Hur vårt systematiska informationssäkerhetsarbete underlättar efterlevnaden av GDPR och andra regleringar

Jan-Olof Andersson, 2018-09-05

Pass 2: 09:45 – 10:20

Vem är JOA?

- **Titel:**
  Informationssäkerhetschef och Dataskyddsombud för ICA Sverige

- **Övriga uppdrag:**
  Ordförande i svenska standardiseringskommittén för informationssäkerhetsstandarder, 27000 serien.

- **Tidigare uppdrag:**
  Yrkesofficer, säkerhetshandläggare på Vattenfall, Säkerhetschef på Ericsson Telecom, Säkerhetsexpert på Trygg-Hansa, Risk manager på Bull och Säkerhetschef på Riksbanken, Läkemedelsverket, Rikspolisstyrelsen och Polismyndigheten.

- **Familj:**
  Fru och två vuxna barn och fyra barnbarn.

- **Intressen:**
  Båt och matlagning. Skriva handböcker inom informations-säkerhetsområdet.

Agenda

1. Kort om ICA
2. Hur bygger vi upp ett informationssäkerhetsarbete som är effektivt?
3. Ledningssystemet

Omsättning 2017

106,5 Mdkr

Rörelseresultat* 2017

4,6 Mdkr

Rörelsemarginal* 2017

4,4%

ICA Rimi ICA Fastigheter APOTEK ICA

ICA Banken ICA Försäkring HEMTEX

Hur bygger vi upp ett informationssäkerhetsarbete som är effektivt?

Tar hänsyn till standarder, integrerar GDPR och skapar ett systematiskt arbetssätt

Vad är LIS – Förväntat resultat av införande

Förväntat resultat av LIS är en integrerad och effektiv process för informationssäkerhetsarbetet som skapar enkelhet, relevant nivå och ansvarstagande, i linje med ICAs värderingar

INPUT:

Krav och förväntningar från organisationen.

Intern och extern påverkan, i form av risker och händelser.

Ha koll/Förstå → Styra och samordna → Skydda (Göra) → Hantera händelser

OUTPUT:

Verksamheten kan utföras utan allvarliga störningar.

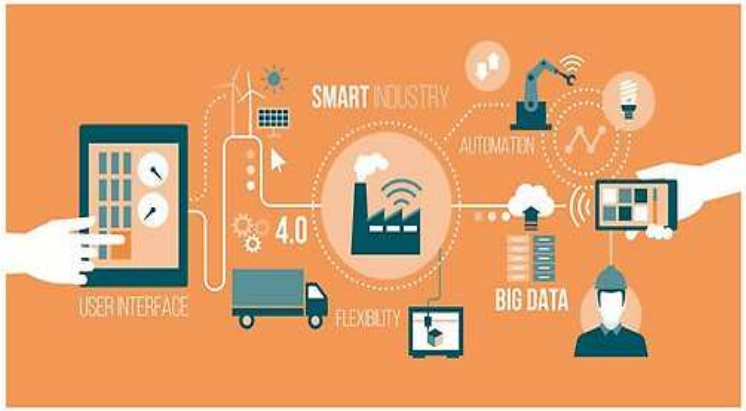
Allvarliga störningar kan hanteras

Introduktion till informationssäkerhet på ICA Sverige – vårt beroende

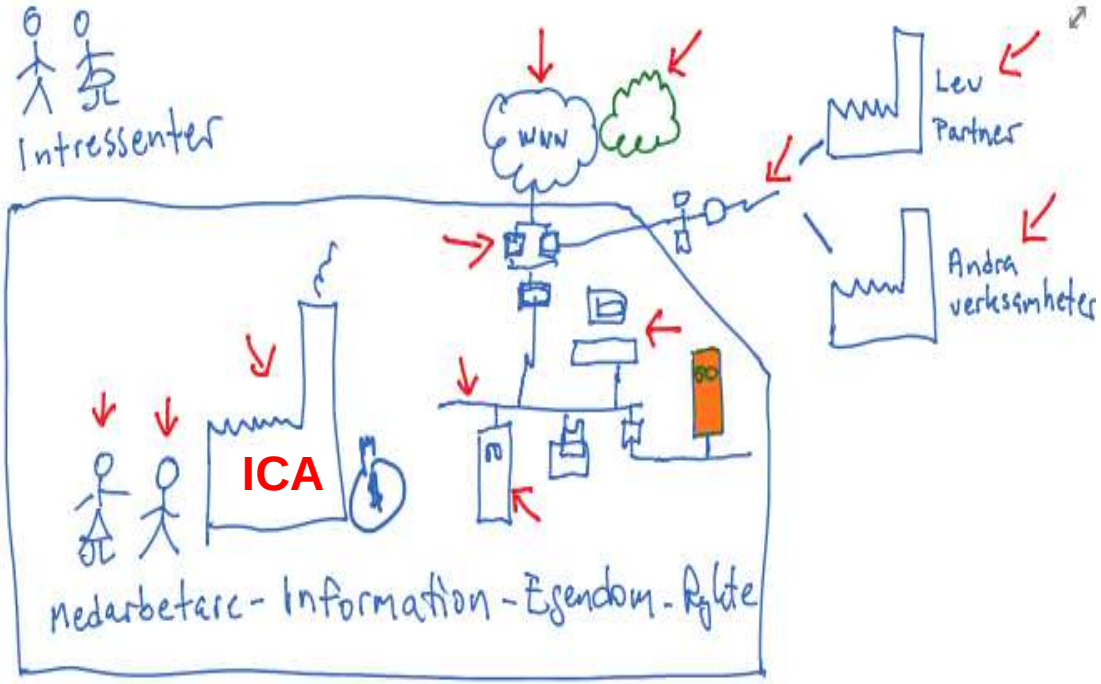
- ICA Sveriges beroende till informationsbehandling och it och genom GDPR har vi skapat ett nytt ekosystem

Principiell bild över IT-miljön

- Förändringar som drivs av den pågående digitaliseringen:
  - Större mängd personuppgifter
  - Flyttar ”affären” till Internet
  - Nya tekniker som Robotics, röststyning etc.



Källa: Örnsköldsviks Kommun



Risker

IT-relaterade risker

Riskbeskrivning
ICA Gruppens verksamheter är i hög grad beroende av en välfungerande IT-miljö. Oförmåga att säkerställa en modern och för verksamheten anpassad IT-miljö kan få en väsentligt negativ påverkan på koncernens verksamhet och resultat. Vidare kan intrång i IT-miljön eller brister i hantering av kund-, medarbetarinformation eller affärskritisk data som hanteras i IT-miljön leda till minskat förtroende samt innebära en negativ påverkan på koncernens resultat.

Möjligheter
I en tid med snabba förändringar av kundbeteende, affärsmodeller och konkurrenssituation samt med ökad digitalisering och mycket höga krav på kommunikation ger en flexibel, motståndskraftig och modern IT-miljö goda möjligheter att tillgodose kundernas önskemål och behov avseende såväl tjänster som produkter. Vidare möjliggör nya tekniska lösningar ofta en högre grad av automatisering samt effektivare processer. Ny teknik ger även möjligheter till att skydda information på ett mer ändamålsenligt och effektivt sätt samt ökar möjligheterna att göra säkerhetslösningar ännu mer kundvänliga och effektiva.

