Informationsklassificering

Enkelt eller skäl till fördjupning?

VITALIS spår för Juridik och informationssäkerhet

2019-05-22, kl. 11:30-12:00

Monika Göransson, VGR och Markus Ekbäck, SKL

Monika Göransson, VGR

- Learning by doing…
- 20 år i landstingets tjänst med spänst
- Från Pul till GDPR
- Från ADB till Digitalisering
- Från satellitenhet inom IT till samordning med krisberedskap och säkerhetsskydd
- Från pappersjournal, till datajournal och nu på väg mot framtidens vårdinformationsmiljö

Markus Ekbäck, SKL

- Fil.kand Datavetenskap
- Certifierad CISSP CISM enl. ISO 17024
- It sedan 1995, informationssäkerhet sedan 2004
- Swedbank IT, Sun Microsystems, KTH, Säkerhetspolisen, Riksgälden, Migrationsverket, Rote Consulting, Kronofogden, Karolinska Universitetssjukhuset, IVO, SKL
- Roller it-ansvarig, CISO informationssäkerhetschef, konsult
- Områden: informationssäkerhet, dataskydd, säkerhetsskydd

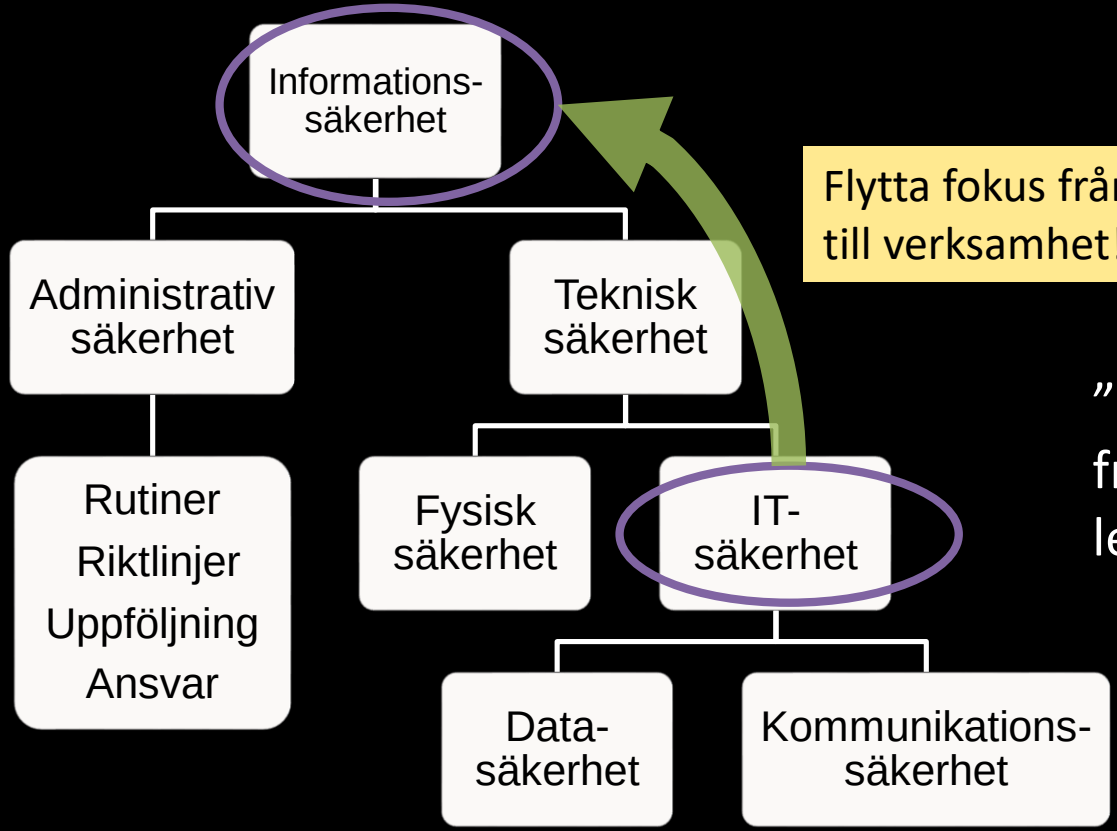
Brinnande behov av säkerhet

Misslyckanden uppmärksammas

- Transportstyrelsen
- Vårdguiden 1177
- Skolplattformen
- Heroma
- Ransomware i sjukvården
  - Hollywood Presbyterian, Tyskland, Thailand

