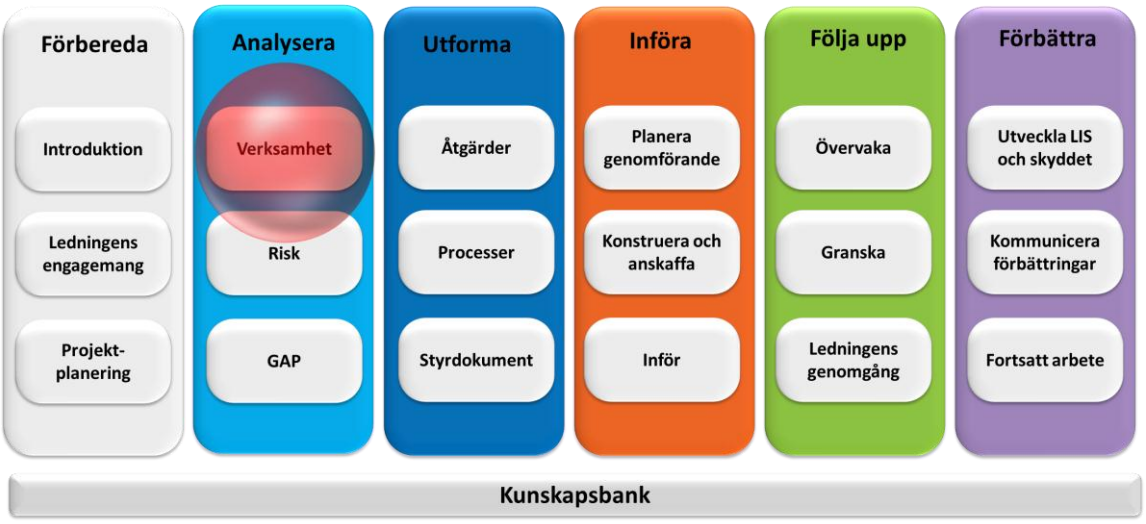
Myndigheten för samhällsskydd och beredskap

Verksamhetsanalys



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

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

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning **4**
2. Verksamhetsanalysens arbetsuppgifter **5**
2.1 Identifiering av informationstillgångar 5
Tidigare kartläggningar 5
Processkartläggningar 6
2.2 Identifiering av krav 9
Legala krav 10
Interna krav 12
2.3 Klassificering av informationstillgångar 13
Modell för klassificering 13
Princip för klassificering 13
Löpande klassificering 14
3. Nästa steg **15**
Bilaga A: Mall för att strukturera informationstillgångar **16**
Bilaga B: Förteckning över lagar **17**
Bilaga C: Interna krav **20**
Bilaga D: Klassificeringsbeslut **21**
Bilaga E: MSB:s klassificeringsmodell **22**

1. Inledning

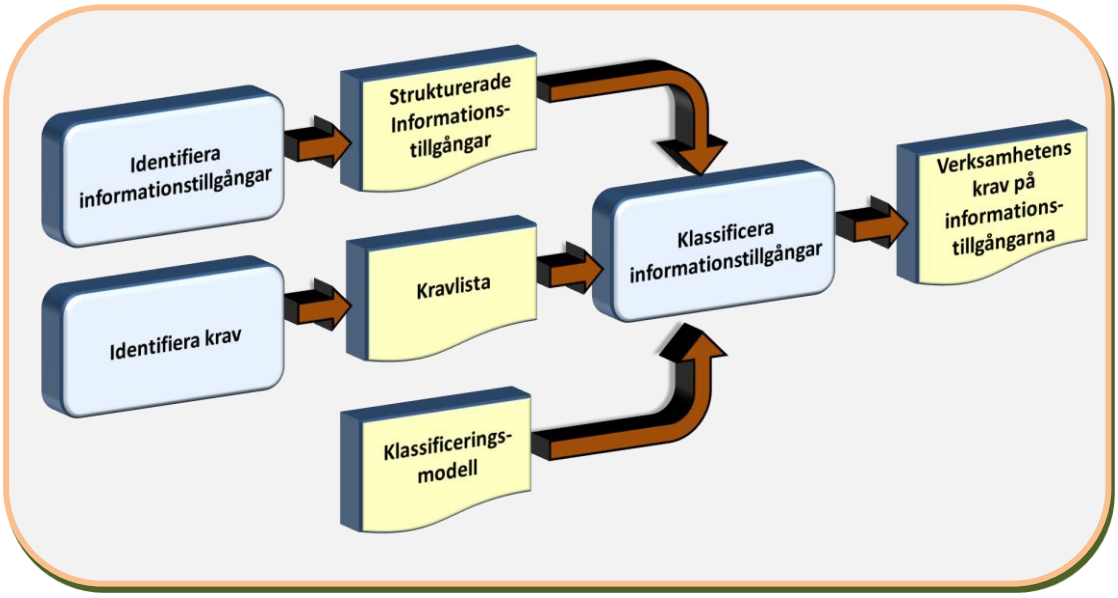
Syftet med det här dokumentet är att ge praktiska tips om hur en organisation kan göra en *verksamhetsanalys* för att identifiera och klassificera sina informationstillgångar. Klassifikationen indikerar sedan hur de olika informationstillgångarna ska hanteras.

