge.
- Konsekvensbedömning av inträffat hot.
- Sannolikhet för inträffat hot.
- Kartläggning av vilken information som är känslig, och ur vilka hänseenden, exempelvis tillgänglighet.
- Beslutsunderlag för realisering av säkerhetsfunktioner.
- Beslutsunderlag för prioritering av åtgärder.
- En plattform för att vidareutveckla policy och regelverk .

En positiv följdverkan av att kontinuerligt genomföra riskanalyser är att nyckelpersoner i verksamheten involveras i en mycket viktig analysprocess och säkerhetsmedvetandet hos dessa stärks. Nya kontakter inom den egna organisationen knyts med fokus på en säkring av den egna verksamheten.

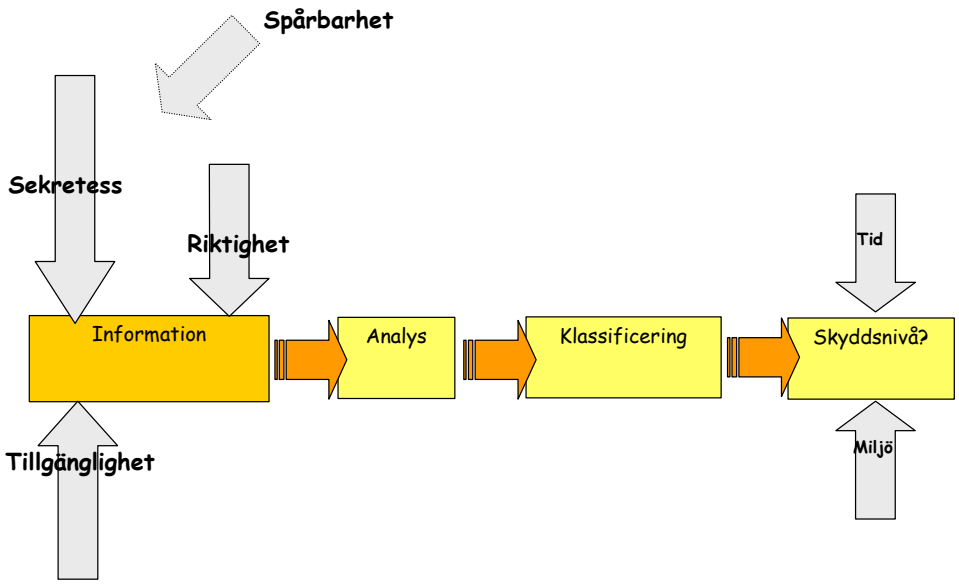
3.3 Klassificering

En viktig komponent i det kontinuerliga säkerhetsarbetet är att klassificera och ha kontroll på sina informationstillgångar. Det ska finnas en förteckning över vilka tillgångar som är förknippade med informationssystem. Förteckningen ska uppdateras kontinuerligt.

Syftet med att klassificera informationstillgångarna är att säkerställa att de ges ett tillräckligt skydd. Att klassificera information är en grundläggande

aktivitet för att särskilja den information som på ett eller annat sätt ställer högre krav på säkerhet. Förutom legala krav på skydd av personrelaterad information ska verksamhetens krav på informationen avseende sekretess, riktighet och tillgänglighet, avgöra formerna för det skydd som skall åstadkommas. Som grund för denna typ av bedömning ska riskanalyser genomföras. När det gäller klassificering avseende Sekretess skall detta inte ses som sekretessklassning eftersom detta i offentlig förvaltning måste göras vid ett eventuellt utlämnande av informationen. Klassificeringen med avseende på Sekretess har inget annat syfte än att bedöma behovet av skyddsnivå. Det är viktigt att påpeka att klassificering av informationstillgångar måste omprövas regelbundet som ett naturligt inslag i den kontinuerliga säkerhetsprocessen.

Bilden nedan illustrerar hur klassificeringsprocessen för en informationsmängd som ska tillföras någon typ av skydd kan se ut. Informationens känslighet påverkas av parametrarna sekretess, riktighet och tillgänglighet. Spårbarhet är en bedömningsfaktor som påverkar framförallt sekretess och riktighet. Höjden på pilarna visar ett exempel på vilken grad av påverkan respektive parameter utgör på informationen. Informationen analyseras och klassificeras beroende på denna påverkan. Därefter erhåller den en lämplig skyddsnivå. Tid och miljö är ytterligare parametrar som kan påverka skyddsnivån på informationen.



Exempel på frågor som kan vara bra att ställa vid bedömning av informationens känslighet:

- Vad blir konsekvensen om förväntade indata från andra interna system inte finns tillgängliga?
- Vad blir konsekvensen om systemet inte finns tillgängligt vid en kritisk tidpunkt?
- Vad blir konsekvensen om det inte går att följa upp vem som har haft tillgång till systemet och vid vilken tid?
- Vad blir konsekvensen om en obehörig får åtkomst till informationen?

Denna bedömning är sedan utgångspunkt när det gäller att placera in informationen i en skyddsnivå och skapa åtgärder för att skydda informationen.

Det är viktigt att fastställa ansvar för klassificeringsarbetet, till exempel genom följande ställningstaganden:

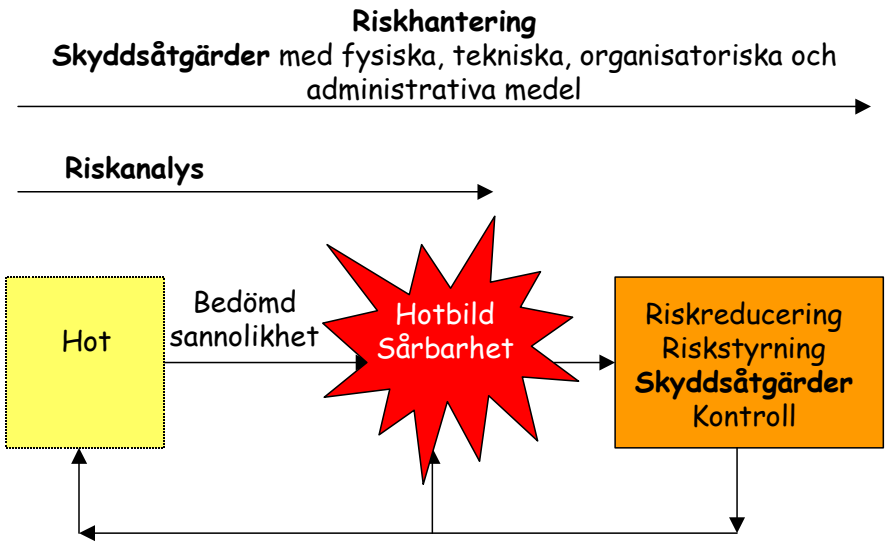
- Systemägaren ansvarar för klassning av den totala mängden information inom sitt IT-system och att skyddet motsvarar de krav som ställs.
- Varje person som upprättar, bearbetar, lagrar eller distribuerar informationen ansvarar för att följa den klassningsmodell som ska användas i verksamheten.
- I nyutvecklingsprojekt ska informationsklassificering ingå som en naturlig del i projektarbetet. Projektledaren har det yttersta ansvaret att se till att den genomförs på ett så tidigt stadium som möjligt.

Det är en väsentlig fördel om klassificeringen, utförs på ett enkelt sätt. Om din organisation har kontakt med andra organisationer, så kan det vara en fördel om ni har samma sätt att klassificera.

3.4 Skyddsåtgärder

Riskanalysen visar på de hot som finns mot verksamheten, liksom vilka brister som finns i säkerheten. Utifrån dessa skall lämpliga skyddsåtgärder tas fram för att motverka bristerna och hoten. En åtgärdsplan bör tas fram där åtgärderna fastställs, tidplan för genomförande samt vem som är ansvarig för genomförandet. Planen bör även beskriva hur uppföljning av arbetet skall ske samt kostnader för eventuella investeringar.

Bilden nedan beskriver processen för riskhantering och illustrerar hur risker mot information kan reduceras/elimineras med hjälp av skyddsåtgärder.



Skyddsåtgärder kan vara av administrativ art såsom riktlinjer, anvisningar och rutiner, se mallregelverket. Där uttrycks kravbilden som sedan ska uppfyllas med hjälp av åtgärder av teknisk, fysisk och organisatoriska karaktär.

Exempel på skyddsåtgärder av teknisk karaktär:

- Behörighetskontrollsystem.
- Stark autentisering.
- IDS.
- Brandväggar.
- VPN-krypto.

Exempel på åtgärder av fysisk karaktär:

- Inpasseringssystem.
- Larm.
- UPS (batteristöd för avbrottsfri drift).
- Ritningar och andra handlingar som pekar ut var känsliga utrymmen finns ska inte vara allmänt tillgängliga.

Exempel på åtgärder av organisatorisk karaktär:

- Utbildning.
- Definition och delegering av ansvar, roller och befogenheter avseende informationssäkerhet.
- Erfarenhetsutbyte med andra organisationer.

Exempel på åtgärder av administrativ karaktär:

- Behörighetsadministration.
- Incidentberedskap.
- Krisledningsrutiner.
- Rutiner för logguppföljning.

Några av de viktigare skyddsåtgärderna är att införa processer för incidenthantering och kontinuitetsplanering. En kontinuitetsplan säkerställer att extraordinära resurser kan avsättas i det fall en oönskad händelse inträffar som bedöms som katastrofal. Berörd personal ska utbildas på planen och den ska övas och utvärderas regelbundet.

Rutiner ska finnas för att dela in olika typer av händelser och incidenter i klasser, samt för att hantera samtliga klasser. Det ska också finnas rutiner och definierat ansvar för att återställa efter en incident.

3.5 Utbildning/information

Den mest kritiska framgångsfaktorn för ett lyckat informationssäkerhetsarbete är att det är känt och förankrat hos all personal i verksamheten. Det är också viktigt att var och en känner till målen med LIS och det kontinuerliga säkerhetsarbetet och på så sätt kan bidra till att de uppnås.

För att öka medvetandet hos alla medarbetare när det gäller LIS och informationssäkerhetsarbetet kan en informations- och utbildningsplan upprättas redan i inledningsskeendet av LIS-arbetet. Viktigt att tänka på när man utformar och väljer de åtgärder som ska ingå i planerna är att skapa förståelse för säkerhetsarbetet och varför utbildning och information behöver genomföras. För att nå acceptans hos individer och grupper som planerna avser måste de känna sig delaktiga i processen.

Personal som har tilldelats något ansvar måste ha kompetens att utföra de uppgifter som krävs. Det kan göras genom följande:

- Identifiera vilken kompetens som krävs för den aktuella uppgiften.
- Erbjuda erforderlig utbildning alternativt anställa eller ta in resurser med den kompetens som krävs.
- Kontinuerligt utvärdera utbildningens effektivitet.
- Ta fram en förteckning över vilken utbildning, kompetens, erfarenhet etc. som personalen besitter.

Nyanställd personal bör så fort de börjat sin anställning genomgå utbildning och få information så att de är medvetna om vilka risker och hot som finns samt vilka säkerhetsrutiner som ska nyttjas. All personal ska fortlöpande informeras om förändringar i regelverket.

