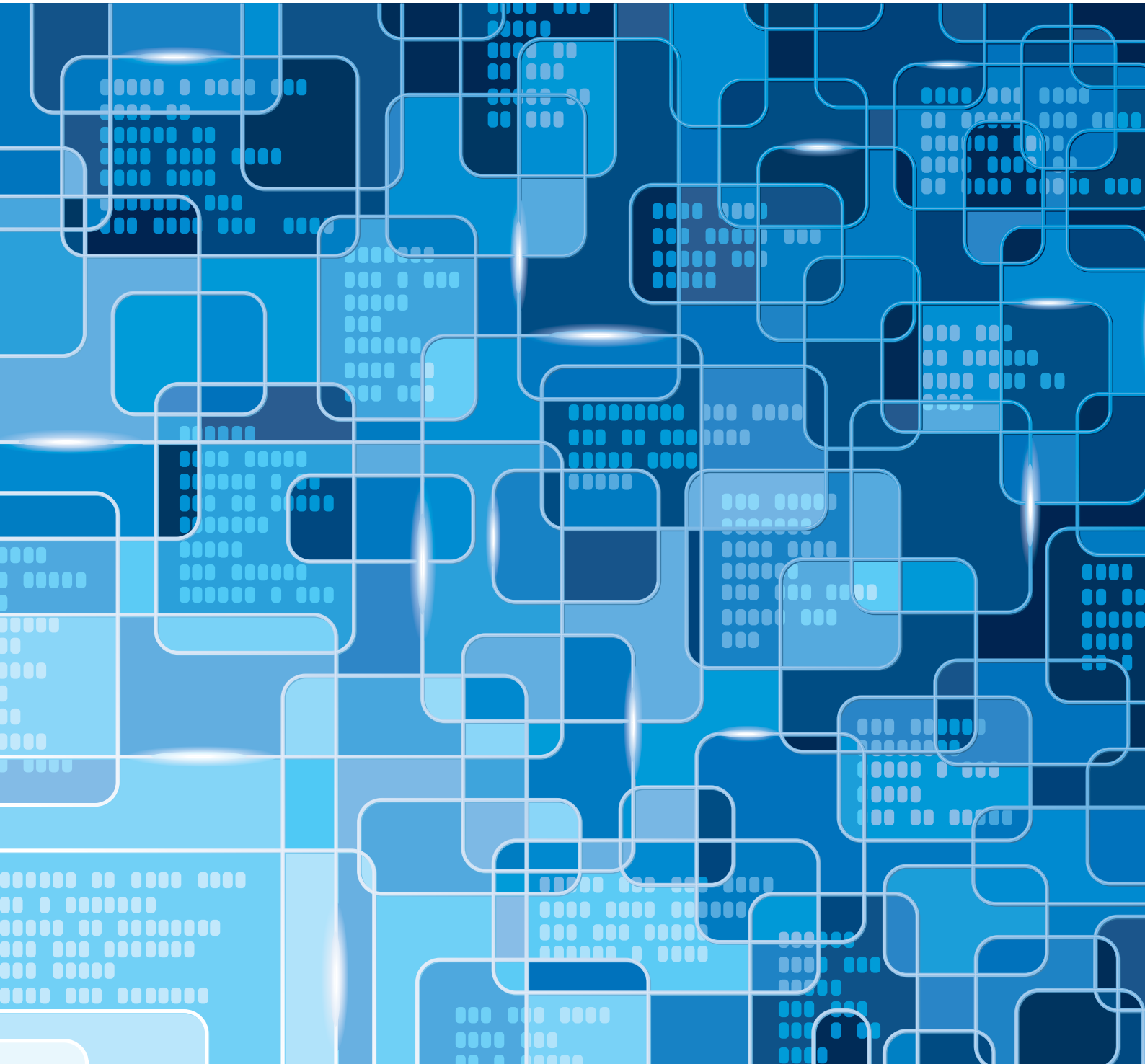
Vägledning för processorienterad informationskartläggning



Vägledning för processorienterad informationskartläggning

Vägledning för processorienterad informationskartläggning

Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet

Layout: Advant Produktionsbyrå AB
Tryckeri: DanagårdLiTHO

Publ.nr MSB493 - november 2012
ISBN 978-91-7383-291-5

Förord

I dagens informationssamhälle bearbetar, lagrar, kommunicerar och mångfaldigar vi information i större mängder än någonsin tidigare. Informationen används av myndigheter och enskilda men utgör även en resurs för samhället i stort där den i allt högre grad hanteras i gemensamma miljöer och tjänster.

Att styra sin informationshantering så att den stödjer verksamheten på ett effektivt och säkert sätt, samtidigt som hänsyn tas till kraven på arkivering, är en utmaning för de flesta organisationer idag. Ett första steg mot en bättre styrning är att skapa en tydlig bild av vilken information som organisationen är beroende av samt de system och tjänster som används för att hantera informationen.

Myndigheten för samhällsskydd och beredskap (MSB) har ansvar för att samordna samhällets informationssäkerhet. Riksarkivets främsta uppgift är att säkerställa samhällets behov av en långsiktig informationsförsörjning som garanterar innehåll, sammanhang och äkthet. I båda dessa uppdrag är en väsentlig del att ge stöd till organisationer för att identifiera och skydda information. En kartläggning av information är nödvändig för att kunna vidta rätt åtgärder för skydd och långsiktigt bevarande. För att underlätta för både myndigheter och andra organisationer att genomföra kartläggningen har MSB och Riksarkivet tillsammans tagit fram denna vägledning.

Stockholm 22 november

Helena Lindberg
Generaldirektör
Myndigheten för
samhällsskydd och beredskap

Björn Jordell
Riksarkivarie
Riksarkivet

Innehåll

Inledning

1. INLEDNING

Dagens samhälle bygger i hög grad på informationshantering. De uppgifter som utförs av företag, myndigheter, kommuner och landsting förutsätter att information inkommer, bearbetas, kommuniceras och lagras. Informationen är en värdefull resurs i den egna verksamheten, både i det dagliga arbetet och på lite längre sikt. Därutöver efterfrågas informationen av andra myndigheter, avtalspartners och andra intressenter

I lagstiftningen ställs olika krav på organisationers verksamhet och informationshantering, såväl generella som verksamhetsspecifika. Det ställs också krav från myndigheter som har ansvar för ett visst område. Här avses bland annat de föreskrifter som utfärdas av Riksarkivet och Myndigheten för samhällsskydd och beredskap (MSB).

Trots att informationshanteringen är en så viktig fråga kan det vara svårt att åstadkomma rätt grad av styrning när det gäller hur informationen ska och får hanteras. Ett första steg för att kunna skydda och effektivt nyttja den viktiga resurs som informationen utgör är att kunna analysera vilken information som organisationen hanterar och på vilket sätt det sker. Denna vägledning är tänkt att vara ett stöd för att kartlägga och analysera den information en organisation är beroende av.

Bakgrund

2. BAKGRUND

2.1 Behov av informationskartläggning

Alla organisationers verksamhet bygger idag på komplexa strukturer av informationshantering. För att kunna skapa en fungerande infrastruktur måste även informationsutbytet, internt och externt, vara identifierat och beskrivet. En tydlig bild av hanteringen behövs för att kunna bedriva ett systematiskt informationssäkerhetsarbete samt för att kunna upprätta en verksamhetsbaserad arkivredovisning. För statliga myndigheter finns krav på föreskriftsnivå gällande dels systematisk informationssäkerhet[1], dels verksamhetsbaserad arkivredovisning[2], men även för organisationer utan krav från föreskrifter är det en fördel att genomföra kartläggningar av sådana informationsflöden.

Informationshanteringen tenderar att bli allt mer komplex. Detta beror inte enbart på att informationsmängden ökar utan också på att ny teknik erbjuder nya kommunikations- sammanställnings-, och lagringsmöjligheter. En annan pådrivande faktor är att antalet aktörer som deltar i verksamhetsprocesserna har ökat. Interaktionen inom och mellan organisationer stöds dessutom genom allt fler tjänster.

En kartläggning av informationsflödet måste därför ta hänsyn inte bara till hur informationen kommuniceras och lagras inom den egna organisationen utan också till vilka externa aktörer och resurser som är involverade. Det kan ske i större eller mindre skala, från outsourcing till användande av kommersiella molntjänster för exempelvis lagring.

Ytterligare en aspekt att ta hänsyn till är de kanaler som mer eller mindre aktivt väljs för kommunikation, till exempel sociala medier eller sms.

2.2 Förutsättningar och avgränsningar för vägledningen

Denna vägledning är avsedd att ge en övergripande förståelse för kartläggning av information och ska inte ses som en fullständig manual.

Utgångspunkten är att det är nödvändigt att identifiera och analysera verksamhetsprocesser för att kunna få grepp om vilken information som organisationen skapar och utnyttjar. Eftersom processkartläggning är en aktivitet som genomförs på olika sätt och med olika syften bör det understrykas att denna vägledning inte avser att ge stöd för verksamhetsutveckling eller organisationsförändringar. Avsikten är istället att ge stöd för en analys av befintliga processer och den information som används för att stödja processerna. Den metod som används har valts med tanke på att den överensstämmer med de metoder som har använts i andra liknande myndighetsvägledningar, som till exempel den modell för nationell informationsstruktur för vård och omsorg som Socialstyrelsen har tagit fram[3].