→ Digitalisering: takten ökar men säkerhetsskulden ökar mer! (”digitaliseringsgapet”)

Vad är informationssäkerhet?



Flytta fokus från IT till verksamhet!

”En organisationsresa från datahallen till ledningsrummet”

Varför klassificera information?

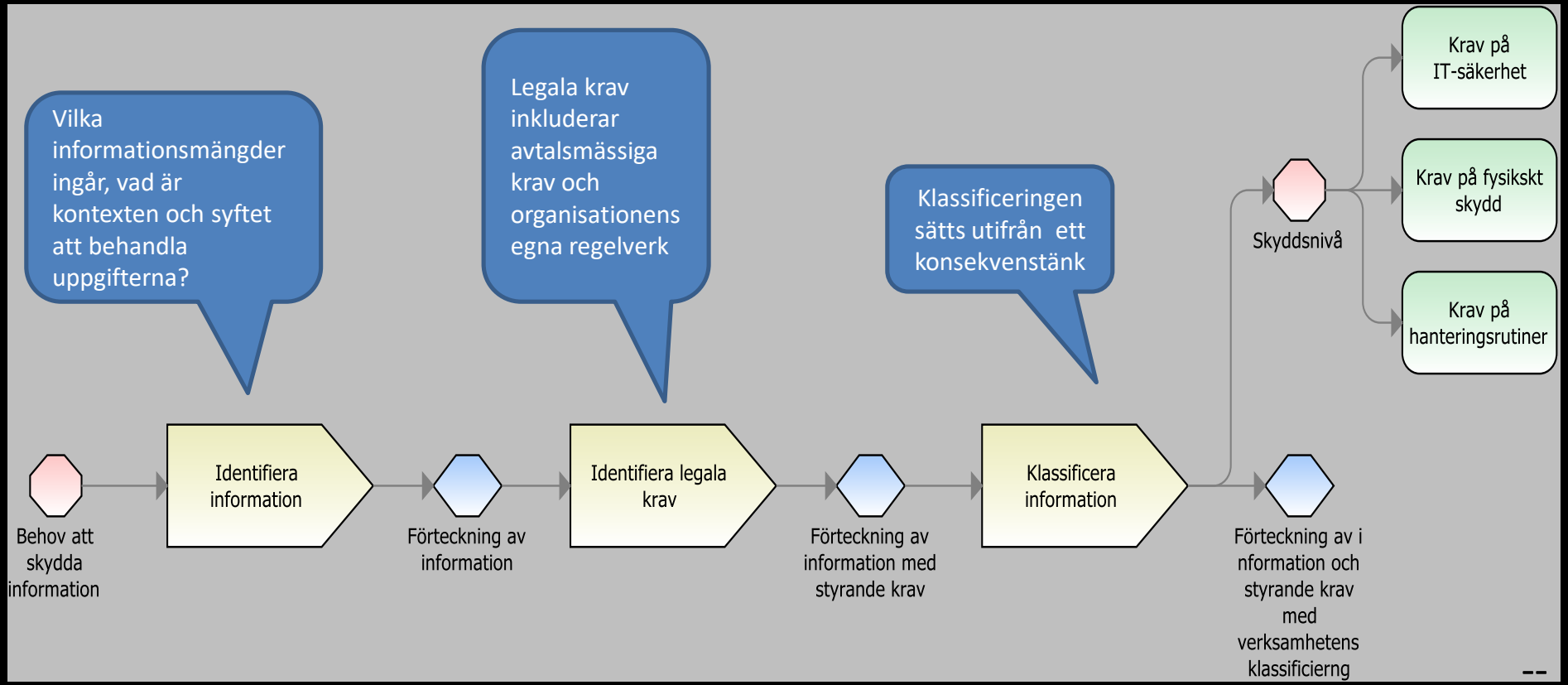
- för att avgöra informationens skyddsvärde