Hantering
Under 2017 har digitaliseringen fortsatt och IT-infrastrukturen har förnyats inom relevanta områden. Projektarbete samt utveckling och införande av ny infrastruktur och system följer fastställda processer som även inkluderar genomförandet av regelbundna riskanalyser. På koncernnivå och inom dotterbolagen pågår kontinuerligt ett strukturerat arbete som förstärker ICA Gruppens IT- och informationssäkerhet.

Källa: ICA årsredovisning 2017

Major technology advances are happening fast

Digital interfaces

- More time spent on digital interfaces (e.g. mobile)
- New digital interfaces evolving (e.g. voice and AR/VR)
- Enables more data collection

Big data and computing power

- Data captured and stored at a massive scale
- Sufficient processing power available for advanced analyses

Advanced analytics/ AI/Machine Learning

- Mathematical/ statistical analytics and algorithms
- AI =“programmed to be smart”; Machine learning = “Learns to be smart”
- Enabled by new technology/tools, data, computing power

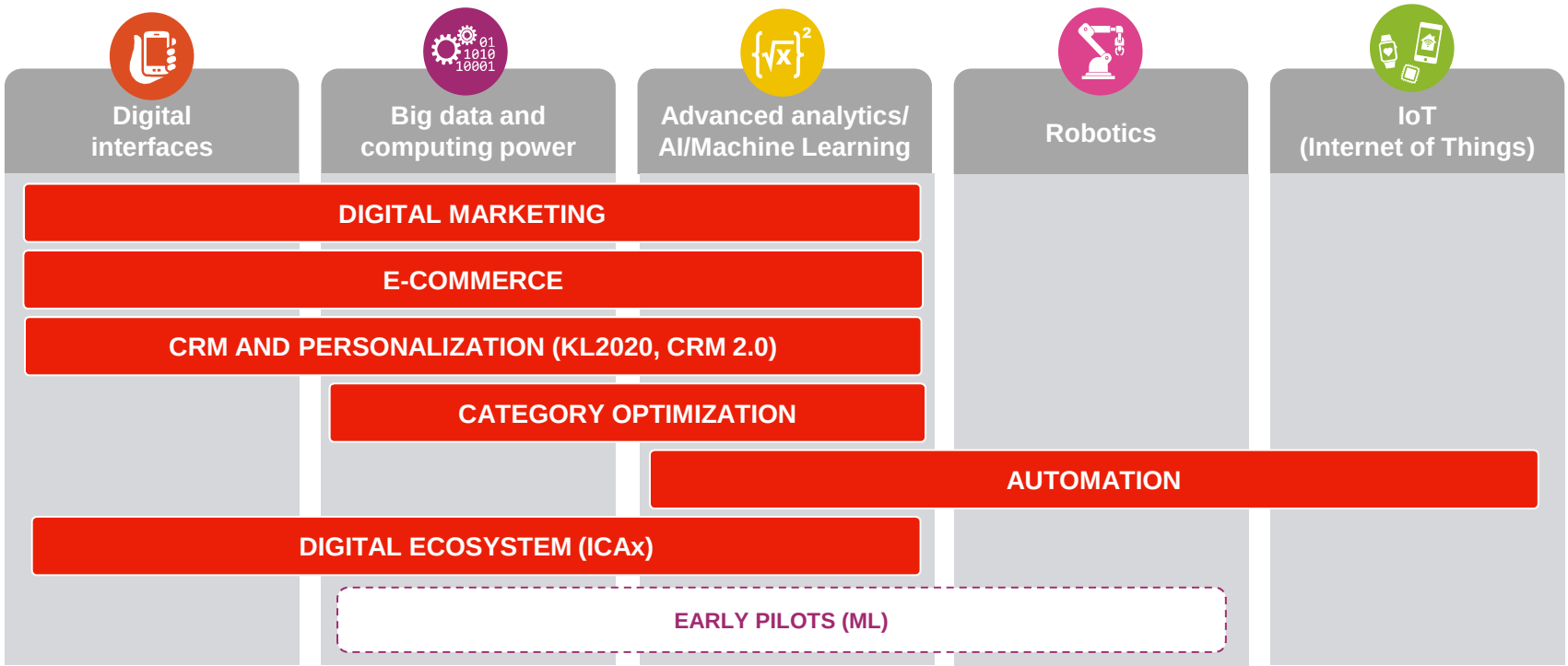
Robotics

- Physical robots move and interact with the environment
- Software robots perform tasks (e.g. RPA: robotic process automation)

IoT (Internet of Things)

- Sensors which collect data
- Added to “everything”
- Creating even more data

Several major initiatives to address digital opportunities

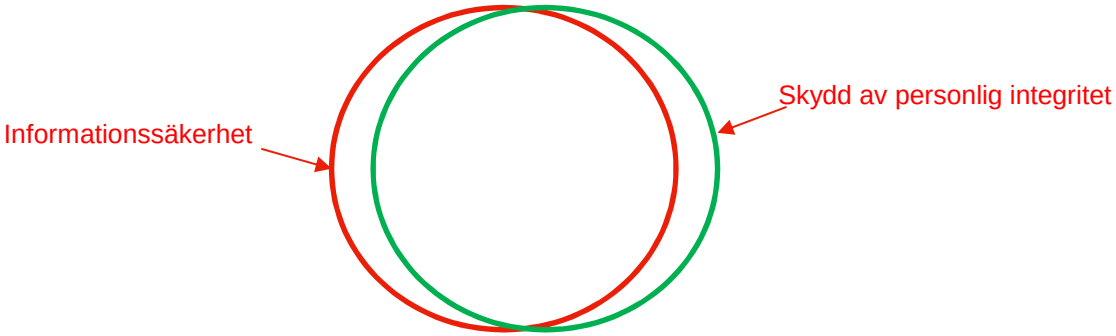


Konsekvenser av bristfälligt informationssäkerhet

- **PCI DSS** – Regler kring korthantering - Konsekvens -> Varje transaktion blir X kr dyrare, rating för banken blir…..
- **Personuppgifter** – I ett vitt perspektiv –Hanteringskostnader, sanktioner, skadestånd och varumärkespåverkan
- **Börsinformation** – Otillbörligt avslöjande, Legal påverkan och sanktioner
- **Bristfälliga beslut** – Vi inte känner till våra risker.
- **Avtalsbrott** – Vi kan inte hålla våra avtal om leveranser.
- **Ineffektivitet** – Vi får inte ut lösningar i tid… Vår interna hanteringskostnad i allmänhet blir större
- **Varumärkespåverkan** – Vårt starka varumärke påverkas
- **Legala krav** – Följa lagstiftning – Skadestånd, rättspåverkan,
- **Samhällspåverkan** – inte kunna förse våra kunder med livsmedel

Kopplingen mellan GDPR och informationssäkerhet

- Informationssäkerhet och skydd av personlig integritet kan synas vara två helt skilda saker men det finns mer gemensamma nämnare är olikheter.
- Informationssäkerhet går ut på att säkra informationstillgångars konfidentialitet, integritet och tillgänglighet. Skydd av personlig integritet innehåller legala rättigheter för registrerade, efterlevnad och risk.