1. MSBFS 2009:10 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet
2. Föreskrifter om ändring i Riksarkivets föreskrifter och allmänna råd (RA-FS 2008:4) om arkiv hos statliga myndigheter
3. Nationell informationsstruktur för vård och omsorg. Modeller med beskrivningar. Socialstyrelsen 2010

Metoden kan också ses som en fördjupning av den verksamhetsanalys som ingår som ett steg i det metodstöd, som har tagits fram av bland annat MSB för att underlätta för införandet av Ledningssystem för informationssäkerhet (LIS).[4]

I kartläggningen bör det därmed ingå en beskrivning av verksamhetsprocesserna, de informationsflöden som stödjer dessa samt av de resurser som används för att hantera informationen. En sådan arkitekturansats kan enkelt sammanfattas i tre lager (se bild 1 nedan) som översiktligt beskrivs här.

- Verksamhetslagret, där man beskriver en organisations verksamhet och hur olika delar samverkar med varandra genom exempelvis målstrukturer, begreppsmodeller och processmodeller (mer om olika modeller i kapitel 7).
- Informationslagret, där man beskriver de informationsmängder som skapas och används i processen.
- Informationsbärarlagret, där man beskriver de informationsbärare/kanaler där processens information hanteras och lagras.

Verksamhetsprocesser och informationshantering

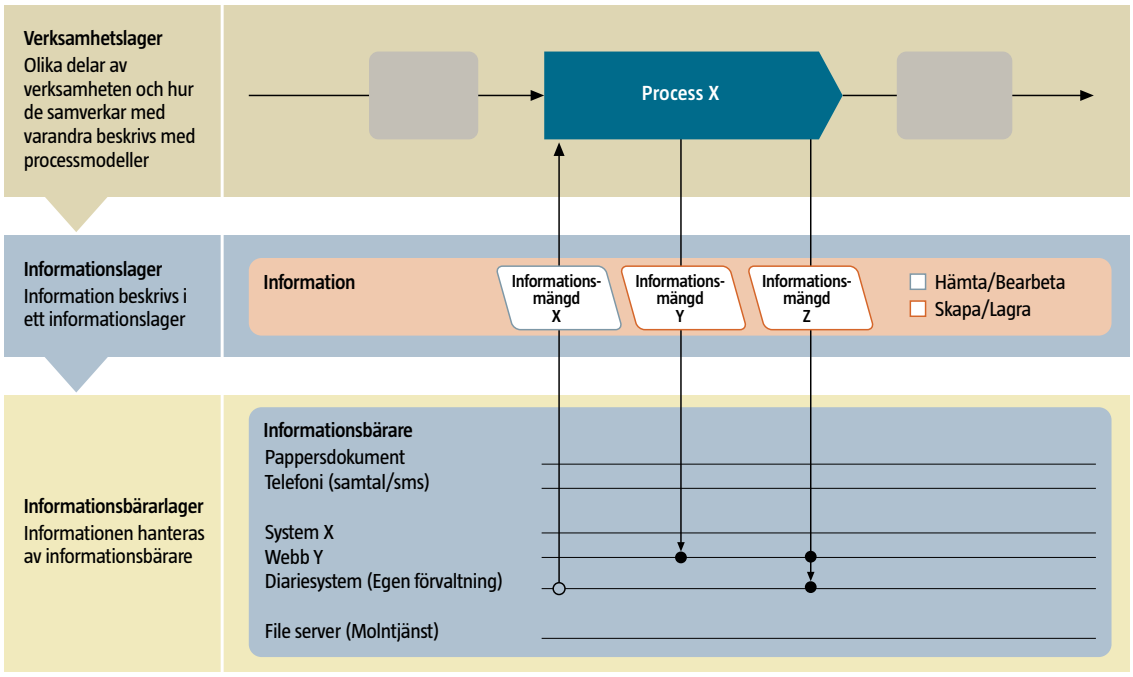


Bild 1. Översiktlig bild över vägledningens tre lager

4. http://www.informationssakerhet.se

Observera att såväl informationslagret som informationsbärarlagret också kan beskriva externa tjänster som till exempel molntjänster för lagring. Informationsbärarlagret kan bestå av andra bärare än just IT-system, till exempel papper eller telefoni.

2.3 Vägledningens terminologi

I denna vägledning har vi valt att använda en allmän terminologi som inte alltid överensstämmer med de termer som används inom områdena informationssäkerhet eller arkivhantering. Skälet till detta är att hitta ett framställningssätt som inte kräver särskilda förkunskaper inom de respektive områdena.

Presentation av metod

3. PRESENTATION AV METOD

3.1 Syfte

Tanken med vägledningen är att den ska kunna användas utan särskild träning i modellering. Därför har vi försökt välja en metod och notation som är lätt att förstå, lära och använda på såväl dator som plast, papper eller whiteboard och som stöds av vanligt förekommande ritverktyg. Samtidigt ska de framtagna modellerna kunna användas för att beskriva avancerade flöden.

Vägledningens fokus ligger på verksamhetsbeskrivningar i form av processer. Genom att beskriva verksamheten i processer blir det lättare att förstå hur helheten samverkar för att skapa värde för uppdragsgivarna. För att processbeskrivningar ska hålla över tiden beskrivs de som regel ur ett organisationsoberoende perspektiv. Processen visar alltså vad som ska göras oavsett vem som gör det. Processerna blir den naturliga beskrivningen av en verksamhet. Det är dessa som förverkligar verksamhetsmålen genom att beskriva

- varför en verksamhet finns till (vilka behov som ska tillfredsställas)
- vad som ska produceras (processernas output)
- hur detta ska gå till (aktiviteter, resurser, information och deras relationer till varandra).

Annorlunda uttryckt, processer är egentligen inget annat än ett gemensamt arbetssätt. I denna vägledning betraktas en process som en struktur av aktiviteter. Dessa aktiviteter genererar och använder information. Därför är processbeskrivningar det enklaste sättet att åskådliggöra en organisations informationsflöden. Processer kan beskrivas på ett antal mer eller mindre komplicerade sätt. I den här vägledningen ligger processbeskrivningarna på en relativt enkel nivå. Processer kan beskrivas enbart med text, men vi har valt en visuell beskrivning som vi tror ökar tydligheten och överskådligheten. Bild 2 på nästa sida visar hur metodkomponenterna hänger ihop.

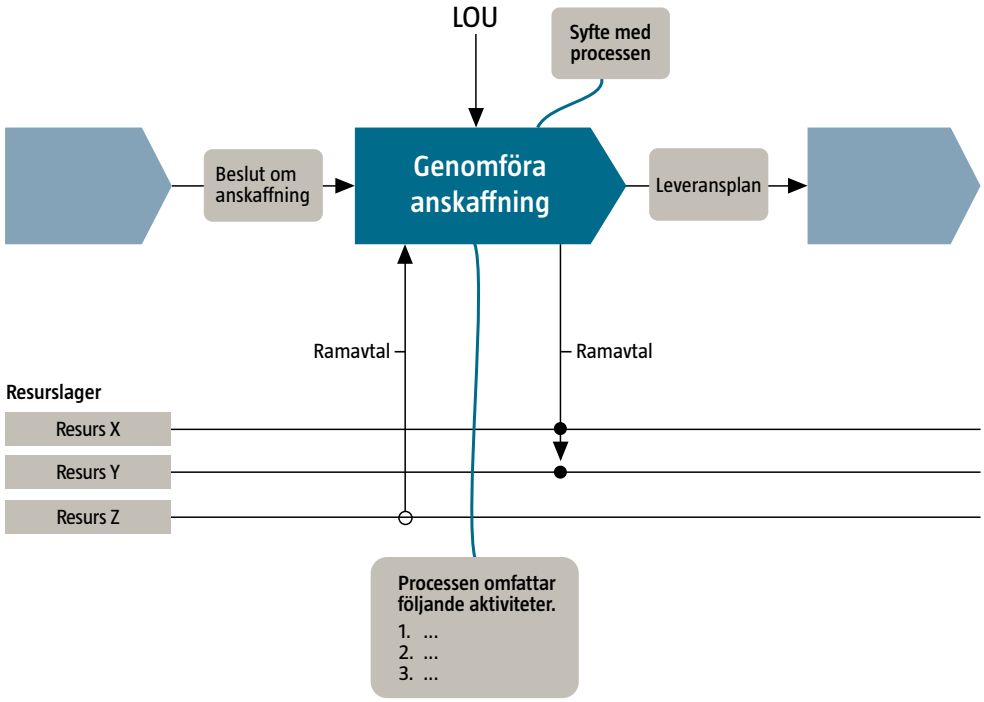


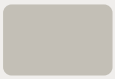
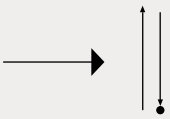
Bild 2. Bilden visar en principskiss av en processkarta

3.2 Notation

Notation är det beskrivningssätt som används för att åskådliggöra processerna. Notationen som används i denna vägledning illustreras genom tabell 1 till höger. Den baseras på UML-Business extensions[5] som har en stor spridning inom såväl näringsliv och offentlig sektor. UML-Business extensions bygger i sin tur på standarden IDEF0 (Integration Definition for Function Modeling)[6]. Det finns även andra etablerade notationer att välja bland och vissa organisationer har utvecklat egna varianter.