De arbetsuppgifter som ska genomföras under verksamhetsanalysen är:

- identifiera informationstillgångarna
- identifiera kraven
- klassificera informationstillgångar.

Figuren nedan visar flödesschemat för dessa arbetsuppgifter.

Figur 1. Flödesschema för verksamhetsanalys



De två första arbetsuppgifterna, identifiera informationstillgångar och identifiera krav, kan göras parallellt och resulterar i två dokument: *strukturerade informationstillgångar* och *kravlista*. De blir i sin tur underlag till den sista arbetsuppgiften – *Klassificera informationstillgångar*.

Verksamhetsanalysen leder till en strukturerad förteckning över informationstillgångar. I förteckningen är varje informationstillgång klassificerad utifrån hur viktigt det är att informationen är *konfidentiell*, *riktig* och *tillgänglig*. Tillsammans med aktiviteten riskanalys definierar verksamhetsanalysens klassificering det skyddsbehov verksamheten har.

2. Verksamhetsanalysens arbetsuppgifter

Arbetet med informationssäkerhet går ut på att skydda sina informationstillgångar mot olika typer av hot. För att skyddet ska kunna utformas optimalt måste utgångspunkten vara kunskap om organisationens verksamhet, vilka informationstillgångar som används i verksamheten, samt vilket behov och vilka krav som finns på informationstillgångarnas informationssäkerhet.

Begreppet verksamhetsanalys används på olika sätt i olika sammanhang. I Det här dokumentet avses med verksamhetsanalys processen att *identifiera och klassificera informationstillgångar* med avseende på säkerhetskrav.

2.1 Identifiering av informationstillgångar

Verksamhetens viktigaste informationstillgångar kan dokumenteras med hjälp av mallen i Bilaga A i detta dokument. Resultatet av det arbetet används senare för att identifiera kraven på respektive informationstillgång.

Med informationstillgångar avses verksamhetens information och tillgångar relaterade till informationshantering, som IT-system, data/information, medarbetare, Internetkapacitet, etc. (se figur 2). Medarbetaren har en speciellt central roll som informationstillgång, i det att medarbetaren exempelvis tar emot, skapar, lagrar, använder, kommunicerar och avvecklar information – i huvudet, i IT-system och på papper. Många rutiner, processer och informationsflöden är odokumenterade och finns bara i medarbetarnas huvuden.

Arbetet med att identifiera informationstillgångarna börjar lämpligast med att leta reda på *tidigare kartläggningar*. Sedan går man vidare med *processkartläggningar*.

Tidigare kartläggningar

En bra början är att den som ansvarar för verksamhetsanalysen letar upp tidigare kartläggningar. Genom att rådfråga verksamhetens nyckelpersoner blir det också lättare att identifiera sådana kartläggningar. Befintliga kartläggningar kan dock vara gjorda i ett annat syfte och behöver oftast omstruktureras något. När inventeringen av tidigare kartläggningar är klar går man lämpligast vidare med processkartläggningar för att identifiera de informationstillgångar som inte tidigare är inventerade.