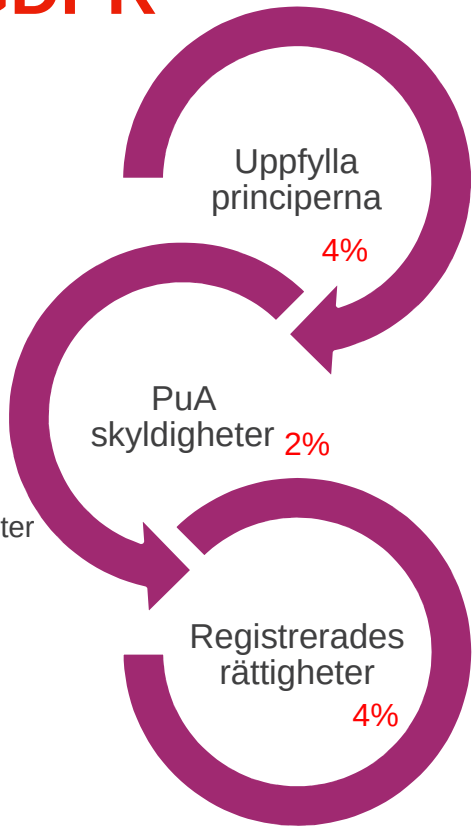


WORK in progress

Säkerställa att ICA Sverige över tiden bibehåller kontrollen på användandet av personuppgifter och förmågan att uppfylla den registrerades rättigheter

Sammanfattning GDPR

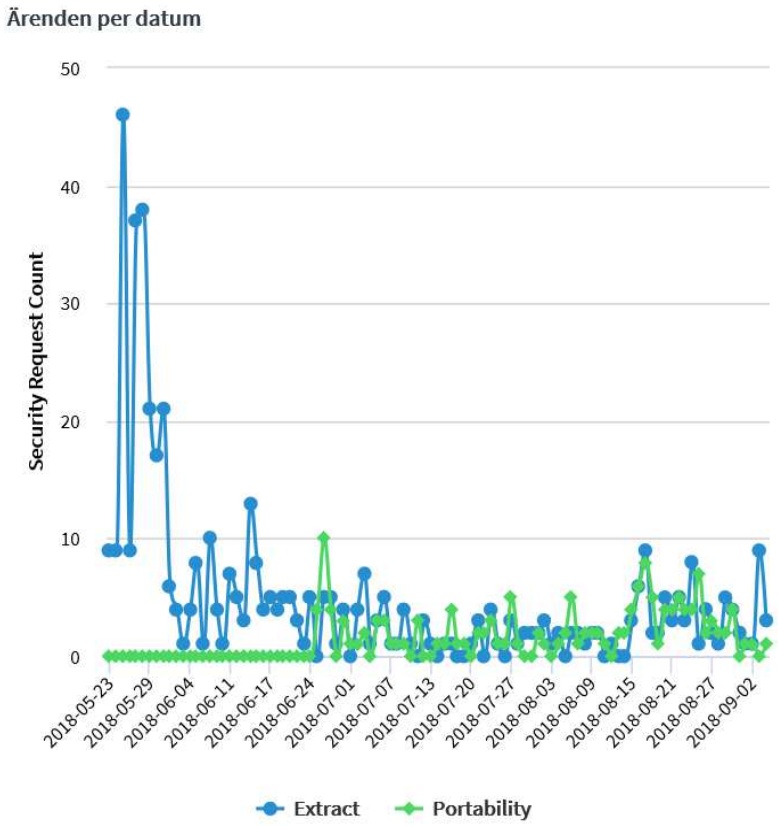
- ”Laglighet”
- Ansvarsfördelning
- Inbyggt dataskydd och dataskydd som standard
- Register över behandling
- Säkerhets för personuppgifter
- Konsekvensbedömning
- Dataskyddsombud



- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

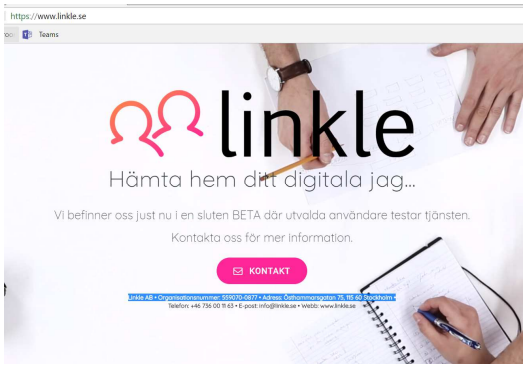
- Information
- Registerutdrag
- Rättelse och radering
- Dataportabilitet
- Rätt att göra invändningar

Läget 3/9



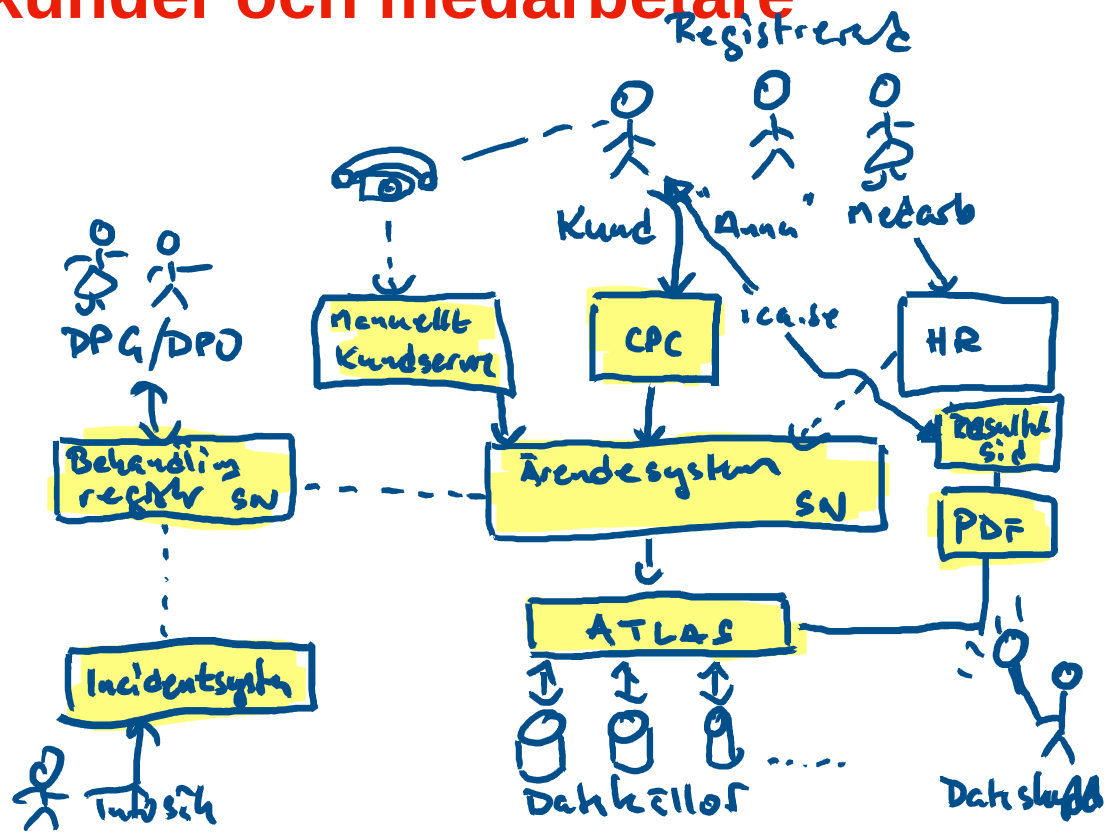
I snitt ca 5/dag

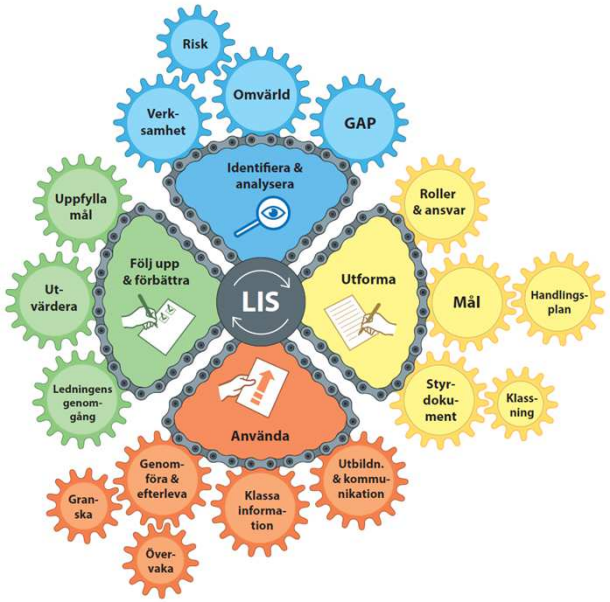
Register-utdrag	Portabiltet	Pu incidenter
476	151	29 (54 totalt)