Det som en process ”producerar” kallas förädlingsobjekt. Det kommer input från vänster i beskrivningen som förädlas till höger. Uppifrån ritas eventuella styrningar in. Underifrån ritar vi in de resurser som processen behöver. Resurser kan vara olika saker som till exempel information, men även kompetens eller material.

5. Business Modeling with UML, Hans-Erik Eriksson och Magnus Penker (2000)
6. http://www.idef.com

	Process – avgränsad följd av aktiviteter som förekommer upprepat i verksamheten och syftar till att uppfylla ett bestämt mål.
	Förädlingsobjekt – det som en process producerar, skapar, förädlar o.s.v.
	Informationsmängd – mängd information som är avgränsad för ett visst ändamål. I denna vägledning avses med informationsmängd den information som en process skapar, nyttjar eller bearbetar.
	Flöde – Förädlingsobjekts- eller informationsflöde. Pilen visar riktning. Text på pilen (ibland med symbol omkring) anger informationsflödets innehåll. Informationsflöden transporterar informationsmängder mellan processer och informationsbärare.

Tabell 1. Grafisk grundnotation

Utlysa och tilldela forskningsmedel (process)

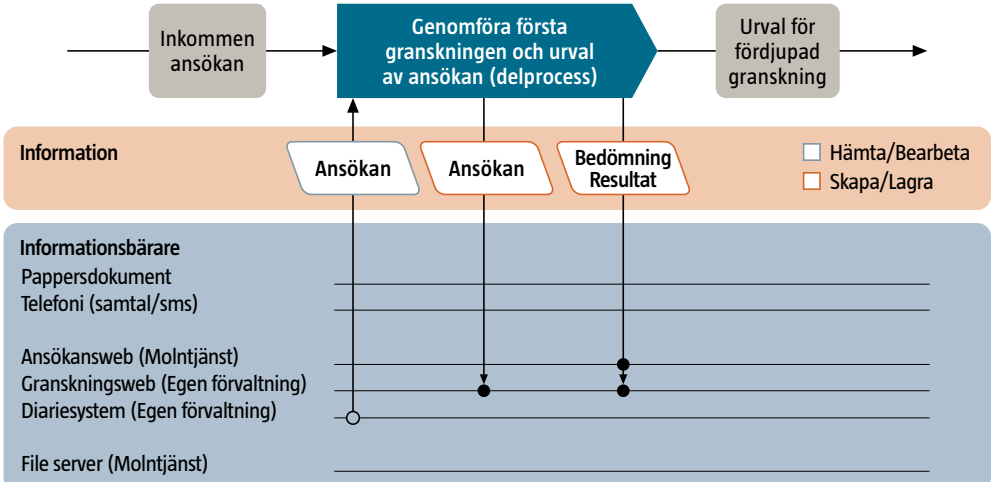


Bild 3. Bilden visar hur notationskomponenterna hänger samman

I denna vägledning vill vi främst fokusera på information och resurser i form av informationsbärare, till exempel IT-system, databaser eller en molntjänst. Därför har resurslagret fått namnet informationsbärare, vilket visar hur informationen flödar och lagras. Vi har också ett informationslager där informationsmängderna som hanteras i processen beskrivs. Dessa informationsmängder kan om man så önskar beskrivas noggrannare i till exempel en begrepps- eller informationsmodell.

För att förstå en verksamhetsprocess krävs att varje delprocess har välavgränsade aktiviteter. Om dessa aktiviteter saknas är processerna bara begrepp som kan tolkas olika av olika betraktare.

En viktig faktor är också att detaljeringsnivån på aktiviteterna ska vara balanserad. Aktiviteter (eller aktivitetssteg om man så vill) ska beskrivas på en generell nivå och därefter kan vid behov fördjupningar göras.

Tillämpning

4. TILLÄMPNING

I detta kapitel visas ett antal sätt att beskriva processer. Samma process beskrivs med olika detaljeringsgrad och utifrån en organisatorisk vy. Gemensamt för beskrivningarna är att de visar en verksamhetsprocess nuläge. Notationen går naturligtvis även att använda för att avbilda ett önskat läge.

Exempelprocessens syfte är att fördela pengar genom så kallade utlysningar, alltså att till exempel en myndighet bereder forskare möjlighet att söka pengar för att forska inom ett speciellt område. Ansökningar tas emot och hanteras enligt en fastställd process och bedöms utifrån ett antal kriterier för att slutligen beviljas eller avslås.

Vi har valt denna exempelprocess eftersom olika former av ansökningsärenden förekommer i många organisationer och därför är lätta att relatera till.

Observera att nedanstående är just ett exempel. Behoven styr detaljeringsgraden och perspektiv. Har man inget behov av att illustrera aktiviteter, utan vill fokusera på informationsflödena, så gör man det. Vill man använda processmodellen som konkret stöd i hanteringen av information kan uppgifter om gallring, sekretess med mera läggas till.

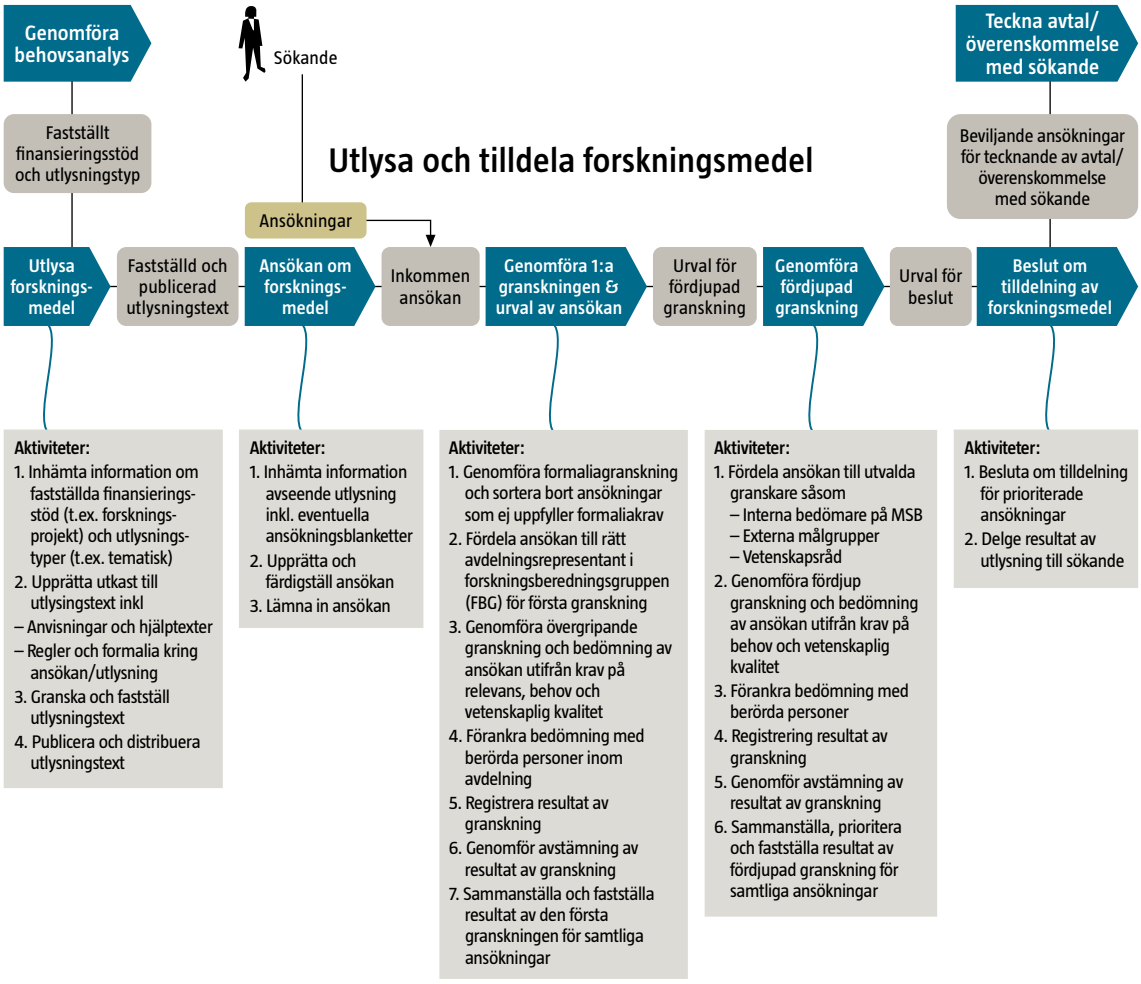


Bild 4. Förenklad processvy

4.1 Förenklad processvy

Ovanstående processbeskrivning visar hur utlysning och tilldelning av forskningsmedel går till. Här har vi utöver själva delprocesspilarna bara illustrerat förädlingsobjektet och aktivitetsstegen.

