Trusler og policies

tor.indstoy@santander.no

Hvem er jeg?

IT-Arkitekt

LISO

Det jeg skal prate om er:

Hvem vi er

Våre utfordringer

Trusler, hvordan ser vi de

Hvordan implementerer vi policies

GRUPO SANTANDER

Posisjon

- ✓ **Blant de 10 største banker i verden**
- ✓ **Tilstedeværelse i 46 land. Den ledende finansinstitusjonen i Euro-sonen og Latin-Amerika.**
- ✓ **59 millioner kunder, 10 000 filialer, 126 000 ansatte.**
- ✓ **2 700 000 aksjeeiere.**

Europa

Santander Consumer

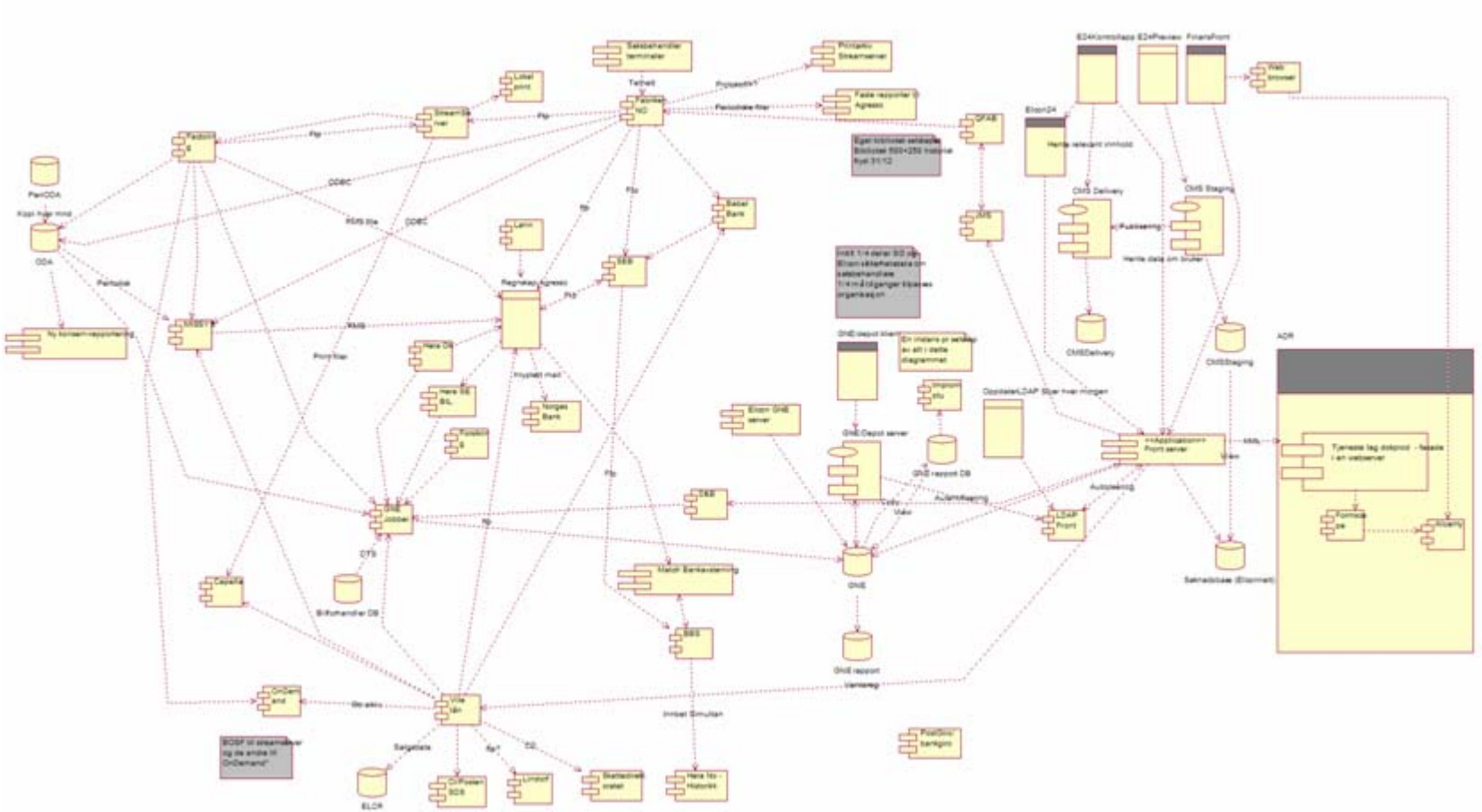
- Leader in consumer financing in Europe.
- Present in:
  - Spain
  - U.K.
  - Portugal
  - Italy
  - Germany
  - Holland
  - Poland
  - Czech Republic
  - Austria
  - Hungary
  - Norway
  - Sweden
- openbank Direct Banking.
- 7.7 million customers.
- 100,000 dealers.
- 257 own branches.
- 5,100 employees.

