Myndigheten för samhällsskydd och beredskap

SWEDISH STANDARDS INSTITUTE

Modell för klassificering av information

Rekommendationer

Version 1.0

Kontaktpersoner:
Per Oscarson, MSB: per.oscarson@msbmyndigheten.se
Wiggo Öberg, MSB: wiggo.oberg@msbmyndigheten.se
Bengt Rydstedt, SIS: bengt.rydstedt@sis.se

Modell för klassificering av information, Version 1.0, 2009-05-25
Publikationsnummer: MSB 0040-09

Förord

Information i alla dess former är en viktig tillgång i samhället som behöver lämpligt skydd. Framväxten av ett samhälle som i ökad omfattning bygger på att information hanteras elektroniskt skapar behov av modeller och metoder för att lägga grunden till detta skydd.

Regeringens handlingsplan för utvecklingen av en elektronisk förvaltning anger informationssäkerhet och säkerhet vid elektroniskt informationsutbyte som särskilt viktigt. Om information skall utbytas och förmedlas säkert måste det finnas gemensamma modeller för att värdera information för att så långt det är möjlig skapa skyddsnivåer som överensstämmer.

I den handlingsplan för informationssäkerhet som förvaltas av Myndigheten för samhällsskydd och beredskap (MSB) återfinns kapitlet ”Informationssäkerhet i verksamheter”. Ett flertal av åtgärdsförslagen i kapitlet innebär att MSB, i samverkan med myndigheter och andra organisationer, tillhandahåller stöd som underlättar informationssäkerhetsarbetet och att tillämpa LIS (Ledningssystem för Informationssäkerhet – SS-ISO/IEC 27001 och SS-ISO/IEC 27002), som sedan 1 januari 2008 är föreskrivet för statliga myndigheter.

Grundläggande informationssäkerhet är ett projekt som hanterar några av dessa åtgärdsförslag. Denna modell för klassificering av information är ett första resultat av projektet och ges ut av Myndigheten för samhällsskydd och beredskap (MSB) tillsammans med Swedish Standards Institute (SIS). Projektgruppen som har tagit fram modellen består av följande personer:

Per Oscarson (projektledare), Helena Andersson, Bengt Janulf, Roger Karlsson, Bertil Lindberg och Wiggo Öberg, KBM/MSB, Jan-Olof Andersson, Läkemedelsverket, Ulf Ekengren, och Göran Hägnemark, Meile AB, Dan Larsson, FRA, Bengt Rydstedt, SIS, Mats Ohlin och Dag Ströman, FMV, Lars Söderlund, Alliansor AB samt Fredrik Karlsson, Örebro universitet.

Detta är en första version av modellen. Efter praktisk tillämpning i verksamheter kan modellen komma att revideras utifrån gjorda erfarenheter. Modellen kan i framtiden även bli en grund för enhetliga riktlinjer för säkerhetsåtgärder för de olika klasser av information som definieras i modellen.

I enlighet med handlingsplanen planeras en mer utförlig vägledning och metod för att stödja organisationers hantering av informationstillgångar (inventering, värdering, klassificering m m) i syfte att stödja organisationers arbete med att tillämpa LIS.

Stockholm i maj 2009

Wiggo Öberg, MSB
Tf. Chef, informationssäkerhetsenheten

Bengt Rydstedt, SIS
Projektledare TK 318, informationssäkerhet

Innehållsförteckning

1. Klassificering av information

Klassificering av information är en grundläggande aktivitet för att information och resurser ges nödvändigt skydd. Det är informationen som är skyddsobjektet, d v s det som ska skyddas.

Information av olika slag är en viktig tillgång för en organisation. Enligt SIS Handbok 550 är informationstillgångar en organisations information och de resurser som används för att hantera informationen, t ex programvaror, tjänster och fysiska tillgångar. Klassificeringsmodellen som presenteras här behandlar den primära delen av tillgångarna, d v s informationen i sig. Av praktiska skäl kan dock system och andra resurser klassificeras, t ex om dessa är starkt knutna till viss information.

Informationen ska klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer etc.

1.1 Kriterier för klassificeringen

Klassificering av information görs utifrån flera kriterier. De kriterier som tas upp i LIS (d v s SS-ISO/IEC 27000-serien) är värde, legala krav, känslighet och betydelse för organisationens verksamhet. Även andra kriterier kan dock vara relevanta för den egna organisationen.