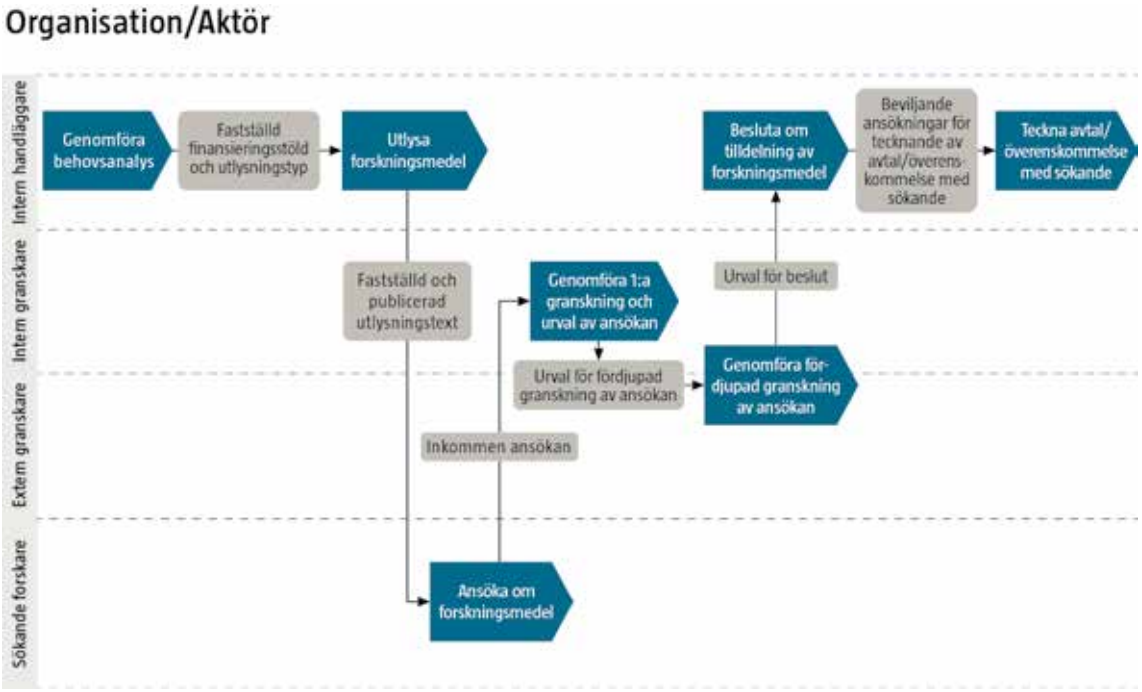


Bild 5. Aktörsvy över processen

4.2 Aktörsvy av processen

Aktörsvyn av processen ser annorlunda ut jämfört med föregående bild, men beskriver fortfarande processen ”utlysa och tilldela forskningsmedel”. Här ser man vilken/vilka aktörer som är aktiva i en viss delprocess. Se bilden ovan.

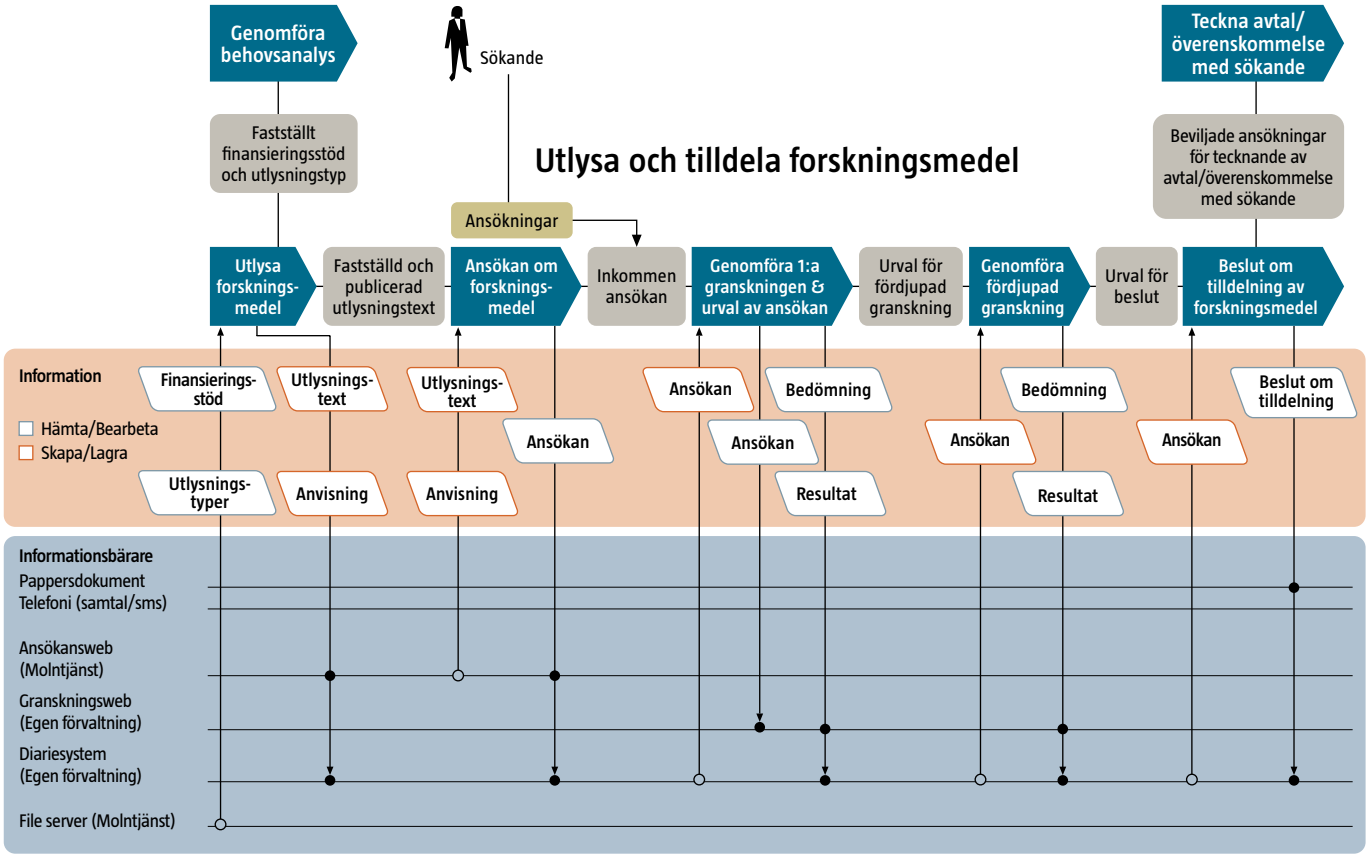


Bild 6. Detaljerad processvy

4.3 Detaljerad process

I bilden nedan har processkartan utökats med ett så kallat resurslager. Med hjälp av resurslagret ser vi hur processen använder och skapar information. Exempelvis måste delprocesserna som rör granskning använda informationsmängden ”ansökan” och de skapar informationsmängden ”bedömning/resultat”. Vi ser också vilka informationsbärare som informationen hämtas från och lagras i. Notera också att aktivitetsstegen lyfts bort från denna bild för att det ska vara enklare att fokusera på informations- och resurslagret.

Genomförande och resultat

5. GENOMFÖRANDE OCH RESULTAT

I tidigare kapitel har en processmodell för att fånga informationsflöden presenterats. I det här kapitlet beskrivs hur en processorienterad informationskartläggning kan genomföras i praktiken.

5.1 Kartläggning som workshop

För att genomföra en ändamålsenlig kartläggning behövs både verksamhetskunskap och metodkunskap. Dessutom kan olika specialister behövas för att de frågeställningar som behandlas ska få sin rätta belysning. Det kan till exempel behövas juridisk bakgrund för att legala kravställningar ska kunna behandlas. Ett annat exempel är medarbetare från it-funktionen kan behöva delta för förståelsen av hur informationslagret utnyttjar informationsbärarlagret. Sammantaget är det viktigt att se att kartläggningen av informationshanteringen i verksamhetens processer inte är en ensam skrivbordsövning utan att den mest lämpliga formen är en workshop där olika kompetenser kan samverka för bästa resultat.

För att en workshop ska fungera bra och kännas meningsfull för deltagarna krävs att den är väl förberedd. Det krävs också att deltagarna känner sig trygga i sina respektive uppgifter och är förberedda på vad de förväntas bidra med i workshopen. Att klargöra rollspelet för deltagarna är därför en viktig del i förberedelserna.

Innan det är möjligt att börja bemanna och förbereda workshopen måste ett viktigt steg tas, nämligen att bestämma vilken process som ska kartläggas. Detta kan förefalla enkelt men leder inte sällan till frågor som bör vara lösta innan förberedelser kan inledas. Vanliga fällor är att organisation träder framför process eller att man inte sätter upp en tydlig avgränsning för den process som ska kartläggas. Definition och avgränsning av processen ger underlaget för vilka aktörer som ska delta och vilka förberedelser som bör göras.

