Föreläsning SARE

Roger Lindblom
Secorum AB
Roger.lindbolom@secorum.se
0737 500 650

Mål med dagens föreläsning

- Dagens logghantering – hur ser den ut?
- Vad är modern logghantering?
- Vad finns utanför ”boxen”
- Kravställ på ett nytt fungerande logghanteringssystem(egna övningar)

SECORUM

Behov av en förbättrad logghantering

- Orsaker
  - Styrande lagstiftning
    - Ex: Patientdatalagen
      - Sammanhållen journalföring mellan vårdgivare
      - Ett uttalat ansvar för behörighetsstyrning
      - Att föra behandlingshistorik (loggar) och att följa upp loggarna
  - Kommande Dataskyddsförordning från EU
  - Kritik från tillsynsorganisation
    - Ex: Datainspektionen
      - DI:s tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet.
  - Skada som uppstått till följd av intrång, bristande detektering med mera
    - Skada redan skedd genom förlust eller läckage av data
    - ”Byxorna nere”
  - Problem med dagens logghantering
    - Bristande information i loggarna
    - Vad ska loggas?
    - Svårförstådda loggar som kräver tolkning av tekniker

SECORUM

General Data Protection Regulation (GDPR)

- This is a Regulation not a Directive - will have immediate effect on all 28 EU Member States after the two-year transition period
- Replaces EU Data Protection Directive 95/46/EC (in Sweden – PUL)
- Timeline: law by the year end 2015, transition period 2 years
- Controversal law with high stakes – further delay is highly probable
- The regulation is still a draft, this presentation is based on European Parliament legislative resolution of 12 March 2014

SECORUM

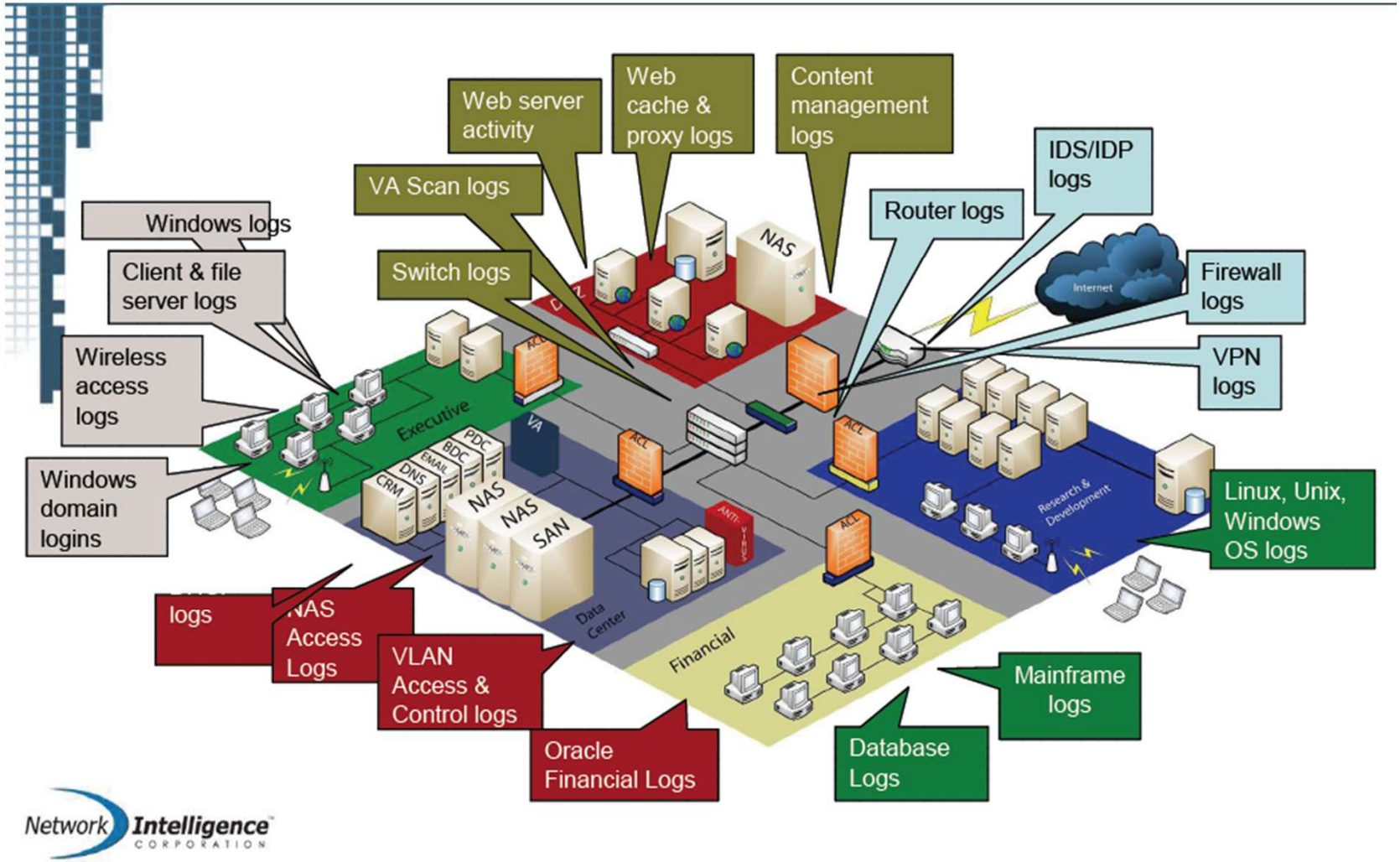
General principles for data subject rights