Figur 2. Exempel på informationstillgångar

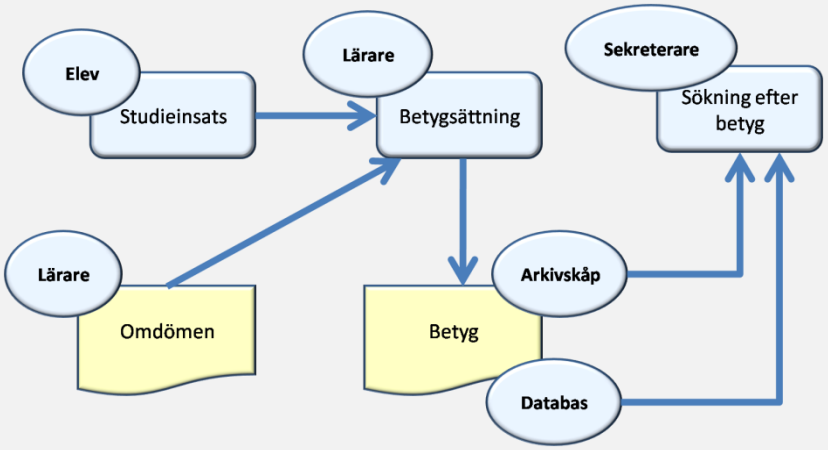
Processkartläggningar

Genom att kartlägga verksamhetens processer och notera processernas in- och utflöden får man en bra bild över alla informationsflöden. Utifrån detta är det ganska lätt att se vilka informationstillgångar som behövs för att processen ska fungera (se figur 3: exempel på verksamhetsprocess).

Det är bäst att göra processkartläggningar under en gruppdiskussion eller ett seminarium med ansvariga från verksamhetens olika delar. Tabell 1 nedan visar ett tänkbart upplägg för ett sådant seminarium. Den som inte har någon erfarenhet av processkartläggningar kan behöva läsa på lite om verksamhetsarkitektur innan arbetet börjar. Det bästa är dock att be om hjälp – kunskap finns ofta i verksamheten. Kom också ihåg att det är viktigt att komma igång. Börja enkelt och förbättra successivt.

Figur 3. Exempel på verksamhetsprocess

Exempel på process – betygsättning



I den här processen används både pappersbaserade och IT-baserade system; informationen produceras och kommuniceras manuellt, samt lagras manuellt och med stöd av IT. Denna ganska enkla process består av fyra aktiviteter:

1. Läraren tolkar elevens insats och ger omdömen som sparas i pappersform hos läraren.
2. Läraren sätter betyg utifrån sin tolkning av elevens insats samt tidigare omdömen.
3. Läraren sparar betygen både i pappersform (arkivskåp B) och digitalt (system X, databas Y).
4. Sekreteraren söker ett betyg (på begäran av till exempel en lärare eller en elev), både i pappersform (arkivskåp B) och digitalt (system X, databas Y).

Genom att beskriva och illustrera informationsflödena i verksamheten går det alltså att se vilka aktiviteter som ingår och vilka aktörer som utför aktiviteterna. Man får också en bra överblick över informationen och dess flöden, samt över de resurser som används (till exempel mjuk- och hårdvara), och olika resurser för pappershantering. Kartläggningen kan även synliggöra perifer utrustning som skrivare, dokumentförstörare och faxar, och dessutom externa resurser som webbtjänster, outsourcade tjänster och molntjänster.

Tabell 1. Exempel på ett seminarium för processkartläggning

Tid	Aktivitet
07:45–08:30	Genomgång av dagen. Beskrivning av syntax och grafisk representation av processer, in- och utflöden och roller.
08:30–10:30	Strukturerad brainstorming. Deltagarna får i tur och ordning försöka definiera verksamhetens processer. Gå bordet runt och ge varje deltagare ordet. Fortsätt ända tills det tar stopp. Man kan också inleda med en halvtimmes brainstorming i smågrupper och sedan fortsätta i hela gruppen. En tredje variant är att alla får fundera ensamma i en halvtimme innan gruppdiskussionen tar vid.
10:30–11:00	Sammanställning och gruppering av processer och delprocesser till lämplig nivå. Detta görs lämpligast av analysledaren medan övriga tar paus.
11:00–12:30	Analys av varje process där in- och utdata definieras.
13:30–15:30	Avgränsning och beskrivning av informationstillgångar. Exempel på beskrivning: ”Webbplatsens syfte är att …”,”Logistiksystemet används för att verksamheten ska kunna planera materialflödet …”, ”Biljettbokningssystemet används både av marknadsavdelningen för prognostisering samt av …”. Med avgränsning avses fysiska, juridiska, organisatoriska, tekniska och andra avgränsningar som är relevanta för att ringa in vad som är med respektive faller utanför det som analyseras och klassificeras.
15:45–17:15	Beskriv det IT-stöd som informationstillgången är beroende av. Exempel på beskrivning: ”Webbplatsen bygger på två servrar med Red Hat Linux, och webbsidorna levereras via webbservern Apache 2.0”, ”Systemet är fysiskt beläget i centrala Göteborg, i nätleverantörens lokaler …”, ”Den hårdvara som används är ler023 (192.168.1.230) och ler025 (192.168.1.231), ”Servern delas med e-postsystemet.”

