www.pwc.dk

Digitaliseringsstyrelsen

Risikovurdering
Marts 2018

pwc

Revision. Skat. Rådgivning.

Klaus Ravn

Cyber security specialist

Baggrund

- **Akkreditering af systemer og apps**
- **Risikovurdering af systemer**
- **Facilitator af it-beredskabsøvelser**
- **24 år i Forsvaret**
  - **It ansvarlig**
  - **Systemejer af klassificeret netværk**

Uddannelse

- **Datatekniker**
- **ISO27001 auditor**
- **Sikkerhedskurser**

Programmet

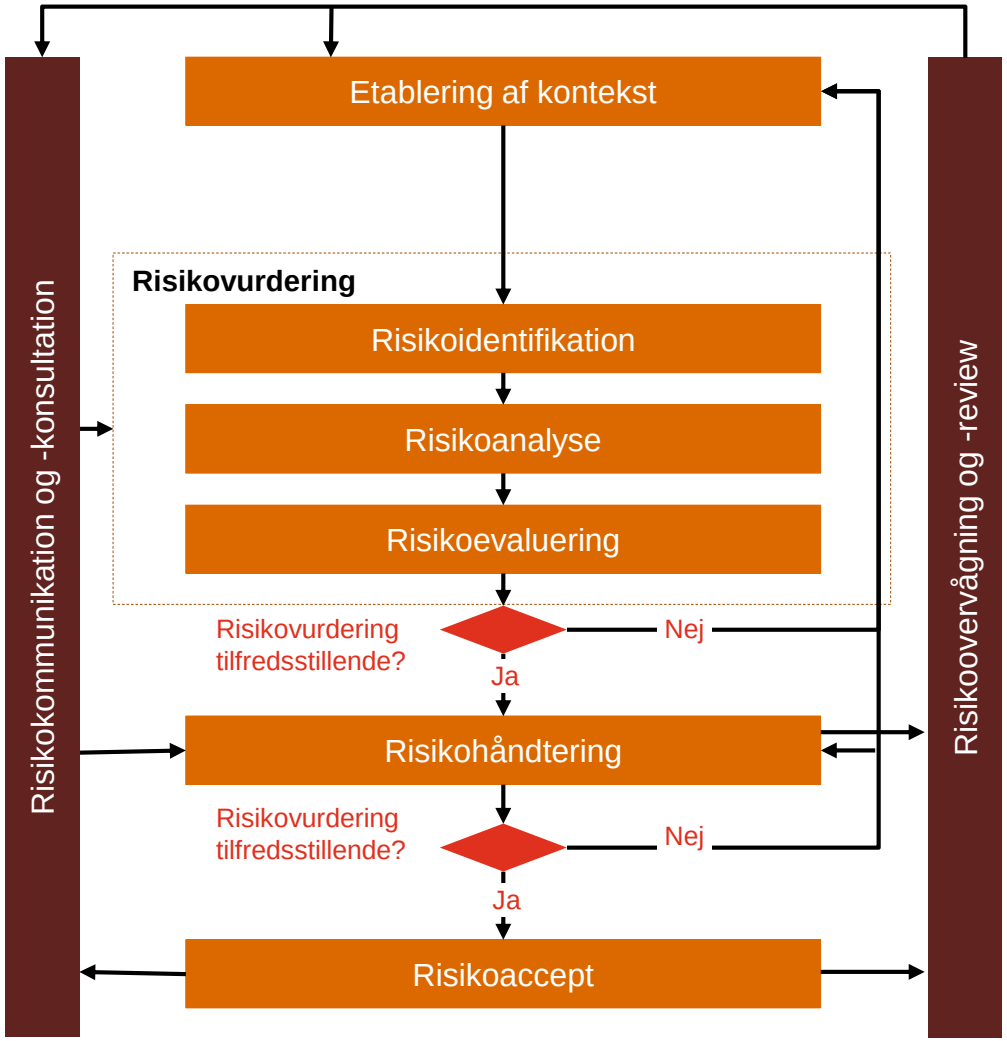
- Oplæg
- Hvad er risikovurdering
- Identifikation af aktiver
- Risikoidentifikation (trusler)
  - Case opgave 1
- Risikoanalyse (sandsynlighed og konsekvens)
  - Case opgave 2
- Risikoevaluering
  - Case opgave 3
- Risikohåndtering
  - Risikohåndteringsplan
  - Statement of Applicability
- Opsummering