- Tydliggöra informationsmängder och -ägare
- bedömning o utformning av **skyddsåtgärder**
- Utformning av **hanteringsrutiner** i verksamheten

- underlag för riskanalys
- underlag för kontinuitetsplanering

Informationsklassificering handlar också om att förstå och se samband i hantering av teknik, verksamhet och människor

Process

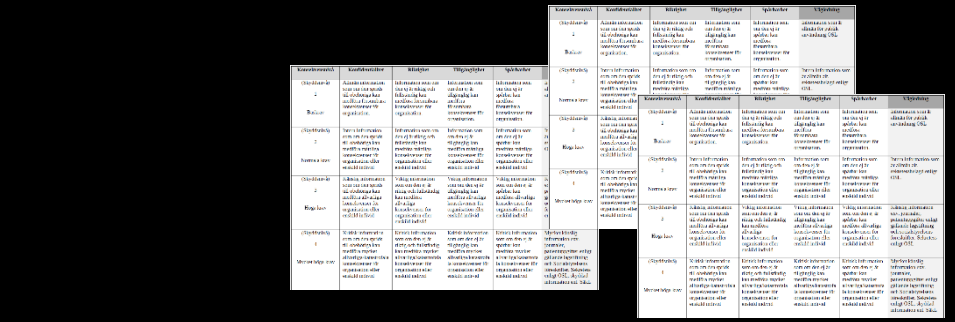

Vilka informationsmängder ingår, vad är kontexten och syftet att behandla uppgifterna?
Legala krav inkluderar avtalsmässiga krav och organisationens egna regelverk
Klassificeringen sätts utifrån ett konsekvenstänk
Behov att skydda information
Identifiera information
Förteckning av information
Identifiera legala krav
Förteckning av information med styrande krav
Klassificera information
Skyddsnivå
Förteckning av information och styrande krav med verksamhetens klassificierng
Krav på IT-säkerhet
Krav på fysikskt skydd
Krav på hanteringsrutiner

Etablerad modell för klassning

Informationsklassificering handlar om att bedöma hur skyddsvärd den aktuella informationen är och vilka konsekvenser det får för verksamheten om informationen inte är;

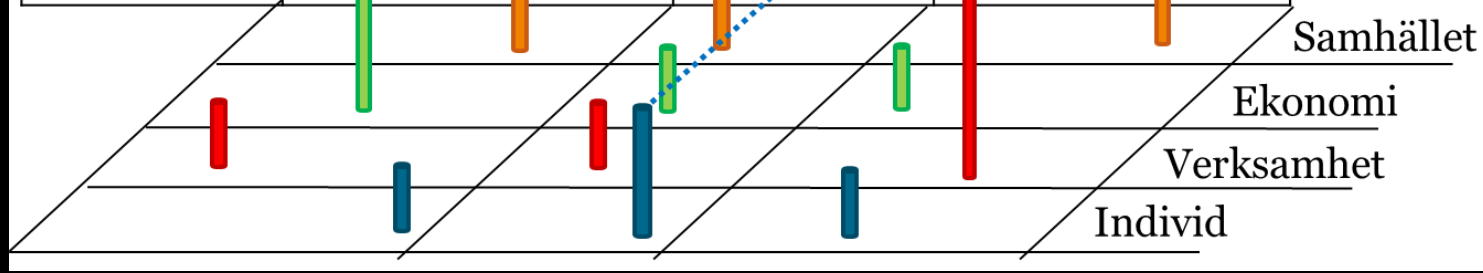
- tillgänglig
- konfidentiell
- riktig
- (spårbar)

i enlighet med legala krav och verksamhetens behov.



