Informationsklassning

2016-09-15, Jan-Olof Andersson

Upplägg

- Beskrivning hur man kan tänka kring informationsklassning utifrån MSB:s metodstöd och egen erfarenhet.

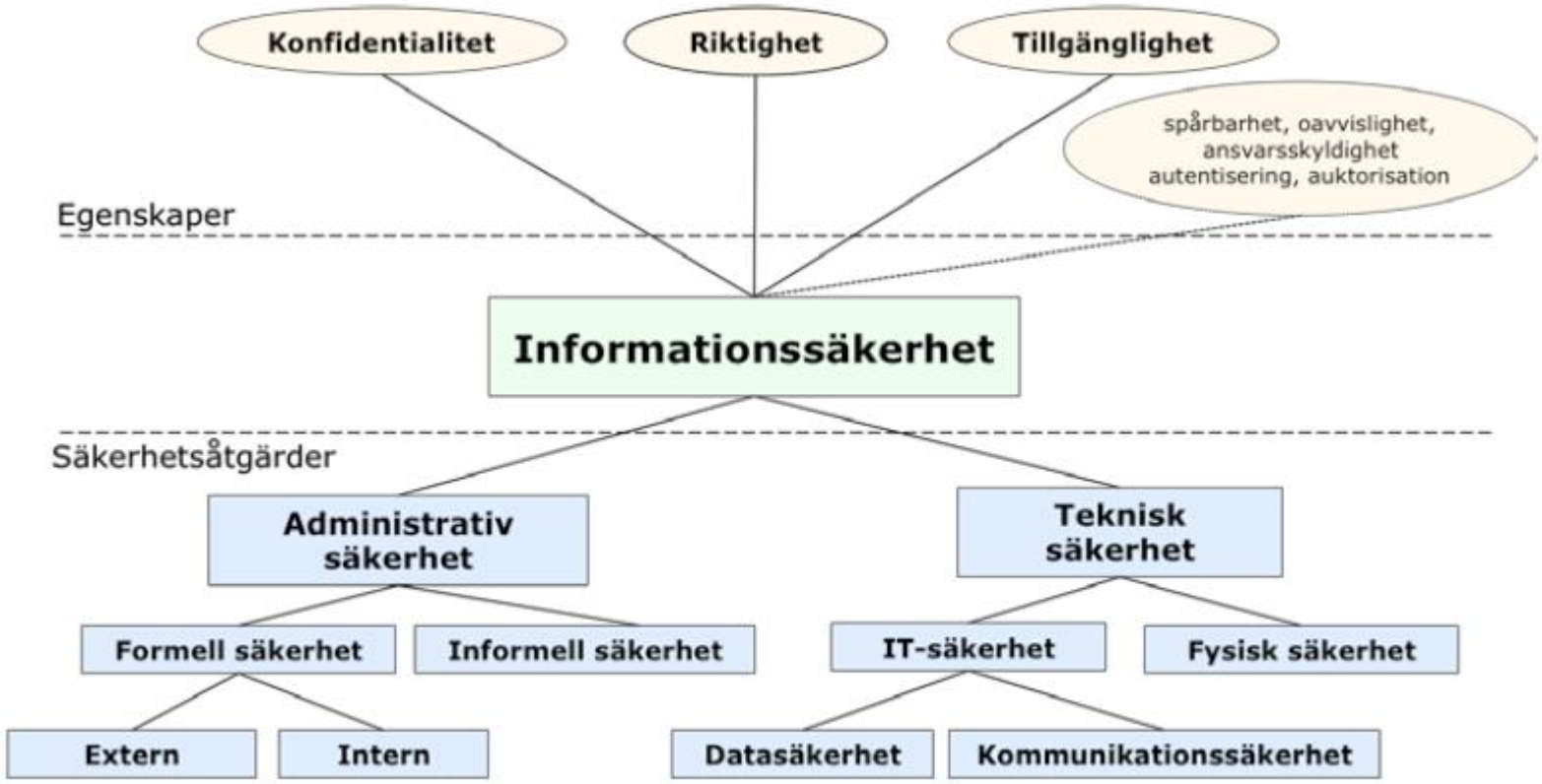
Agenda

- Inledning och presentation av området
- Metodbeskrivning
- Erfarenheter

Definitioner TR-50