Oplæg

Programmet

- Oplæg
- Hvad er risikovurdering
- Identifikation af aktiver
- Risikoidentifikation (trusler)
  - Case opgave 1
- Risikoanalyse (sandsynlighed og konsekvens)
  - Case opgave 2
- Risikoevaluering
  - Case opgave 3
- Risikohåndtering
  - Risikohåndteringsplan
  - Statement of Applicability
- Opsummering

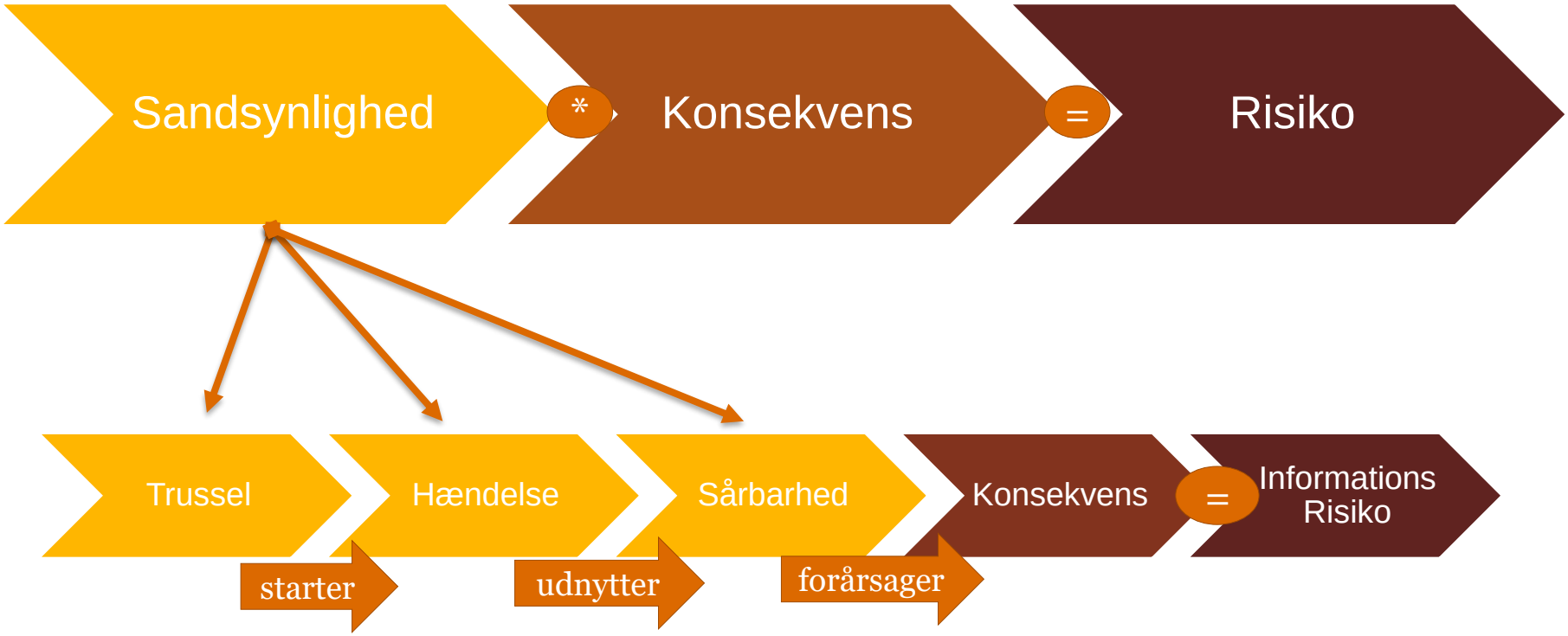
ISO27005 om risikovurdering



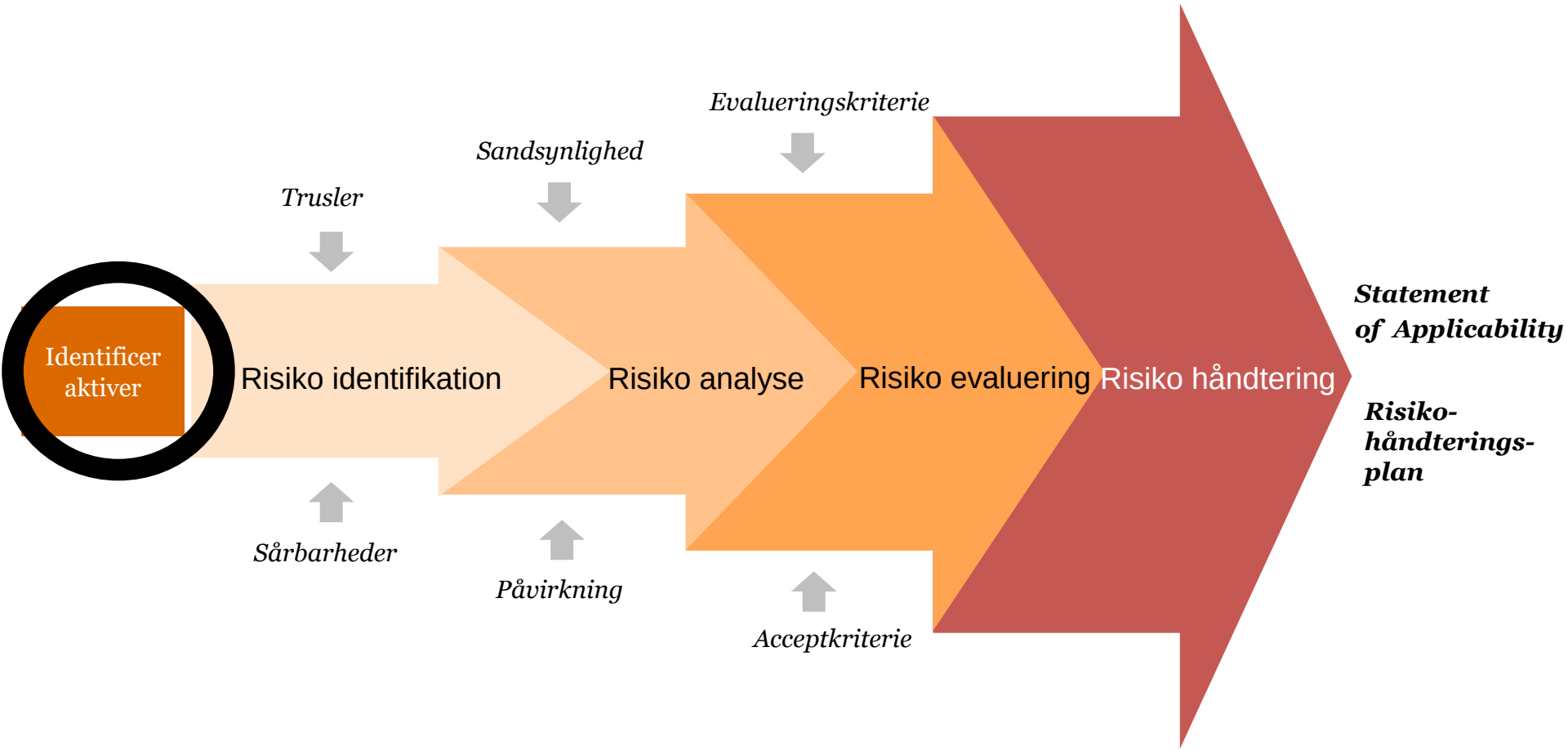
Risiko –> effekten af usikkerhed på målsætninger:

Dvs. en afvigelse fra det ønskede –> positivt og/eller negativ

Basal risikovurdering



Risiko-vurdering og -håndtering



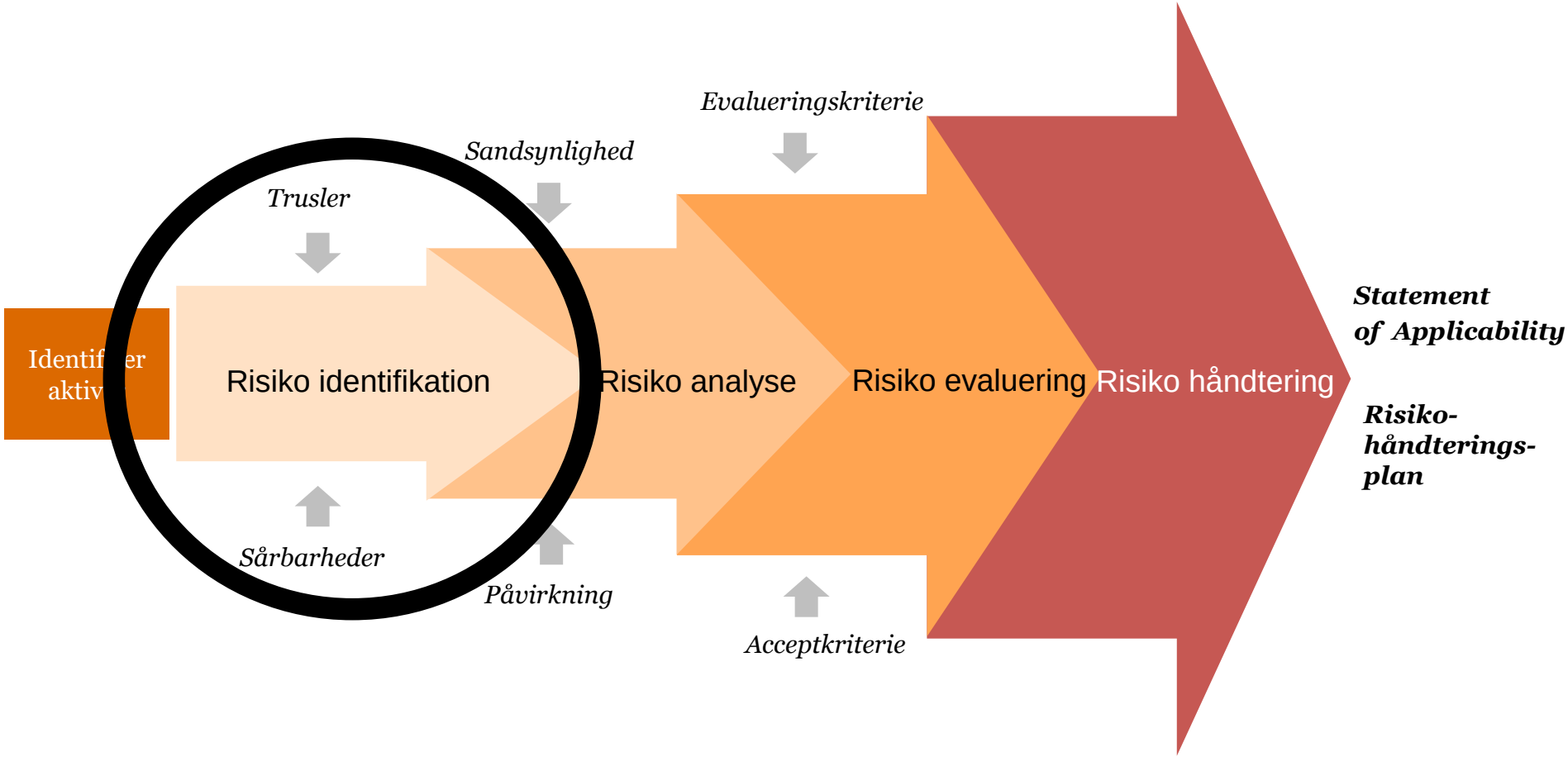
Aktiver

Kan være processer eller ”håndgribelige” ting

- Skal altid beskrives

01	**Kommunikation**	Kommunikation kan foretages både som tekst og voice, og der findes på systemet flere HW/SW som understøtter dette aktiv.
02	**Lagring af data**	Det er muligt at lagre data både lokalt og på de opsatte servere. Dette data kan gemmes i gruppemapper og i brugermappe.
03	**Deling af data**	Det er muligt at dele data ved at placere dette i gruppe mapper, men det er ligeledes også muligt at dele data som vedhæftede filer i mailsystemet. Data kan også deles ved at udprinte fra de opstillede printere og/eller ved at indsætte et flytbar medie.
04	**Analyse af data**	Det er muligt at analysere på lagret data ved hjælp af speciel software, som kan indlæse data og lagre dette i sin egen database.
05	**Serverfarm**	Serverfarm er virtualiseret og holder de lagrede data. Serverfarm er opdelt i 43 virtuelle servere