Any person should have:

- **Right of access** - to data which has been collected concerning them, including information about the purposes of the processing, recipients to whom data has been disclosed, period for storage and the rights of the subject.
- **Right to erasure** – of personal data concerning them, for example where the storage period consented to has expired or consent is withdrawn.
- …

SECORUM

Loggar inom organisationen



Regelstyrd loggning

FAP 174-1

- Loggning ska ske av varje ***åtkomst*** till och aktiviteter i IT-system som är avsedda för behandling av ***särskilt skyddsvärda*** uppgifter i PUL 13, 21§§ samt som omfattas av Offentlighets- och sekretesslagen)
- Åtkomst är ”allt”
- Ger ingen eller ringa vägledning i frågan om vad som ska loggas

Effekt:

Ingen kan logga ”allt”, vilket innebär en begränsning som skiljer sig från projekt till projekt

Resultat:

Alla IT-system loggar olika information

För att bygga en gemensam analysfunktion MÅSTE vi kravställa på vad vi ska logga

SECORUM

Ytterligare exempel på regelstyrd loggning

- Behovet av loggning och uppföljning av loggar bestäms av objektsägaren och utgår från verksamhetens behov och en informationsklassificering.
- Loggar ska finnas så att aktiviteter som utförs av personer med hög behörighet kan spåras. De ska även skyddas mot radering, manipulation och obehörig åtkomst.

- Vad ska då loggas?
- Vem inom ”verksamheten” kan kravställa på vad som ska loggas?

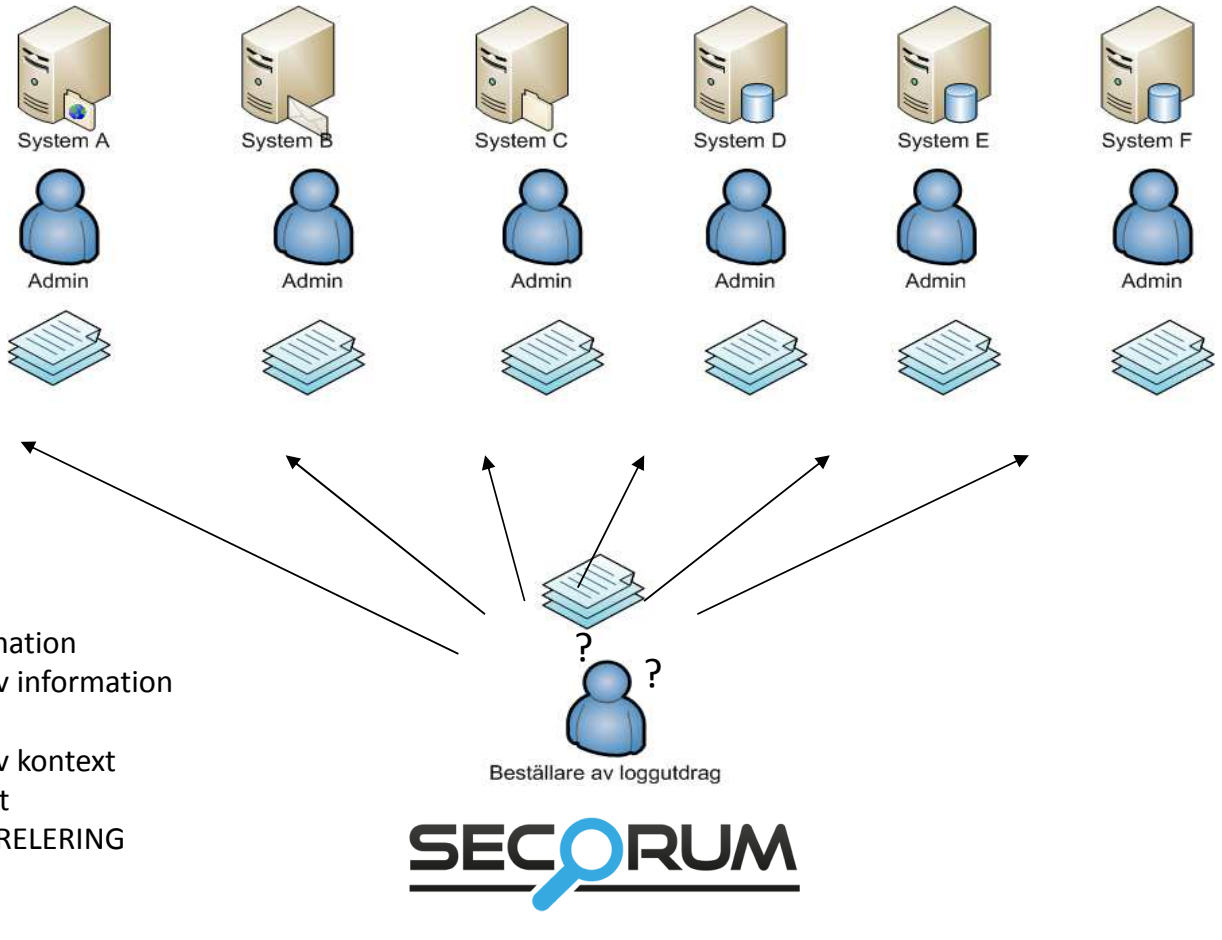
SECORUM

Några problemområden inom myndigheter

- Är loggposten en allmänna handlingar?
- Rätt att ta del av allmän handling i form av globalfil, RegR dom 1999-04-14, mål nr 5556-1998
- När uppstår loggposten som allmän handling?
- Tryckfrihetsförordningen 2 kap 3 § (förklarar vad en allmän handling är).
- När uppstår loggposten som en allmän handling?
- Vad gäller om vi vill:
- Filtrera
- Berika
- Överföra loggdata till ett centralt arkiv – Vad är kopia och vad är original?
- Krävs en enskild sekretessprövning av varje enskild loggpost vid begäran om ett utlämnande?
- ?