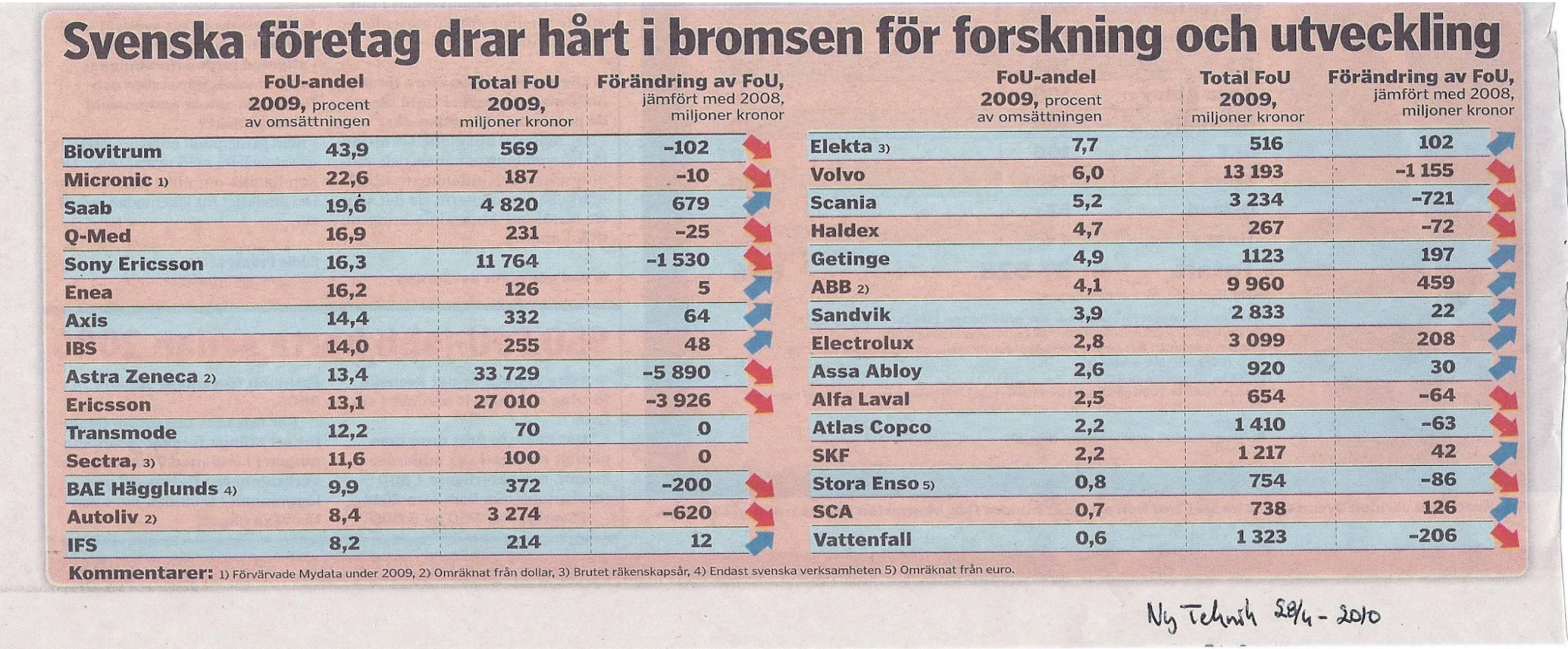
- Konfidentialitet
  - Skydd mot obehörig insyn
- Riktighet
  - Skydd mot oönskad förändring
- Tillgänglighet
  - Åtkomst för behörig person vid rätt tillfälle
- Säkerhetsåtgärder
  - Identifierad uppsättning åtgärder för att möta en organisations risker
- Tillgång
  - Allt som har ett värde för en organisation