1.2 Konsekvensnivåer

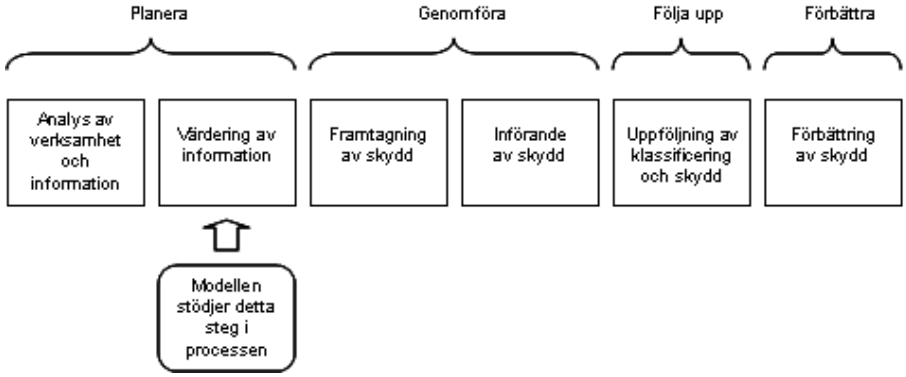
I modellen klassificeras information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet bedöms leda till. Konsekvenserna värderas i termer av oönskad påverkan på verksamheten eller annan part till följd av otillräcklig konfidentialitet, riktighet eller tillgänglighet. Om exempelvis organisationen lider allvarlig skada av att viktig information för verksamheten blir tillgänglig för obehöriga, ska informationen placeras i en klass med hög konsekvensnivå avseende konfidentialitet.

1.3 Del i ledningssystemet

Den här beskrivningen överensstämmer med ledningssystem enligt SS-ISO/IEC 27001. Vid upprättande av ett ledningssystem (d v s planeringsfasen i PDCA-cykeln[1]) är ett huvudsteg att hantera organisationens risker. Den processen beskrivs översiktligt i SS-ISO/IEC 27001. I standarden för riskhantering (SS-ISO/IEC 27005) finns en något mer utförlig vägledning för identifiering och värdering av informationstillgångar, vilket är en viktig del i

[1] Med PDCA-cykeln avses processen Plan-Do-Check-Act enligt ledningssystem för informationssäkerhet, SS-ISO/IEC 27001 (Planera-Genomföra-Följa upp-Förbättra).

denna process. I figur 1 återfinns en översiktlig illustration av var klassificering av information återfinns i informationssäkerhetsprocessen enligt LIS.



Figur 1: Klassificeringen i informationssäkerhetsprocessen

Klassificeringen kan även fungera som ett stöd och beslutsunderlag vid motivering av investeringar inom informationssäkerhet för en organisations verksamhetsledning.

2. Modell för klassificering av information

Modellen avses utgöra grund för angivandet av lämpliga säkerhetsåtgärder anpassade till respektive informations värde och utgör alltså en förutsättning för att likvärdig information ges ett konsistent skydd, oavsett var eller i vilken organisation den förekommer.

2.1 Säkerhetsaspekter

Klassificeringsmodellen omfattar de tre informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Det finns i Sverige två allmänt vedertagna definitioner av dessa aspekter: i SIS Handbok 550 och i SS-ISO/IEC 27001. Modellen kan användas med utgångspunkt från definitionerna i båda dessa dokument, se tabell nedan.

Säkerhetsaspekt	**SIS Handbok 550**	**SS-ISO/IEC 27001**
Konfidentialitet	Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga	Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter, eller processer
Riktighet	Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
Tillgänglighet	Skyddsmål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid	Egenskapen att vara åtkomlig och användbar vid begäran av behörig enhet

Andra aspekter kan givetvis förekomma i en organisations klassningsarbete, såsom spårbarhet, oavvislighet mm, men behandlas inte i denna generella modell. Spårbarhet kan exempelvis både ses som en särskild aspekt för klassificering och som en säkerhetsåtgärd för att tillgodose krav på konfidentialitet och riktighet.

2.2 Konsekvensnivåer

I denna modell anges informationens värde genom att relatera den till konsekvensen som förlust av, otillåten spridning av eller annan skada på informationen, leder till. Varje säkerhetsaspekt (konfidentialitet, riktighet, tillgänglighet) är i modellen värderad i en av tre nivåer av sådana konsekvenser: **måttlig**, **betydande** respektive **allvarlig** nivå.

I ett senare steg (efter riskanalysen där hänsyn tagits till sannolikheten för olika hot) utgör konsekvensnivåerna ett av de primära ingångsvärdena vid bedömningen av vilka krav som bör ställas på skyddet av information.

Måttliga konsekvenser

Definition:
Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär **måttlig** negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ.

Förklaring:
Med måttlig negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en minskning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamhetens primära uppgifter kan fullföljas, men att effektiviteten är påvisbart reducerad; b) resultera i mindre skador på verksamhetens tillgångar; c) resultera i smärre ekonomiska förluster; d) förorsaka begränsad negativ påverkan på enskild individs rättigheter eller hälsa.