Det underlättar att använda olika perspektiv

Aspekt / Nivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	K3	R3	T3
Betydande	K2	R2	T2
Måttlig	K1	R1	T1
Ingen	K0	R0	T0



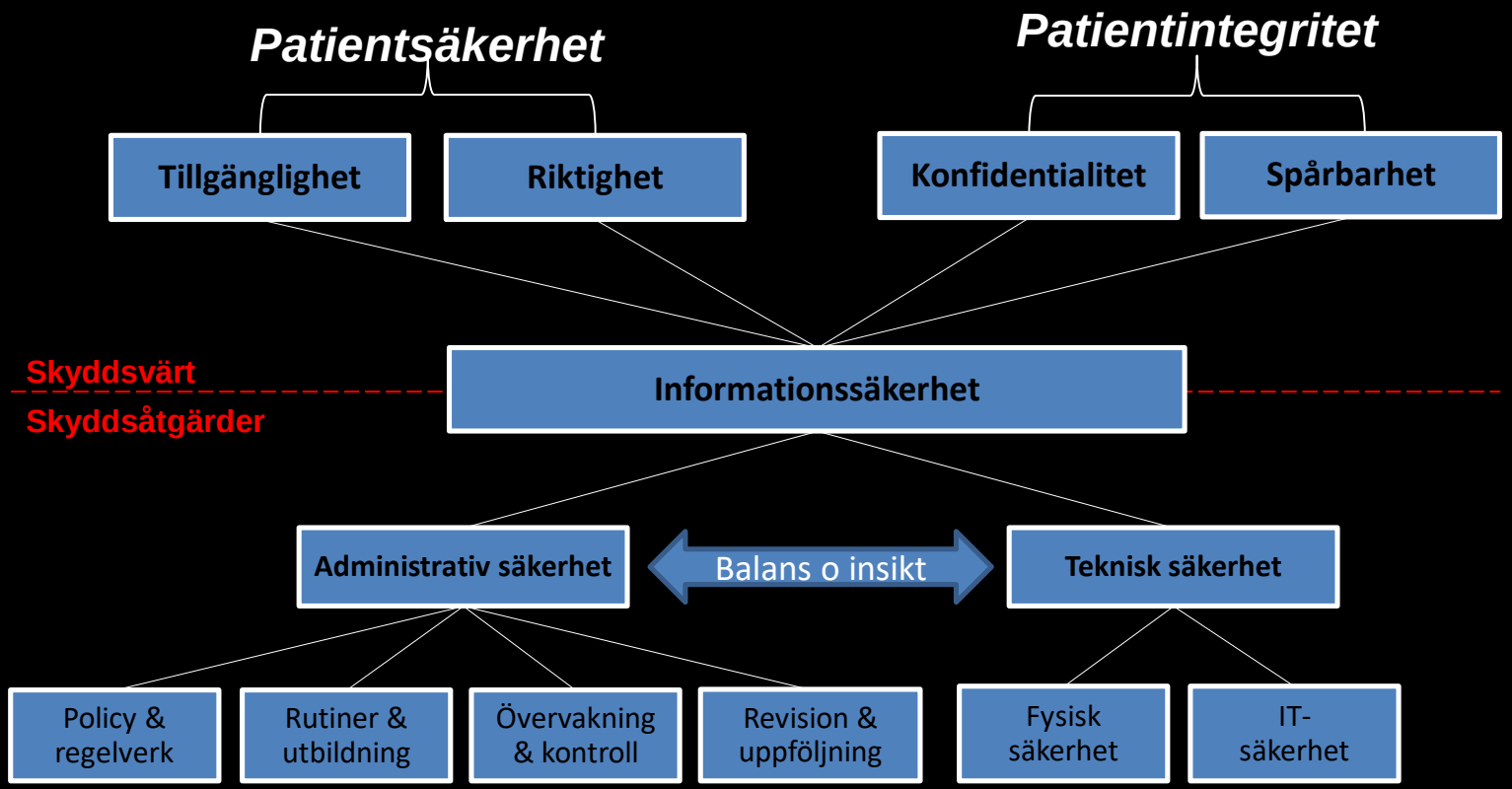
Källa: informationssäkerhet.se

Förenklad klassificering (Sic)