TR 50 - informationssäkerhetsmodellen



Figur 1. Informationssäkerhetsmodell

Behovet av klassning - FoU 2010



Svenska företag drar hårt i bromsen för forskning och utveckling

	FoU-andel 2009, procent av omsättningen	Total FoU 2009, miljoner kronor	Förändring av FoU, jämfört med 2008, miljoner kronor
Biovitrum	43,9	569	-102
Micronic 1)	22,6	187	-10
Saab	19,6	4 820	679
Q-Med	16,9	231	-25
Sony Ericsson	16,3	11 764	-1 530
Enea	16,2	126	5
Axis	14,4	332	64
IBS	14,0	255	48
Astra Zeneca 2)	13,4	33 729	-5 890
Ericsson	13,1	27 010	-3 926
Transmode	12,2	70	0
Sectra, 3)	11,6	100	0
BAE Hägglunds 4)	9,9	372	-200
Autoliv 2)	8,4	3 274	-620
IFS	8,2	214	12

	FoU-andel 2009, procent av omsättningen	Total FoU 2009, miljoner kronor	Förändring av FoU, jämfört med 2008, miljoner kronor
Elekta 3)	7,7	516	102
Volvo	6,0	13 193	-1 155
Scania	5,2	3 234	-721
Haldex	4,7	267	-72
Getinge	4,9	1123	197
ABB 2)	4,1	9 960	459
Sandvik	3,9	2 833	22
Electrolux	2,8	3 099	208
Assa Abloy	2,6	920	30
Alfa Laval	2,5	654	-64
Atlas Copco	2,2	1 410	-63
SKF	2,2	1 217	42
Stora Enso 5)	0,8	754	-86
SCA	0,7	738	126
Vattenfall	0,6	1 323	-206

Kommentarer: 1) Förvärvade Mydata under 2009, 2) Omräknat från dollar, 3) Brutet räkenskapsår, 4) Endast svenska verksamheten 5) Omräknat från euro.

Ny Teknik 28/4 - 2010

Varför informationsklassning

- Enartad bedömning
- Lika skydd IT och dokument
- Känslighetsgradera
- Beslutsstöd för införande av skyddsåtgärder
- Minimera skyddskostnader
- Medvetandegöra

Vad säger standarden 27002?

- **8.2 Informationsklassning**
- **Mål:**
  - Att säkerställa att information får en lämplig skyddsnivå i enlighet med dess betydelse för organisationen.
    - **Klassning av information**

8.2.1 Klassning av information

- **Säkerhetsåtgärd**
  - Information bör klassas i termer av rättsliga krav, värde, verksamhetsbetydelse och känslighet för obehörigt röjande eller modifiering.
- **Vägledning för införande**
  - Klassning och tillhörande säkerhetsåtgärder för informationen bör ta hänsyn till verksamhetens behov av spridning eller begränsning av informationen samt till de legala kraven. Andra tillgångar än information kan också klassas i överensstämmelse med klassningen av den information som är lagrad i, behandlas av eller på annat sätt hanteras eller skyddas av tillgången.
  - Ägare av informationstillgångar bör ansvara för deras klassning.
  - Modellen för informationsklassning bör omfatta regler för klassning samt kriterier för granskning av klassificering över tid. Skyddsnivån i modellen bör bedömas genom att analysera konfidentialitet, riktighet och tillgänglighet samt andra krav för den aktuella informationen. Modellen bör anpassas till regler för styrning av åtkomst (se 9.1.1).
  - Varje nivå bör ges ett namn som passar i det sammanhang där klassningsmodellen tillämpas.
  - Modellen bör vara gemensam för hela organisationen så att alla klassar information och relaterade tillgångar på samma sätt och därmed skapa en gemensam förståelse för krav på skydd och för tillämpningen av lämpliga skydd.
  - Klassningen bör ingå i organisationens processer och vara konsekvent och sammanhängande i organisationen. Resultatet av klassningen bör ange värdet av tillgångar beroende på deras känslighet och betydelse för organisationen, t.ex. när det gäller konfidentialitet, riktighet och tillgänglighet. Resultatet av klassningen bör uppdateras vid ändringar av tillgångens värde, känslighet och betydelse under dess livscykel.