Hur själva kartläggningen ska utformas beror på den aktuella verksamhetens organisation och regelverk. Processkartläggningar bör ses som en rutin som genomförs regelbundet och det är därför bra om det finns dokumenterade regler för hur en kartläggning ska vara utformad. I detta kapitel presenteras generella förslag som kan användas på lämpligt sätt i den egna organisationen.

5.2 Roller

Med samma reservation som ovan, att allt beror på den egna organisationens förutsättningar, kan ändå fyra rolltyper ses som lämpliga:

Verksamhetsrepresentanter
När det gäller informationssäkerhet används ofta begreppet informationsägare, d.v.s. den som har ansvar för en viss verksamhet har också ansvar för informationshanteringen. Under ideala former är informationsägaren delaktig i kartläggningen eftersom det ju är han eller hon som ytterst är den som bäst kan bedöma vilken funktion och betydelse en viss informationsmängd har för verksamheten.

Detta är inte alltid möjligt att få till stånd och då är alternativet att välja verksamhetsrepresentanter som både har djupare kunskap om den aktuella processen och som har ett stort förtroende hos informationsägaren. Förtroendet är viktigt för att de bedömningar som görs ska ha fäste hos den som har ansvar för processen.

Om den processen passerar organisatoriska gränser måste detta avspeglas i bemanningen av workshopen så att de olika organisatoriska enheternas intressen tillvaratas.

Specialister
Beroende på vilken process som kartläggs kan olika typer av specialister vara lämpliga deltagare. Förutom arkivarier och informationssäkerhetsansvariga bör bland annat följande specialister övervägas som deltagare:

- jurist
- it-ansvarig
- kvalitetsansvarig
- personuppgiftsombud.

Analysledare
För att workshopen ska fungera måste den ledas av någon som utgör metodstöd, här kallad analysledare. Analysledaren kan vara arkivarie eller informationssäkerhetsansvarig men också någon annan. Det viktiga är att analysledaren besitter rätt kompetens och personliga egenskaper för att kunna leda kartläggningen på ett bra sätt. De personliga egenskaperna är viktiga eftersom analysledaren är ansvarig för att förbereda och genomföra workshopen samt för att säkerställa att det finns ett dokumenterat resultat av workshopen. För att klara detta bör man vara strukturerad och analytisk som person, kunna leda och entusiasmera en grupp samt kunna förstå verksamhetens behov. Kompetensmässigt bör analysledaren vara kunnig inom informationshantering och processkartläggning.

Sekreterare
Även om diskussionerna under en workshop i sig kan skapa samförstånd och nya insikter är det också viktigt att workshopen efterlämnar mer bestående resultat, som en ordentlig dokumentation. Dokumentationen kan innehålla visuella beskrivningar av den kartlagda processen men som tidigare påpekats används den bildmässiga beskrivningen av processen i första hand som stöd för en analys. Huvudsaken är alltså de resonemang och slutsatser som framkommer under kartläggningen. Detta kräver en insats under själva workshopen som analysledaren knappast hinner med. Att ha en medarbetare som fungerar som sekreterare har en kvalitetshöjande effekt både på workshopen, eftersom analysledaren då kan koncentrera sig på sin uppgift, och sekreteraren på den rapport som bör vara resultatet från workshopen.

5.3 Förberedelser

Analysledaren bör ha ansvar även för förberedelsefasen för att få systematik i arbetet och för att de verksamhetsansvariga inte ska tyngas av uppgifter som de inte har rutin på att utföra.

I korthet kan förberedelserna delas in i följande steg:

1. Överenskommelse om att kartläggning ska ske mellan informationsägare eller motsvarande funktion och den organisatoriska enhet som ansvarar för kartläggning av processer. I överenskommelsen ska ingå en tydlig avgränsning av vilken process som ska kartläggas.
2. Analysledaren fördjupar sig i processen och dess förutsättningar. Här ingår även förslag på tidsomfattning för workshop, vanligen 3-4 timmar. Därefter skickas förslag på tid och deltagare till informationsägare eller motsvarande funktion för godkännande.
3. Efter godkännande samlar analysledaren in det bakgrundsmaterial som kan vara relevant i sammanhanget.
4. Inbjudan skickas ut med tydlig beskrivning av syfte med och utformning av workshopen.
5. Analysledaren förbereder workshopen med rum, materiel och eventuell förtäring.

Dessutom bör naturligtvis analysledaren och den medarbetare som ska fungera som sekreterare tillsammans förbereda arbetsfördelningen och gå igenom de förväntningar man har på varandra.

5.4 Genomförande av workshopen

I beskrivningen av metoden framgick att denna vägledning eftersträvar att ge stöd för olika arbetssätt. Detta gäller även själva genomförandet av workshopen. Förslagsvis används notis-lappar och whiteboard för att beskriva aktiviteterna i processen för att uppnå stor flexibilitet.

Analysledaren ska ha ett positivt förhållningssätt men också kunna ställa penetrerande frågor för att motverka den eventuella hemmablindhet som kan finnas hos de deltagare som har verksamhetskunskap.

Vid workshopen är det viktigt att analysledaren är uppmärksam på styrande faktorer och tar ett ansvar för att analysera dessa närmare med stöd av specialistkompetens som till exempel en deltagande jurist. Likaså bör viktiga tekniska sammanhang klarläggas med hjälp av it-ansvariga.

Sekreteraren antecknar och sammanställer de gemensamma ställningstaganden som görs under kartläggningen.

5.5 Kvalitetskontroll

När analysledaren och sekreteraren är klara med rapporten efter workshopen bör denna kvalitetskontrolleras med den grupp som deltog i workshopen och med informationsägaren. Ett bra tillvägagångssätt är att gruppen återsamlas för ett kortare möte med genomgång av rapporten där deltagarna får bedöma hur väl den överensstämmer med deras uppfattning. Om informationsägaren inte deltar bör hon eller han få möjlighet att godkänna kartläggningen på annat sätt.

5.6 Och sedan?

I nästa kapitel beskrivs hur kartläggningen kan användas i arkivhanteringen och i arbetet med att förbättra informationssäkerheten. Men det finns också vissa generella aspekter som bör regleras. Exempel på detta är hur kartläggningarna ska förvaltas och återanvändas. En rekommendation är ju att kartläggningarna sker på ett rutinmässigt sätt och att processer gås igenom regelbundet. Därför behövs beskrivningar av bland annat versions- och ändringshantering.

Processorienterad informations-kartläggning

6. Processorienterad informationskartläggning – ett gemensamt intresse för arkiv och informationssäkerhet

Att fokusera på sin huvuduppgift, kärnverksamheten, är ledord för de flesta organisationer idag. Alla aktiviteter som inte tillför verksamheten ett mervärde rensas bort. Frågor som är relaterade till informationshantering har en tendens att betraktas som onödiga och byråkratiska, trots informationshanteringens faktiska betydelse för verksamheten. Därför är det av vikt att lyfta fram de nyttoeffekter som finns i en styrd informationshantering och också som en konkret rationalisering. Rationaliseringen ligger i att sammanföra de närliggande aktiviteter som är påkallade från arkivsidan och från informationssäkerhetssidan.

De som arbetar med arkivfrågor och de som arbetar med informationssäkerhetsfrågor har ett gemensamt intresse: informationshantering. Samarbetet mellan dessa två grupper har dock inte varit särskilt utvecklat. Vår utgångspunkt är att alla vinner på ett bättre samarbete. Ett första steg är att utnyttja den gemensamma kompetensen för att identifiera information samt för att både klassificera och klassa den. Med klassificera avses här att koppla informationen till den verksamhet den tillkommit i. Klassningen innebär i informationssäkerhetssammanhang att informationens skyddsbehov definieras.

Vid processorienterad informationskartläggning identifieras informationsmängder och de resurser som används för att hantera dem. I och med att informationen är satt i sitt sammanhang går det att se dess funktion i organisationen och därmed går det också att se vilket behov av skydd som finns på kort och lång sikt.

Både MSB och Riksarkivet ger ut föreskrifter, vägledningar och rekommendationer för att uppnå god arkivhantering och god informationssäkerhet. I detta kapitel presenteras hur den processorienterade informationskartläggningen kan fungera som en grund för centrala aktiviteter inom respektive område. Även här är genomgången översiktlig, för den som vill veta mer rekommenderas MSB:s och Riksarkivets webbplatser samt informationssäkerhet.se.

6.1 Arkivredovisning

Enkelt uttryckt är en arkivredovisning ett styr- och sökinstrument till en organisations hela handlingsbestånd. Den används för att göra handlingarna sökbara och användbara på såväl kort som lång sikt. För den offentliga förvaltningen finns regler om arkivredovisning, där Riksarkivets föreskrifter om arkivredovisning gäller för statliga myndigheter och organ som hanterar allmänna handlingar. En myndighets arkiv består av de allmänna handlingarna som bildas i verksamheten.

Den verksamhetsbaserade arkivredovisningen innebär i korthet att informationen klassificeras enligt en struktur som representerar verksamheten, att processerna och de handlingar som avsätts under processens genomförande beskrivs samt att informationens förvar redovisas.

För arkivredovisningens syften kan processmodelleringen användas för att bland annat identifiera och beskriva var, när och hur handlingar inkommer och upprättas samt hanteras i verksamheten.