Efter diskussionerna dokumenterar analysledaren informationstillgångarna på ett enkelt och begripligt sätt, se till exempel mallen i bilaga A.

Tips för seminariet

- Begränsa antalet deltagare. Är man fler än tio blir det svårare att hantera diskussionerna.
- Undvik att ”debattera” under brainstormingen. Alla behöver inte vara överens i detta skede.
- Det spelar mindre roll ifall några definierar ”små lokala” processer medan andra definierar ”stora övergripande” processer. Det löses i och med grupperingen.
- Se till att alla deltagare känner sig sedda och får komma till tals.
- Skicka ut dokumentation på remiss till deltagarna för att få in deras synpunkter.

Betydande informationstillgångar har nu identifierats och finns beskrivna med avseende på benämning, ägare, användning i verksamheten, samt IT-stöd (i enlighet med mallen i Bilaga A).

Vad som räknas som informationstillgångar, och vad verksamheten identifierar som sådana i analysen styr inriktningen på arbetet. En strategi är att rikta in sig på exempelvis bara IT-system (med information) inledningsvis för att i ett senare skede lyfta in tillgångar som exempelvis medarbetare och elförsörjning.

2.2 Identifiering av krav

För att senare kunna klassificera informationstillgångarna måste man ta reda på vilka krav som ställs på respektive tillgång. Arbetet med att hitta kraven kan delas upp på krav som kommer från avtal, lagar och förordningar, *legala krav*, och krav som verksamheten ställer för att kunna uppnå sina mål, *interna krav*.

Analysledaren kan göra mycket av den legala kravanalysen på egen hand, kanske med hjälp för att hitta lagar, förordningar, avtal och kontrakt. Ta gärna hjälp av verksamhetens jurister för att identifiera och tolka texterna.

De interna kraven är lättast att kartlägga i en gruppdiskussion eftersom den analysen kräver insikter från verksamhetens olika delar och dess behov. Deltagarna kan vara desamma som i processkartläggningen som beskrivs ovan, ifall man har gjort en sådan.

Legala krav

De legala kraven gäller främst rättsliga krav och krav som regleras av olika avtal och kontrakt. Det här är krav som *måste* vara uppfyllda. Det första steget i analysen är att samla på sig alla förordningar och kontrakt som gäller för organisationens informationssäkerhet. I bilaga B finns en förteckning över ett antal författningar. Denna förteckning är inte fullständig, utan varje organisation måste själv komplettera den beroende på sin verksamhetsinriktning. Analysledaren måste också ta del av de avtal som organisationen har ingått med andra parter. Tabell 2 kan användas för att säkerställa de legala kraven.

Vägledning

För *varje* informationstillgång och lagrum eller kontrakt gör man följande:

1. Läs igenom innehållet och betydelsen.
2. Bedöm och markera med ett kryss om författningen eller avtalet gäller för informationstillgången genom att kryssa i rutan (j/n). Innehåller författningen sådant som ställer krav på tillgångens säkerhet?
3. Motivera på vilket sätt författningen är tillämplig eller inte, och vilken information som påverkas av kravet.

Exempel på legala krav:

- En privat vårdgivare har fått kommunens uppdrag att driva ett demensboende. Kommunen kräver att företaget ska vara försiktig när det gäller hanteringen av personlig information om enskilda patienter. Ingen information får till exempel lämnas ut via telefon.
- Ett investmentföretag köper analystjänster av ett litet konsultbolag. Investmentföretaget förser konsultbolaget med konfidentiell information och kräver att bolaget aldrig flyttar okrypterad information mellan olika lagringsmedier. Nivån av kryptering regleras i avtalet.

Tabell 2. Dokumentation om vilka legala krav som gäller för respektive informationstillgång.