1. Öppna uppgifter / öppna data
2. Interna uppgifter
3. Personuppgifter (PU)
4. Känsliga personuppgifter (t.ex. hälsa/vård, fack, sexuell läggning)

→ Fördelar: förenklar, snabbare, lättare med hanteringsregler

→ Nackdelar: fråntar verksamhetens ansvar för sin information, ej riskbaserat



Bildens ursprung Ph.D. Rose-Mharie Åhlfeldt, Högskolan i Skövde

Självklart och lekande lätt?

Information hanteras i dokumentform, i enskilda avgränsade system eller information som ingår i komplexa miljöer.

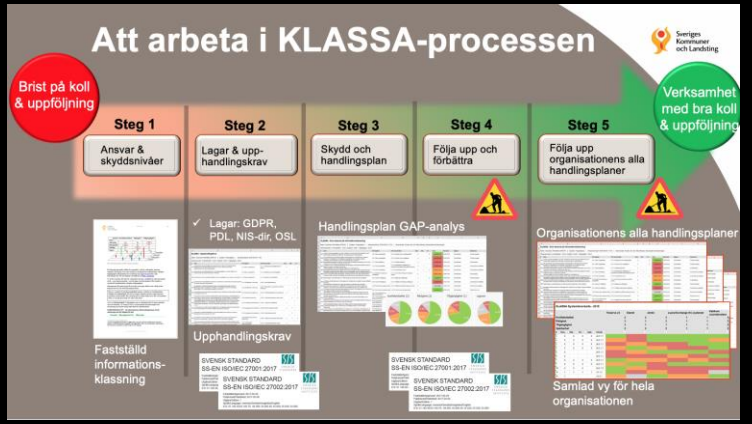
Det går en vattendelare när det gäller information som den enskilde användaren själv måste kunna klassificera jämfört med information som hanteras i en etablerad tjänst (jämför excelfilen och e-receptet)

Därför behöver metoder för klassificering nyanseras och utvecklas så att modellen kan appliceras på både det lilla och det stora

Framgångsfaktorer

- En iterativ process som ger fördjupad förståelse och resultat
- Använd befintliga och förvaltningsbara strukturer

- Att få ut ett tydligt resultat, t.ex. handlingsplaner och upphandlingskrav



SKL:s it-stöd ”KLASSA”: klassa-info.skl.se

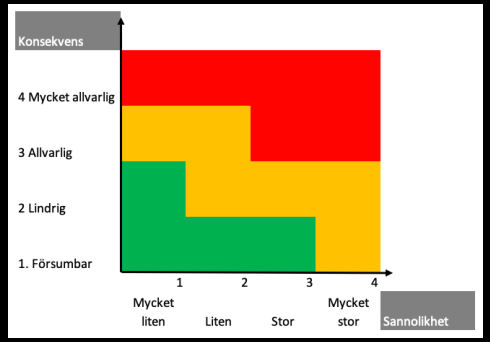
Synergier
– närliggande områden som kan stötta

- Registerförteckning enl GDPR
- Arkivredogörelse
- Informatik
- Arkitektur
- Datakatalog – BI

Information beskrivs på flera olika sätt, det kan leda till förvirring,

– men det kan också nyttjas och stötta varandra

RISK



Hur hänger RISK ihop med klassningar?

Det som tillförs är sårbarheter och sannolikhet!

RISK består av avsikt och förmåga respektive sannolikhet och konsekvens

→ RISK hjälper för att prioritera åtgärder

Summering

- Informationsklassning – olika synsätt
- Problematiseringar
- Närliggande områden
- Risk som möjliggörare
- Summering