Latin-Amerika

Latin America Division

- Leading financial group in the region (10% market share).
- Leadership position in key markets: Brazil, Mexico and Chile.
- Prominent presence in Argentina, Venezuela, Puerto Rico, Colombia, Uruguay, Bolivia and Peru.
- 20 million bank customers.
- 8 million subscribers to pension plans.
- 4,100 branches.
- 62,700 employees.

Systemene, sterkt forenklet



Hva gjør vi?

Trusselvurderinger

- Konsekvens og sannsynlighet
- Enkelte systemer og grupper av systemer, basert på intervjuer av systemspesialister og brukere.

Policies

- Madrid
- USA
- Norske
- Finske
- Svenske
- Selvpålagte

Trusler

Utfordringer:

- Personlig radar (tankesett)
- Gruppetenking
- Det å være norsk

Policies

Hva gjør man med håpløse krav?

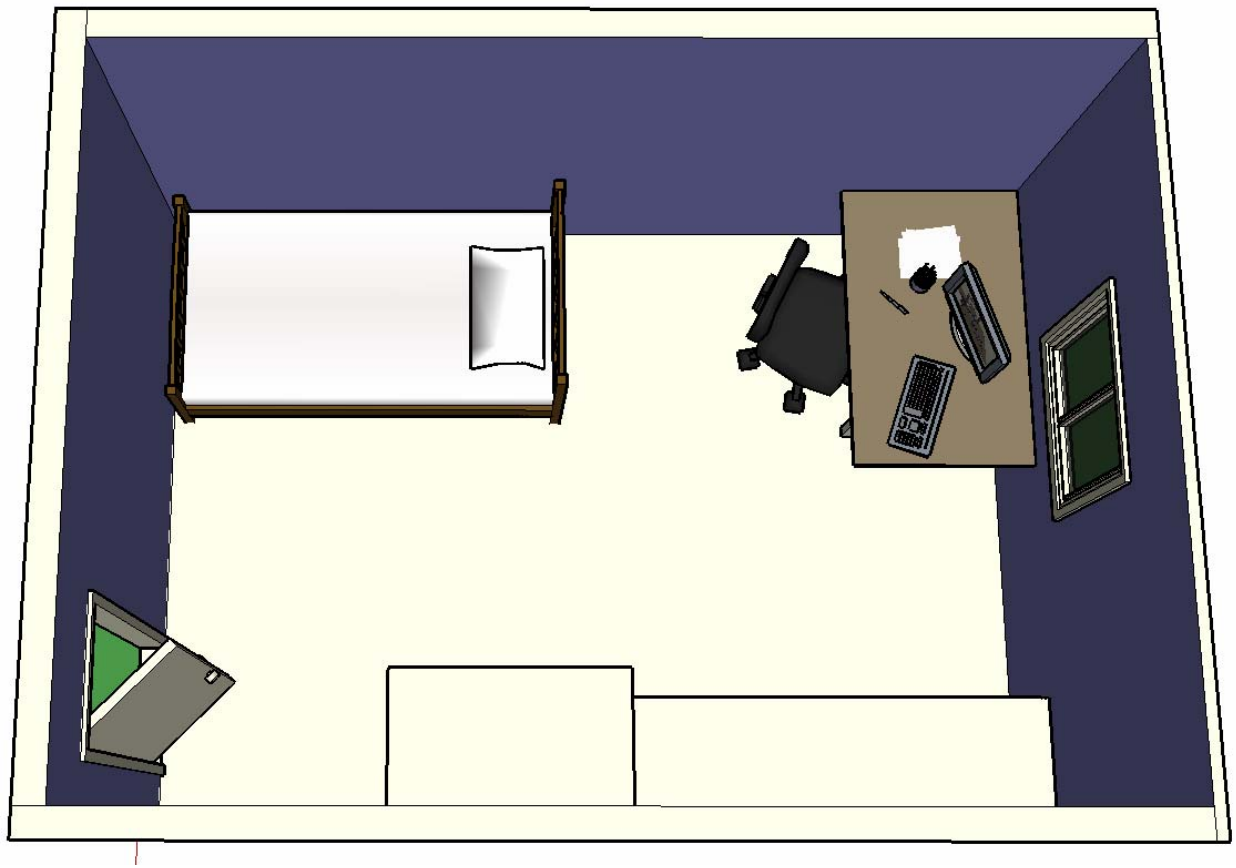
Hvordan kan de etterleves?