3.6 Uppföljning

En viktig del av säkerhetsprocessen är att följa upp att verksamheten lever efter gällande regler och tillgodoser ställda säkerhetskrav. Det ger möjlighet för chefer, ansvariga och systemägare eller motsvarande att försäkra sig om:

- Att ledningssystemet är känt i verksamheten och att det efterlevs.
- Att de säkerhetsåtgärder som är vidtagna underhålls och tjänar sina syften.
- Att ansvarsfördelningen i organisationen fungerar.
- Att säkerhetsåtgärder och regelverk uppdateras allteftersom förutsättningarna förändras eller när nya krav tillkommer.
- Att lärdomar tillämpas från säkerhetserfarenheter i den egna liksom i andra organisationer.

Resultatet av uppföljningsverksamhet är en väsentlig del i förbättring av säkerheten för verksamhetens informationsresurser och även förbättring av ledningssystemet i sig.

Uppföljningsinsatserna ska också omfatta systemutvecklingsprojekt och informationssystem i drift och ingå som en del av projektplaner och förvaltningsplaner.

Den tekniska efterlevnaden av system, applikationer och infrastruktur bör också följas upp med hjälp av penetrationstester och andra tekniska kontroller och granskningar. Det gäller även vid uppdateringar, uppgraderingar, reparationer etc. av implementerat skydd. Syftet är att verifiera att de tekniska säkerhetsåtgärder som är vidtagna uppfyller de krav och möter den hotbild som ställts och att de är korrekt implementerade.

Uppföljning av informationssäkerhet kan med fördel inkluderas i verksamhetens övriga internkontroll så att processen integreras i den normala interna kontrollen.

Det finns en mängd modeller och verktyg för uppföljning, nedan beskrivs kortfattat några av de vanligaste:

Självdeklaration - En metod där användare med hjälp av ett antal frågor deklarerar aktuellt läge avseende informationssäkerheten. Exempel på frågor som kan ingå:

- Vet du var du ska vända dig i informationssäkerhetsfrågor?
- Känner du till innehållet i verksamhetens informationssäkerhetspolicy?
- Vet du vilka regler som gäller för klassificering av information?
- Känner du till hur du ska agera vid upptäckt av en incident?

Intern revision - Verifierande besiktningar och intervjuer i syfte att kontrollera att samtliga delar av LIS fungerar som avsett. Intervjuer genomförs med personer i ledningen, chefer, IT/Driftspersonal, säkerhetsansvariga och medarbetare. Vid besiktningar kontrolleras den fysiska säkerheten i datorhallar, serverutrymmen och vid användarnas arbetsplatser. Intervjuer genomförs med stöd av frågeunderlag som belyser samtliga aspekter av informationssäkerhetsområdet. Kontroll bör ske av att det finns bevis som bekräftar:

- att informationssäkerhetspolicyn korrekt speglar verksamhetskraven.
- att en lämplig riskanalysmetod används.
- att de dokumenterade rutinerna följs
- att tekniska styrmedel är installerade, är rätt konfigurerade och fungerar som avsett.
- att kvarvarande risker har bedömts korrekt och fortfarande är godtagbara.
- att överenskomna åtgärder från föregående revisioner och granskningar har införts.

Checklistor - Utifrån regelverket tas checklistor som används för att följa upp efterlevnaden av ledningssystemet. Checklistorna kan anpassas för olika målgrupper och kravområden.

Utöver intern uppföljning och kontroll kan extern kompetens utnyttjas i de fall verksamheten kräver en oberoende värdering av informationssäkerheten.

Det är viktigt att definiera ansvar för uppföljningen:

- Säkerhetschef/enhet kan ha det övergripande ansvaret för att ledningssystemet följs upp och även tillhandahålla metoder och verktyg för regelbunden sammanställning.

- Ansvariga chefer bör ansvara för att följa upp ledningssystemet för den egna enheten och rapportera resultatet till sammanhållande funktion.
- Systemägare bör ansvara för att följa upp säkerheten i sina respektive system..

3.7 Andra kritiska informationssäkerhetsprocesser

Några av de viktigare informationssäkerhetsprocesserna jämte riskanalys och informationsklassificering är att införa processer för incidenthantering och kontinuitetsplanering. För att säkra systems riktighet, sekretess och tillgänglighet måste säkerhetskrav och risker beaktas som en naturlig del av systemutveckling och systemanskaffning. Att godkänna ett system inför driftsättning i produktionsmiljön garanterar stabilitet och förhindrar negativ påverkan på andra system eller infrastruktur. Nedan beskrivs dessa processer översiktligt.

3.7.1 Incidenthantering

Incidenter uttrycker en handling eller händelse som påverkar informationstillgångars sekretess, riktighet och tillgänglighet på ett negativt sätt d.v.s. innebär skada för verksamheten. Det är alltså inte incidenten i sig som är negativ för tillgången utan den eller de skador, konsekvenser, som incidenten leder till.

Om ett hot blir till verklighet inträffar en eller flera händelser som kallas för en incident. Om ett hot har realiserats kan hotet fortfarande kvarstå eftersom de flesta typer av hot kan realiseras flera gånger. Vanligt är dock att sannolikheten att ett hot ska realiseras minskar i takt med antalet gånger det har realiserats, eftersom man ofta ökar skyddet mot sådana hot.

Ansvar och rutiner för hantering av incidenter skall fastställas för att säkerställa snabb, effektiv och metodisk reaktion vid inträffade säkerhetsincidenter samt för att insamla incidentrelaterade data såsom revisionsspår och loggar.

Rutiner ska finnas för att dela in olika typer av händelser och incidenter i klasser, samt för att hantera samtliga klasser. Det ska också finnas rutiner och definierat ansvar för att återställa efter en incident. Ansvar ska också regleras avseende upptäckt och rapportering av incidenter.

Rutinerna ska omfatta:

- analys och identifikation av incidentens orsak
- planering och införande av åtgärder för att förhindra upprepande.
- spårbarhet.
- kontakt med dem som berörs av återställande efter incidenten.
- rapportering av åtgärd till lämplig instans.

Spårbarheten är viktig för följande ändamål:

- intern problemanalys.
- användning som bevismaterial vid eventuellt handlande i strid mot lagar och andra författningar.
- förordningar, avtal och eventuella andra yttre säkerhetskrav.
- eventuell kompensation från program- eller tjänsteleverantör.

Åtgärder som vidtas för att återställa efter incidenter ska styras noggrant och formellt. Alla åtgärder som vidtas ska dokumenteras i detalj.

3.7.2 Kontinuitetsplanering

Det skall finnas en styrd process för att utveckla och upprätthålla kontinuitet i organisationens olika verksamheter.

En kontinuitetsplan säkerställer att extraordinära resurser kan avsättas i det fall en oönskad händelse inträffar som bedöms som katastrofal. Planen ska baseras på en genomförd riskanalys. I planen bör ingå att prioritera informationsobjekt, system, etc., att identifiera och minska risker, begränsa följderna av eventuella skadliga händelser och att säkerställa att återgång till normal drift för viktiga verksamheter kan göras inom rimlig tid.

Berörd personal ska utbildas på planen och den ska övas och utvärderas regelbundet.

Kontinuitetsplanen är ett levande dokument som kontinuerligt måste revideras i takt med förändringar för att vara effektiv.

3.7.3 Säkerhet vid utveckling och anskaffning

I kravspecifikationen på nya system eller vid ändring av befintliga system skall kraven på styrmedel och säkerhetsåtgärder specificeras. Systemägaren ansvarar för att säkerställa att kraven definieras och inarbetas i kravspecifi-

kationen. Detta ska ske med utgångspunkt av resultatet från en verksamhetsbeskrivning och en riskanalys.

Kravspecifikationen ska omfatta de krav som ställs med avseende på:

- Sekretess.
- Tillgänglighet.
- Riktighet.

Systemägaren ska i samband med att dessa krav definieras ange vilka tester som måste göras för att kunna kontrollera att ställda krav tillgodoses.

Systemägaren ska även definiera vilka krav som ställs på dokumentation av systemet, såväl systemdokumentation, användardokumentation som driftsdokumentation.

3.7.4 Systemgodkännande

En process för systemgodkännande med tillhörande fastställda rutiner ska finnas på plats i verksamheten. Den ska innehålla kriterier för godkännande av nya informationssystem, uppgraderingar eller nya versioner samt ställa krav på lämpliga systemtestester innan ett godkännande.

Innan ett system införs i produktionsmiljön ska systemägaren ta fram ett underlag för beslut om systemgodkännande. Detta beslutsunderlag ska ges till verksamhetsansvarig som har det formella ansvaret att besluta om systemgodkännande. Beslutet ska baseras på resultatet av kontroll av funktionell och säkerhetsmässig kravuppfyllelse. Det görs genom att genomföra formell test av systemet.

Ett systemgodkännande innebär att verksamhetsansvarig gör en bedömning av att verksamheten kan utnyttja systemet med hänsyn till de säkerhetsrisker som är förknippande med systemet/produkten. Bedömningen ska baseras på identifierade risker samt de bevis som finns på att genomförda skyddsåtgärder i systemet uppfyller de krav som ställts med tillräcklig säkerhet. Med "tillräcklig säkerhet" menas att bevisningen är i enlighet med den nivå på bevisning som definierats i kravarbetet.

4 SIS Handledning för planeringsfasen av ett säkerhetsarbete enligt LIS (ISO/IEC 17799).

Detta kapitel är ett nära nog komplett utdrag av resultatet av ett delprojekt (AG10) under SIS huvudprojekt för LIS (TK318). Handledningen har en logisk koppling till vägledningen för att skapa regelverk enligt standarden i kapitel 5.

4.1 Inledning och bakgrund

Att tillämpa svensk standard för informationssäkerhet kan tyckas vara ett självklart val för svenska organisationer, både i näringslivet och i offentlig förvaltning. En ökad spridning av standarden är nödvändig med hänsyn till nyttan av och ett helt uppenbart beroende av IT, samt de hot och risker som man förknippar med informationsbehandling.

Denna handledning har tillkommit på grund av behovet att avdramatisera och förenkla arbetet med att låta standarden vara grunden för en organisations informationssäkerhetsarbete. En förutsättning för att lyckas är bl.a. att det inledande informationssäkerhetsarbetet kan ske i för verksamheten hanterliga steg.

4.2 Syfte och avgränsningar

Syftet är att ge praktisk vägledning i arbetet med att starta upp och genomföra planeringsfasen av ett informationssäkerhetsarbete enligt SS-ISO/IEC 17799. Arbetet är koncentrerat till de första stegen som leder fram till en beskrivning av organisationens ledningssystem för informationssäkerhet i form av ett grundläggande regelverk bestående av policy, riktlinjer och anvisningar (Bild 1). Det syftar därmed även till att ge en grund för fortsatt planering och tillämpning.

Hantering av akuta brister som upptäcks i det inledande stegen (nuläges-, och verksamhetsanalyser) behandlas inte i denna handledning. Detta innebär inte att åtgärder av det slaget är mindre viktiga.

Slutprodukten från den fas som handledningen beskriver är ett sammanhållande regelverk där man har tagit hänsyn till resultatet från verksamhets-, nuläges- och riskanalyser.

