KONFERENSEN
INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

14–15 SEPTEMBER 2016

Verksamhetsdriven informationssäkerhet genom informationsklassning och målgruppsanpassade riktlinjer

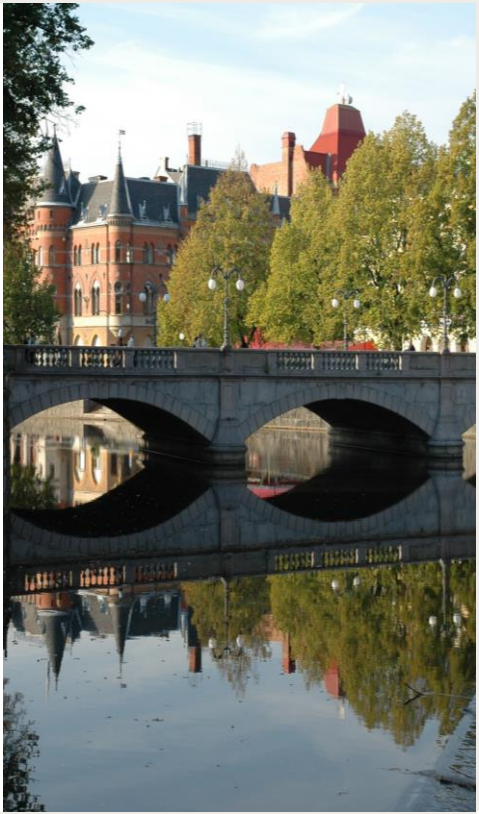
Per Oscarson
Informationssäkerhetsansvarig
Örebro kommun

Per Oscarson

- Informationssäkerhetsansvarig på Örebro kommun
- Medlem i SIS TK 318 (SS-ISO/IEC 27000-serien)
- Fil Dr och Fil Lic vid Linköpings universitet
- Har tidigare varit
  - CISO/CSO på Folksam
  - Informationssäkerhetsexpert på MSB
  - Informationssäkerhetskonsult på Nexus och Transcendent Group
  - Universitetslärare, Örebro universitet

Örebro

- Ca 142 000 invånare (7:e största i Sverige
- Mitt i Sveriges befolkningsmässiga centrum
- Örebro är 750 år gammal. Slottet började byggas redan på 1200-talet
- Logistikcentrum: Flyg, järnväg, Europavägar
- Örebro universitet, 16 gymnasieskolor, över 40 kommunala grundskolor och 15 friskolor