6.1.1 Verksamhetsbeskrivning i arkivredovisningen

I den verksamhetsbaserade arkivredovisningen är det verksamheten som är utgångspunkt för redovisning av myndighetens information. Processerna ska beskrivas för att synliggöra det sammanhang som handlingarna tillkommit i och för att upprätthålla informationens autenticitet och rättssäkerhet över tid.

Nedanstående begreppsmodell visar arkivredovisningens beståndsdelar och hur begreppen förhåller sig till varandra. Se mer om begreppen och beskrivningsnivåerna i Riksarkivets vägledning Redovisa verksamhetsinformation.

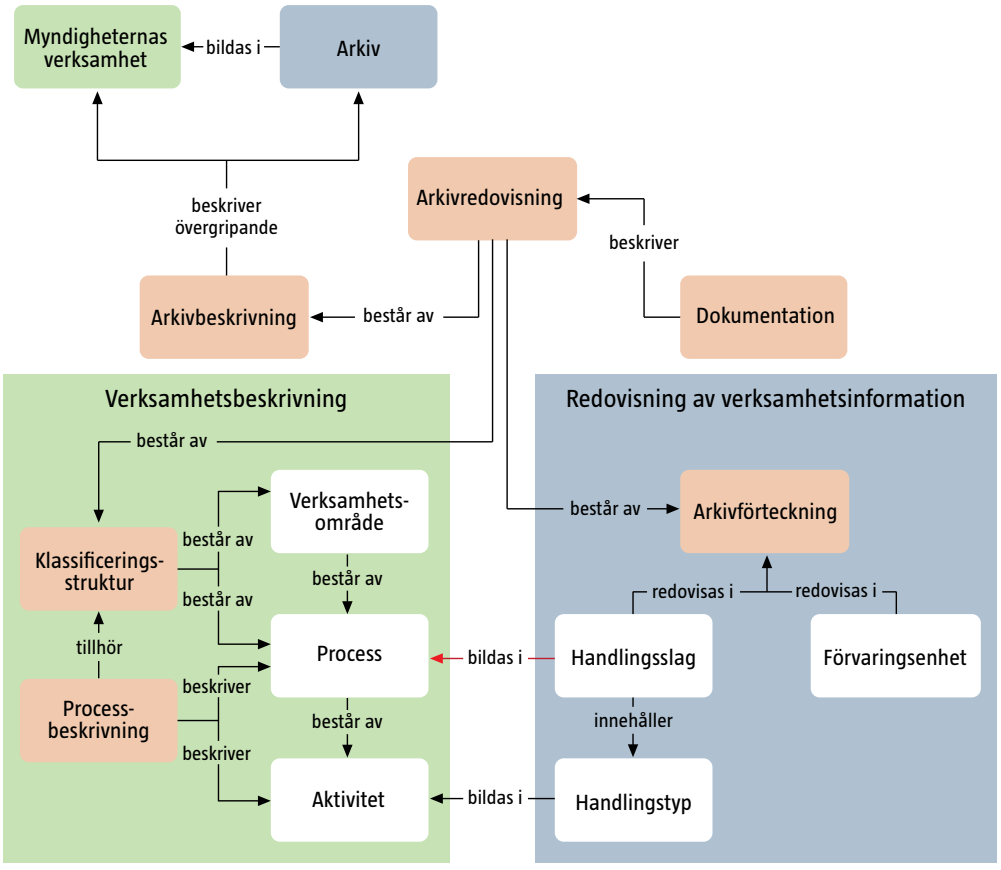


Bild 7. Arkivredovisningens beståndsdelar – hämtad från Riksarkivets vägledning Redovisa verksamhetsinformation 2012

Arkivredovisningen består av ett antal uppgifter om verksamhet, handlingar och handlingarnas förvar. Uppgifterna ska kunna presenteras i form av ett antal sammanställningar (uppgiftsmängder): arkivbeskrivning, klassificeringsstruktur med processbeskrivningar, arkivförteckning och dokumentation. Dessa uppgiftsmängder ska relateras till varandra.

För att ge struktur åt och klassificera den information som skapas och hanteras i myndighetens verksamhet används en klassificeringsstruktur. Verksamhetsområdena och processerna ordnas i denna struktur och beskrivs genom tillhörande processbeskrivningar. Den översta nivån i klassificeringsstrukturen ska representera myndighetens verksamhetsområden, och den nedersta nivån de processer som har identifierats i verksamheten.

Processbeskrivningarna syftar till att ge kontext till de handlingar som har inkommit eller upprättats i processerna. Av processbeskrivningen ska det framgå vad som initierar och avslutar en process samt vilka aktiviteter som vanligtvis ingår i processen. I de fall myndigheten arbetar i en process som är gemensam med en annan myndighet eller enskild ska detta framgå. Genom att förstå hur handlingarna har tillkommit ökar även förståelsen för handlingarna.

Varje process som tas upp i klassificeringsstrukturen motsvaras av ett handlingsslag. De två begrepp som används för att beskriva informationsmängder i arkivredovisningen är handlingsslag och handlingstyp. Skillnaden mellan begreppen handlingsslag och handlingstyp är att den förra ligger på processnivå medan den senare hör till aktivitetsnivån.

Informationsmängderna hanteras och lagras i förvaringsenheter, exempelvis IT-system. Begreppet förvaringsenheter i arkivredovisningen kan motsvara det begrepp som i denna vägledning benämns som informationsbärare.

6.1.2 Arkivredovisning och registrering

Det finns ett nära samband mellan arkivredovisning och registrering. I båda fallen handlar det om att klassificera och förse handlingarna med metadata för att möjliggöra organisation, sökbarhet och återanvändning av information i sitt sammanhang. Föreskrifterna om arkivredovisning omfattar samtliga allmänna handlingar hos myndigheten, oberoende av medium och oberoende av om handlingarna är ärendeanknutna eller inte, gallringsbara eller inte. För att uppnå effektivitet i både ärendehantering och arkivering bör en samordning eftersträvas mellan ärenderegistrering och arkivredovisning. Klassificeringsstrukturen bör därför även användas som utgångspunkt vid registrering av handlingar enligt 5 kap. offentlighets- och sekretesslagen (2009:400). Klassificeringsstrukturen kan då ersätta diarieplan eller andra klassificeringsplaner hos myndigheten. Detta underlättar insyn och återsökning av myndighetens samtliga handlingar.

6.1.3 Arkivredovisning som styrmedel i informationshanteringen

Genom kraven på klassificering och hantering utgör arkivredovisningen ett viktigt styrmedel i informationshanteringsprocessen. Om arkivredovisningen samordnas med uppgifter som ska registreras eller dokumenteras i enlighet med

annan reglering kan redovisningen bli ett kraftfullt verktyg för informationsstyrning som kan underlätta en utveckling mot e-förvaltningen. Här avses bland annat offentlighets- och sekretesslagen och lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (PSI-lagen).

Arkivredovisningen kan bidra till följande nyttoeffekter:

- **Insyn –** tillgänglighet, öppenhet, sökbarhet. Genom att myndighetens hela handlingsbestånd blir synligt och redovisas i arkivredovisningen, såväl elektroniska handlingar som gallringsbara handlingar, får allmänheten vetskap om vilka handlingar som kan finnas (eller har funnits) hos myndigheten och vilka som går att begära ut (Offentlighetsprincipen). Genom att handlingsslag och handlingstyper synliggörs underlättas även sökbarheten av handlingar.
- **Trovärdighet –** kontext, autenticitet, rättssäkerhet. Genom att processer beskrivs och handlingstyper kopplas till processer och i vissa fall till aktiviteter skapas samband mellan verksamhet och information. Om man vet i vilket sammanhang handlingar har skapats förbättras informationens spårbarhet och möjligheterna att bedöma handlingarnas autenticitet.
- **Effektiv styrning** – automatisering, verksamhetsnytta, rätt från början, interoperabilitet. Genom kraven på klassificering och hantering utgör arkivredovisningen ett viktigt styrmedel i informationshanteringsprocessen. Uppgifter om sekretess, gallring och bevarande används för att säkerställa att myndighetens information hanteras utifrån gällande regelverk. I automatiserade processer kan metadata från redovisningen styra behandlingen av informationen så att hanteringen förenklas och processen kvalitetssäkras. Uppgifterna från arkivredovisningen följer handlingarna under hela deras livslopp, från framställning till det långsiktiga bevarandet. För att uppnå effektivitet i informationshanteringen bör myndigheten integrera registrering och arkivredovisning.
- **Övrig verksamhetsnytta** – anpassningsbarhet, verksamhetsperspektiv, kompatibilitet. Genom att uppgifterna i föreskrifterna endast är minimikrav har myndigheterna möjlighet att lägga till metadata utifrån verksamhetens behov från exempelvis olika nationella och internationella standarder. Dessutom kan sökingångar utformas utifrån olika återsökningsbehov.

6.2 Informationssäkerhet

Informationssäkerhet syftar, som begreppet antyder, till att skydda information. Med skydd avses att kunna upprätthålla rätt nivå av

- konfidentialitet
- riktighet
- tillgänglighet
- spårbarhet.