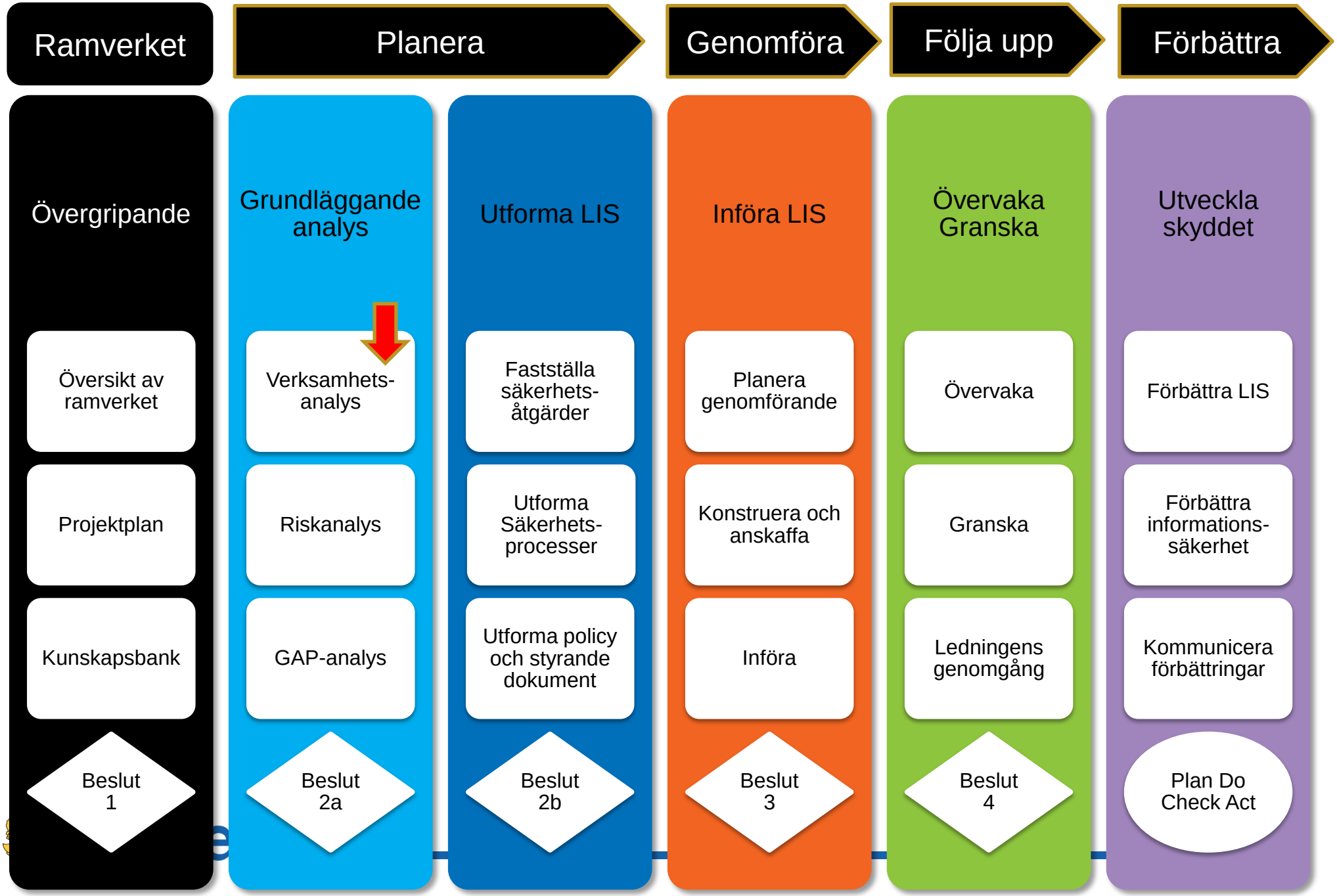
Övrig information

- Klassningen ger dem som arbetar med information en tydlig indikation på hur den bör hanteras och skyddas. Att skapa grupper av information med liknande behov av skydd och specificera informationssäkerhetsrutiner som gäller för all information i varje grupp underlättar detta. Detta tillvägagångssätt minskar behovet av att utföra en riskbedömning från fall till fall samt egendesign av säkerhetsåtgärderna.
- Information kan upphöra att vara känslig eller kritisk efter en viss tidsperiod, t.ex. när information har offentliggjorts. Dessa aspekter bör beaktas eftersom överdriven klassning kan leda till införandet av onödiga säkerhetsåtgärder vilket resulterar i extra kostnader medan motsatsen kan äventyra uppnåendet av verksamhetsmålen.
- Ett exempel på ett klassningsschema avseende konfidentialitet skulle kunna baseras på följande fyra nivåer:
  - a) utlämnande eller röjande orsakar ingen skada;
  - b) utlämnande eller röjande orsakar mindre problem eller mindre olägenheter för verksamheten;
  - c) utlämnande eller röjande har en betydande kortsiktig effekt på verksamheten eller taktiska mål;
  - d) utlämnande eller röjande har en allvarlig inverkan på långsiktiga strategiska mål eller äventyrar organisationens överlevnad.