Författningar, avtal och andra överenskommelser	**Tillämplig**	**Motiv**
Tryckfrihetsförordningen	☐	
Offentlighets- och sekretesslagen	☐	
Personuppgiftslagen	☐	
Säkerhetsskyddslagen	☐	
Säkerhetsskydds-förordningen	☐	
Lagen om upphovsrätt till litterära och konstnärliga verk	☐	
Arkivlagen	☐	
MSB:s föreskrift om statliga myndigheters informationssäkerhet	☐	
Förordningen om höjd krisberedskap och höjd beredskap	☐	
Förordning om statliga myndigheters riskhantering	☐	
[Övrig författning]	☐	
[Avtal X]	☐	
[Avtal Y]	☐	
[Överenskommelse Z]	☐	

Interna krav

Verksamheten är beroende av att det finns ett fungerande informationsflöde mellan olika processer. Om detta informationsflöde störs finns en risk för att vissa verksamhetskritiska uppgifter inte går att utföra. De interna kraven ska beskriva dessa kritiska beroenden.

När det gäller de interna kraven måste man komma ihåg att varje verksamhet är unik och har sina specifika krav som bland annat beror på dess bransch- och sektorstillhörighet, ägandeform, uppdrag och affärsidé. Verksamhetens övergripande krav på informationssäkerhet framgår ofta i dokument som uttrycker verksamhetens vision, målsättning, affärsidé, affärsplan, värdegrund och så vidare.

För att systematiskt dokumentera verksamhetens interna krav kan man, för varje informationstillgång, använda tabell 3 och dokumentera i mallen i bilaga C.

Tabell 3. Stöd för dokumentation av interna krav

Aspekt	**Beskriv**	**Exempel på stödfrågor**
Nyttan	Utgå från användningen av informationstillgången och beskriv vilken nytta verksamheten har av den.	Vad används tillgången till? Vilka processer eller aktiviteter stöds av tillgången? Vilka mål vill man uppnå med hjälp av tillgången?
Konsekvens vid förlust av konfidentialitet	Beskriv konsekvensen om informationen röjs för obehöriga.	Vad händer om informationen läcker till • massmedier • konkurrenter • allmänheten • personalen? Hur påverkar det organisationens ”goodwill”?

Aspekt	Beskriv	Exempel på stödfrågor
Konsekvens vid bortfall av riktighet	Beskriv konsekvensen för verksamheten om informationstillgången är felaktig eller inaktuell.	Vad blir konsekvensen om en obehörig person eller process förändrar informationen? Vad blir konsekvensen om verksamheten inte upptäcker detta?
Konsekvens vid bortfall av tillgänglighet	Beskriv konsekvensen för verksamheten om informationen inte är tillräckligt tillgänglig för behöriga användare.	Vad blir konsekvensen om tillgången inte alls kan användas? Vad blir konsekvensen om tillgången endast kan användas i begränsad utsträckning eller med vissa svårigheter?

2.3 Klassificering av informationstillgångar

Nu ska de betydande informationstillgångarna klassificeras utifrån de identifierade kraven. Efter den första gången sker också klassificering därefter löpande i verksamheten vid behov.