För att en organisation ska kunna skapa och upprätthålla en god informationssäkerhet är det lämpligt att införa ett ledningssystem för informationssäkerhet (LIS), vilket också är vad den svenska och internationella standarden för informationssäkerhet SS-ISO/IEC 27001 och 27002 förordar. MSB har i en föreskrift[7] ålagt

7. MSBFS 2009:10

de statliga myndigheterna att arbeta systematiskt med informationssäkerhet och införa ett ledningssystem i enlighet med SS-ISO/IEC 27001 och 27002. Föreskrifter med ett liknande innehåll finns även för de svenska vårdgivarna[8] och standarden får anses etablerad inom allt fler verksamheter, både privata och offentliga.

För den som önskar stöd för att införa ett ledningssystem är det lämpligt att ta del av metodstödet på informationssäkerhet.se. Nedan kommer några centrala aktiviteter i ett systematiskt informationssäkerhetsarbete att tas upp för att visa hur processorienterad informationskartläggning kan användas.

6.2.1 Informationsklassning

All information i en organisation har inte samma behov av skydd och därför är en central aktivitet i säkerhetsarbetet informationsklassning vars funktion är att bedöma informationens värde och känslighet. Bedömningen sker både utifrån den egna verksamhetens behov och utifrån externa krav. Avsikten är att varje informationstillgång ska omges med rätt skydd.

Informationsklassningen är i sig en process som innebär en kravställning på säkerhetsåtgärder från verksamheten till interna och externa leverantörer av system samt it (drift och förvaltning) och av resurser som lokaler och annan utrustning som påverkar informationshanteringen. Klassningen innebär även krav på användare av informationstillgångar.

Informationsklassning kan ses som en typ av riskanalys där det görs en bedömning av vilka konsekvenser som kan bli följden av att inte skyddet kan upprätthållas. Det kan till exempel gälla om känsliga personuppgifter kan läsas av obehöriga eller att informationen inte längre finns tillgänglig eftersom det it-system verksamheten är beroende av har slutat fungera. Informationsklassningen är därför en viktig del av en organisations arbete med generella riskanalyser eftersom informationshanteringen blir en allt viktigare faktor för att organisationen ska fungera.

Oavsett vilken metod för informationsklassning som den enskilda organisationen väljer att använda är en förutsättning för att få ett användbart resultat från klassningen att det sker en identifiering av skyddsobjektet, d.v.s. informationen. Detta är också viktigt för att fastställa ansvarsförhållanden för informationen i en organisation. För att få en god informationssäkerhet är det bra att utse roller som är ansvariga för de olika komponenter som ingår i organisationens informationshantering, och då framförallt för informationen. Ansvarsförhållandena för informationen blir allt viktigare eftersom många organisationer idag väljer att använda outsourcing eller olika typer av molntjänster. I den typen av lösningar måste det stå fullständigt klart för alla parter att det är kunden som äger informationen och därmed är kravställare på leverantören. Vid informationsklassningen måste det därför också klarläggas vem som är informationsägare till olika informationsmängder och vilka krav denne ställer på både intern och extern hantering av informationen.

8. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)

Informationsklassning innebär att klassa information, inte system eller tjänster. Klassningen ger informationsägaren möjlighet att ställa krav på system – eller tjänsteägaren så att denne kan utforma sitt system eller tjänst så att det motsvarar kraven. Nomenklatur och modell för informationsklassning skiftar mellan olika organisationer men grundelementen är desamma, som till exempel att det finns ett samband mellan konsekvenser och skydd:

KONSEKVENSER	SKYDDSNIVÅ
Lindriga	Grund
Allvarliga	Hög
Mycket allvarliga	Mycket hög

Tabell 2 Skyddsnivå i förhållande till konsekvenser.

För att få systematik i informationsklassningen krävs en gemensam modell som omfattar samtliga aktiviteter från att identifiera information till att vidta skyddsåtgärder (se bild 8 nedan).

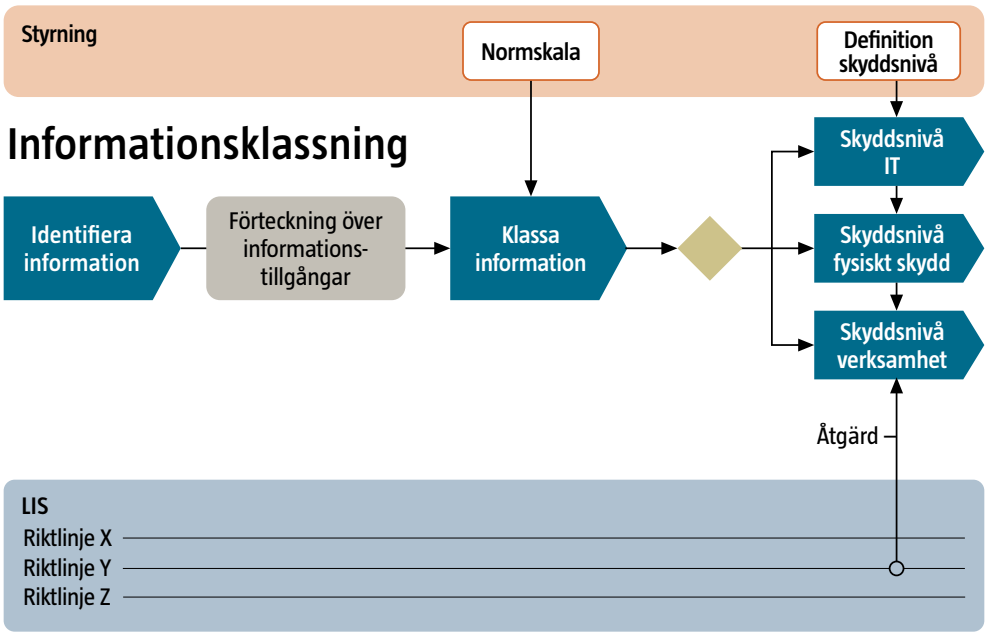


Bild 8. Översiktlig modell för informationsklassning.

Denna vägledning ger endast stöd i den första aktiviteten, att identifiera information som används i en viss process, men det är viktigt att se identifieringen av information i sitt sammanhang.

Att identifiera information i ett processperspektiv ger möjlighet att klassa den rätt. Två fördelar bör särskilt framhållas. För det första innebär kartläggning av

processen i de flesta fall att man upptäcker viktiga informationsflöden som annars är lätt att glömma bort. Exempel på detta kan vara att det är nödvändigt att ha tillgång till ett visst stödsystem för att lösa en uppgift eller att ärenden initieras via ett telefonsamtal. För det andra är det ofta svårt att bedöma en viss informationsmängds betydelse förrän man ser processens hantering av informationen. Här avtäcks beroenden inte bara till information utan också till de system och tjänster som används för att hantera informationen liksom till andra aktörer.

Kraven på ett system kan ställas från en eller flera informationsägare på samma sätt som en informationsägare i de allra flesta fall använder mer än ett system eller tjänst.

6.2.2 Riskanalys

I både privat och offentlig sektor har blivit allt viktigare att förstå och kunna hantera de risker som organisationen är utsatt för. Förutom att riskanalys är ett betydelsefullt styrinstrument för den egna organisationen ställs också krav utifrån, som till exempel i Basel III[9] för banker och i MSB:s föreskrifter om risk- och sårbarhetsanalyser för myndigheter, landsting och kommuner[10]. I riskanalyserna har informationssäkerhet fått en mer framskjuten plats som riskområde i samma takt som organisationernas beroende av sin informationshantering har blivit allt mer tydlig.

Som tidigare nämnts är informationsklassning en typ av riskanalys med inriktning på informationshantering. Utöver informationsklassning bör de flesta organisationer genomföra även andra typer av riskanalyser där informationshanteringen har betydelse. Att göra en övergripande riskanalys för hela organisationen är ett bra verktyg för ledningen för att kunna prioritera insatser av olika typ. I en sådan analys identifieras ofta knutpunkter och sårbarheter i informationshanteringen, vilka kan leda till allvarliga konsekvenser för hela organisationen. För att få förståelse för hot, sannolikhet och konsekvenser är det en stor fördel att känna till processen eller processerna som utnyttjar ett visst it-stöd.

En annan situation där riskanalyser är nödvändiga att genomföra är vid utveckling eller upphandling av it-system och it-tjänster. Den organisation som överväger att köpa en molntjänst måste känna till vilka processer i verksamheten som ska stödjas av tjänsten och vilka risker som kan uppstå om tjänsten inte är tillgänglig eller om information kommer i orätta händer. Samma sak gäller då organisationen själv ska utveckla ett system.

Att använda processorienterad informationskartläggning i denna typ av aktiviteter gör också att informationsägare kan identifieras och involveras i utvecklings- och upphandlingsprojekt på ett tidigt stadium.