För att kunna klassificera måste du veta på vad, vilken tillgång?

- Det finns många typer av tillgångar, inklusive:
  - **information:** databaser och datafiler, avtal och överenskommelser, systemdokumentation, forskningsinformation, användarmanualer, utbildningsmaterial, drift- och stödrutiner, organisationens kontinuitetsplaner, nödrutiner, revisionsspår och arkiverad information
  - **programvarutillgångar:** tillämpningsprogram, systemprogram, utvecklingsverktyg och stödprogram
  - **fysiska tillgångar:** datorutrustning, kommunikationsutrustning, flyttbara datamedia och annan utrustning
  - **tjänster:** data- och kommunikationstjänster, försörjningssystem för t.ex. värme, ljus, elkraft och luftkonditionering
  - **personal** och deras kvalifikationer, talanger och erfarenhet
  - **immateriella**, såsom organisationens rykte och profil.

Informationstillgångar

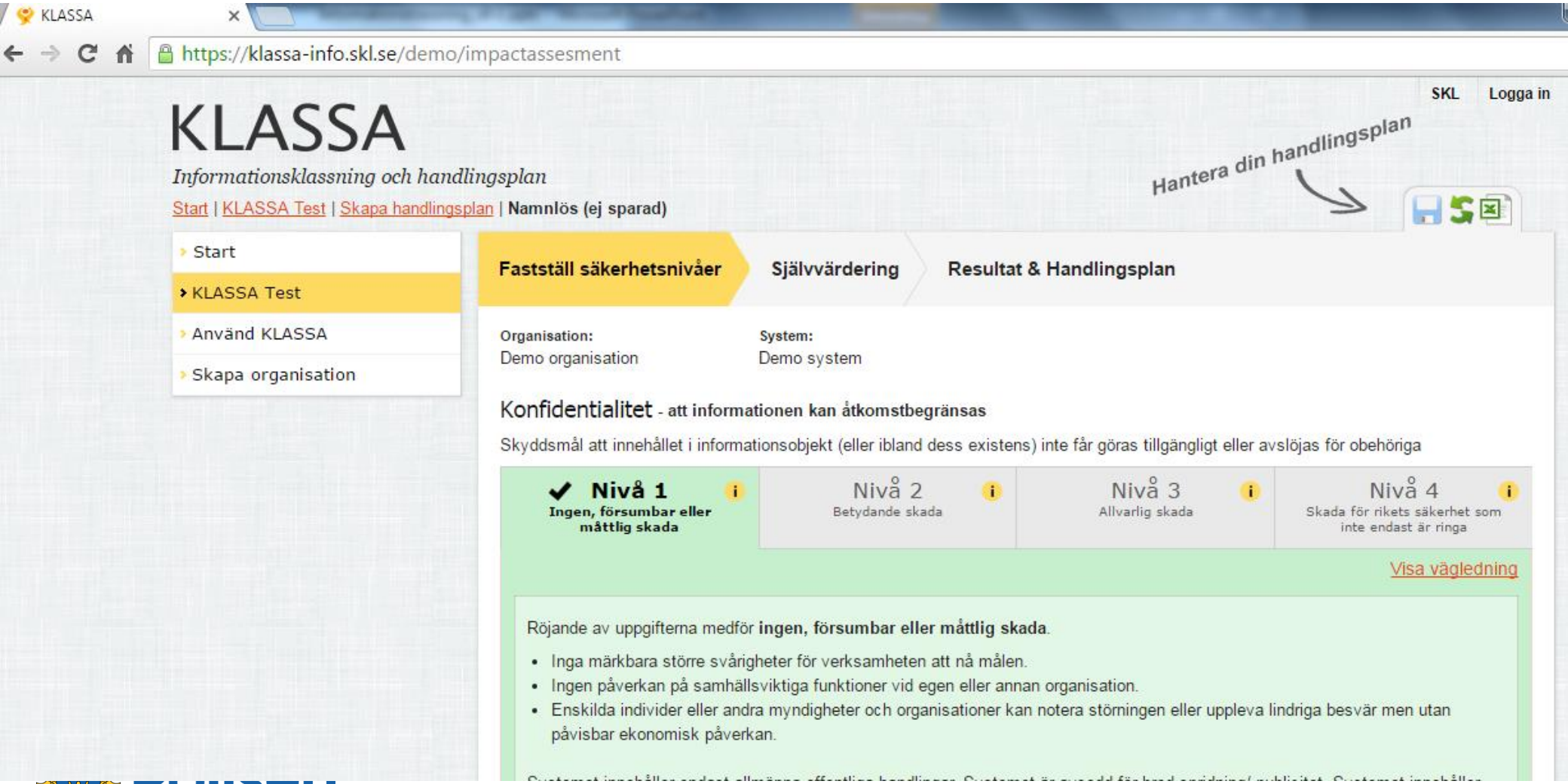

Ramverket
Planera
Genomföra
Följa upp
Förbättra
Övergripande
Grundläggande analys
Utforma LIS
Införa LIS
Övervaka Granska
Utveckla skyddet
Översikt av ramverket
Projektplan
Kunskapsbank
Beslut 1
Verksamhets-analys
Riskanalys
GAP-analys
Beslut 2a
Fastställa säkerhets-åtgärder
Utforma Säkerhets-processer
Utforma policy och styrande dokument
Beslut 2b
Planera genomförande
Konstruera och anskaffa
Införa
Beslut 3
Övervaka
Granska
Ledningens genomgång
Beslut 4
Förbättra LIS
Förbättra informations-säkerhet
Kommunicera förbättringar
Plan Do Check Act

MSB:s matris i metodstödet, verksamhetsanalys

Konsekvensnivå	Säkerhetsaspekt: Konfidentialitet	Säkerhetsaspekt: Riktighet	Säkerhetsaspekt: Tillgänglighet
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.**