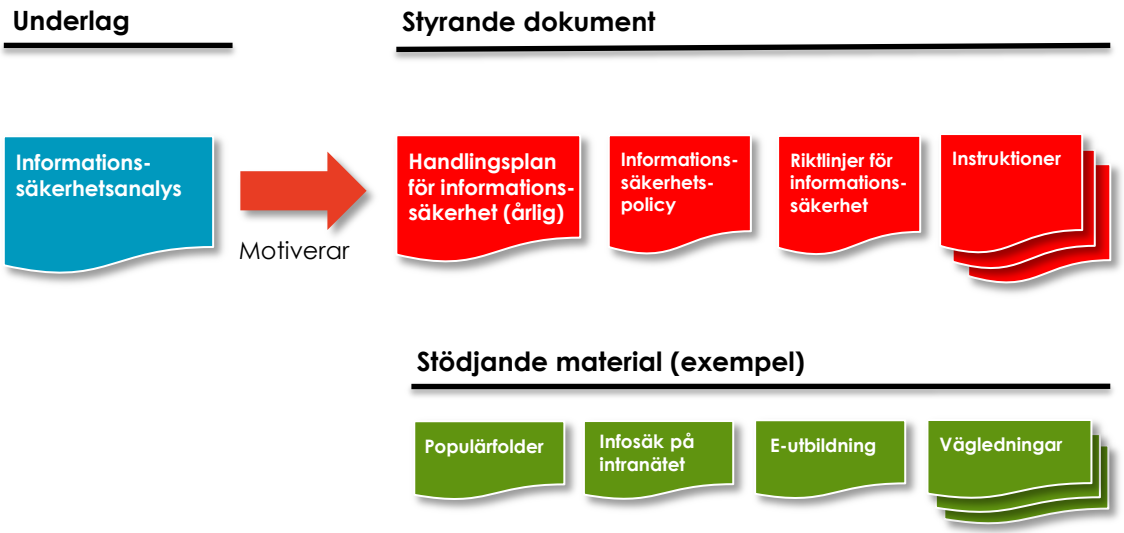


Örebro kommun

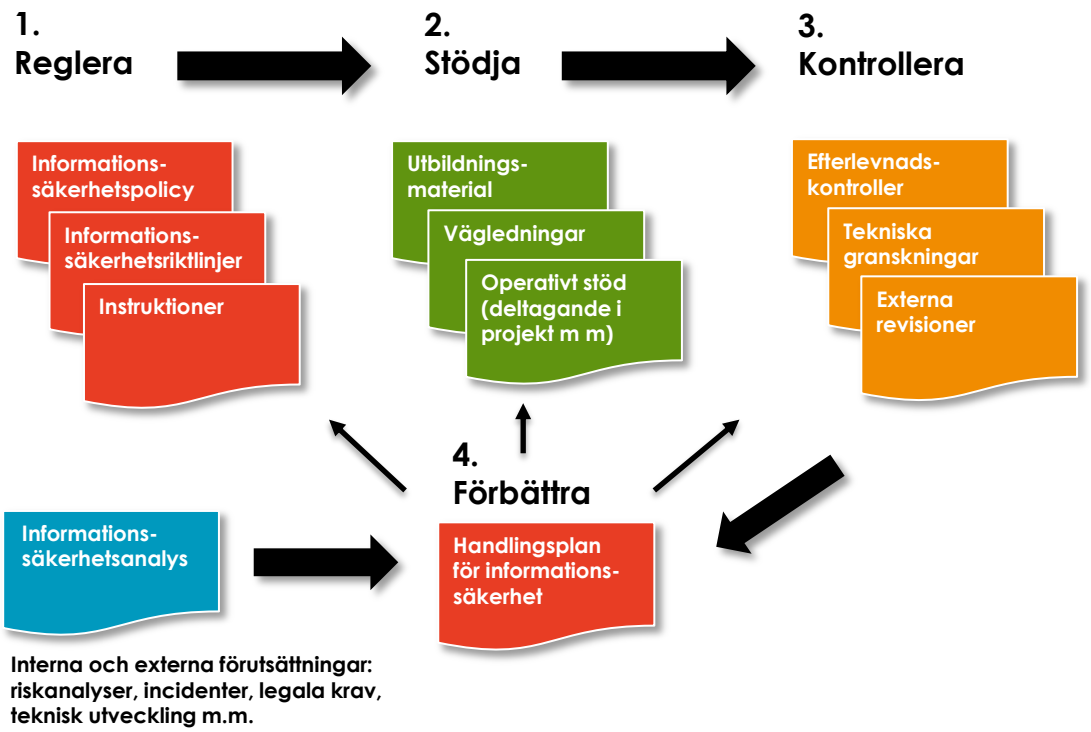
- Leds av S, KD och C
- Ca 12 000 anställda
- Ca 20 nämnder
- Tre programområden
  - Barn och utbildning
  - Samhällsbyggnad
  - Social välfärd

- Central styrning och administration i kommunstyrelseförvaltningen
- Informationssäkerhetsansvarig placerad på IT-avdelningens IT-strategienhet

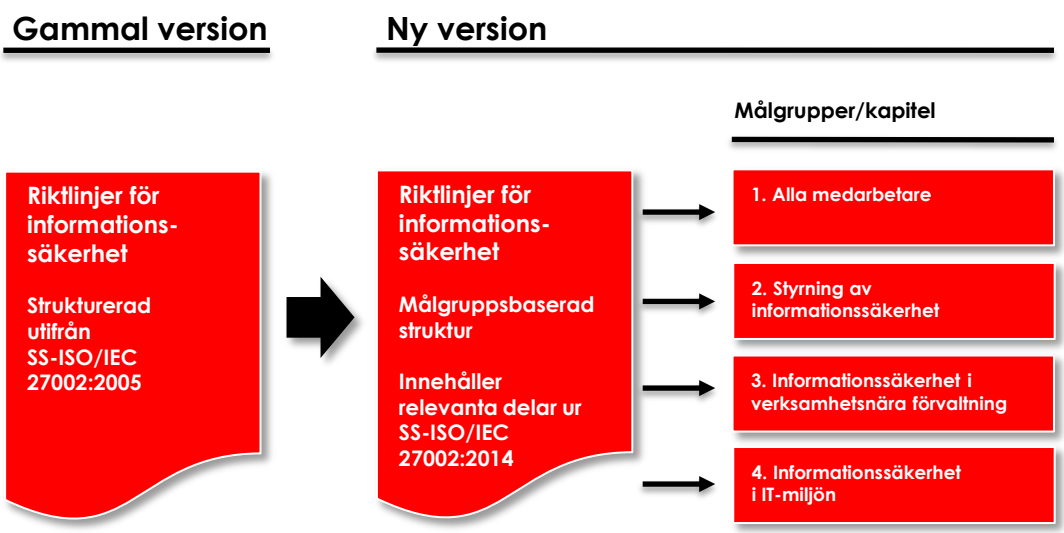
Informationssäkerhet – övergripande dokumentstruktur