Betydande konsekvenser

Definition:
Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär **betydande** negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ.

Förklaring:
Med betydande negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en signifikant minskning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamhetens primära uppgifter kan fullföljas, men att effektiviteten är påtagligt reducerad; b) resultera i betydande skador på verksamhetens tillgångar; c) resultera i betydande ekonomiska förluster, eller d) förorsakar betydande negativ påverkan på enskild individs rättigheter eller hälsa.

Allvarliga konsekvenser

Definition:
Förlust av konfidentialitet, riktighet eller tillgänglighet hos information som innebär **allvarlig** eller katastrofal negativ påverkan på egen eller annan verksamhet och dess tillgångar, eller på enskild individ.

Förklaring:
Med allvarlig/katastrofal negativ påverkan avses t ex förlust av konfidentialitet, riktighet eller tillgänglighet som för egen eller annan verksamhet kan a) orsaka en allvarlig begränsning i förmågan att lösa verksamhetsuppgifterna i en utsträckning och varaktighet innebärande att verksamheten inte kan fullgöra en eller flera av sina primära uppgifter; b) resultera i omfattande skador på verksamhetens tillgångar; c) resultera i stora ekonomiska förluster, eller d) förorsakar allvarligt negativ påverkan på enskild individs rättigheter eller liv och hälsa.

Det bör noteras att konsekvenser som uppstår externt, utanför den egna organisationen (”annan verksamhet”) skall tas med vid bedömningen. Detta är särskilt aktuellt för information som är kritisk för olika typer av samhällsviktiga funktioner.

2.3 Klassificeringsmodellen i matrisform

Säkerhetsaspekt Konsekvensnivå	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar*	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. **	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. **

* Då information som bedöms höra till denna nivå inte medför någon eller endast försumbar negativ påverkan, är det inte nödvändigt att genomföra någon risk- och hotanalys i senare skeden. Av samma anledning blir information som hör till denna nivå inte föremål för några särskilda skyddsåtgärder. Nivån finns med i modellen för att den ska vara komplett och omfatta alla olika typer av information.

** Denna klassning kan förväntas vara mycket sällsynt.

3. Tillämpning av modellen

Tillämpning av modellen innebär att verksamheten placerar in sin information i de olika konsekvensnivåerna. Varje typ information ska klassificeras i en av konsekvensnivåerna för varje säkerhetsaspekt (konfidentialitet, riktighet, tillgänglighet). Notera att varje säkerhetsaspekt skall klassificeras separat; en viss informationstyp kan alltså ges olika konsekvensnivå för respektive aspekt. Möjlighet till, och risker vid, aggregering av information (i synnerhet när det gäller hänsyn till konfidentialitet) bör beaktas och är ofta starkt beroende av berörda, förekommande informationstyper.

Strävan är att åstadkomma en konsistent bedömning av en och samma informations värde – oavsett var (eller hos vilken organisation) informationen hanteras. Ansvaret för den slutliga bedömningen av säkerhetsåtgärder och accepterande av kvarstående risker ligger som alltid på den informationshanterande organisationen.

Tillgänglighet är normalt ett verksamhetskrav. Utan tillgång till för verksamheten nödvändig information kan organisationsuppgifterna inte fullgöras. Normalt skapas tillgänglighet genom olika tekniska och/eller administrativa åtgärder baserade på extra kopior, redundant lagring etc. Det är normalt inte rimligt att märka enskilda informationsmängder med någon typ av tillgänglighetsmärkning. Däremot leder de övergripande verksamhetskraven på tillgänglighet, i ett senare skede, till krav på specifika egenskaper hos de informationshanterande systemen. Det är därför viktigt att kunna identifiera de olika *informationstyper* som förekommer i verksamheten och därefter (för varje typ) ange på vilken nivå tillgänglighetsbehovet ligger.

Notera att förlust av tillgänglighet kan graderas. Förlust kan uppstå genom fördröjning (där tidsgränser för allvarlig, betydande etc. är beroende av sammanhanget) eller genom att information förstörts.

Behov av att säkerställa spårbarhet föreligger ofta i de realiserade systemen. Spårbarhetskrav finns tydligast i samband med hanteringen av konfidentiell information, men också ofta när det gäller krav på riktighet. Liksom vad gäller tillgänglighetskraven, säkerställs spårbarhet normalt genom olika kontrollåtgärder i systemen, t ex genom loggning och oavvislighetsfunktioner.

Mer utförliga exempel för hur vanliga informationstyper kan klassificeras kommer att beskrivas i en separat vägledning. Även vägledningar för val av säkerhetsåtgärder och riskhantering planeras.