SECORUM

Så här ser det ut idag (regelstyrd loggning)



- Olika Information
- Avsaknad av information
- Obegripligt
- Avsaknad av kontext
- Olika format
- INGEN KORRELERING

SECORUM

Att ta sig utanför boxen

- Vägen till förståelse mot en fungerande logghantering
  - Genom att utgå från analysbehoven
  - Genom kravställning

SECORUM

Vad är logghantering

Googla på orden ”logghantering” och ”definition”

Högst rankat resultat: En föreläsning av Roger Lindblom från konferensen Rätt Säkerhet 5 maj 2010 utlagd på www.sis.se

Ranking nr 2: E-uppsats angående Försvarsmaktens upphandlingsunderlag av ett nytt logghanteringssystem, en uppsats om ett upphandlingsunderlag skrivet av bland annat Roger Lindblom på Försvarsmakten åren 2008 – 2009.

www.diva-portal.org (Digitala Vetenskapliga Arkivet)

VÅR DEFINITION AV LOGGHANTERING

utgörs av loggpostens livscykel kopplat till en modern logghanteringsprodukt

- Skapa (kräver kravställning på vad som ska loggas)
- Insamla (kräver kravställning på hur insamlingen ska gå till)
- Bearbeta (kräver kravställning på vad som kan bearbetas i form av adderas, filtreras, berikas m.m.)
- Lagra (Kräver kravställning på vad som är en säker lagras, lagringstider m.m.)
- Analysera (Kräver kravställning på vad som är våra analysbehov)
- Radera (Kräver kravställning på vad som ska raderas, hur det ska ske och var)

SECORUM

Begrepp inom området logghantering

- SIEM system:

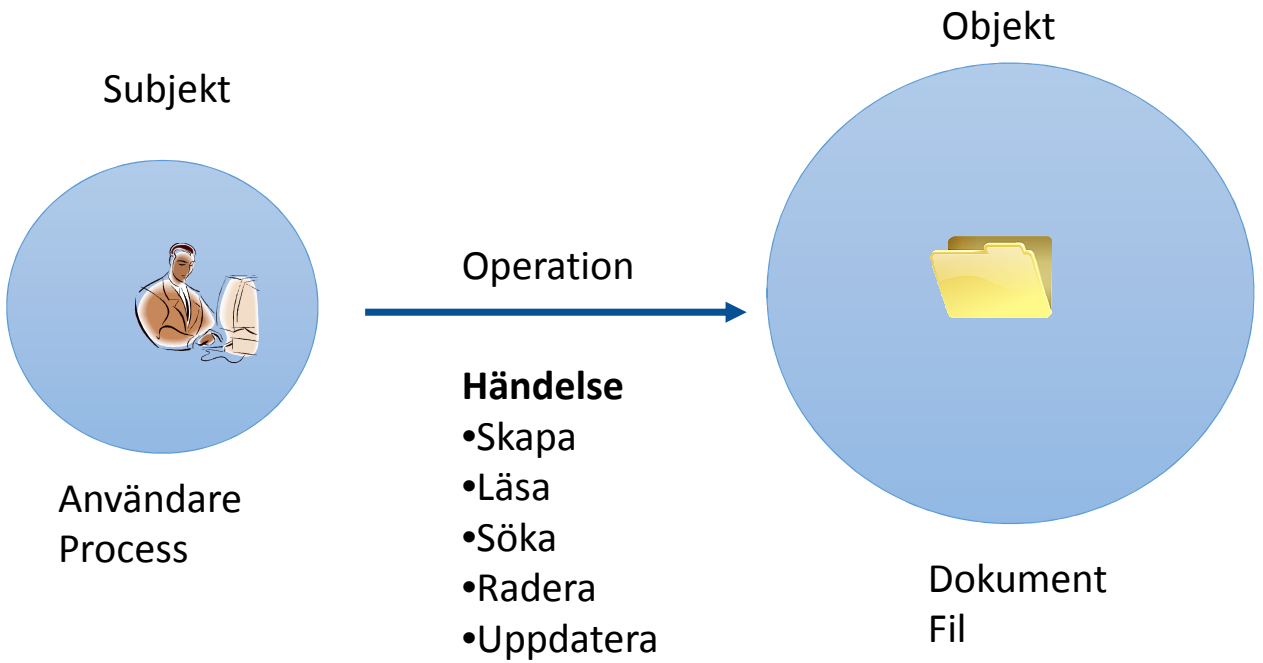
  Security Information &
  Event Management

  Kombination av logghantering
  och realtidsanalys

- **Normalisering**
  - Mappning mot analysfunktionens schema
- **Kategorisering**
  - Identifiering av loggpostens andemening
- **Korrelering**
  - Beskriv andemeningen i en enskild loggpost
- **Aggregering**
  - 1.000 → visas som 1
- **Taxonomi**
  - Produktens schema och ”bild av världen”