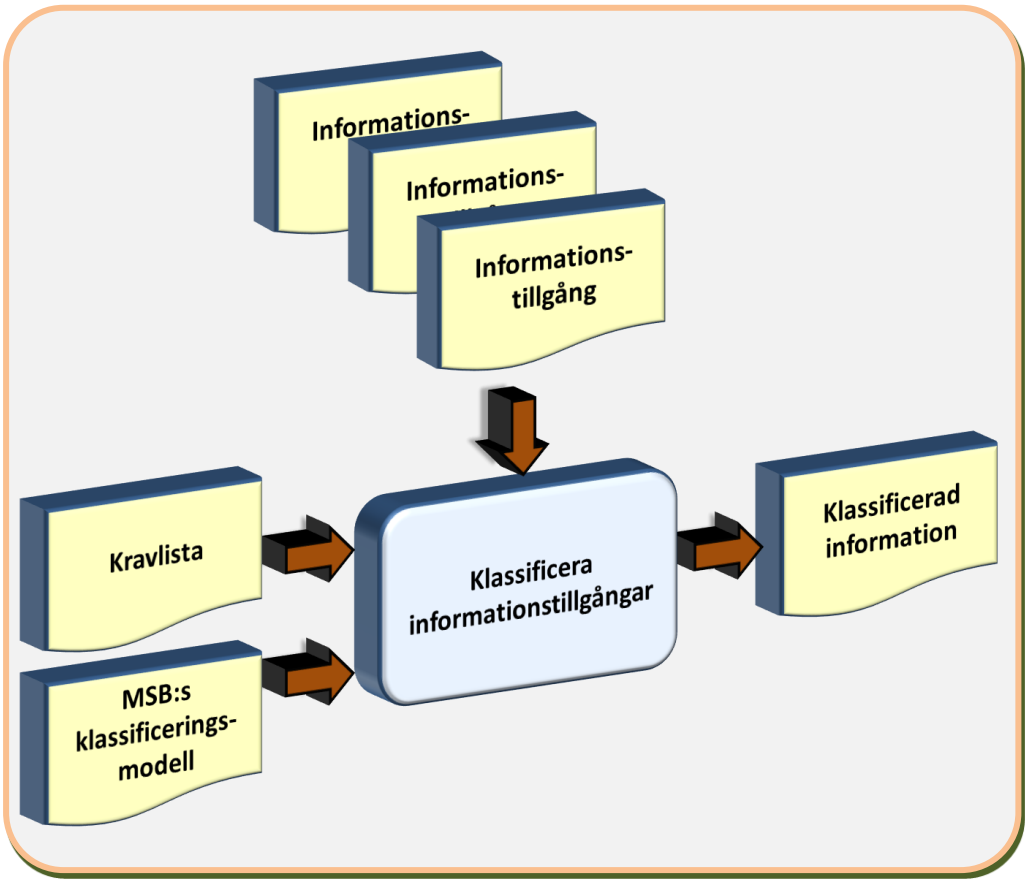
Modell för klassificering

För att klassificera sina informationstillgångar kan man använda MSBs klassificeringsmodell (se bilaga E) som kan anpassas till den egna verksamheten.

Princip för klassificering

Alla *betydande* informationstillgångar ska analyseras mot de identifierade kraven (både de interna (verksamhetens behov) och de legala för att se vilka konsekvenserna kan bli om informationen inte längre är konfidentiell, riktig eller tillgänglig (se figur 4). Man kan även klassificera efter andra aspekter, såsom ”spårbarhet”.

Figur 4. Klassificering av informationstillgångar.



Varje informationstillgång klassificeras separat med hjälp av kravlistan och MSB:s klassificeringsmodell. Varje informationstillgång klassificeras för sig. Resultatet kan dokumenteras med hjälp av mallen i bilaga D.

Slutresultatet från verksamhetsanalysen är att betydande informationstillgångar är beskrivna och klassificerade i termer av vad konsekvensen (allvarlig, betydande, måttlig, försumbar) skulle bli vid bristande informationssäkerhet.

Löpande klassificering

Både verksamheter och omvärlden förändras ständigt. En klassificering gäller inte för evigt eftersom information tillkommer, försvinner, förändras, får förändrad status, slås samman med annan information och så vidare. Därför behövs rutiner för hur förändringen ska hanteras i verksamheten. Alla informationsägare (eller motsvarande) har ansvar för att deras informationstillgång är korrekt klassificerad, och det är viktigt att de har resurser och kunskap för att klara av detta. Till exempel ska de förstå principerna för informationsklassificeringen som beskrivs ovan. De måste också kunna identifiera kraven och bedöma konsekvensnivåerna för att kunna göra lämpliga klassificeringar. För att stödja det här löpande arbetet behövs ett formulär där informationsägaren (eller motsvarande) kan svara på ett antal

frågor som leder informationstillgången till rätt klass. Formuläret kan skapas utifrån innehållet bilagorna A till E.

3. Nästa steg

När verksamhetsanalysen är klar är betydande informationstillgångar kartlagda och klassificerade. Nästa steg är att identifiera vilka hot som finns mot tillgångar och verksamhet. Detta görs i riskanalysen.

Bilaga A: Mall för att strukturera informationstillgångar

Allmänt

Benämning informationstillgång	
Datum för analys	
System-/informationsägare	

Deltagare

Namn	Roll	Kontaktinformation

Beskriv informationstillgången

Beskriv IT-stödet

Beskriv avgränsningarna

Bilaga B: Förteckning över lagar

Det kan finnas författningar som ställer krav på verksamheten i stort och på en specifik informationstillgång. Målet med denna analys är att identifiera alla de författningskrav som verksamheten måste uppfylla och som rör informationssäkerheten.