Hvem pålegges policies?

Hvem skriver policies?

Sitter de alene i lukkede rom?

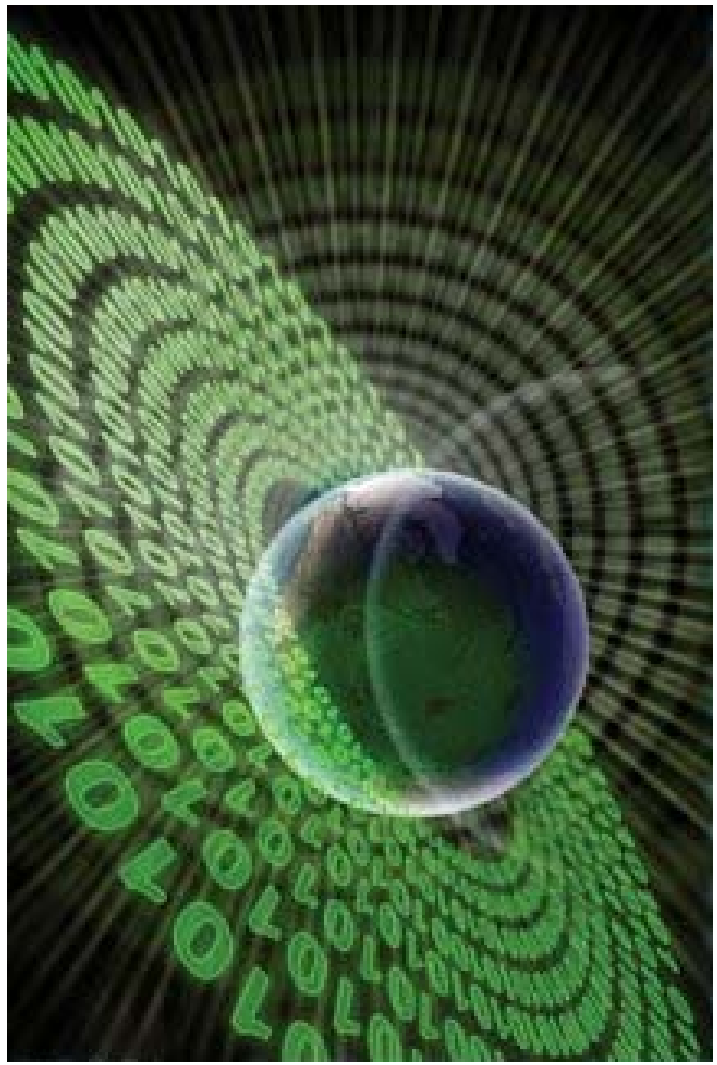
Hva tenker de på?