3.1 Mottagare av modellen

Huvudansvaret för en organisations hantering av information ligger alltid ytterst hos organisationsledaren. Denne eller denna delegerar normalt ut uppgifter till internt ansvariga för olika funktioner. Nyckelroller vid användning av klassificeringsmodellen är verksamhetsansvarig, informationsägare, funktionsföreträdare eller motsvarande, eftersom dessa normalt är ansvariga för att information inom deras verksamhetsansvar får en korrekt klassificering.

Att tillämpa modellen kan också vara ett verktyg för att öka förståelsen och medvetenheten hos olika aktörer i en verksamhet. En viktig mottagare är de individer som arbetar med att anskaffa och/eller bygga system som skall stödja verksamheten. Att förankra modellen med tillhörande riktlinjer, lathundar och liknande hos medarbetare, är ett viktigt led i att nå en hög kvalitet i hantering av verksamhetens information.

3.2 Vad ska klassificeras?

Modellen förutsätter att all information som hanteras inom myndigheten skall klassificeras. Här åsyftas inte att i varje situation klassificera varje enskilt informationsobjekt/dokument. I stället bör den inledande identifieringen syfta till att identifiera de grupper eller huvudtyper av den hanterade informationen. Syftet är att undvika att man av misstag inte tar med vissa typer av information.

Modellen utgår från information som det primära skyddsobjektet och det som ska klassificeras. Det är informationen som har det primära värdet för organisationen och det är detta värde, uttryckt som konsekvensnivå, som tillsammans med och riskanalysen skall styra i vilken grad och på vilket sätt informationen ska skyddas.

3.3 Juridiska aspekter

Modellen är generell och definierar inte legala krav i specifika klasser. I enlighet med LIS är legala krav ett av flera ingångsvärden vid klassificering av information. Legala krav kan styra krav på alla de tre säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

Exempel:

- krav på *konfidentialitet* i 9 kap 7 § Lag (2007:1091) om offentlig upphandling,
- krav på *riktighet* i 6 § Arkivlagen (1990:782), och
- krav på *tillgänglighet* i 2 kap 1 § Tryckfrihetsförordningen (1949:105)

Konfidentialitet innebär att ingen obehörig ska ha åtkomst till informationen. Konsekvensnivån med avseende på konfidentialitet har inget annat syfte än att vara ingångsparameter vid bedömning av skyddsbehov. Det ska inte jämställas med ett beslut att sekretess enligt sekretesslagen (1980:100) gäller för en viss

informationsmängd. Sådan rättslig sekretessprövning skall alltid göras i samband med begäran om utlämning av informationen.

Detta innebär dock inte att man ska bortse från sekretesslagens bestämmelser. Information som bedöms kunna komma att ges sekretesskydd enligt sekretesslagen bör hanteras med försiktighet för att myndigheten inte skall riskera att bryta mot sekretesslagens krav på konfidentialitet om lagen visar sig vara tillämplig. Information som kan sekretessbeläggas enligt sekretesslagen har generellt sett ett högt skyddsvärde när den exempelvis rör rikets säkerhet, brottsbekämpning eller enskilds personliga förhållanden. Det kan även anmärkas att allmänna handlingar som bedöms troligtvis vara offentliga vid begäran om utlämning trots detta inte bör ges den lägsta konsekvensnivån (”ingen eller försumbar”) när det gäller konfidentialitet. Omständigheterna i det enskilda fallet kan göra att även till synes harmlös information kan komma att få sekretesskydd.[2]

Det bör också noteras att Förordningen om intern styrning och kontroll (2007:603) ställer generella krav på en myndighet och dess förmåga att leva upp till sitt förvaltningsansvar. Dessa krav bör därför kunna relateras till de säkerhetsåtgärder som följer av nivån ”måttlig”.

3.4 Tidsaspekten

Organisationen och dess omvärld förändras ständigt och organisationens information likaså. Nytt innehåll i eller ny prioritering av verksamheten kan få konsekvenser för värdering och klassificering av information. Detta ska ses som en ständig förbättringsprocess i likhet med allt säkerhetsarbete. Viss information är av sådan typ att den vandrar mellan olika klasser i modellen över tiden, exempelvis upphandlingsinformation. Det är upp till ansvarig informations-, systemägare eller motsvarande att tillse att information är värderad på rätt sätt vid varje tidpunkt.

[2] Detta gäller exempelvis om man har anledning att anta att utlämnandet av en personuppgift skulle medföra att uppgiften behandlas i strid med personuppgiftslagen (1998:204), se 7:16 sekretesslagen.

MSB Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msbmyndigheten.se
Publ.nr MSB 0040-09