Lagrum	Innehåll
Tryckfrihetsförordningen (1949:105)	Om allmänna handlingars offentlighet: ”Till främjande av ett fritt meningsutbyte och en allsidig upplysning ska varje svensk medborgare ha rätt att taga del av allmänna handlingar.”
Offentlighets- och sekretesslagen (2009:400)	”En uppgift för vilken sekretess gäller enligt denna lag får inte röjas för enskilda eller för andra myndigheter, om inte annat anges i denna lag eller i lag eller förordning som denna lag hänvisar till [t.ex. i samband med en upphandling].”
Personuppgiftslagen (1998:204), § 31	”Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter som behandlas.” Åtgärderna ska baseras på en riskanalys.
Säkerhetsskyddslagen (1996:627)	Myndigheter, kommuner, landsting, statliga bolag etc. och även enskilda ska beakta säkerhetsskyddslagens bestämmelser för att motverka möjligheten till exempelvis sabotage, om den verksamhet som bedrivs är av betydelse för skyddet av rikets säkerhet eller särskilt måste skyddas mot terrorism.
Säkerhetsskyddsförordningen (1996:633)	De som omfattas av säkerhetsskyddsförordningen ska göra en särskild säkerhetsskyddsanalys som visar ”vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet […] och skyddas mot exempelvis sabotage. Resultatet av denna undersökning (säkerhetsanalys) skall dokumenteras”.

Lagrum	**Innehåll**
Lagen om upphovsrätt till litterära och konstnärliga verk (1960:729)	”Den som har skapat ett litterärt eller konstnärligt verk har upphovsrätt till verket”. ”Upphovsrätt innefattar, med de inskränkningar som föreskrivs i det följande, uteslutande rätt att förfoga över verket genom att framställa exemplar av det och genom att göra det tillgängligt för allmänheten”.
Arkivlagen (1990:782)	”I arkivvården ingår att myndigheten skall 1. organisera arkivet på ett sådant sätt att rätten att ta del av allmänna handlingar underlättas, 2. upprätta dels en arkivbeskrivning som ger information om vilka slag av handlingar som kan finnas i myndighetens arkiv och hur arkivet är organiserat, dels en systematisk arkivförteckning, 3. skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst, 4. avgränsa arkivet genom att fastställa vilka handlingar som skall vara arkivhandlingar, och 5. verkställa föreskriven gallring i arkivet.”
MSB:s föreskrift (2009:10) om statliga myndigheters informationssäkerhet	Myndigheter ska ”tillämpa ett ledningssystem för informationssäkerhet”. Det innebär att myndigheten ska upprätta en informationssäkerhetspolicy och andra styrande dokument, utse en informationssäkerhetsansvarig som ska rapportera direkt till myndighetsledningen minst årligen, genomföra risk- och sårbarhetsanalyser, dokumentera incidenter samt avgöra hur identifierade risker ska hanteras.
Förordning (2006:942) om krisberedskap och höjd beredskap	Myndigheter ska en gång per år ”analysera om det finns sådan sårbarhet eller sådana hot och risker […] som synnerligen kan försämra förmågan till verksamhet inom området”. Analysen ska skickas in till regeringen och MSB.

Lagrum	**Innehåll**
Förordning (1995:1300) om statliga myndigheters riskhantering	”Varje myndighet skall identifiera vilka risker för skador eller förluster som finns i myndighetens verksamhet. Myndigheten skall värdera riskerna och beräkna vilka kostnader som staten har eller kan få med hänsyn till dessa risker. Resultatet skall sammanställas i en riskanalys. Varje myndighet skall vidta lämpliga åtgärder för att begränsa risker och förebygga skador eller förluster.”
Övriga författningar:	

Bilaga C: Interna krav

Informationstillgång	

Beskriv nyttan

Beskriv nyttan

Konsekvens vid bortfall av konfidentialitet

Konsekvens vid bortfall av riktighet

Konsekvens vid bortfall av tillgänglighet

Bilaga D: Klassificeringsbeslut

Informationstillgången klassificeras i följande klasser:

Kravområde	Klass	Motivering
Konfidentialitet	☐ Allvarlig ☐ Betydande ☐ Måttlig ☐ Försumbar	
Riktighet	☐ Allvarlig ☐ Betydande ☐ Måttlig ☐ Försumbar	
Tillgänglighet	☐ Allvarlig ☐ Betydande ☐ Måttlig ☐ Försumbar	

Bilaga E: MSB:s klassificeringsmodell

Vid behov, ladda ner mer information på:

http://www.informationssäkerhet.se/Dokumentbanken/Modell-for-klassificering-av-

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

information-/