Tjänst för att hantera portabilitet med fullmakt från registrerad

Vi har en systemlösning för hantering av GDPR både för kunder och medarbetare

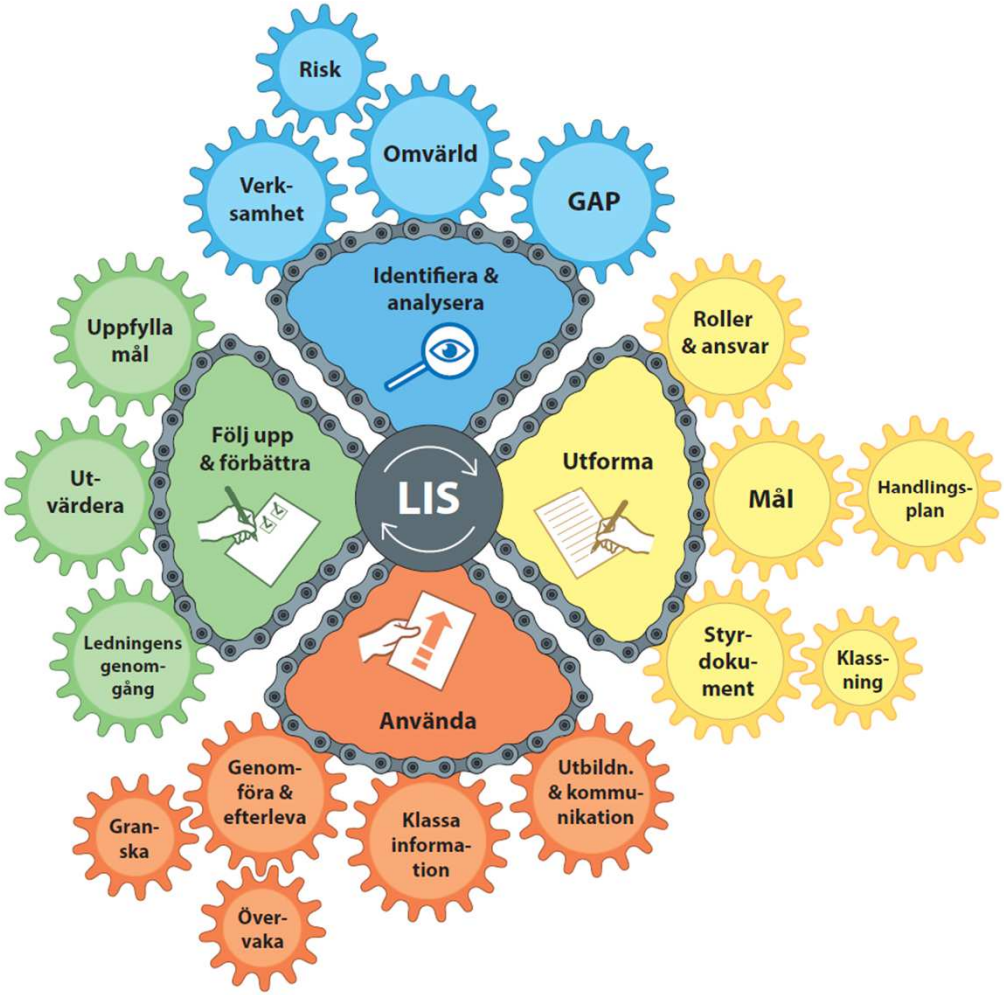




Ledningssystem för informationssäkerhet

Vad är det och hur kan det användas

LIS


Risk
Omvärld
Verk-
samhet
GAP
Identifiera &
analysera
Uppfylla
mål
Roller
& ansvar
Följ upp
& förbättra
Ut-
värdera
LIS
Utforma
Mål
Handlings-
plan
Ledningens
genom-
gång
Styr-
doku-
ment
Klass-
ning
Använda
Genom-
föra &
efterleva
Utbildn.
& kommu-
nikation
Gran-
ska
Klassa
informa-
tion
Över-
vaka

Information System Management System and Cloud/GDPR

Risk Management

ISO/IEC 27005: Information security risk management

ISO/IEC 29134: Privacy impact assessment

GDPR och infosäk

ISO/IEC 27002:2013 Riktlinjer för informations-säkerhetsåtgärder

ISO/IEC 29151: Code of practice for personally identifiable information protection

ISO/IEC 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processor

ISO/IEC 29101: Privacy architecture framework

IISO/IEC 29190: Privacy capability assessment model

ISO/IEC 27550 Privacy engineering

ISO/IEC 29184: Online privacy notices and consent

Security measures

ISO/IEC 27001:2013 ISMS — Requirements
ISO/IEC 27552: Enhancement to ISO/IEC 27001 for privacy management — Requirements
ISO/IEC 29100: Privacy framework

ISMS

Vad är Ledningssystem för informationssäkerhet (LIS)?

- **Ledningssystem** – uppbyggd struktur för att styra vårt informationssäkerhetsarbete. Mer konkret innebär detta mål och krav, metoder, rutiner, processer m.m. för hantering av informationssäkerheten.
- **Vi arbetar** – Styrt, riskbaserat, systematiskt, ledningen är medveten och engagerad, med ständig förbättring.

Systematiskt är att man arbetar planenligt, ordnat som följer en plan

Hur hänger allt ihop

Strategin beskriver hur vi når den vision och mål vi har för informationssäkerheten inom ICA. De saker vi beskriver i strategin ska stödja och ligga i linje med de olika mål vi har på kort och lång sikt.