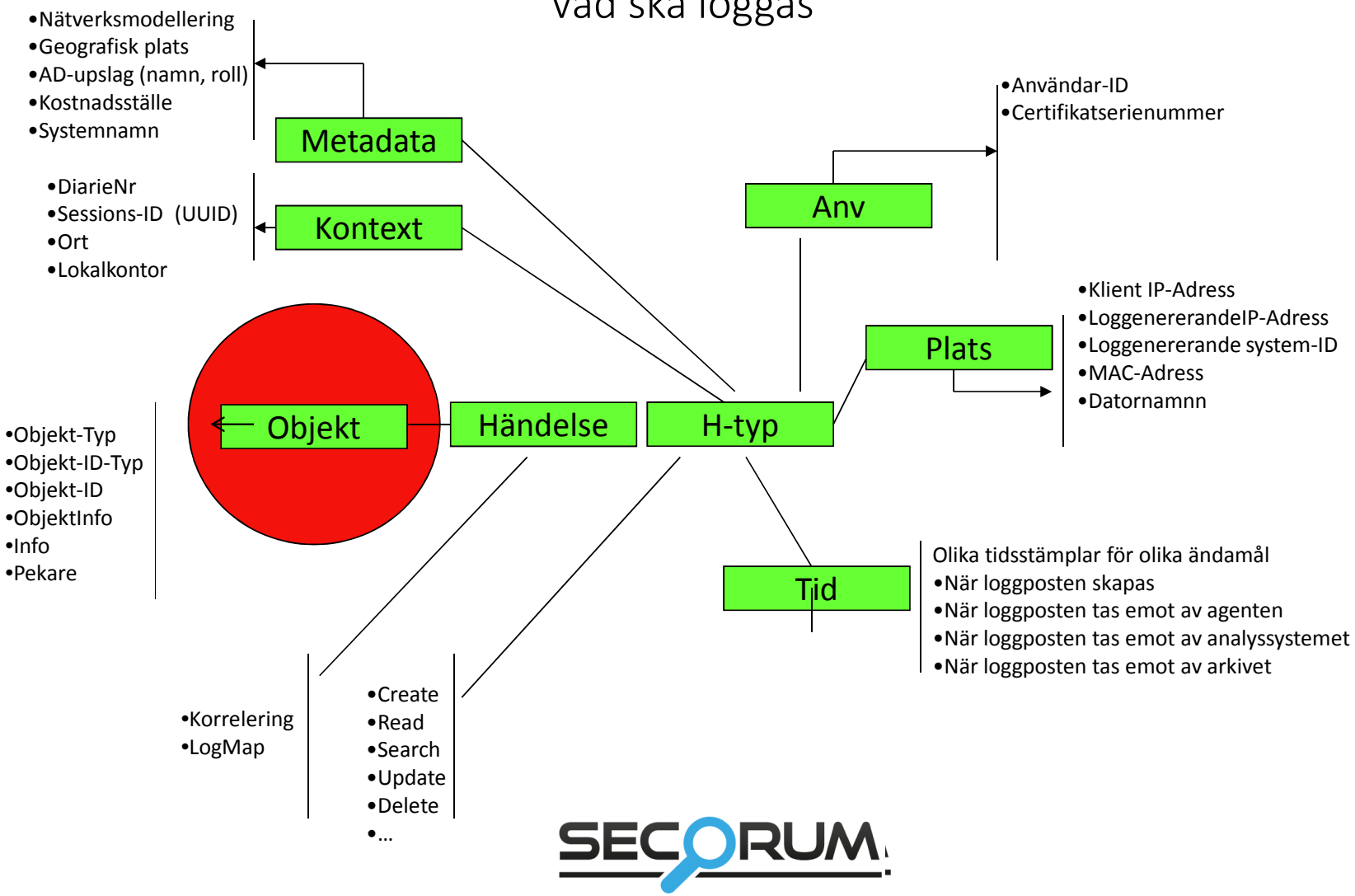
SECORUM

Vad är en loggpost?



Mer utvecklad loggpost

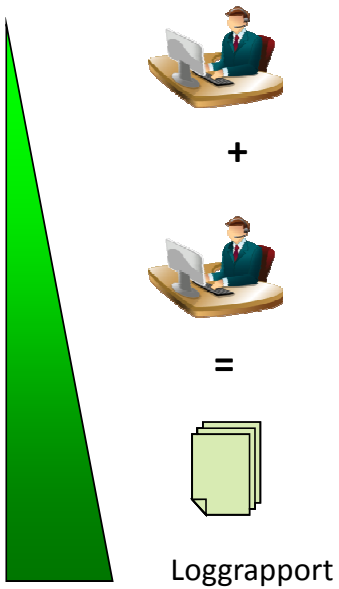
Vad ska loggas



Lokal loggkontroll (kodade värden i loggen)

Kombination av logg och databas

Lågt informationsvärde



Högt informationsvärde

1. 2010:04:15
   12:00:10+0200|Läsa|191212121212|Intervju|Dokument_id|
   5068799|0|319752|1|319752|20100505140000|EXD_REFRESH|TB
   E|938|1|1|938|191212121212|1|

2. SELECT dokumentnamn, forfattare FROM Tabell_X
   WHERE Dokument_id=”5068799”;

3. 12:00:10+0200|Läsa|191212121212|Intervju|Dokument_id|506879
   9|0|Intervju med Sture Svensson 2010-05-05 kl 14:00|Roger
   Lindblom|0|319752|1|319752|20020529135723| EXD_REFRESH|
   TBE|938|1|1|938|191212121212|1|