9. Internationellt regelverk för bankverksamhet.
10. MSBFS 2010:7 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser…

6.2.3 Kontinuitetshantering

Riskanalyserna kan i sin tur ses som ett stöd för en annan central aktivitet inom informationssäkerhetsområdet, kontinuitetshantering. Kontinuitetshantering handlar om en organisations förmåga att kunna upprätthålla sina centrala processer även under svåra förhållanden. För att klara det behövs framför allt en god kännedom om vilka de viktigaste processerna är och vilka resurser som är nödvändiga för att upprätthålla dem. Informationshantering är en avgörande resurs för de flesta verksamhetsprocesser. Av den anledningen förutsätter en fungerande kontinuitetsplanering en beskriven koppling mellan verksamhetsprocesser och informationshantering. Tidigare har en organisation i hög grad kunnat skapa sin egen it-infrastruktur. Nu skapas gemensamma infrastrukturer genom outsourcing, nationella tjänster och kommersiella tjänster. Därmed måste en kontinuitetshantering byggas upp kring en förståelse av hur de egna resurserna samverkar med utomstående tjänster. Även detta kan beskrivas som resurslager som stödjer processer.

Genom att använda den föreslagna metoden, processorienterad informationskartläggning, kan organisationen få en god bild av vilka hårdvaru- och driftresurser som används för informationshanteringen. En krissituation kräver i de flesta fall att organisationen använder sina resurser på alternativa sätt, till exempel genom att en högre prioriterad process får överta hårdvara från en lägre prioriterad. Om en kartläggning av processer och de resurser de utnyttjar har skett är en sådan omställning betydligt enklare att genomföra.

6.2.4 Incidenthantering

Frågan är inte om incidenter kommer att inträffa utan när. Informationssamhället är sårbart och incidenter kan orsaka allvarliga konsekvenser inte enbart för enskilda organisationer. Även för att kunna bedöma en it-incidents konsekvenser och de spridningseffekter den kan ha i organisationen behövs en bild över verksamhetsprocesser och stödjande informationshantering.

Att gå vidare

7. ATT GÅ VIDARE

Denna vägledning har introducerat processkartor som ett sätt att identifiera en organisations informationsflöden, främst utifrån de krav Riksarkivet och MSB ställer på myndigheter. En organisation kan förstås ha andra eller mer detaljerade krav på att beskriva sina processer och sin information. Verksamheter och informationsflöden kan också beskrivas ur ett flertal perspektiv och på flera olika sätt. Analogt med detta finns fler modeller än processkartor att tillgripa beroende på vilka behov en organisation har.

Bilden nedan (bild nummer 9) visar hur processer, som visar hur något görs, hänger ihop med begrepps- och informationsmodeller som förklarar vad som görs. Målmodellen visar varför processen genomförs. Man kan också addera andra resurser än informationsbärare, till exempel organisationsenheter.

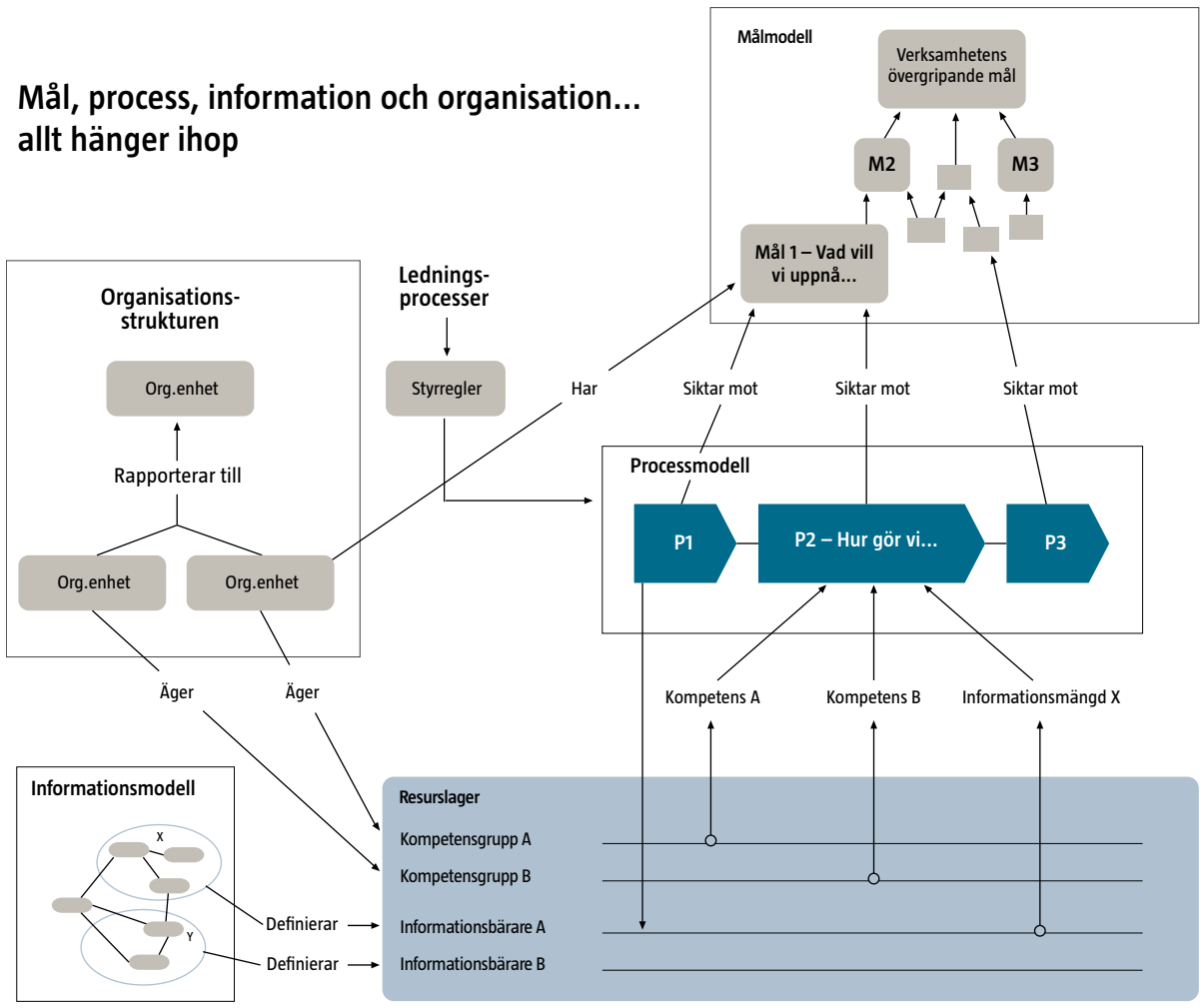


Bild 9. Översiktsbild som visar hur olika modeller hänger ihop och beskriver olika delar av verkligheten.

Begreppsmodeller är ett viktigt komplement till processkartor eftersom det många gånger krävs att man är överens om inte bara hur informationsflödena i en verksamhet går. Det är också viktigt att definiera informationsmängdernas betydelse och deras relation till andra informationsmängder. Under utvecklingen av en informationsmodell kommer man att ha nytta av begreppsmodellen. Modellerna kommer troligtvis att påminna om varandra i strukturen men medan informationsmodellen visar vilken information som är intressant för en viss företeelse visar begreppsmodellen definitionen av företeelsen[11].

Att beskriva verksamheter i modeller kan förefalla enkelt i teorin, men är betydligt svårare att genomföra i praktiken. Denna vägledning kan därför ses som en inledning till ett större arbete för att styra en organisations informationshantering.

11. Begreppsmodeller vid informationsstandardisering – Stanli, ett projektområde inom SIS, Swedish Standards Institute

Bilaga

Bilaga A: Förkortningar och vissa begrepp

Aktivitet (arbetssteg) - identifierbar sekvens av avsiktliga händelser. En mängd sammanhörande aktiviteter bildar en (del)process.

Arkivredovisning – ett styr- och sökinstrument till en organisations hela handlingsbestånd som används för att göra handlingarna sökbara och för att de ska kunna användas på såväl kort som lång sikt.

Delprocess - process som utgör en del av en överliggande process. Begreppet är nivålöst.

Förädlingsobjekt – det som en process producerar, skapar eller förädlar.

Informationsbärarlagret – där man i vägledningen beskriver de informationsbärare/kanaler där processens information hanteras och lagras.

Informationsflöde - Informationsflöden transporterar informationsmängder mellan processer och informationsbärare/kanaler.

Informationsmängd – mängd information som är avgränsad för ett visst ändamål. I denna vägledning avses med informationsmängd den information som en process skapar, nyttjar eller bearbetar.

LIS – Ledningssystem för informationssäkerhet enligt SS-ISO/IEC 27001.

MSBFS – Myndigheten för samhällsskydd och beredskaps författningssamling.

Process – avgränsad följd av aktiviteter som förekommer upprepat i verksamheten och syftar till att uppfylla ett bestämt mål. En process kan till exempel vara att handlägga ansökan om bidrag, att förvalta IT-system eller att utveckla och organisera arbetet.

I denna vägledning betraktas en process främst som en struktur av aktiviteter.

RA-FS – Riksarkivets författningssamling.

UML – Unified Modeling Language är ett objektorienterat generellt språk för modellering.

Ett samarbete mellan

Myndigheten för
samhällsskydd
och beredskap

Riksarkivet

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB493 - november 2012 ISBN 978-91-7383-291-5