Vision och mål spjutspetsen för informationssäkerheten

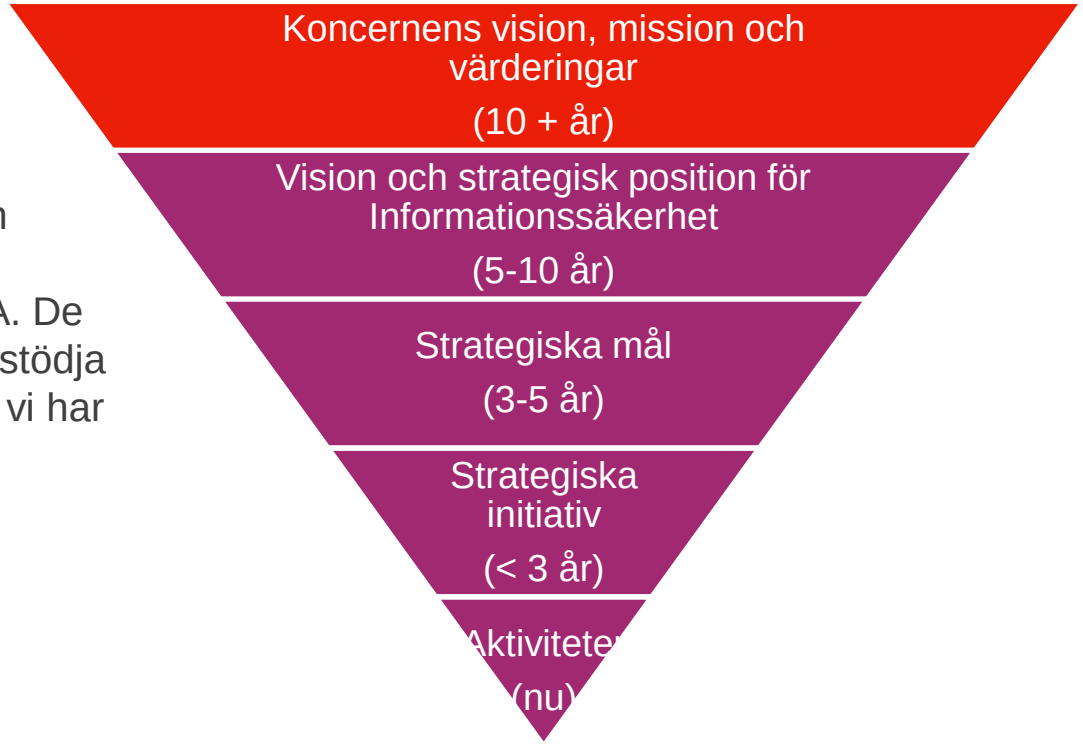


Bild 22

SG2 JOA beskriver kortfattat

Stefano Goudarzi; 2018-03-12

Exempel på ”mål karta” för informationssäkerhet

- **Vision:**
  - Informationssäkerhet möjliggör, skyddar och stödjer ICAs affär i alla lägen.
- **Effektmål:**
  - Verksamheten ska inte drabbas av någon allvarlig störning och gör den det så ska den kunna hanteras.
- **Strategiskt mål:**
  - Informationen skyddas utifrån externa och interna krav på konfidentialitet, riktighet och tillgänglighet.
- **Mål:**
  - Styrande dokument enligt ISO 27001/27002 är upprättade och aktuella.
  - Målen enligt 27002 är uppfyllda.
  - Informationsskyddet är riskbaserat.
  - Process för informationssäkerhetsarbetet är upprättad och införd

Dokumentstruktur inom ICA Sverige

ICA Sveriges
instruktion för
informationssäkerhet

ICA Sveriges
instruktion för
Styrning och ledning av
informationssäkerhetsarbetet

ICA Sveriges
instruktion för
Mål och riktlinjer för
informationssäkerhetsarbetet

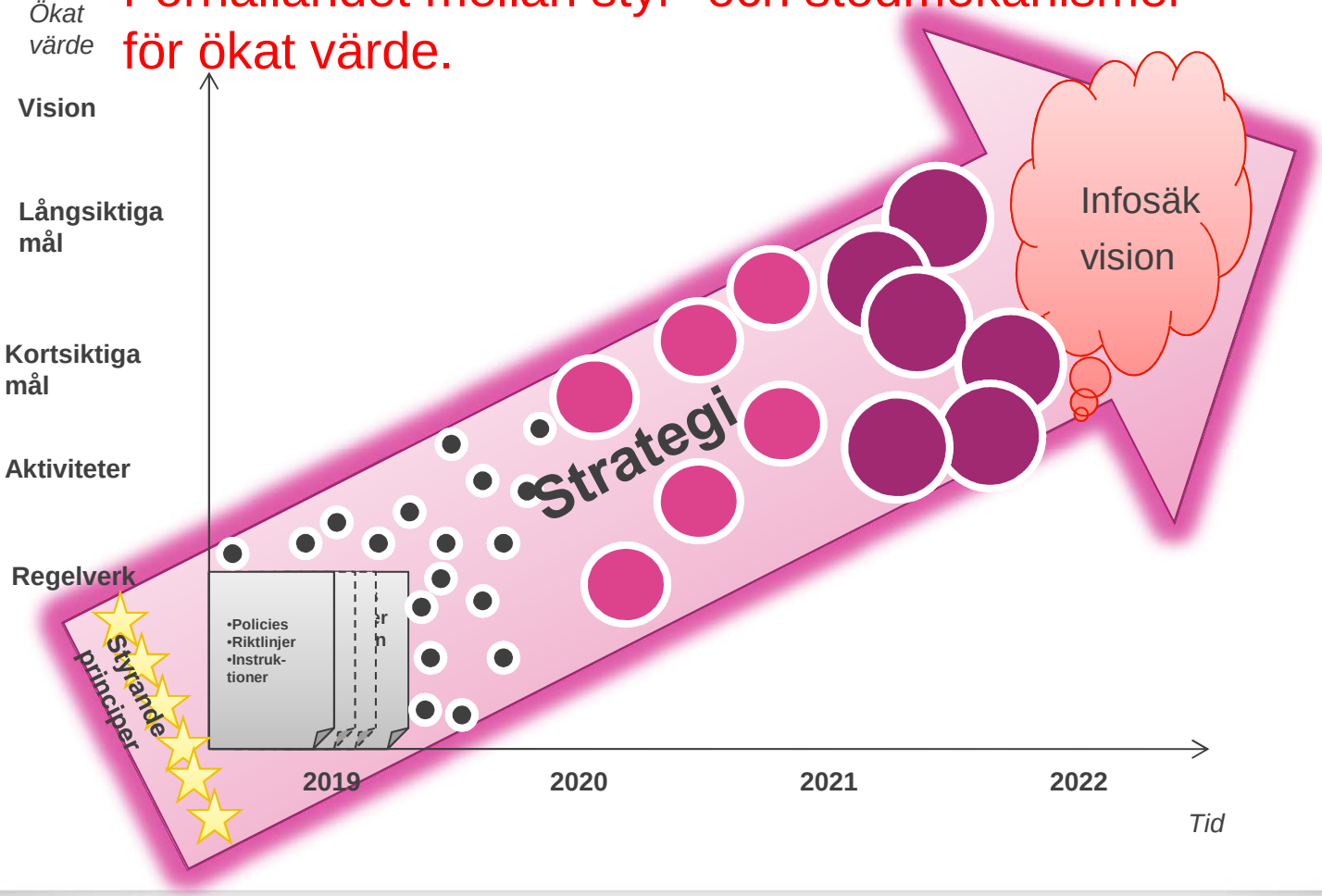
ICA Sveriges
instruktion för
Informationssäkerhet för chefer