RESULTAT

En loggrapport som är helt OK

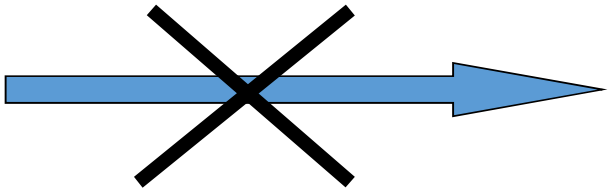
SECORUM

Central logganalys

Samma logg

2010:04:15 12:00:10+0200|Läsa|191212121212|Intervju|Dokument_id |5068799|0|319752|1|
319752|20100505140000|EXD_REFRESH|TBE|938|1|1|938|191212121212|1|

+



Applikationens databas nås ej

=

2010:04:15 12:00:10+0200|Läsa|191212121212|Intervju|Dokument_id |5068799|0|319752|1|
319752|20100505140000|EXD_REFRESH|TBE|938|1|1|938|191212121212|1|

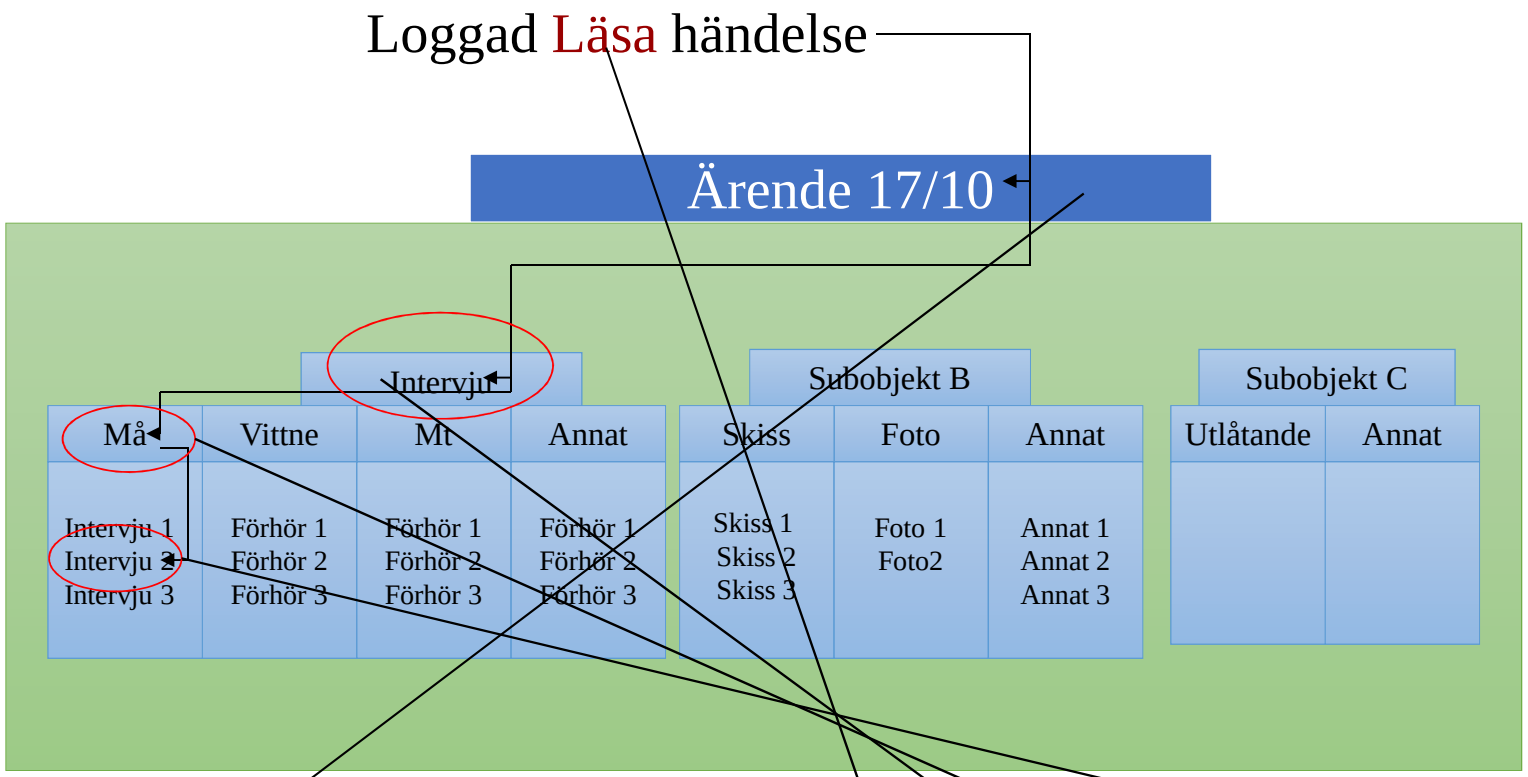
=

RESULTAT

Analysen kan inte fullföljas utan uppslag mot applikationens databas. Dokument-ID 5068799 säger inget utan översättning

SECORUM

Exempel på en fungerande loggning



FV1|1455|System A|KFM|20140303T17:14:05.438+0200|EX123456|||3b86c21c264a4117bbda4878fe95f14|
192.168.10.12|173.122.10.22|PC-1234|systemA.rsv.se|Read||0|Intervju,Må|Intervju-ID|Intervju2|||
Diarienr=0203-K17-10||||||||||