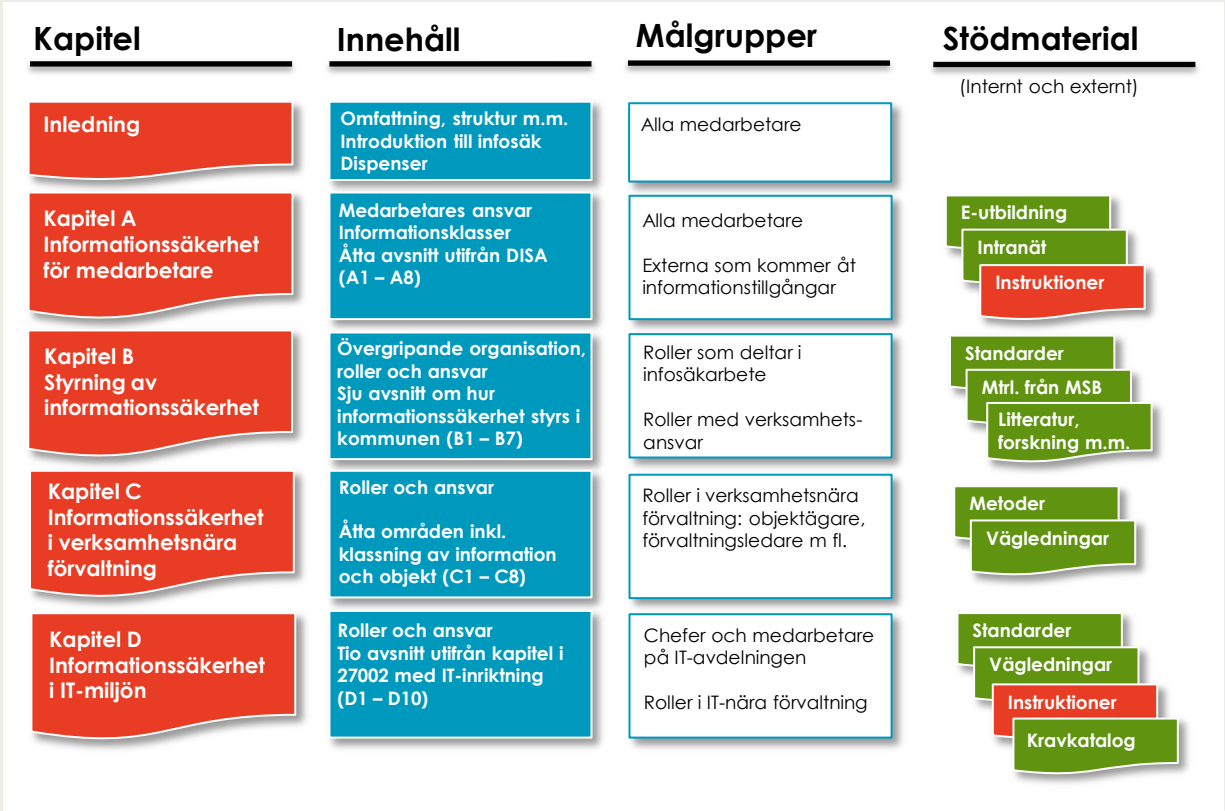
Essensen av informationssäkerhetsstyrning



Målgruppsindelade riktlinjer



Målgruppsindelade riktlinjer



Tydligare riktlinjer

För att underlätta efterlevnad och uppföljning har dokumentet tydliggjorts bl.a. genom att separera informativ och motiverande text och obligatoriska riktlinjer.

Riktlinjerna är i tabellform med rött tabellhuvud medan andra tabeller, figurer m.m. är i blått. Exempel:

Ett lösenord ska vara ”starkt”, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet. Krav på lösenord:

Riktlinjer för utformning av lösenord	
A.1.1	Lösenord ska vara minst X tecken långt, gärna längre.
A.1.2	Lösenord ska innehålla minst en gemen, en versal och en siffra.

Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Justera sedan stora och små bokstäver och bilda lösenordet. Exempel:

Örebro kommuns modell för informationsklassning

Kravnivå	Konfidentialitet	Riktighet	Tillgänglighet
2 Höga skydds-krav	**Konfidentiell** information som, om den sprids till obehöriga, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer	Information som, om den ej är riktig och fullständig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer	Information som, om den ej är tillgänglig, kan medföra allvarliga konsekvenser för Örebro kommun, externa aktörer eller individer
1 Normala skydds-krav	**Intern** information som, om den sprids till obehöriga, kan medföra måttliga negativ påverkan på Örebro kommun, externa aktörer eller individer	Information som, om den ej är riktig och fullständig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer	Information som, om den ej är tillgänglig, kan medföra måttlig negativ påverkan på Örebro kommun, externa aktörer eller individer
0 Inga skydds-krav*	**Öppen** information som kan spridas fritt inom och utom Örebro kommun		