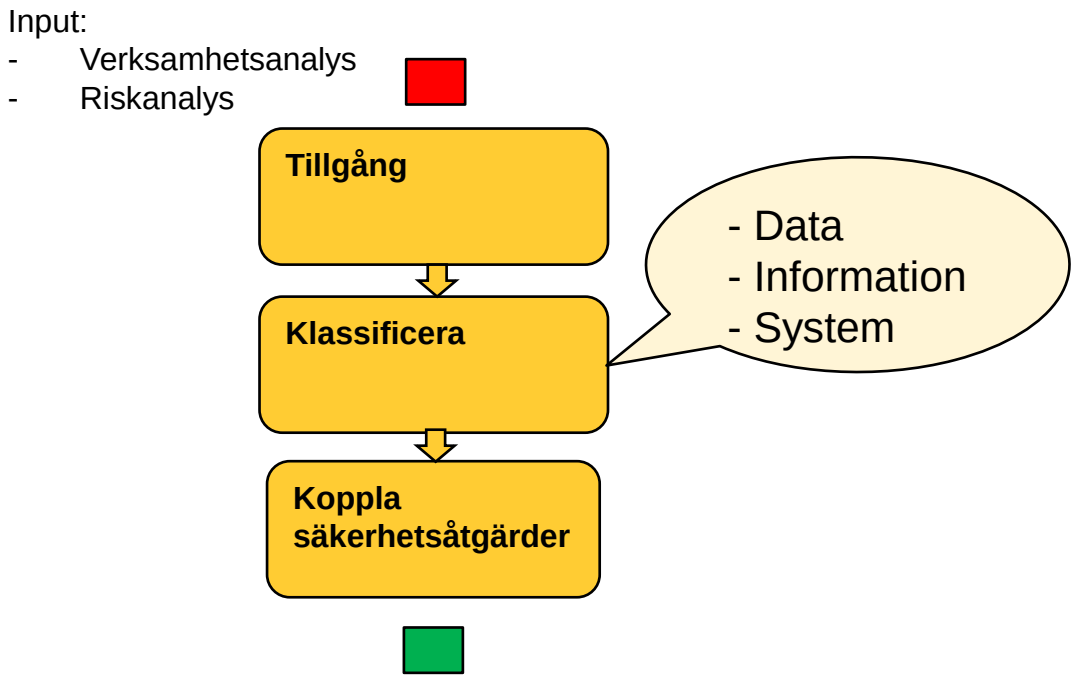
Verktyget klassa

Verktyget


KLASSA
https://klassa-info.skl.se/demo/impactassesment
SKL
Logga in
KLASSA
Informationsklassning och handlingsplan
Start | KLASSA Test | Skapa handlingsplan | Namnlös (ej sparad)
Hantera din handlingsplan
Start
KLASSA Test
Använd KLASSA
Skapa organisation
Fastställ säkerhetsnivåer
Självvärdering
Resultat & Handlingsplan
Organisation:
Demo organisation
System:
Demo system
Konfidentialitet - att informationen kan åtkomstbegränsas
Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga
Nivå 1
Ingen, försumbar eller måttlig skada
Nivå 2
Betydande skada
Nivå 3
Allvarlig skada
Nivå 4
Skada för rikets säkerhet som inte endast är ringa
Visa vägledning
Röjande av uppgifterna medför ingen, försumbar eller måttlig skada.
Inga märkbara större svårigheter för verksamheten att nå målen.
Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation.
Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

Hur används klassningen praktiskt?

- Som underlag för hantering av informationen och vilka skyddsåtgärder som skall införas!
- Kan man koppla klassen till en direkt skyddsåtgärd??



Baslinje för säkerhetsnivån

Code 17799	Security Domain	Objectives	Baseline Controls/Security Requirements	Baseline Measures/Specifications	Guideline	Links	Critical	Risk, Recommendation and Action	URD Requirements and Measures	Operational Procedures	ESCB wide policies, procedures	TP	L	M	H	C	I	A	Compliance Check	Compliance Score	Comme
5	Säkerhetspolicy						☐				G		n/a	n/a	n/a	☐	☐	☐			
5.1	Informationssäkerhetspolicy	Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med			Dokumentet ligger i vårt ledningssystem.	www..regelverk.se	☐				G		n/a	n/a	n/a	☐	☐	☐			Dokumentet togs 2008. HH