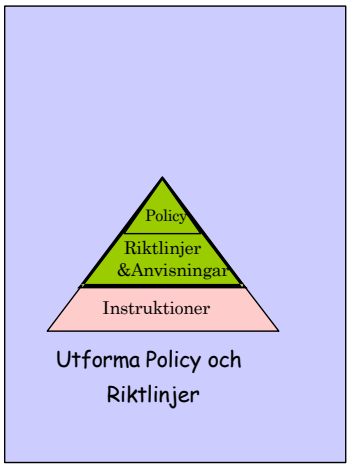
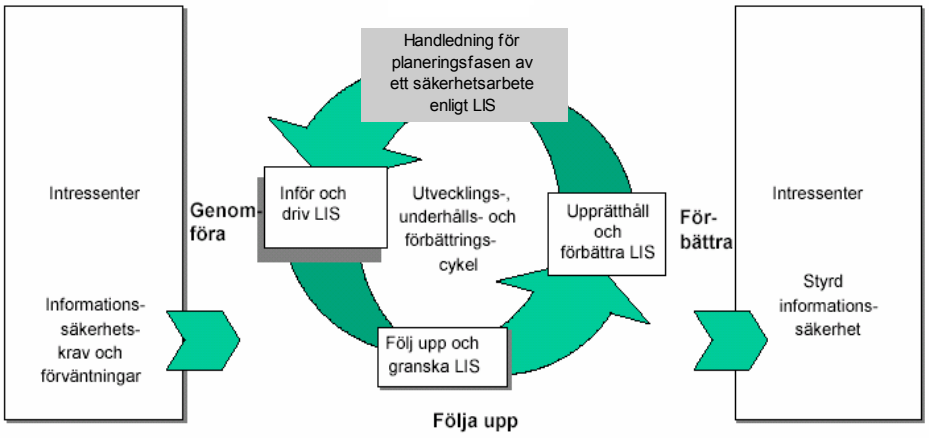


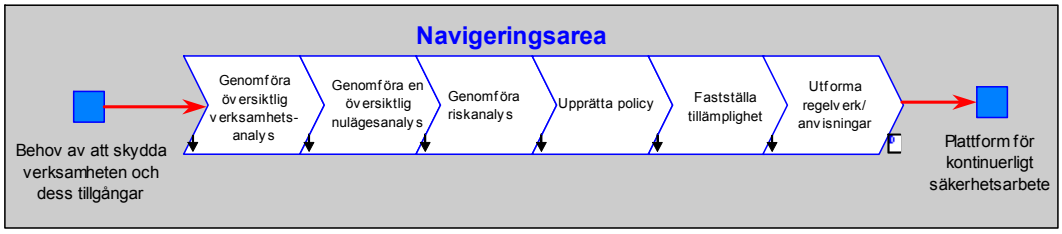
Bild 1 – Dokumenthierarki

Policy	Kortfattat dokument som avspeglar ledningens viljeinriktning.
Riktlinjer	Den del av regelverket som anger VAD som skall uppnås i övergripande termer.
Anvisningar	Regler som anger HUR skyddsåtgärder skall åstadkommas.

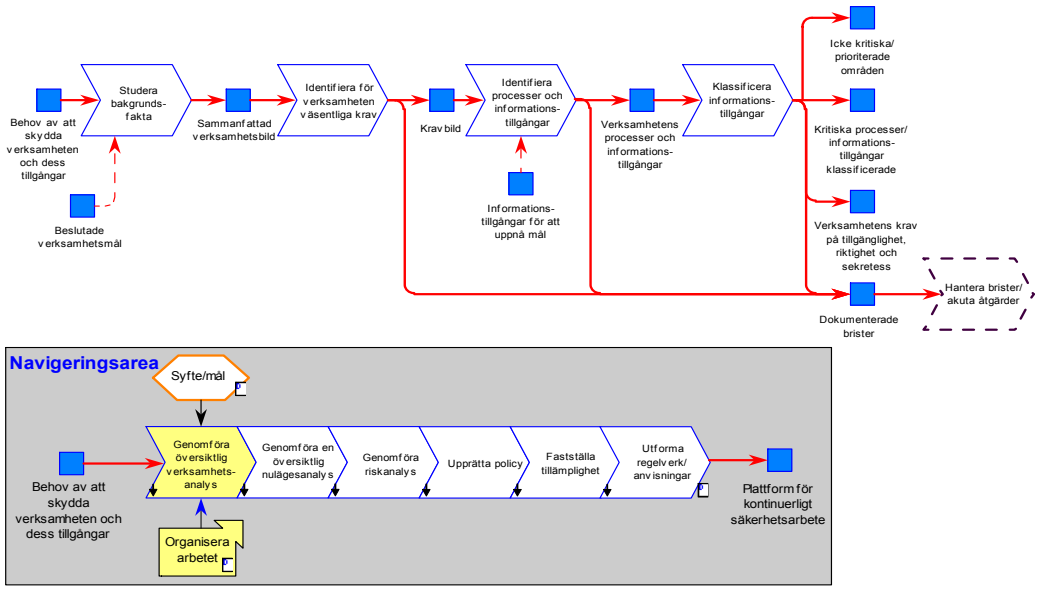
.

I resultatet ingår även en modellstruktur för navigering (se bild nedan) i html (webb-gränssnitt) där delprocesserna hanteras separat med information om vart i helheten man befinner sig. Webb-gränssnittet kan användas alternativt till textdokumentet. och finns tillgängligt via www.sis.se Varje aktuellt textavsnitt erhålls genom att ”klicka” på önskad figur.





4.3 Genomföra översiktlig verksamhetsanalys



4.3.1 Syfte/mål

Att skapa underlag för utformning av ett ledningssystem för informationssäkerhet som är avpassat till den verksamhet det är avsett. Eftersom ledningssystemet måste ta fasta på varje verksamhets speciella situation för att ge en optimal skyddsnivå måste utgångspunkten vara riktig. Oftast finns en bra och väletablerad uppfattning om en verksamhet vilket då underlättar sammanställning av önskad information för det fortsatta arbetet.

Verksamhetsanalysen kan göras för hela eller en del av verksamheten men bör motsvara den avgränsning som det tilltänkta ledningssystemet för informationssäkerhet skall omfatta. Syftet är att identifiera och dokumentera förutsättningar för genomförandet så att ledningssystemet får rätt inriktning.

4.3.2 Organisera arbetet

Personer som bör medverka är de med god kunskap om verksamheten såsom verksamhetsledning, chefer och processägare för viktiga verksamhetsområden. Omfattning av arbetet är beroende av tillgång till dokumentation enligt nedan.

4.3.3 Underlag för genomförandet

- Beslutade verksamhetsmål.
- Behov av informationstillgångar (materiella och immateriella) för att möta målen.
- Konstaterade risker / hot mot målen.
- Kritiska verksamhetsprocesser för att nå verksamhetsmålen.
- Väsentliga omvärldsfaktorer i övrigt.

4.3.4 Genomförande

Se till att verksamhetsanalysen verkligen blir övergripande och att den genomförs koncentrerat under begränsad tid.

Eventuella intervjuer av deltagare enligt ovan bör begränsas.

Viktiga utgångspunkter är befintliga dokument där uttryck för verksamhetsmål ingår, exempelvis årsredovisningen.

Använd de verksamhetsbeskrivningar som ofta finns för att skapa en sammanfattad verksamhetsbild.

Ta fasta på verksamhetens kärnverksamhet och ”roll” i ett omvärldsperspektiv.

Identifiera för verksamheten väsentliga krav i form av lagar, förordningar, branschnormer, kund/leverantörsavtal, försäkringsvillkor etc.

Åskådliggör verksamhetens huvudprocesser/funktioner. Viktigt att bibehålla ett ”helikopterperspektiv”.

Belys väsentliga delar av informationstillgångarna (både i form av ekonomiska termer och humankapital) och betydelsen av dessa för verksamheten. Ta reda på verksamhetsvisioner och deras inverkan på framtida informationsbehandling.

Se till att skapa dej en uppfattning om aktuella former för informationsbehandling, systemtillämpningar, kommunikationsnät, lokalisering av verksamhet och IT-resurser, etc.

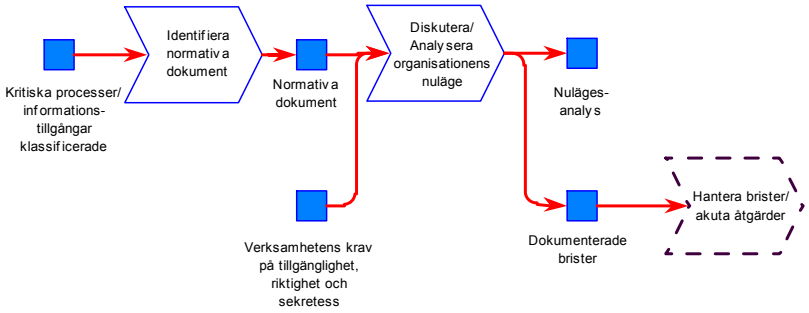
Dokumentera ”lagom” mycket.

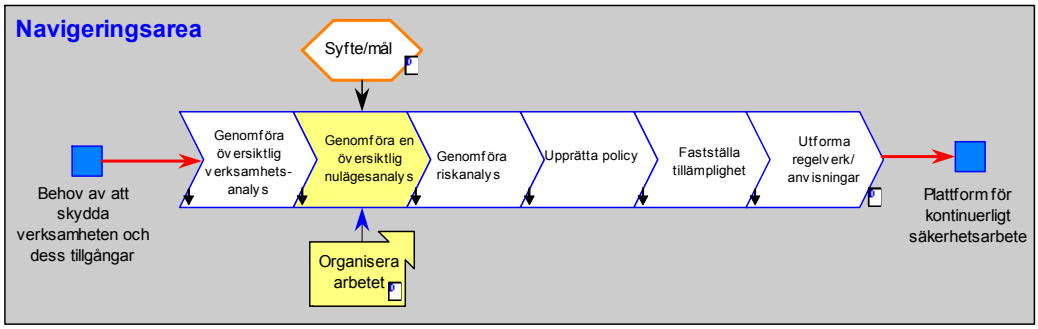
En övergripande avstämning med deltagare och verksamhetens ledning är lämpligt.

4.3.5 Processens resultat

En väsentlig del av resultatet är att huvudprocesser/funktioner och informationstillgångar är klassificerade med hänsyn till verksamhetens krav på tillgänglighet, riktighet och sekretess så att en prioritering kan göras. Ett sätt att prioritera är att utifrån ledningens syn på konsekvenser av brister ange klasser i olika nivåer (t.ex. Mycket kritiskt, Viktigt, Mindre viktigt).
Dokumentera genomförande och resultat kortfattat.

4.4 Genomföra översiktlig nulägesanalys





4.4.1 Syfte/mål

För att det fortsatta arbetet med att beskriva ledningssystemet för informationssäkerhet skall få rätt inriktning och stöd är det nödvändigt att också konstatera vilken befintlig nivå av informationssäkerhet man har för att säkerställa verksamhetens kontinuitet ur ett helhetsperspektiv

Resultatet av en nulägesanalys tillsammans med verksamhetens mål är ofta en viktig del av motivet för framtida insatser för informationssäkerhet.

Även om det grundläggande syftet med nulägesanalysen i detta sammanhang är att ge underlag för beskrivningen av det önskade ledningssystemet i form av policy och riktlinjer skall man naturligtvis se till att identifierade uppenbara brister hanteras parallellt i en prioriterad handlingsplan.