ICA Sveriges
instruktion för
Informationssäkerhet för
medarbetare

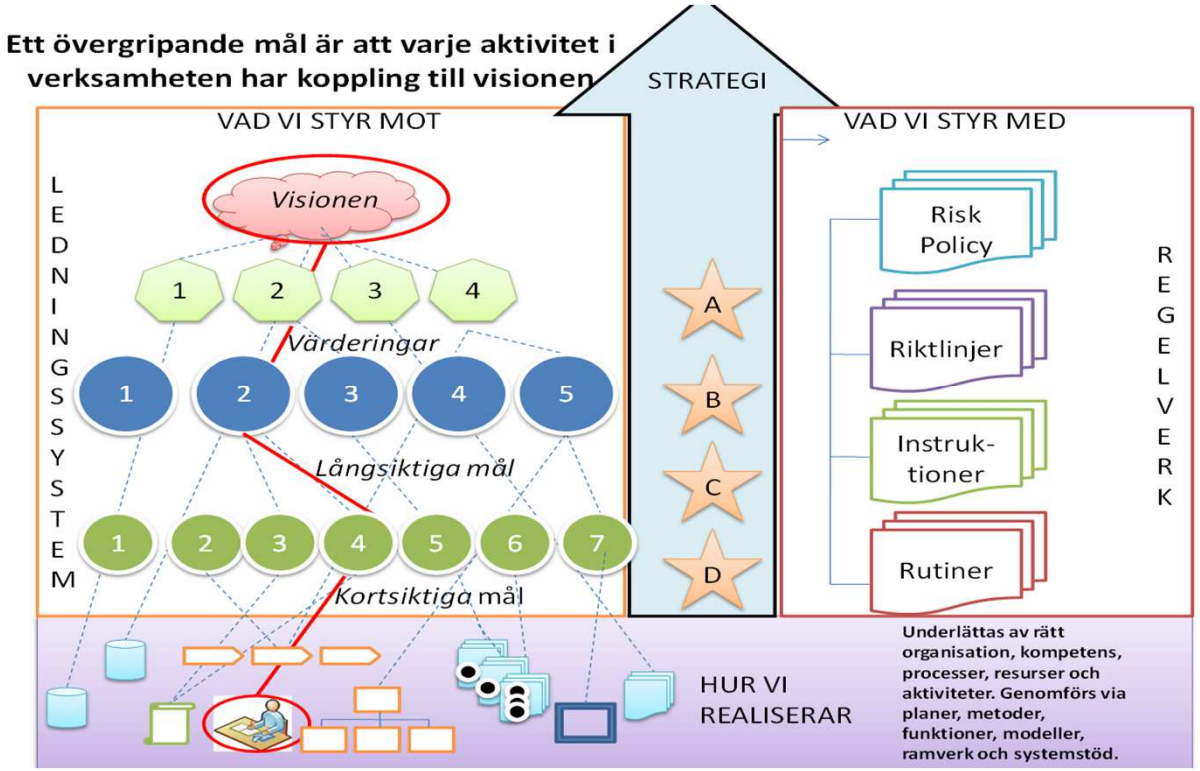
ICA Sveriges
instruktion för
Säker it

ICA Sveriges
instruktion för
Ledningens genomgång

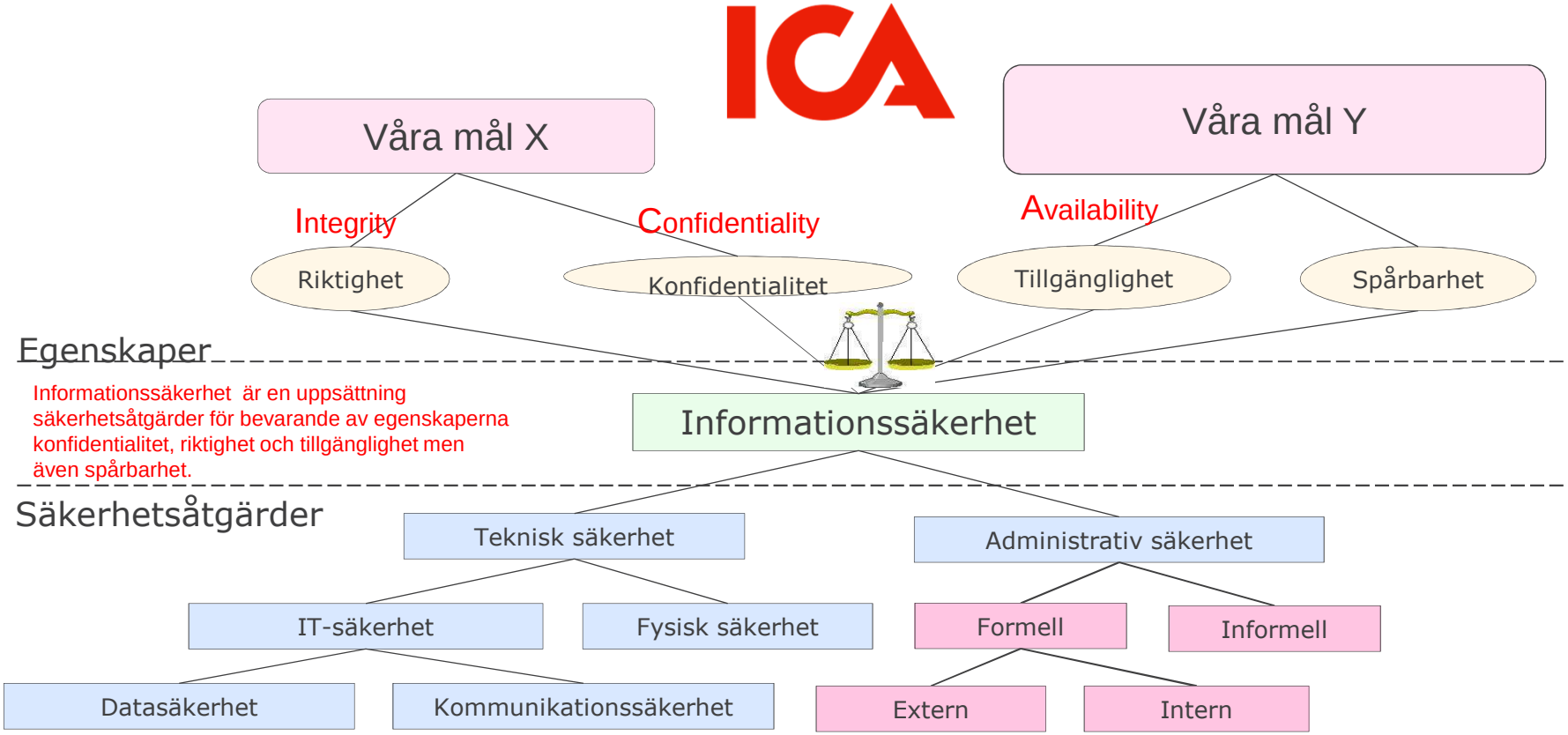
Förhållandet mellan styr- och stödmekanismer för ökat värde.



Sambanden mellan strategin, ledningssystem och regel-styrning



Vad är informationssäkerhet?



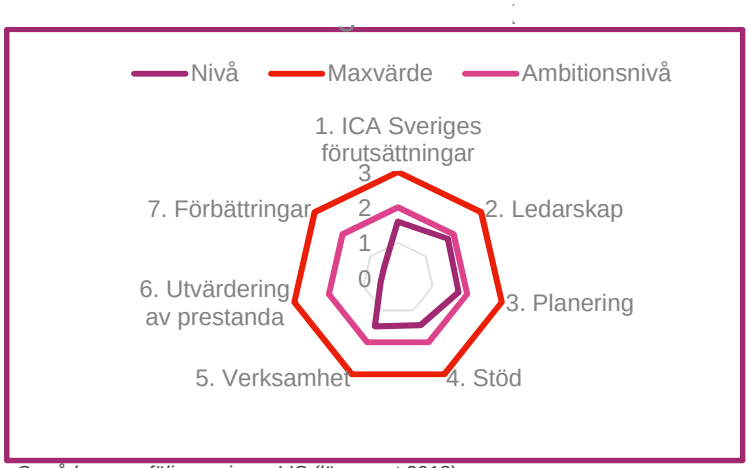
Källa: Rose-Mharie Åhlfeldt

Vad är LIS – Mål och principer för införande av LIS

- Mål: Under 2017 och 2018 sätta strukturen, därefter ständig förbättring

- Effektmål: Inom ICA Sverige ska verksamheten utföras utan att allvarliga störningar inträffar och uppkommer sådana ska de kunna hanteras. Arbetssätt runt säkerhet ska uppfattas trygga, enkla och relevanta.