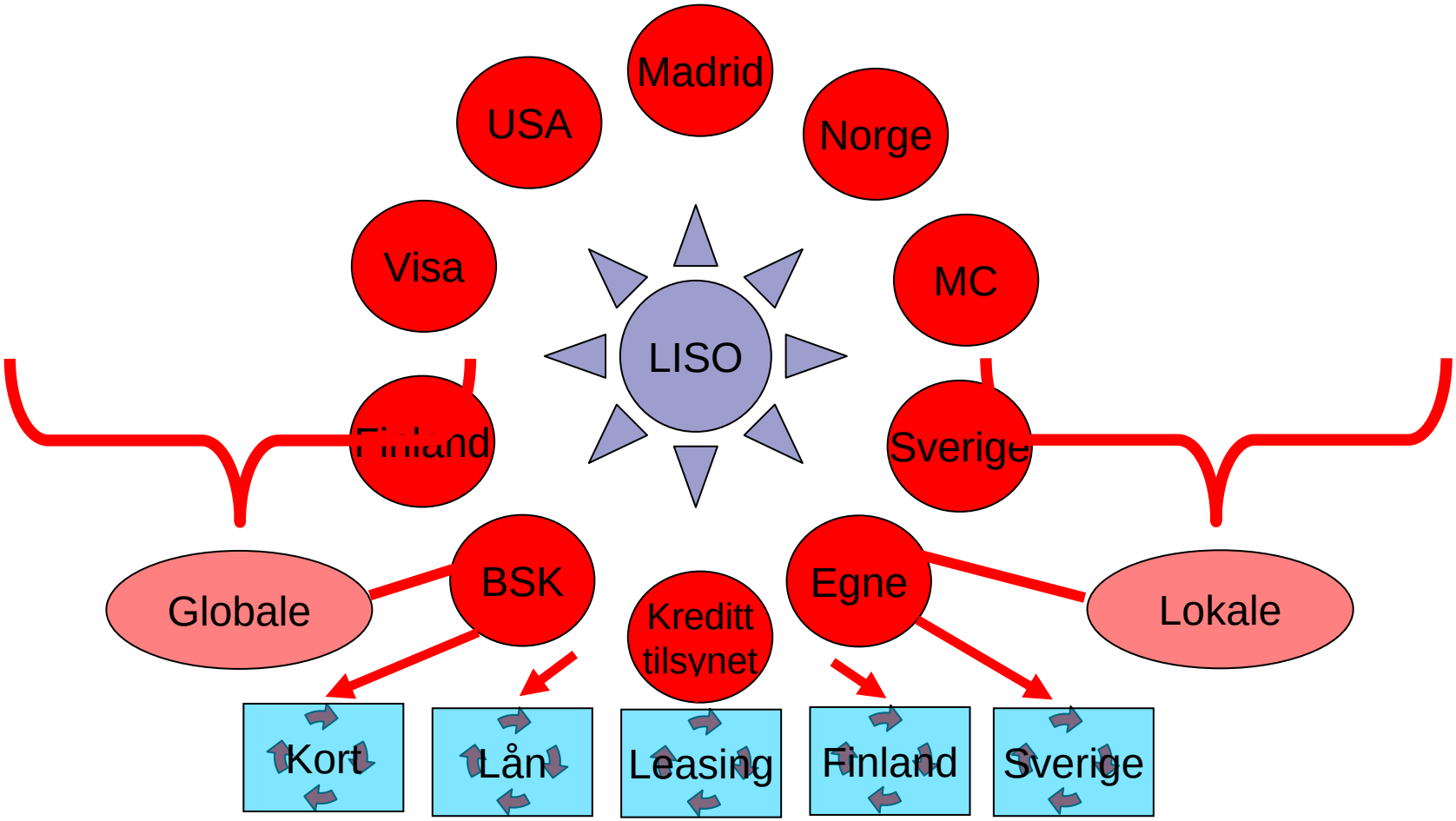
Hvordan kan policies etterleves?