5.1.1	Information (system) security policy document		Ett policydokumentet för informationssäkerhet bör godkännas av ledningen samt publiceras och				☑	Risk: Without clear direction set out and communicated by management, risks may be			G		M	M	M	☑	☑	☑		0	

Polisen

Hantering

Kategori	ÖPPEN	KÄNSLIG	MYCKET KÄNSLIG
1. Konsekvens vid förlust	Ingen skada	Kan orsaka skada	Kan orsaka stor skada
2. Behörighet	Inga restriktioner	Begränsad spridning till de som har behov av informationen i arbetet	Starkt begränsad spridning till de som har behov av informationen i arbetet
3. Märkning	Ingen märkning, alternativt ”Hanteringsklass: ÖPPEN”	”Hanteringsklass: KÄNSLIG”	”Hanteringsklass: MYCKET KÄNSLIG”
4. Telefonsamtal	Inga restriktioner	Samtal ska föras avskilt, undvik mobiltelefoni.	Kryptotelefon ska användas
5. E-post internt	Inga restriktioner	Märkning ska framgå i ämnesraden	Ska krypteras med bankens lösning för e-post
6. E-post externt	Inga restriktioner	Ska krypteras med bankens lösning för e-post	Ska krypteras med bankens lösning för e-post
7. Intern post	Inga restriktioner	Personligen eller i igenklistrat kuvert	Personligen eller i dubbla kuvert och säkerhetstape
8. Extern post	Inga restriktioner	Ess-brev/rek	Dubbla kuvert, säkerhets-tape och Ess-brev/rek
9. Fax	Inga restriktioner	Fax övervakas under sändning/ mottagning	Kryptofax ska användas
10. Information lagrad i DHS	Inga restriktioner	Begränsad åtkomst genom behörighetstilldelning	Inte tillåtet

Erfarenheter

- Kommunicerbart
- Snabbt
- Enkelt
- Beslutsunderlag
- Utbildning/information

Frågor

För kontakt: jan-olof.andersson@polisen.se

Polisen