- Principer vi följer under arbetet:
  - Vi gör det lätt att göra rätt
  - Vi eftersträvar transparens i risker och kostnader så att vi styr rätt
  - Vi utgår ifrån att det proaktiva informationssäkerhetsarbetet kommer att kräva mer av ledningens engagemang än tidigare
  - Vi utgår ifrån standardserien 27000 (utan certifiering)
  - 7 områden följs upp, se bild



Områden som följs upp inom LIS (läge sept 2018)

Ett **systematiskt** informationssäkerhetsarbete i form av ett LIS främjar GDPR compliance, och mitigerar kraftfullt risken för eventuella sanktioner.

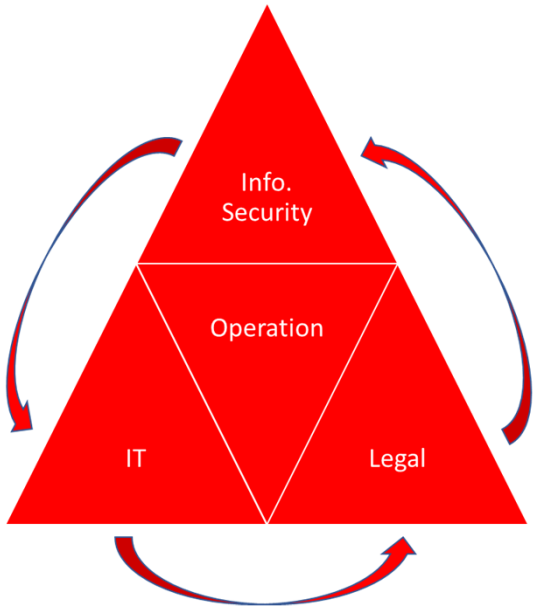
Ledningssystemet och säkerhetsåtgärder enligt ISO 27001 & 27002

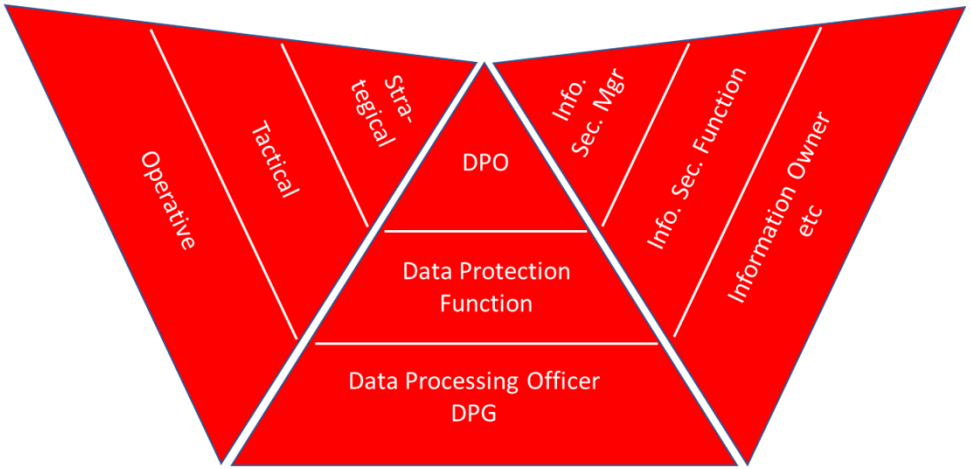
- **Organisationens förutsättningar**
  - Att förstå organisationen och dess förutsättningar
  - Att förstå intressenters behov och förväntningar
  - Att bestämma ledningssystemets omfattning
  - Ledningssystem för infosäkerhet
- **Ledarskap**
  - Ledarskap och engagemang
  - Policy
  - Befattningar, ansvar och befogenheter inom organisationen
- **Planering**
  - Åtgärder för att hantera risker och möjligheter
  - Infosäkerhetsmål och planering för att nå dem
- **Stöd**
  - Resurser
  - Kompetens
  - Medvetenhet
  - Kommunikation
  - Dokumenterad information
- **Verksamhet**
  - Planering och styrning av verksamheten
  - Bedömning av infosäkerhetsrisker
  - Behandling av infosäkerhetsrisker
- **Utvärdering och prestanda**
  - Övervakning, mätning, analys och utvärdering
  - Internrevision
  - Ledningens genomgång
- **Förbättringar**
  - Avvikelse och korrigerande säkerhetsåtgärder
  - Ständig förbättring

Bilaga A i 27001 och 27002: Åtgärdsmål och säkerhetsåtgärder

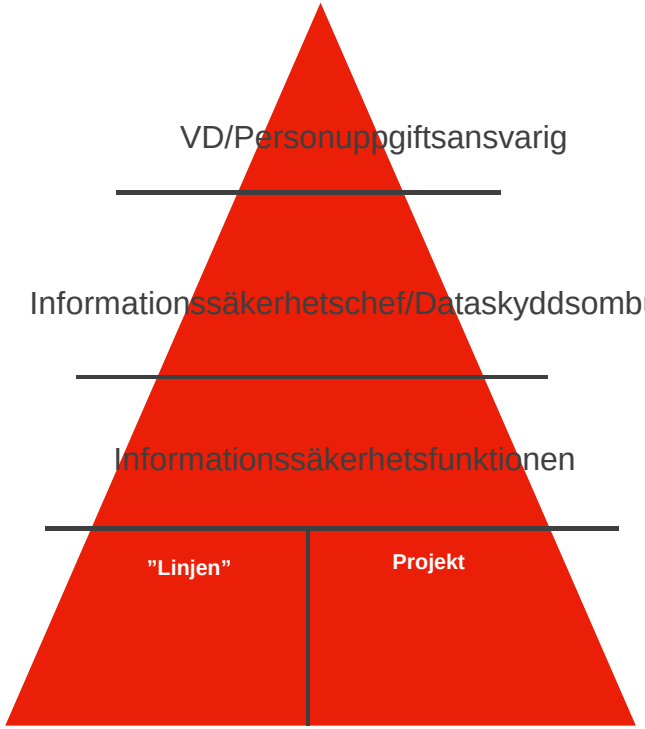
- Infosäkpolicy
- Org. av infosäk
- Personalsäkerhet
- Hantering av tillgångar
- Styrning av åtkomst
- Kryptografi
- Fysisk säkerhet
- Driftsäkerhet
- Kommunikations-säkerhet
- Anskaffning, utveckling och underhåll av system
- Leverantörs-relationer
- Incidenthantering
- Kontinuitetsskydd
- Efterlevnad