4.4.2 Organisera arbetet

Lämplig bemanning för nulägesanalys är ledningspersoner med god insyn i verksamheten, personer med god insyn i nuläget vad gäller informationssäkerhet för såväl administrativ- som IT-säkerhet. Nulägesanalysen skall utföras av intern eller extern resurs med oberoende ställning till verksamheten.

4.4.3 Förutsättningar för genomförandet

Viktiga förutsättningar för genomförandet är resultatet av verksamhetsanalysen och tillgång till lämpliga ledningspersoner.

4.4.4 Genomförande

Identifiera för verksamheten relevanta standarder och normativa dokument och förteckna dem. Med dessa som referensdokument görs en grov uppskattning av verksamhetens aktuella behov avseende nivå på informationssäkerhet.

Den prioritering som gjorts i samband med verksamhetsanalysen utgör grund för vilka skyddsåtgärder/kontroller som skall beaktas.

Ett lämpligt inledande steg i nulägesanalysen kan vara att skapa ett övergripande flödesschema över verksamhetens huvudprocesser inklusive infrastruktur (logisk och teknisk), om inte detta redan finns eller gjorts vid verksamhetsanalysen.

Ett lämpligt sätt att genomföra nulägesanalysen är följande:

- Välj ut viktiga processer/processteg med avseende på kravbilden (på tillgänglighet, riktighet och sekretess).
- Analys i workshopform med lämpliga nyckelpersoner i verksamheten. Det är viktigt att de som deltar har god kompetens inom sitt verksamhetsområde. Diskutera/Analysera organisationens nuläge i förhållande

till kravbilden. Vilka processer är kritiska, hur väl fungerar dom idag med avseende på tillgänglighet, riktighet och sekretess? (Resultatet används vid senare arbete med riskanalys.)

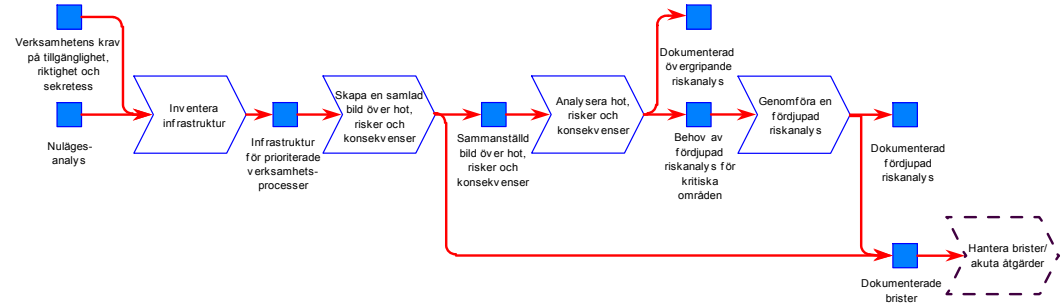
Identifierade brister vid nulägesanalysen tillsammans med risk- och sårbarhetsanalysernas resultat ger vägledning för inriktning av policy och riktlinjer.

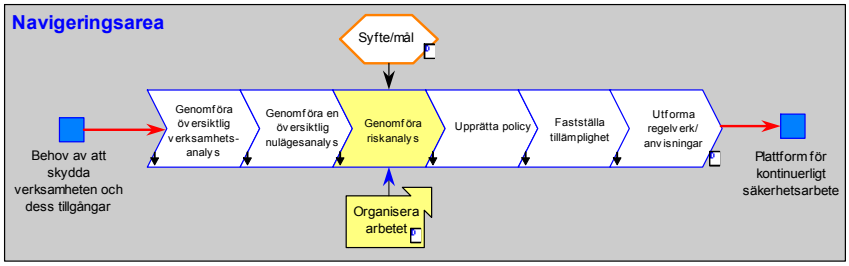
Nulägesanalysens resultat presenteras lämpligen för verksamhetens ledning. Brister av mera akut karaktär överlämnas till verksamheten för prioritering och nödvändiga åtgärder.

4.4.5 Processens resultat

En beskrivning av verksamhetens faktiska informationssäkerhetsnivå.

4.5 Genomföra riskanalys





4.5.1 Syfte/mål

Att genom en övergripande riksanalys kunna ge en vägledning till att formulera den i säkerhetspolicyn önskade säkerhetsnivån. I denna riskanalys identifieras övergripande hot och risker för hela verksamheten.

Att genom en fördjupad riskanalys få fram önskad säkerhetsnivå som utgör riktmärke i arbetet med att ta fram regelverket i form av riktlinjer och anvisningar. Ledningen kan även önska en fördjupad riskanalys om det konstateras att den övergripande riskanalysen ej täcker hela verksamheten, att en eller flera processer ej blivit tillfredsställande belysta eller att uppenbara risker/hot ej blivit dokumenterade.

4.5.2 Organisera arbetet

Den övergripande analysen kan med fördel genomföras i workshopform med representanter för olika delar av verksamheten med förmåga att se i ett ”helikopterperspektiv” utan fördjupning i alltför mycket detaljer. En erfaren person, extern eller intern, bör utses som håller i workshopen och ser till att arbetet drivs framåt.

Den fördjupade riskanalysen sker med representanter med kompetens inom det aktuella området. Dock är det viktigt att såväl verksamhets- som teknisk kompetens är representerade.

Det finns ett antal beprövade metoder som man med fördel bör använda som stöd i arbetet. Exempel på riskanalysmetoder är SBA Scenario, RiscPac, CRAMM, RA, ISAP, ISF Sprint och Proteus. Många konsultföretag har egna metoder.

4.5.3 Förutsättningar för genomförandet

För att skapa en bas att utgå ifrån är det viktigt att verksamhetsanalys och nulägesanalys är genomförda.

4.5.4 Genomförande

I workshopform identifiera hot och risker tillsammans med vid nulägesanalysen konstaterade logiska och tekniska brister.

Bedöma konsekvenserna av identifierade hot och risker utifrån ett helhetsperspektiv på verksamheten.

När den övergripande riskanalysen är genomförd finns en översiktlig bild över konsekvenser för verksamheten i händelse av att identifierade hot blir verklighet. Detta ger en uppfattning om hur det fortsatta informationssäkerhetsarbetet skall prioriteras.

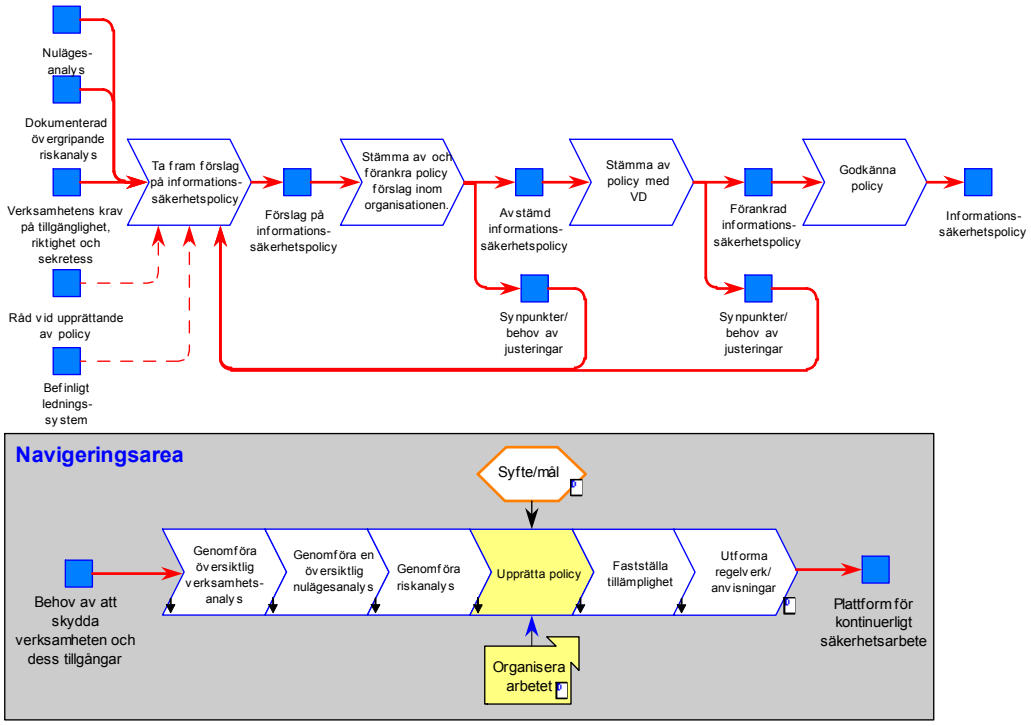
Vid en fördjupade riskanalyserna görs inriktningen på de mest kritiska processerna/funktionerna som identifierats under verksamhetsanalysen. De får utgöra riktmärke för övriga processer i verksamheten.

I arbetet, oavsett typ av riskanalys, kan det förekomma att uppenbara brister i den nuvarande miljön identifieras. Denna hantering ingår inte i arbetet med att införa Ledningssystem för Informationssäkerhet. Dock skall givetvis dessa brister tas om hand och hanteras parallellt i en prioriterad handlingsplan i det ordinarie säkerhetsarbetet.

4.5.5 Processens resultat:

Dokumenterad övergripande riskanalys.
Behov av fördjupad riskanalys för kritiska områden.
Dokumenterad fördjupad riskanalys.

4.6 Upprätta informationssäkerhetspolicy



4.6.1 Syfte/mål

Policyn ska spegla verksamhetens behov av informationssäkerhet och fungera som motivationshöjare. I policyn uttrycker ledningen sin viljeinriktning och organisationens ansvar/ansvarsfördelning.

4.6.2 Organisera arbetet

Arbetet utförs oftast av säkerhetsansvarig/säkerhetsorganisationen men ledningen måste vara nära involverad eftersom det är deras viljeinriktning som skall speglas.

Hur arbetet skall förankras bör bestämmas innan arbetet påbörjas.

4.6.3 Förutsättningar för genomförandet

Indata till policyn bygger på resultat från processerna:

- *översiktlig verksamhetsanalys* (Intressenternas krav (legala, affärsmässiga etc.)

- *översiktlig nulägesanalys.*
- *övergripande riskanalys* samt.
- hur *befintlig organisation och andra ledningssystem* ser ut.

Skrivs policyn utan detta indata speglar inte policyn verksamhetens krav på säkerhet.

4.6.4 Genomförande

4.6.4.1 Grundförutsättningar

Policyn skrivs utifrån ovan nämnda information och kunskap. Det ledningen har identifierat som viktigt i de tidigare gjorda analyserna skall framgå och poängteras i policyn för att verka motivationshöjande i organisationen. Det är viktigt att även peka på vad som händer om man inte följer policyn. Lagar som påverkar den aktuella verksamheten bör också lyftas fram. Inspiration kan hämtas från t ex referenslitteratur, Internet, intresseföreningar och branschföreningar. Formuleringar/tonläge kan hämtas från t ex årsredovisningar, andra policydokument eller andra dokument som ledningen står bakom.

Det kan finnas olika uppfattningar och behov rörande en policys omfattning. Den skall vara tillräckligt kortfattad för att personal skall orka och kunna ta den till sig samtidigt som den skall vara tillräckligt distinkt och tydlig så att den blir ett riktmärke i det fortsatta arbetet med regelverket. Ett riktmärke till omfattning kan vara ca 2-4 sidor. Om man väljer att hålla policyn väldigt kortfattad bör ett mer omfattande måldokument biläggas som kan användas i nästa steg i processen med att införa LIS.