- **Lover og regelverk:**
  - Nasjonale lover
  - EU-direktiver

- **Hvordan påvirke i pre-pipelinefasen?**

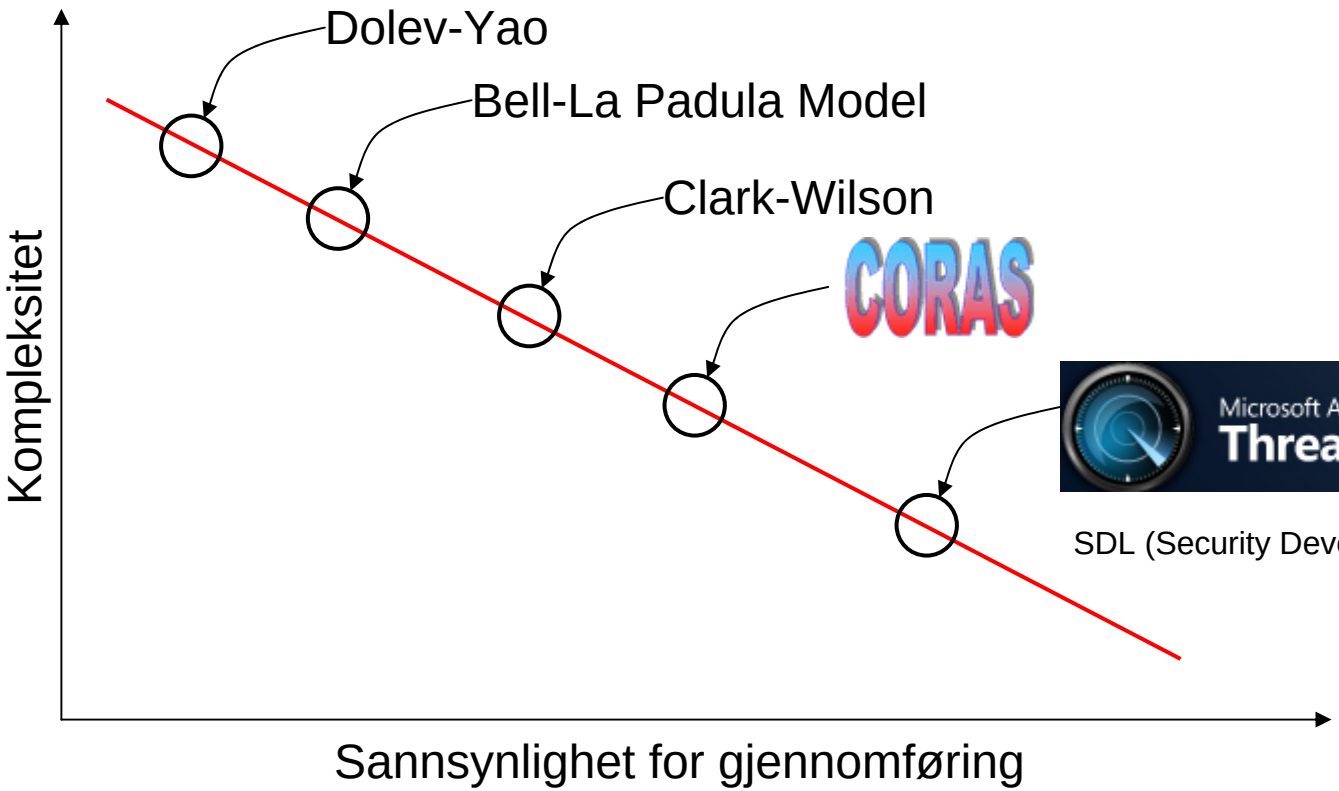


Policies, hvordan håndteres dette i dag?



Hvem bør foreta trusselvurderingen?