Relationer mellan funktioner och roller





Roller i verksamheten

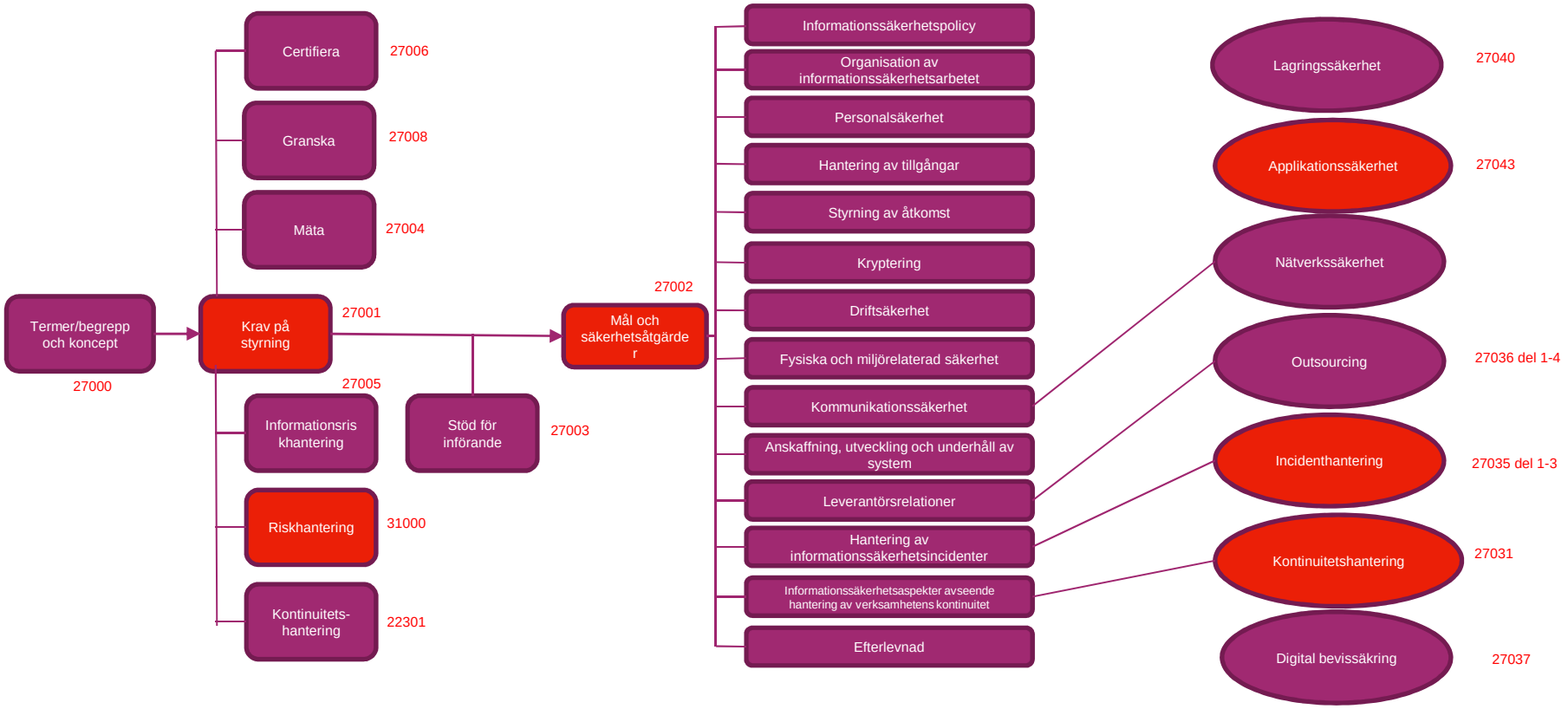


Behandlingsansvarig

Data Protection Guardian

Informationssäkerhetsspecialister

Standarder som stöd och vägledning



Integration i andra processer…..

11 april 2017

ICA förändringsmodell

Här hittar du aktiviteter, mallar, stöddokument, beslutspunkter mm kopplat till ICA förändringsmodell

Information Security & Privacy activities – ICA's Project model

	DP0	DP1	DP2	DP3	DP4	DP5	DP6
Project model phases	**Project Idea**	**Prestudy**	**Start-up**	**Execution**	**Roll-out & Handover**	**Conclusion**	**Benefit realization**
Information & IT Security & Privacy Activities		**1. Understand the purpose of solution and establish overall context to discover information & Privacy Protection needs (DP1)** • Information Classification • High-level Risk & Impact assessment • High-level security & privacy objectives • Project staffing needs	**2. Define solution security & privacy requirements based on agreed protection needs (DP2)** • Threat Analysis & mitigation plan • Security & Privacy Architecture Analysis • Define detailed Security & Privacy objectives and requirements	**3. Design, Develop and implement detailed security & privacy controls, based on security & privacy objectives and requirements (DP3)** • Define & design security & privacy controls; • Develop security & privacy controls; • Implement security & privacy controls in accordance **4. Validate the effectiveness of security & privacy controls (DP4)** • Develop test & evaluation plan for verification & validation of security & privacy controls • Conduct security & privacy testing and evaluation on target solution • Obtain solution approval, from an security & privacy perspective	**5.** Safe transition is ensured and the project provides support for as long as necessary until the operation is stable from an Security & Privacy perspective **6**. The hand-over checklist is reviewed and closed. Unresolved issues are passed to the core maintenance organization		

Vad är LIS – Förväntat resultat av införande

Förväntat resultat av LIS är en integrerad och effektiv process för informationssäkerhetsarbetet som skapar enkelhet, relevant nivå och ansvarstagande, i linje med ICAs värderingar

INPUT:

Krav och förväntningar från organisationen.

Intern och extern påverkan, i form av risker och händelser.

Ha koll/Förstå → Styra och samordna → Skydda → Hantera händelser

OUTPUT:

Verksamheten kan utföras utan allvarliga störningar.

Allvarliga störningar kan hanteras

Förväntat resultat av LIS är en integrerad och effektiv process för informationssäkerhetsarbetet som skapar enkelhet, relevant nivå och ansvarstagande, i linje med ICAs värderingar.

Skapa säkerhetskultur i linje med ICAs värderingar som täcker Linjeverksamhet / Projekt & Utveckling / Förvaltning & Drift

INPUT:

Krav och förväntningar från organisationen.

Intern och extern påverkan, i form av risker och händelser.

Ha koll/Förstå

- *Identifiera risker*
- *Omvärldsanalys*
- *Samverkan internt/externt*
- *Dimensionerande hotbild*
- *Infosäkerhetsanalys*
- *Gemensam lägesbild av behov och risker*

Styra och samordna

- *Riskhantering*
- *Planering/budget*
- *Resurssäkring*
- *Uppföljning*
- *Granskningar/ kontroller*
- *Mätning*
- *Utbildningsplanering*
- *Ledningens genomgång*
- *Kompetensanalys*
- *Kommunikation*
- *Ärendehantering*
- *Metodutveckling*
- *Upprätta handlingsplan*

Skydda

- *Framtagande av regler*
- *Framtagande och införande av säkerhetsåtgärder*
- *Kontroll av nivån*
- *Operativ övervakning/mätning*
- *Stöd/rådgivning*
- *Information/utbildning*
- *Avvikelsehantering*
- *Säkra upphandlingar*
- *Kontinuitetsplanering*
- *Livscykelhantering*

Hantera händelser

- *Incidenthantering*
- *Kris- och kontinuitets-hantering*

OUTPUT:

Verksamheten kan utföras utan allvarliga störningar.

Allvarliga störningar kan hanteras

Tack