Policyn skall vara övergripande och inte uppdateras så ofta. Vem som har ansvar för policy och dess underhåll bör skrivas i policy och/eller i Regelverket, t ex under kapitel om Uppföljning & Efterlevnad.

För stora och komplexa verksamheter (t ex med vitt skilda verksamhetsområden) kan det vara nödvändigt att upprätta en övergripande policy och ett antal underliggande verksamhetsanpassade policies.

4.6.4.2 Policyn bör omfatta följande:

- En definition av informationssäkerhet, dess allmänna mål och omfattning och vikten av säkerhet som möjliggör att information på ett säkert sätt kan delas med andra.
- Ett uttalande om ledningens viljeinriktning som ger stöd för informationssäkerhetens mål och principer;

- En kort framställning av allmän säkerhetspolicy, principer, riktlinjer, och efterlevnadskrav av särskild betydelse för organisationen, t.ex.:
    - efterlevnad av lagar, förordningar, avtal och andra yttre säkerhetskrav;
    - krav på säkerhetsutbildning;
    - virusskydd och skydd mot andra skadliga program;
    - kontinuitetsplan för verksamheten;
    - konsekvenser vid åsidosättande av säkerhetspolicy;
    - riskanalys.
- En definition av allmänt och särskilt ansvar för informationssäkerhet inklusive rapportering av incidenter.
- Hänvisning till annan styrande dokumentation och rutiner för individuella informationssystem eller andra säkerhetsregler som skall följas.

Policyn skall delges alla berörda inom hela organisationen.

4.6.5 Beslutsprocess

När ett förslag på policy finns färdigt (med versionsnummer och datum) så skall det stämmas av och förankras inom organisationen och av verksamhetschef. Efter förankring i ledningsgrupp eller motsvarande godkänner verksamhetschefen informationssäkerhetspolicyn. Den kommuniceras därefter ut till samtliga i organisationen på sådant sätt att den är relevant, tillgänglig och begriplig för läsarna.

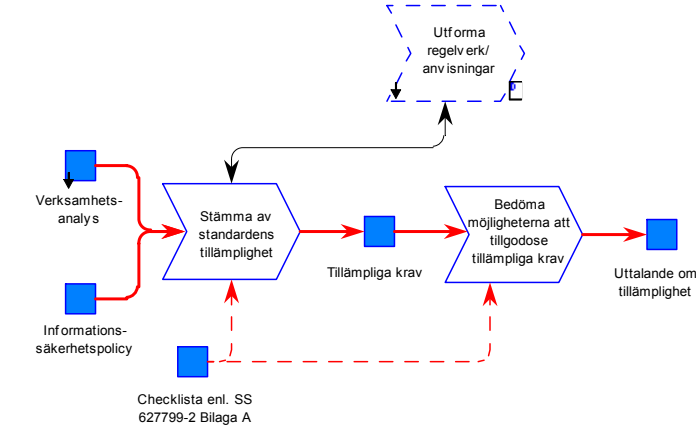
4.6.6 Referenser

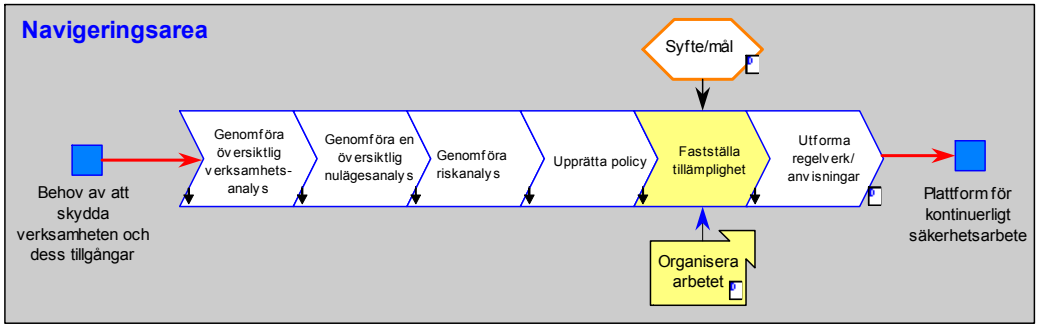
Mer information om vad som bör finnas med i en policy finns beskrivet i t ex:
- SS-ISO/IEC 17799.
- SS 62 77 99 del 2 Utgåva 2.
– Handbok i Informationssäkerhetsarbete, SIS Förlag.
- Riktlinjer för god informationssäkerhet, SIG Security.

4.6.7 Processens resultat

Informationssäkerhetspolicy

4.7 Fastställa tillämplighet





4.7.1 Syfte/mål

Att beskriva vilka delar av standarden som är relevanta och tillämpbara på verksamhetens ledningssystem för informationssäkerhet baserat på resultat och slutsatser av genomförda verksamhets- och riskanalyser. Om verksamheten avser att certifiera sig mot standarden är detta en obligatorisk aktivitet.

4.7.2 Organisera arbetet

Föreberedelserna för uttalande om tillämplighet bör ingå som en del av arbetet med utformning av policy och övergripande riktlinjer och följaktligen utföras av samma arbetsgrupp (se nedan ”Att utforma regelverk och anvisningar”).

4.7.3 Förutsättningar för genomförandet

Som underlag används Bilaga A till SS 62 77 99-2, utgåva 2. De styrmål och styrmedel som anges i bilagan är dock inte uttömmande varför ytterligare styrmål och styrmedel också kan väljas. Genomförda verksamhets-, nuläges- och riskanalyser används som underlag.

4.7.4 Genomförande

I samband med framtagandet av policy alternativt efter att ett första förslag på regelverk tagits fram, görs en avstämning mot SS 62 77 99 – 2:2003 bilaga A .

Punkt för punkt bör det kontrolleras om kontrollkraven i Bilaga A är tillämpbart eller ej. Om kontrollkrav är tillämpbart – hänvisa till kontrollpunkt i regelverket. Om kontrollkravet däremot inte anses tillämpbart – ange skälet till att så är fallet (t ex kraven på outsourcing är inte tillämpbart om man inte har någon outsourcing).

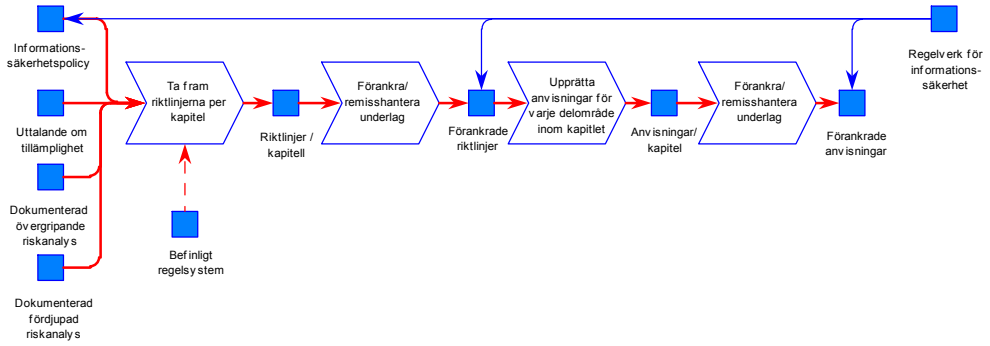
Om krav är tillämpbart, men inte bedöms vara möjligt att uppfylla – ange hur och när detta skall åtgärdas (åtgärdsplan).

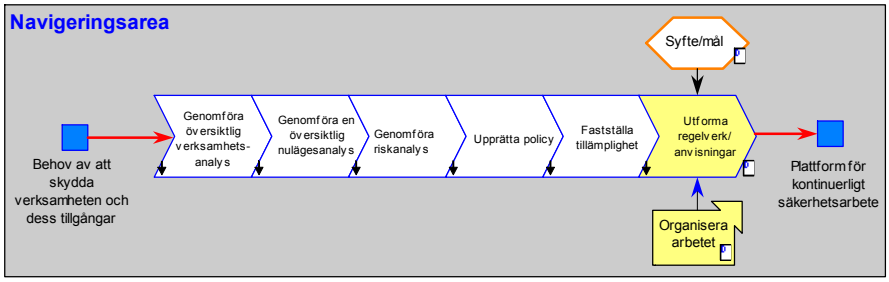
Utnyttja gärna tabellen i Annex A och lägg till en kolumn med tillämpbarhet samt referens till regelverk.

4.7.5 Processens resultat

Dokumenterat och av ledningen fastställt uttalande om tillämplighet inklusive motivering för utelämnande av styrmedel.

4.8 Att utforma regelverk och anvisningar





4.8.1 Syfte/mål

I ett regelverk, bestående av riktlinjer och anvisningar, beskriva hela ledningssystemet (ramar) för informationssäkerhet. Upprättat dokument om tillämplighet beskriver vilka riktlinjer och anvisningar som skall ingå i regelverket. Riktlinjerna och anvisningarna skall gälla hela verksamheten eller en tydligt avgränsad del.

Resultatet skall ge en grund för informationssäkerhetsarbetet i organisationen. Regelverket skall innehålla målformuleringar om VAD som skall åstadkommas men också anvisningar på en övergripande nivå om HUR målen uppnås till exempel vilka delprocesser som skall bedrivas och vilka skyddsåtgärder som skall finnas.

Arbetet omfattar både riktlinjer och anvisningar för att ge tillräckligt stöd till verksamheten för införandet med att utforma mera detaljerade anvisningar och instruktioner. (I nästa nivå utformas anvisningar anpassade till HUR man jobbar.)

Arbetet med att ta fram policy och riktlinjer leds av företrädare för säkerhetsarbetet (på ledningens uppdrag) och görs med hjälp av representanter för verksamheten.

Resultatet skall kunna tas emot av organisationens delar som underlag för vidare utformning av instruktioner/rutiner och dess tillämpning.

Resultatet skall kunna användas för kontroll av att organisationen följer riktlinjerna.

4.8.2 Organisera arbetet

I arbetet med att ta fram riktlinjer och anvisningar bör företrädare för olika delar i organisationen delta. Vilka delar av organisationen som deltar är beroende av område. Företrädarna bör lämpligen i första hand arbeta med delar som ligger inom deras arbetsområde för att skapa så god verksamhetsanpassning som möjligt. Detta underlättar sedan senare förädling i form av instruktioner och rutiner på verksamhetsnivå. Exempel på roller som kan delta är:

- Verksamhetsrepresentanter.
- Informationssäkerhetsansvarig.
- Representanter för fysisk säkerhet.
- Systemägare.

Engagera resurser i verksamheten som har kompetens inom de områden som riktlinjerna skall omfatta. Deltagandet från organisationen måste uppfattas så att verksamheten känner delaktighet och har fått företräda sina frågor. De som deltar måste ha tyngd och ha organisationens förtroende. God relation med ledning för respektive område är viktigt. Skapa en så liten grupp som möjligt som redaktionsgrupp med möjlighet till att kalla in specialkompetens.

Undvik alltför stora projekt. Försök att få fram en första version relativt snabbt. Gör en bedömning av gamla regelverk t.ex. om det kan förädlas/vidareutvecklas i ny version eller ersättas med ett helt nytt.