Vad vi kan göra idag med modern logghantering

- Korrelera, det vill säga se samband mellan händelser som sker i loggposter från samma eller olika IT-system
  - Samordningsvinsten inom en organisation
    - Vilka gör slagningar mot objekt under bevakning?
    - Vilka hanterar samma ärende ovetande om varandra?
  - Logistiklösningar inom flyget
    - Passagerare och bagage ombord på samma plan
  - Jämförelse mellan teori och verklighet
    - En organisations bedömning av framgång efter nya tekniska installationer för att minimera hot och en felaktig informationshantering
  - Användarnas hantering av informationen i ett eller flera IT-system före, under och efter en utbildning
  - Visualisera organisationens minne och lära av genomförda misstag
    - Spela upp ett beteende och följ varje steg i syfte att lära inför framtiden
  - Visualisering av flöden mellan olika IT-system och dess funktioner
    - Patientremisser

SECORUM

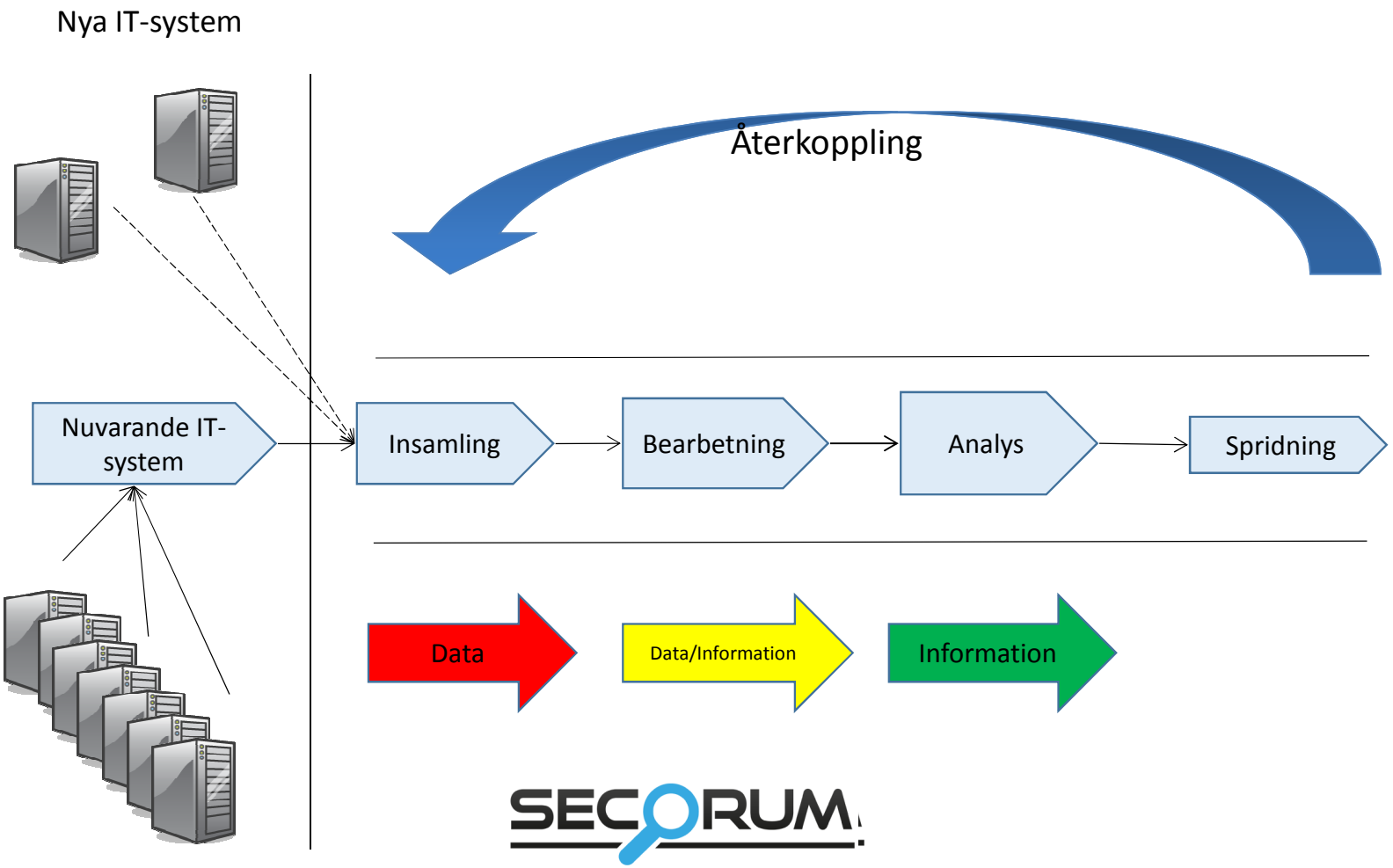
Kravställning och metoder

SECORUM

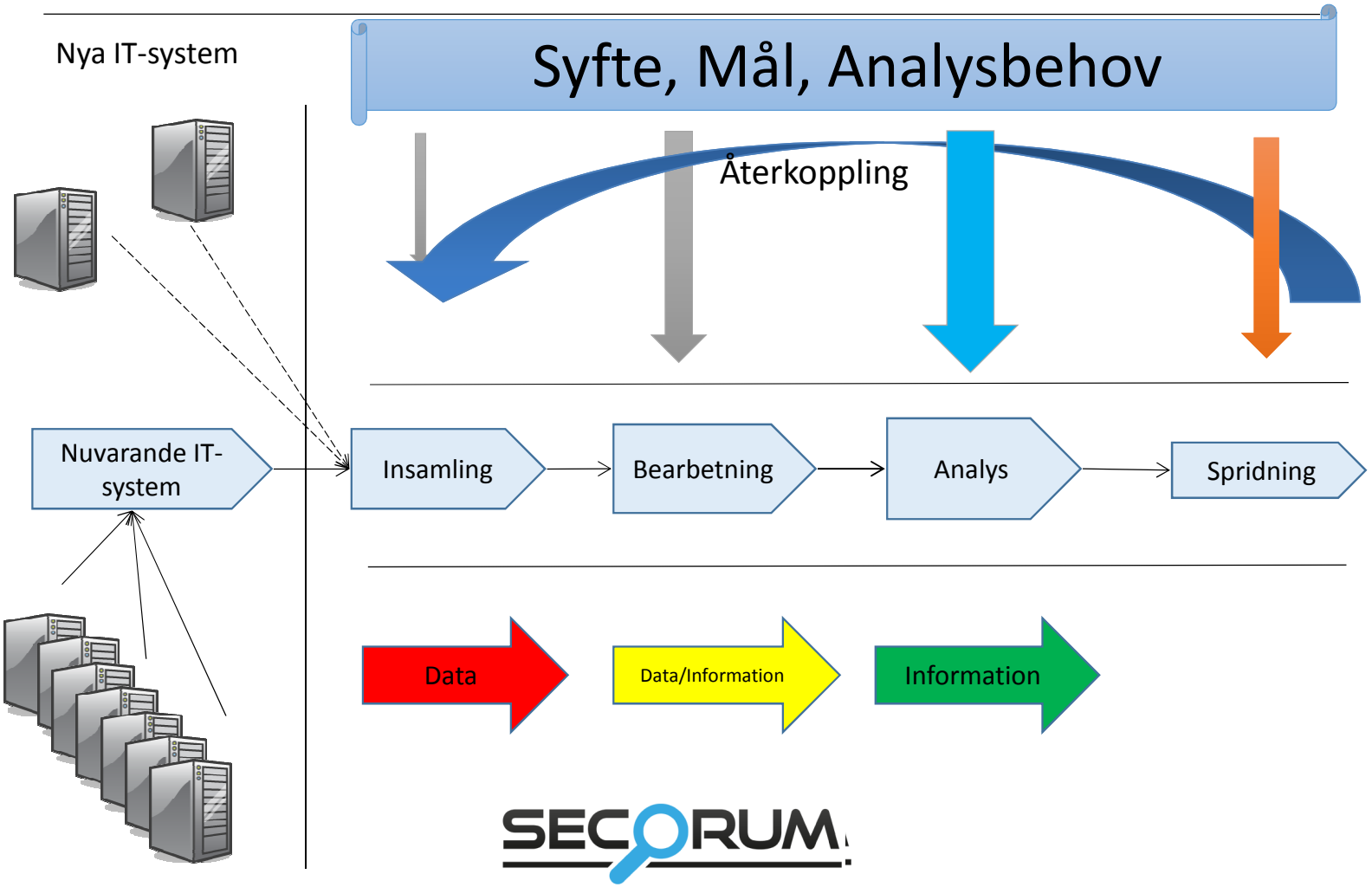
Logghantering
Top down

SECORUM

Vi snor en modell som redan finns



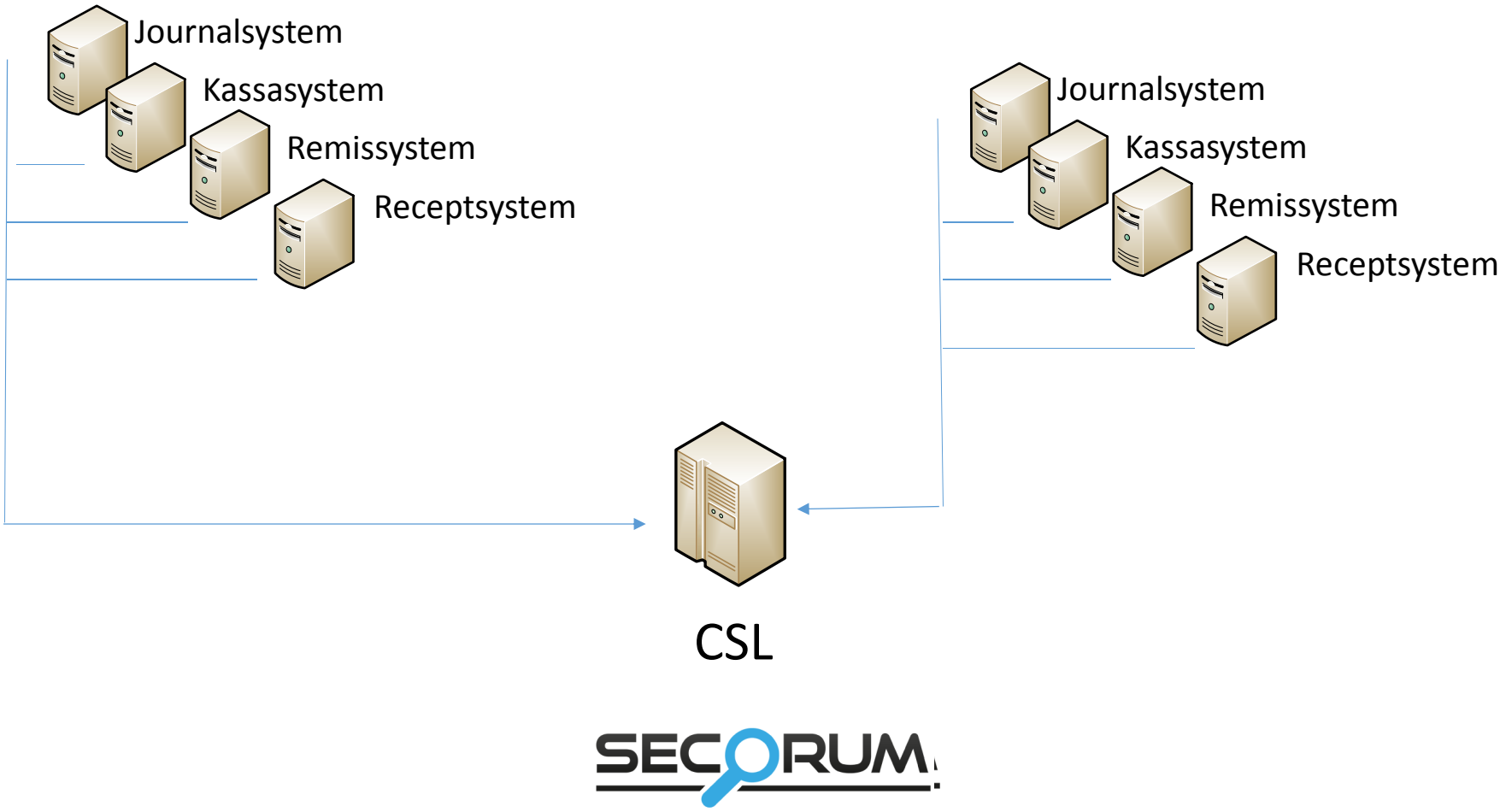
Som anpassas den till våra behov och syften