Valg av verktøy / metode

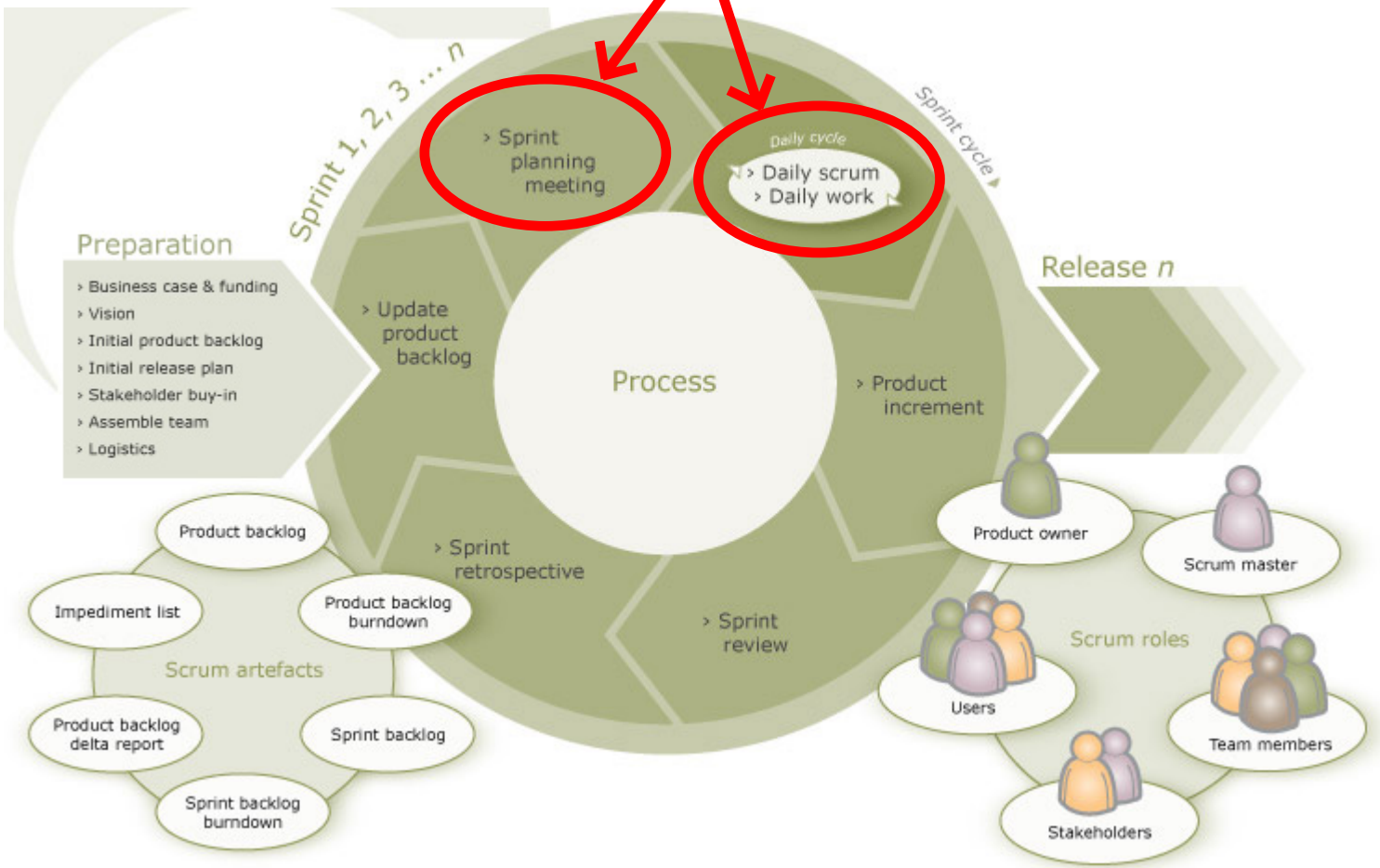


Microsoft Application Security
Threat Analysis & Modeling

SDL (Security Development Lifecycle) process

Scrum metoden

Sikkerhetsdesign og implementasjon



IKT forskriften fra Kredittilsynet

§ 3 Risikoanalyse

…

Foretaket skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor ***akseptable grenser*** *i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.*

IKT forskriften fra Kredittilsynet

§ 5 Sikkerhet

Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal ***så langt det er praktisk mulig være målbare.***

IKT forskriften fra Kredittilsynet

§ 7 Systemvedlikehold
Foretaket skal sikre at IKT-systemene vedlikeholdes og forvaltes på en måte som gir en ***stabil, planlagt og forutsigbar drift.***

IKT forskriften fra Kredittilsynet

§ 11 Driftsavbrudd og katastrofeberedskap

…

Det skal minst ***en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt.*** *Resultatet av testen skal dokumenteres slik at det er mulig å kontrollere.*

Oppsummering

Det ER vanskeig å implementere policies

Trusselvurderinger bør ned på laveste nivå

Periodiske penetreringstester

Grupo
Santander