Förankringsprocessen måste klarläggas tidigt. Kontinuerlig förankring behövs oftast. En strategi skall upprättas för hur information om resultatet skall spridas.

4.8.3 Förutsättningar för genomförandet

Samtliga inblandade parter skall vara väl insatta i tidigare fasers resultat för att kunna omsätta det i arbetet med riktlinjer och anvisningar.

Vid behov fattas beslut om att genomföra fördjupade riskanalyser inom specifika områden för att få rätt säkerhetsnivå i riktlinjer och anvisningar. Spårbarhet, i detalj, mellan riskanalys och säkerhetsnivå i riktlinjer och anvisningar är troligen inte möjligt.

4.8.4 Genomförande

4.8.4.1 Grundförutsättningar

Utgå från helheten, de som är generella och gemensamma krav för hela organisationen Resultatet från tillämplighetsavsnittet styr vilka riktlinjer och anvisningar som skall skrivas. Resultatet från riskanalyserna styr vilken säkerhetsnivå de olika riktlinjerna skall ha.

Man kan med fördel utgå från strukturen i standarden Del 1 och dess kapitelindelning. Alternativt kan annan struktur för regelverket väljas. Överväg behovet av att förmedla regelverkets information i verksamheten, till exempel genom separata instruktioner för att stödja användare eller andra målgrupper.

Riktlinjerna kan antingen skrivas för grundsäkerhetsnivå eller flera säkerhetsnivåer (t.ex. 3 nivåer baserat på bedömning av behov för sekretess, riktighet och tillgänglighet).

4.8.4.2 Arbetsprocess

Skriv regler och förankra successivt med verksamheten. Varje deltagare i eventuell arbetsgrupp kan lämpligen svara för förankring inom sitt tilldelade regelavsnitt. Skriv riktlinjerna som en målbild för ett kapitel, fortsätt sedan med mer detaljerade anvisningar för varje delområde inom kapitlet där det är möjligt. Anvisningarna skall innehålla hur man åstadkommer målen som beskrivs i riktlinjerna. Omfattning av riktlinjer bedöms vara ca en ½ A4: sida och anvisningarna ca 1 A4-sida. Anvisningar kan anges för olika säkerhetsnivåer enligt ovan där så är lämpligt.

4.8.4.3 Beslutsprocess

Förankring i verksamheten genom remissförfarande är väsentligt. Beroende på organisationens storlek, ledningens motivation och mognad kan det ta sin

tid. Det är å andra sidan avgörande för acceptansen att resultatet är väl avstämt med de som kommer att beröras.

4.8.5 Processens resultat

Ett referensregelverk bestående av policy, riktlinjer och anvisningar för informationssäkerhet. Resultatet från arbetet skall ge en plattform och inriktning till de mer detaljerade rutiner och användarinstruktioner som måste göras. Texten i riktlinjer och anvisningar skall ange om det finns krav på en detaljnivå ytterligare i dokumentation. Det är oftast lämpligt att också åstadkomma mera lättlästa små utdrag ur reglerna riktade till lämpliga målgrupper. Helheten uppfattas av medarbetarna som alltför omfattande eftersom mycket riktar sig till andra kategorier, inte minst mot IT-driftorganisationen eller motsvarande.

5 OffLIS – mallregelverk och modell för LIS för 24-timmarsmyndigheten

5.1 Översikt

Att ta till sig och införa ett arbetssätt som beskrivs av standarden uppfattas ofta som mycket omfattande, tungt och byråkratiskt. Det man då gärna glömmer är att standarden beskriver genomförandet av ett komplett säkerhetsarbete i en organisation som bedrivs i en kontinuerlig process. Man behöver inte se det som något som fullt ut skall finnas på plats vid en given tidpunkt utan mera som en metodanvisning för säkerhetsarbetet. Ett införande kan och bör ske stegvis i lämpliga etapper prioriterade efter identifierade risker i verksamheten.

Denna tillämpningsanvisning med verktyg och mallar för att utforma väsentliga dokument har tagits fram för att avdramatisera användningen av standarden och att förenkla de första stegen i säkerhetsarbetet, att ta fram policy och riktlinjer som beskriver förutsättningar, mål och övergripande anvisningar för informationssäkerhetsarbetet.

Som ett komplement till handbokens metodbeskrivning att utforma policy och riktlinjer för informationssäkerhet har en accessdatabas skapats. Ursprungsmodellen för databasen har ställts till förfogande av Luftfartsverket. Databasen utgör ett mallregelverk för Ledningssystem för informationssäkerhet, omfattande:

- Klassificeringsmodell för styrning av skyddsåtgärder beroende på nivå av sekretess, riktighet och tillgänglighet.
- Anvisningar för utformning informationssäkerhetspolicy,
- Mall till riktlinjer för informationssäkerhet med förslag till nivåindelning med hänsyn till klassificeringsnivåer enligt ovan. Mallen är tänkt att användas som utgångspunkt för att utforma ett eget regelverk för en önskad grundskyddsnivå för organisationen.
- Anvisningar hur mallregelverket i den tillhörande accessdatabasen kan utnyttjas för att anpassa information ur regelverket på olika sätt genom:
-
    - indelning på riktlinjer och anvisningar (”katalogdel”),
    - rollstyrning av databasens innehåll av regler (”roller”),
    - utformning av ”ledningssammanfattning” av regelverket,
    - stöd för annan indelningsgrund av regelverket (”kravinriktning”).

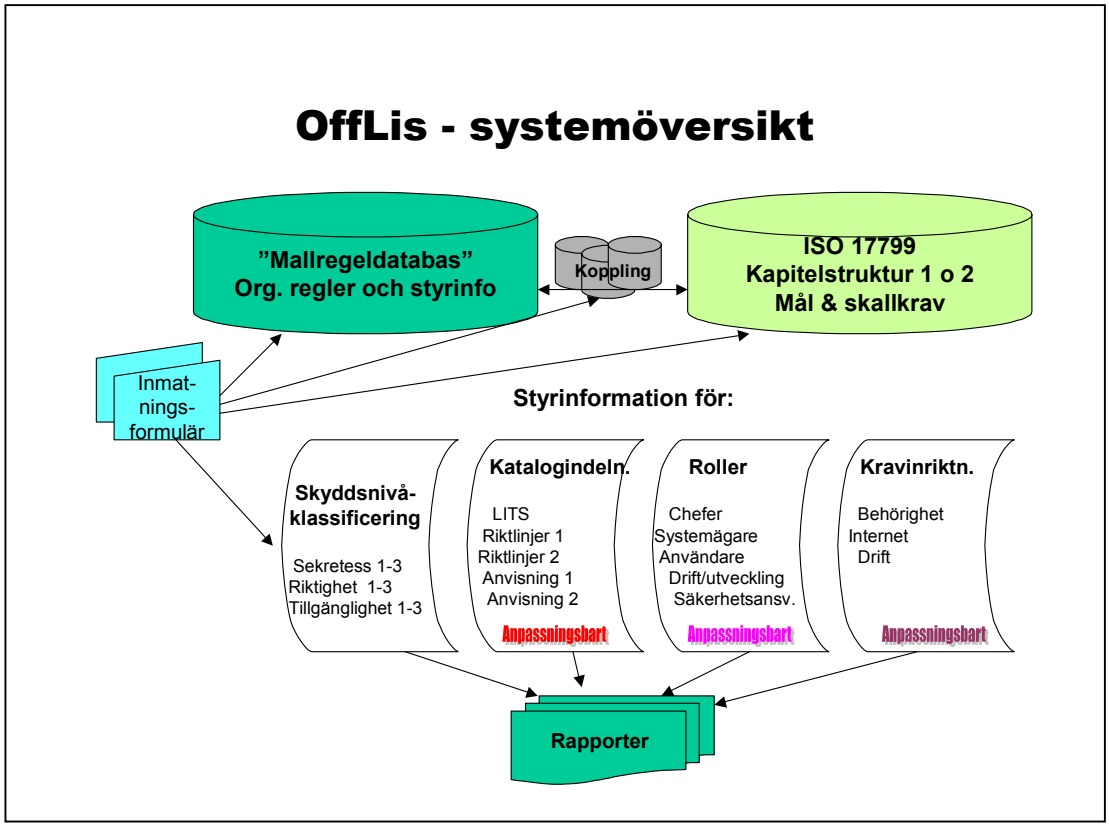
Databasmallen är utformad enligt standardens struktur och är mycket lätt att anpassa efter egna behov. Det underlättar också jämförelsen med standardens krav.

Utskrifter av databasens regler kan göras med hjälp av accessdatabashanteringens rapportgenerator eller exporteras till Wordformat för förfinad design.

Föreliggande version av rapporter etc. skall ses som exempel och förslag till utformning och är tänkta att anpassas av den organisation som utnyttjar dem.

Accessdatabasen kan hämtas på Statskontorets hemsida
www.statskontoret.se/publi/2003/OffLIS mallregelverk ver 1.zip

Produktöversikt/Accessdatabas



5.2 Vägledning för informationssäkarbete med mallregelverket/OffLIS som arbetsmetod

5.2.1 Skapa regelverket i form av policy, riktlinjer och anvisningar.

Mallregelverket använder beteckningarna policy, riktlinjer och anvisningar eftersom dessa är vanligt förekommande i många organisationer. Hos vissa myndigheter kan det finnas behov av att i stället tillämpa andra beteckningar på regelverket, t.ex. föreskrifter och instruktioner. Denna typ av ändring är lätt att göra om behov finns.

Mallregelverket har upprättats i form av texter som anknyter till respektive kapitel i standarden. Vill man ha en annan kapitelstruktur kan man utnyttja möjligheterna till informationsstyrning som finns förberedda i modellen eller göra en egen komplettering av databasen. Accesstekniken medger relativt enkelt stora möjligheter till egna anpassningar. Databastekniken ger dock begränsningar när det gäller hantering av text.

Varje text är kategoriserad på olika sätt för att kunna sorteras och skrivas ut på lämpligt sätt. Sättet att kategorisera och skriva ut kan anpassas efter den egna organisationens behov. Kategoriernas indelning är dock något flytande. Det finns ingen standard för vad ”riktlinje” respektive ”anvisning” står för varför tillämpningen kan variera beroende på det synsätt som respektive organisation har. < > används i texterna för att markera att här behöver en komplettering ske med namn eller text som anger vad som gäller i den aktuella organisationen.

Mallregelverkets tabell som innehåller standardens SS-ISO/IEC 17799 struktur omfattar också textutdrag från SS 62 77 99-2 i form av målformuleringar och skallkrav. Denna publicering har skett med tillstånd av SIS, Swedish Standards Institute. Innehållet ger därmed möjlighet till översiktlig kontroll av en organisations följsamhet mot standarden. Tillgång till standarden i sin helhet är dock en förutsättning för att informationssäkerhetsarbetet bedrivs i enlighet med densamma och för certifiering. Ytterligare information om standarden och tillhörande hjälpmedel finns på www.sis.se.

Följande textkategorier och syften tillämpas i modellen:

Katalogdel	Syfte
LITS	Text som anknyter till krav som övergripande ställs för att regelverket skall uppfattas som ett ledningssystem för informationssäkerhet enligt SS-ISO/IEC 17799.
Riktlinje 1	Anger generella riktlinjer för VAD som skall uppnås vad beträffar informationens informationssäkerhet.