***Krav finns alltid att information ska vara riktig och tillgänglig!**

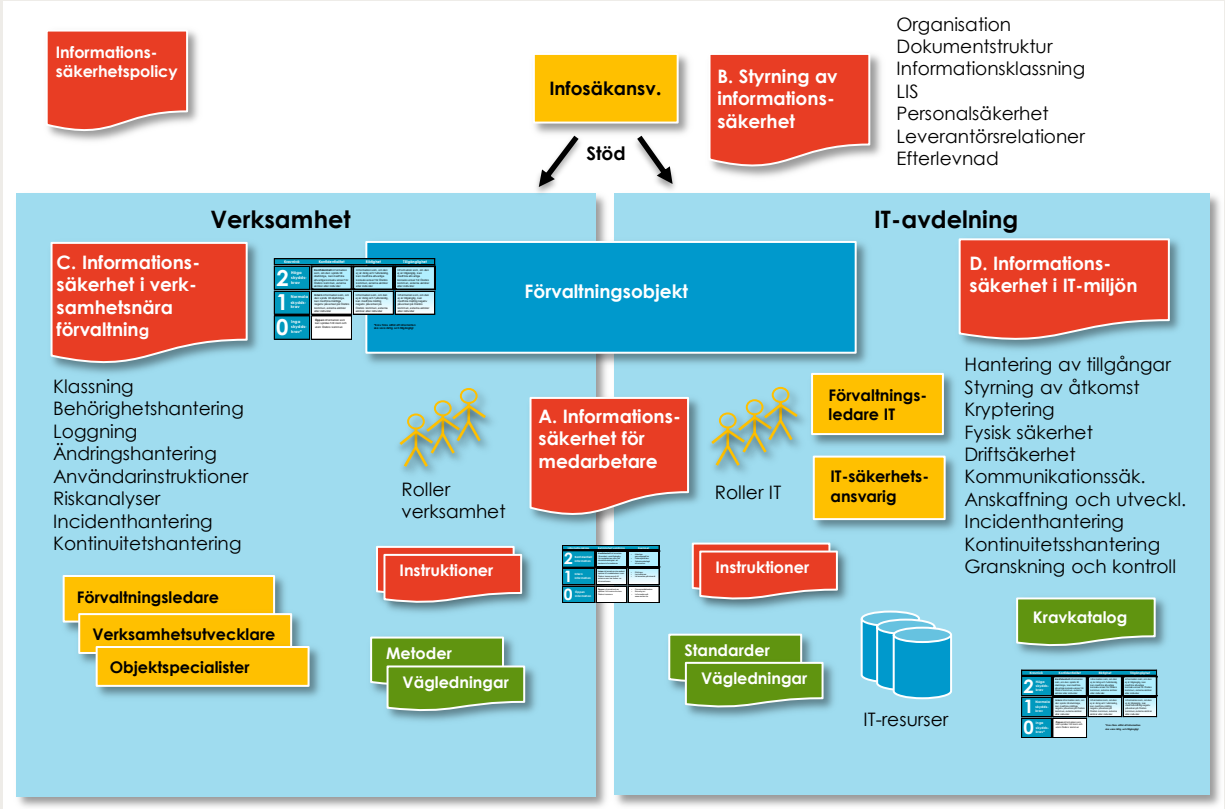
Modell för medarbetare – endast konfidentialitet

Informationsklass	Behörighet/spridning	Exempel
2 Konfidentiell information	**Konfidentiell** information får endast vara tillgänglig för medarbetare som har särskild behörighet att hantera informationen	• Känsliga personuppgifter • Patientjournaler • Sekretessbelagd information
1 Intern information	**Intern** information ska endast spridas till medarbetare inom Örebro kommun och till externa som har behov av informationen	• Riktlinjer • Instruktioner • Information på intranät
0 Öppen information	**Öppen** information kan spridas fritt inom och utom Örebro kommun	• Pressmeddelanden • Broschyrer • Information på www.orebro.se

Informationsklassning i riktlinjerna

- Kapitel A – Informationssäkerhet för medarbetare
  - Del av modellen: konfidentialitet
  - Särskilda hanteringsregler för konfidentiell information
- Kapitel B – Styrning av informationssäkerhet
  - Övergripande om informationsklassning
  - Klassningsmodellen
- Kapitel C – Informationssäkerhet för verksamhetsnära förvaltning
  - Riktlinjer för klassning av information och objekt
- Kapitel D – Informationssäkerhet i IT-miljön
  - Normala och höga skyddskrav på säkerhetsåtgärder gällande konfidentalitet, riktighet och tillgänglighet

Verksamhetsdriven informationssäkerhet



Informationssäkerhet för offentlig sektor 2016

Frågor?

Per Oscarson
Informationssäkerhetsansvarig
Örebro kommun
per.oscarson@orebro.se