Syfte (utgångsläge grupparbete)

1. Det ska gå att leverera loggutdrag som är **förståeliga** för en lekman.
2. Övergå från en manuell reaktiv analys till en maskinell **regelbaserad realtidsanalys**
3. Använda loggdata i syfte att minimera eller eliminera fortsatt **informationsläckage** eller **informationsförlust** (detektering och reaktion) genom att analysera loggdata i realtid
4. Det ska vara möjligt att fatta långtgående interna och externa beslut baserat på tilltron till loggpostens informationsinnehåll
5. Loggposten ska återspegla användarens operationer i IT-systemet, inte systemets operationer
6. Analysen ska kunna baseras på åtkomsten till den samlade mängden information (korrelering)

SECORUM


Journalsystem
Kassasystem
Remissystem
Receptsystem
Journalsystem
Kassasystem
Remissystem
Receptsystem
CSL

Patientdatalagen kravställer på en:

- **Sammanhållen journalföring**, vilket innebär att flera vårdgivare kan ge och få direktåtkomst till varandras journalhandlingar om de uppfyller patientdatalagens krav.
- **Inre sekretess** – en reglering som innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter. Detta förtydligas genom att det i lagen ställs krav på behörighetstilldelning och åtkomstkontroll. (Räcker det? Kan man på förhand säga vem som blir sjuk?)
- Patienten har rätt att **spärra** uppgifter både i vårdgivarens journalsystem och för andra vårdgivare vid sammanhållen journalföring.
- Vårdgivare har en möjlighet att ge patienten **direktåtkomst**, exempelvis via internet, till vårddokumentation och loggar (det vill säga historiken för behandlingen av personuppgifterna).

SECORUM

Grupparbete

- Grupparbete med 6 -7 deltagare i varje grupp
- Varje grupp får samma arbetsuppgift:
  - Ni utgör förvaltning och verksamhet kring ett (av fyra) sjukjournalsystem som ska anslutas till en Central Säkerhetslogg
    - Beroenden finns mellan följande system:
      - Patientavgift (kassan)
      - Sjukgymnastik
      - Remiss
      - Recept

  - 1. Vilken *känslig info* kan tänkas finnas i de olika patientjournalsystemen?
  - 2. Vilka *analysbehov* kan tänkas finnas (vad vill vi kunna upptäcka?)
  - 3. Vilka händelsetyper är aktuella att logga (Söka, Läsa, Uppdatera, Inloggning m.m.)
  - REDOVISNING
  - 3. Vilka *händelsetyper* i systemet bör loggas (läsa, skriva …?)

  - 4. Vad ska loggas för att uppfylla analysbehoven? (ingår inte i övningen)
    - Härledning från dina analysbehov

SECORUM

Analysbehov i övningen

- Följa olika remissflöden
- Kedjan provtagning, labbundersökningar och svar
- Förekommer överdosering av läkemedel
- Missbruk av mediciner
  - Besöker en patient flera olika sjukvårdsinrättningar med samma besvär
- Fanns en vårdrelationer mellan patient och vårdinrättning dagen för slagningen eller ej
  - Remisser
  - Kassan
  - Sjukgymnastik
- Vilka har läst min journal
- När spärras en patient sin journal
- Vilka läser spärrade journaler
- Tilldelade behörigheter i journalsystemet (alla gånger ett AD)

SECORUM

Var finns dina kravställare?

- Dagens beställaren av loggrapporter
- Internrevision
- Systemägare
- Incidentutredningsteam
- Interna utredningsenheter
- Chefsjurist
- Säkerhetschef
- Hos personal som gör dagens loggutdrag
- Hos logganalytiker inom andra organisationer (samverkan)
- **Konsulter som byggt upp logghanteringsförmågan tidigare**

SECORUM