Riktlinje 2	Anger övergripande säkerhetskrav som gäller i hela organisationen.
Anvisning 1	Anger säkerhetskrav på en mera detaljerad nivå som kan gälla specifika informationsobjekt som system, register, del av verksamhet eller informationsmängder i annan form.
Anvisning 2	Anger övergripande anvisningar för HUR skyddsåtgärder eller administrativa processer skall utformas. < > anger att här är det lämpligt att dokumentera organisationens egen tillämpning av aktuell anvisning.

Indelningen i katalogdelar används för sortering av texterna när man vill skriva ut hela eller delar av dokumentet. Vid utskrift av hela dokumentet medför detta att dokumentets texter får en ordning som känns så logisk som möjligt.

Regeltexterna har också kopplats till ett antal roller i organisationen. Syftet är att kunna skriva ut eller i ett Intranät kunna tillhandahålla regler riktade till en eller flera specifika verksamhetsroller.

Följande roller har använts i mallregelverket:

Roll	Innebörd
Användare	Användare av IT-stöd / IT-system eller informationssystem i annan form.
Chefer	Chefer med ansvar för hela eller del av verksamheten. Kan också vara en processägare med ett motsvarande ansvar.
Systemägare	Ägare av IT-system eller informationssystem med ett ansvar kopplat till ägarrollen.
Utveckling/Drift	Personal för utveckling, anskaffning och drift av informationsbehandlingsresurser och/eller IT-system. Inbegriper både tillämpningssystem och infrastruktur som operativsystem etc.
Säkerhetsansvarig	Befattningshavare med särskilda uppgifter att samordna informationssäkerhetsfrågor på uppdrag av verksamhetsledning.

För att kunna skriva ut regeltexter med ytterligare urvalskriterium kan texterna också behöva kopplas till ytterligare attribut. I modellen finns därför ytterligare en indelningsgrund som kallas för ”kravinriktning”.

Som exempel har följande attribut för kravinriktning använts:

Kravinriktning	**Ändamål**
Drift	De regler som berör driftorganisationen
Internet	Regler för internetanvändning.
Behörighet	Regler med inriktning på behörighet.

En tänkbar användning av detta som urvals-/utskriftskriterium är om behov finns att plocka ut allt som gäller exempelvis Internetsäkerhet. Alternativt kan denna indelning också användas till att skapa en regelstruktur som är mera anpassad till organisationens uppfattning. Det vill säga. en annan kapitelordning än standardens.

För att underlätta registrering och underhåll av mallregelverket har tre registreringsformulär skapats:

- Registrering av riktlinjer och anvisningar
- Registrering av roller
- Registrering av kravinriktning

Dessa registreringsformulär nås via menyformuläret.

Menyformuläret innehåller också möjlighet till utskrift av ett urval av rapporter.

Registrering och korrigering kan naturligtvis också ske direkt i tabellerna.

Förslag till arbetsprocess med befintligt mallregelverk som grund och med hjälp av befintligt registreringsformulär ”Registrering av riktlinjer och anvisningar” som nås från menyformuläret:

1. Bedöm angivna kravtexter indelade i Riktlinje 1, Riktlinje 2, Anvisning 1 och Anvisning 2. Korrigera vid behov namnen på ”Katalogdel” för att bättre motsvara organisationens eget språkbruk. Man har god nytta av den rapport som kan nås via Accessmenyn och som heter ”Riktlinjer arbetslista 1” för att se idnr på kravtext (för att söka upp eller ner) och vilken katalogdel texten är registrerad som. Namn och ordningsföljden för utskrift i rapporter anges i tabell ”Katalogdel”

2. Inventera organisationens befintliga regelverk och för in dessa på lämplig plats i strukturen genom att ersätta eller komplettera befintliga kravtexter.

3. Lägg vid behov till ytterligare kravtexter. Observera att vid registrering av nya kravtexter enligt Anvisning 1 så måste en koppling ske till nivåer för Sekretess, Riktighet och Tillgänglighet. Detta sker i en sär-

skild tabell ”Kraven för grundsäkerhetsprocessen” och styr utskrift av krav enligt skyddsnivåklassificeringen (Se nedan).

4. Anpassa befintliga rollbenämningar till vad som passar organisationen och koppla regelverkets kravtexter till dessa. Mallregelverket innehåller kopplingar till angivna roller i viss utsträckning men detta behöver säkert anpassas efter organisationens egen uppfattning.

5. För varje kravtext kan också en koppling ske till en alternativ indelning av regelverket som benämnts ”Kravinriktning”. Detta kan användas för att skriva ut regler med vald inriktning t.ex. ”Drift”, ”Internet”, ”Behörighet” etc. Detta alternativ kan också användas för en alternativ struktur av hela regelverket.

6. Varje ny kravtext kopplas också till aktuellt kapitel i SS-ISO/IEC 17799. Tabelldatabasen innehåller också kapitelindelning från SS 62 77 99-2 eftersom där finns målformuleringar och skallkrav som tilllämpas vid certifiering. Detta innebär att det är möjligt att skapa en egen kapitelstruktur i kolumnen för kapitel del 1 om detta upplevs lämpligare för den aktuella organisationen.

Fältbeskrivning inmatningsformulär ”Registrering av riktlinjer och anvisningar”

Fält	**Registreringsanvisning**
Nr	Tabellpostens idnr. Erhålls automatiskt vid registrering av ny kravtext.
Katalogdel	Markera genom att välja i ”rullgardinsmenyn”.
Kravtext	Textfält för riktlinjer och anvisningar.
Kravsammanfattning	Textfält att disponera för sammanfattning.
Kravinriktning	Möjlig koppling av kravtext till särskilda attribut.
Skyddsnivå	Önskad nivå, 1 – 3, för angivet klassificeringsområde.
Klassificeringsområden	Sekretess, Riktighet, Tillgänglighet.
Kopplingar Kravtext till LIS-standard	Kopplar kravtext till kapitel i LIS-standarden. Välj ”Ny koppling” och sök fram rätt kapitelnr och kapitelrubrik. Välj ”Ta bort koppling” vid borttag.
Kopplingar Kravtext till Roller	Kopplar kravtext till roll. Välj ”Ny koppling” och därefter önskad Roll i listan. Vid borttag välj ”Ta bort koppling”.
<< < > >>	För bläddring i kravkatalogen.
Nytt krav	När ny kravtext skall registreras och kopplas.
Ta bort krav	För borttag av tabellpost och samtliga kopplingar.

Uppsättningen roller kan anpassas i enlighet med varje organisations behov i formuläret ”Registrering av roller”. Rollbenämning respektive sorteringsordning vid rapportutskrift kan anges.

En annan indelningsgrund, t.ex. utifrån särskilda informationsbehov kan skapas genom att använda begrepp under ”kravinriktning”. Dessa begrepp kan anpassas i enlighet med varje organisations behov i formuläret ”Registrering av kravinriktning”. Önskat begrepp respektive sorteringsordning vid rapportutskrift kan anges.

5.2.2 Utforma övergripande anvisningar för väsentliga delar av informationssäkerhetsarbetet.

Mallregelverket innehåller markeringen < > i många fall. Avsikten är att på detta sätt markera där respektive organisation skall ange sina uppgifter. Katalogdel Anvisning 2 innehåller många områden där organisationens egna anvisningar för skyddsåtgärder, rutiner etc. bör utformas. I ett antal fall finns dock exempel på vad som dessa anvisningar bör omfatta eller vad som bör vara styrande för den egna utformningen.

5.2.3 Klassificera informationsobjekt och ange tillämpliga skyddsnivåkrav.

Klassificering av informationsobjekt (system, register, databas eller annan forma av informationsresurs) sker med utgångspunkt att information och informationsbehandling är skyddsvärda resurser för den aktuella verksamheten. Klassificering görs med inriktning på tre områden:

- Sekretess.
- Riktighet.
- Tillgänglighet.

I modellen tillämpas tre nivåer där 3 är den högsta. Nivåbestämningen utgår från bedömd skada vid obehörig åtkomst, brister i riktighet eller informationskvalitet och bristande tillgänglighet av information och/eller systemtjänster. Nivå 1 innebär ingen eller ringa skada och nivå 3 innebär allvarlig skada.

Nedanstående matris för skyddsnivåklassificering är tänkt som ett hjälpmedel vid diskussion och förslag till klassificering.

Klassificering föregås lämpligen av en hot-, riskanalys som anger konsekvenser för att bedöma skadenivån för det aktuella objektet.

N	Sekretess	Riktighet	Tillgänglighet
3	IT-system eller informationsobjekt som innehåller känslig information som om den kommer i orätta händer kan medföra **allvarlig skada**. Skadenivå sätts genom *riskanalys*. Generellt tillämpligt: 1. IT-system med information som är/kan bli/ föremål för sekretess enligt sekretesslagen. (exempelvis 5:1-3, 6;2, 7:11, 7:18, och 7:31, 8;10) 2. IT-system med information som kan bli föremål för tillämpningskrav enligt särskild lagstiftning inom organisationens verksamhetsområde (t.ex. socialförsäkringslagstiftning, patientjournallagen). *(Sekretesslagen 2;1 och 2;2 förhållande till främmande makt och krav på försvarssekretess omfattas ej utan behandlas särskilt).*	Oriktig information kan medföra **allvarlig skada**. Skadenivå sätts genom *riskanalys*. Generellt tillämpligt: 1. IT-system eller informationsobjekt med särskilt höga krav på riktighet. T.ex. där personligt ansvar uppenbart kan utkrävas vid felaktigheter. (Ekonomiadministrativa system, behandling av personuppgifter etc.) 2. IT-system eller informationsobjekt för kritiska processer i verksamheten.	IT-system eller informationsobjekt som ingår i eller stöder kontinuerlig verksamhet där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå i produktionen med alternativa metoder och procedurer. Avbrott kan medföra **allvarlig skada**. Generellt tillämpligt: 1. För verksamheten mycket kritiska IT-system eller informationsobjekt. 2. E-tjänster mot allmänhet och andra intressenter med krav på mycket hög servicenivå.
2	IT-system eller informationsobjekt innehåller känslig information som om den kommer i orätta händer kan medföra **skada**. Skadenivå sätts genom *riskanalys*. Generellt tillämpligt för: 1. Information där information skall föregås av menprövning. 2. Personuppgifter i allmänhet eller som enligt PUL är att betrakta som känsliga. 3. Information som kan bli föremål för sekretess. 4. Information som styrs av verksamhetsspecifik lagstiftning. 5. Uppgifter av intern karaktär vilka, utan andra restriktioner, endast egen personal bör ha tillgång till.	Oriktig information kan medföra **skada**. Generellt tillämpligt: 1. IT-system eller informationsobjekt som omfattas av lagrum där riktighetskrav anges (t.ex. PUL, eller speciallagstiftning). 2. IT-system eller informationsobjekt som ingår i myndighetsutövning. 3. Information eller tillämpningar där krav på spårbarhet eller oavvislighet föreligger.	IT-system eller informationsobjekt som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada**. Generellt tillämpligt: 3. IT-system eller informationsobjekt som ingår i eller utgör stöd för myndighetsutövning och/eller kärnverksamhet. 4. E-tjänster mot allmänhet och andra intressenter.
1	IT-system eller informationsobjekt som endast innehåller information som är offentlig allmän uppgift eller information som om den kommer obehöriga till del medför **ingen skada**. Information som är avsedd för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser.	Oriktig information kan endast medföra **ringa eller ingen skada**.	IT-system eller informationsobjekt där verksamhetsberoendet är lågt och avbrott endast kan medföra **ringa eller ingen skada**.

När diskussionen lett fram till en uppfattning om nivåer S1-3, R1-3 och T1-3 anges dessa i inmatningsformuläret ”Utskrift av krav enligt skyddsnivå-

klassificering” varpå en lista över säkerhetskrav presenteras. Denna lista kan sedan tjäna som kontrollinstrument av systemets eller informationsobjektets aktuella läge eller utgöra en kravlista vid utveckling/upphandling av ett nytt system etc.

Riskanalys och klassificering görs av eller i medverkan av verksamhetsansvarig och/eller systemägare.

5.2.4 Mallregelverkets utformade rapporter

Access har en relativt väl utvecklad rapportgenerator som medför att informationen enkelt kan skräddarsys för att passa många behov.

Följande rapporter kan väljas från menyformuläret i mallregelverket:

Namn	**Innehåll**
Regler i LIS-ordning (urval av katalogdelar)	Formulär som styr innehållet i en rapport som presenterar kravtexter för en eller flera katalogdelar.
Regler enligt skyddsnivåklassificering	Formulär där nivå enligt skyddsnivåklassificering anges för rapportutskrift av aktuella säkerhetskrav.
Regler enligt kravinriktning	Kravtexter som kopplats med hjälp av angivna attribut under kravinriktning. I mallregelverket anges ”Drift”, ”Internet” och ”Behörighet” som exempel.
Regler enligt roller	Formulär som ger möjlighet att välja kravtexter som kopplats till en eller flera roller.
Ledningssammanfattning	Ett exempel på ett urval av regler som kan vara intressanta för exempelvis en verksamhetsledning. Kan också användas för att ange någon form av Informationssäkerhetsstrategi. För denna sammanfattning finns inget särskilt formulär utan textinmatning sker direkt i databastabellen ”Kravkatalog” kolumn ”Kravsammanfattning”
Komplett utskrift regelverk i LIS-ordning	Ger en utskrift av hela regelverket med standardens kapitelindelning. En komplett version av mallregelverket finns at hämta hem i pdf-format.

5.3 Sammanfattning - OffLIS i det kontinuerliga informationssäkerhetsarbetet.

OffLIS är framtaget för att underlätta, främst för offentlig verksamhet att införa och driva informationssäkerhetsarbete enligt SS-ISO/IEC 17799. Även om OffLIS vid tillkomsten varit inriktad på 24-timmarsmyndighetsutvecklingen kan verktyget med fördel användas för all offentlig förvaltning.

Lägsta nivån för informationssäkerheten i en organisation bestäms av

- analyser av risker för verksamheten,
- legala krav och myndighetsrekommendationer (Tryckfrihetsförordningen, Sekretesslagen, Säkerhetsskyddslagstiftningen, Personuppgiftslagen, registerlagar, Arkivlag, Riksarkivets föreskrifter, KBM: s rekommendation BITS etc.),
- avtal som organisationen ingått och
- särskilda principer som organisationens ledning har fastställt, t.ex. SS-ISO/IEC 17799.

För den enskilde medarbetaren, med ansvar för att verksamheten lever upp till den lägsta nivån, är det viktigt att organisationen har så få regelverk som möjligt med liknande krav. Tillämpning av den säkerhetsprocess som OffLIS mallregelverket beskriver medför att övergripande krav från offentlighetslagstiftning, Personuppgiftslagen (PUL) och myndighetsrekommendationer i annan form t.ex. Krisberedskapsmyndighetens BITS innefattas av det egna regelverket.

Följer man den säkerhetsprocess som beskrivs av standardens PDCA-cykel kan OffLIS tillämpas enligt nedan.

5.3.1 Plan

Med verksamhets-, nuläges- och riskanalys som grund upprättas informationssäkerhetspolicy, fastställs ansvar, roller och organisationsstruktur. Det övergripande regelverket produceras, fastställs och läggs in i en organisationsunik version av OffLIS utifrån vald katalogindelning.

OffLIS innehåller malldokument och inriktningsförslag till organisationsstruktur och rollbeskrivningar samt ett förslag till skyddsnivåklassificering av informationstillgångar som är anpassat för offentlig verksamhet.

Här fastställs också ett arbetssätt och metod för att kontinuerligt arbeta med riskanalyser och riskhantering.

5.3.2 Do

Riskanalys och skyddsnivåklassificering ger underlag för säkerhetskrav på informationstillgångar. OffLIS erbjuder en formaliserad klassificeringsprocess.

Klassificeringsprocessen kan t.ex. innehålla följande aktiviteter:

1) Beskrivning och avgränsning.
   - Informationen används för de förteckningar en offentlig verksamhet är skyldig att hålla.

2) Notering av ansvarsförhållanden.
   - Vem är ”informationsägare/systemägare” etc. för tillgången

3) Notering av ”externa krav”
   - Innehåller informationstillgången allmän handling?
   - Finns legala krav på informationstillgången? (Sekretesslagen, PUL etc.)
   - Finns avtal med extern organisation som styr kraven på informationstillgången? (Nyttjanderättsavtal, EDI-avtal, Certifikatpolicies etc.)

Skyddsnivåklassificering enligt fastställd mall (förslag finns i OffLIS). Organisation, skyddsåtgärder och rutiner fastställs och införs.

OffLIS innehåller förslag till regelverk där organisationsspecifika förhållanden som måste anpassas är markerade.

Regelverket är databasbaserat och reglerna är mappade både mot informationssäkerhetsarbetets roller och mot aktiviteter. Dokumentationen kan därför lätt anpassas till aktuellt behov vid utbildning och information.

5.3.3 Check

För att forma en modell för uppföljning som är relevant är det lämpligt att den anpassas till den struktur och rollindelning som regelverket i OffLIS följer. Ett annat förslag kan vara att strukturera uppföljning utifrån kategorier av tillgångar som identifierats som skyddsvärda, t ex information, anläggningar, persona etc.

Modellen bör innebära kontinuerlig uppföljning av

- ”kvantitativt informationssäkerhetsarbete” - att informationssäkerhetsarbetet genomförs dvs.;
    - tillgångar klassificeras (och därmed skyddsnivån fastställs),
    - bristerna dokumenteras och
    - åtgärder planeras och införs.
- ”kvalitativt informationssäkerhetsarbete”;
    - att informationstillgångar defacto har de skydd regelverket föreskriver och
    - verksamheter har den kunskap och de rutiner som krävs.

Organisationen beslutar om genomförande av kontinuerlig uppföljning och kontroll av informationssäkerheten. Detta skall också omfatta återkommande riskanalyser och skyddsnivåklassificering enligt OffLIS modell för alla informationstillgångar, t.ex. vart tredje år.

För att effektivisera och förenkla för de som ska genomföra uppföljningen kan Dataföreningens verktyg SBA Check eller motsvarande användas. I detta verktyg kan egna checklistor skapas, det är också möjligt att automatgenerera rapporter. Det finns möjlighet att skapa centrala mallar/checklistor som alla i en organisation kommer åt, samtidigt som användaren också kan skapa sina egna. Det går också att styra en granskning/ett uppföljningstillfälle till att enbart omfatta en delmängd av frågorna, t ex om man vill fokusera på ett visst område. Det faktiska upplägget i SBA Check utifrån struktur i OffLIS utgörs då i verktyget av databaser, domäner och sektioner. Under respektive sektion finns sedan ett antal kontrollpunkter.

Organisationer som använder verktyg för uppföljning, SBA Check eller likvärdigt, kan enkelt importera[1] OffLIS-databasens krav i sitt verktyg och därigenom automatisera processen ytterligare.

Resultat från uppföljningsaktiviteterna:

- Upprättad ”bristlista”

  OffLIS krav på informationstillgångar är samtliga hänförda till en viss nivå i skyddsnivåklassificeringen. Med hjälp av OffLIS databas tar man enkelt fram en förteckning över exakt de krav som ställs för ett objekt med aktuell skyddsklassnivå. Därefter kan informationsobjektets

[1] Myndigheter och annan offentlig verksamhet som använder SBA Check kan erhålla verktyg för import från Luftfartsverket.

skyddsåtgärder enkelt jämföras med kraven och en bristlista upprättas.

- Upprättat protokoll över skyddsnivåklassificeringen och bifogad bristlistan.

Tekniken med att generera kravförteckningar ur OffLIS kan även användas för roller, verksamheter etc. Observera även nyttan av att genomföra skyddsnivåklassificering på planerade informationstillgångar, t.ex. nya system och kunna generera för tillgången anpassade kravförteckningar ur OffLIS databas.

5.3.4 Act

Genomföra korrigerande åtgärder.

Komplettera och utveckla regelverket.

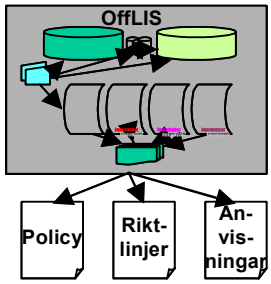
Med bristlistor enligt ovan förenklas för de ansvariga att planera vidareutveckling av rutiner och skyddsåtgärder.

De sammanställda protokollen från skyddsnivåklassificeringen ger informationssäkerhetsansvariga en god bild av organisationens informationstillgångar och utgör underlag för anpassning av regelverket.

Sammanfattning/exempel – OffLIS i säkerhetsprocessen

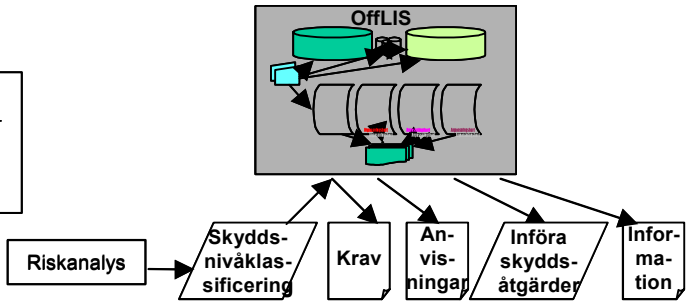
Plan

Med verksamhets-, nuläges- och riskanalys som grund upprättas informationssäkerhetspolicy och övergripande regelverk.
Struktur och rollindelning enligt behov



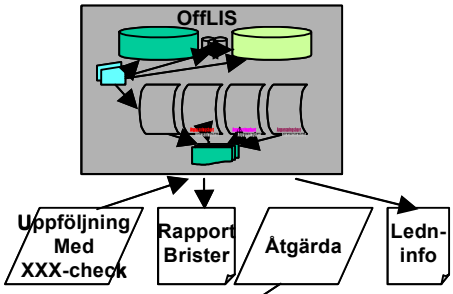
Do

Riskanalys och skyddsnivåklassificering ger underlag för säkerhetskrav på informations-objekt (system e.dyl.)
Dokumentation av skyddsåtgärder och rutiner.
Införande av skyddsåtgärder och rutiner.



Check

Kontinuerlig uppföljning mot regelverket av införda åtgärder i system och verksamhet t.ex. med hjälp av SBA Check – ger åtgärdsprogram.



Act

Genomföra korrigerande åtgärder.
Komplettera och förbättra regelverket.