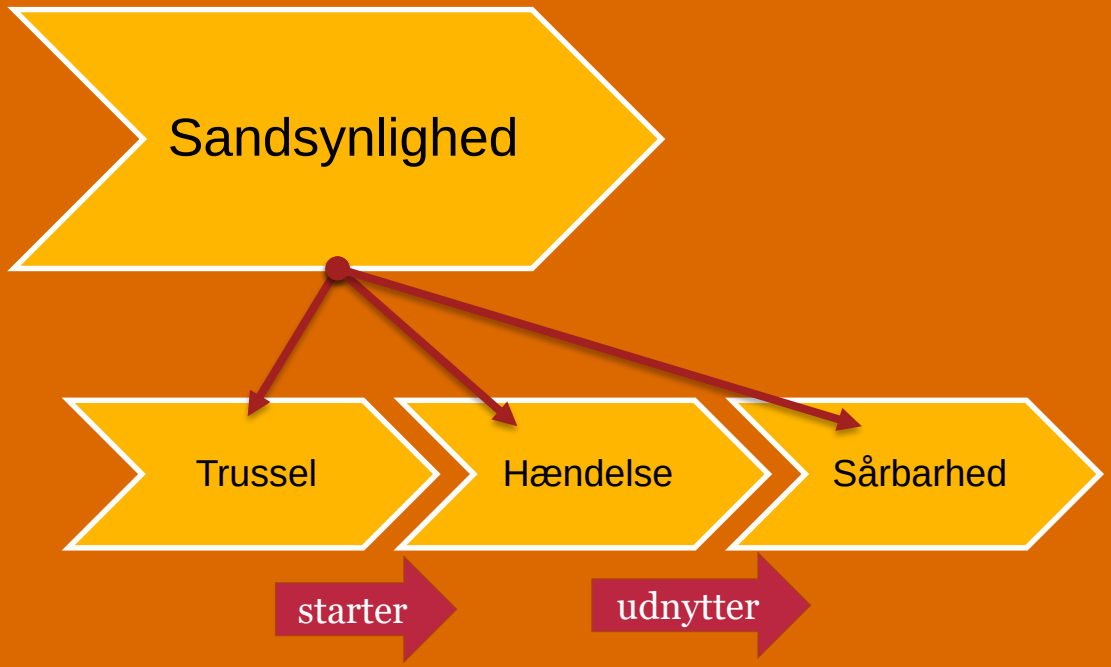
Risiko-vurdering og -håndtering



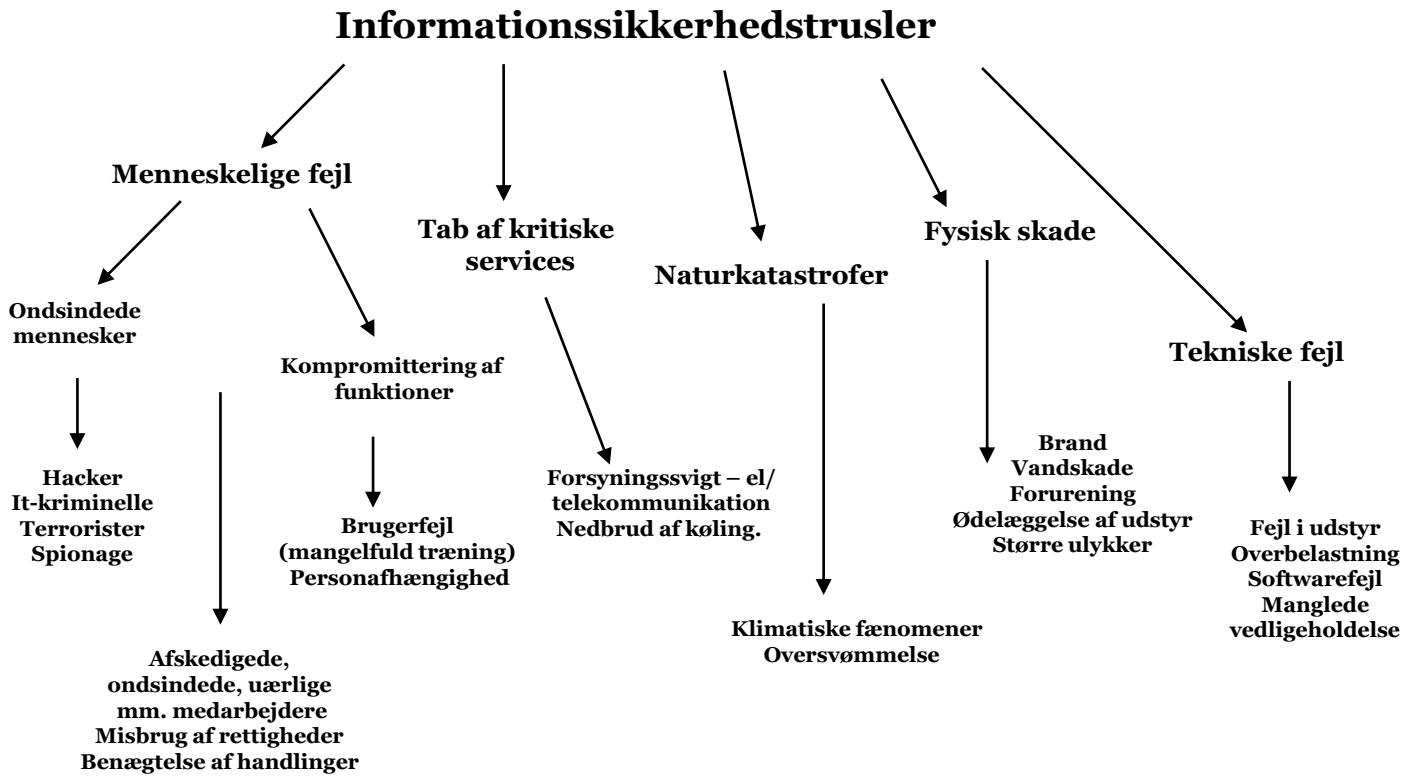
Trusler

Trusler samles normalt i et trusselskatalog

- Menneskeskabte trusler
- Tekniske trusler
- Miljømæssige trusler



Trusselkatalog



CASE
GladeBananer A/S sælger frugt & grønt

It-system: bruges til håndtering og formidling af informationer

- Anvendes af alle medarbejdere
- Indvejning af varer,
- Arbejdstid,
- Lønsystem,
- Kundekartotek

Denne case er gældende for hele workshoppen

Hands-on

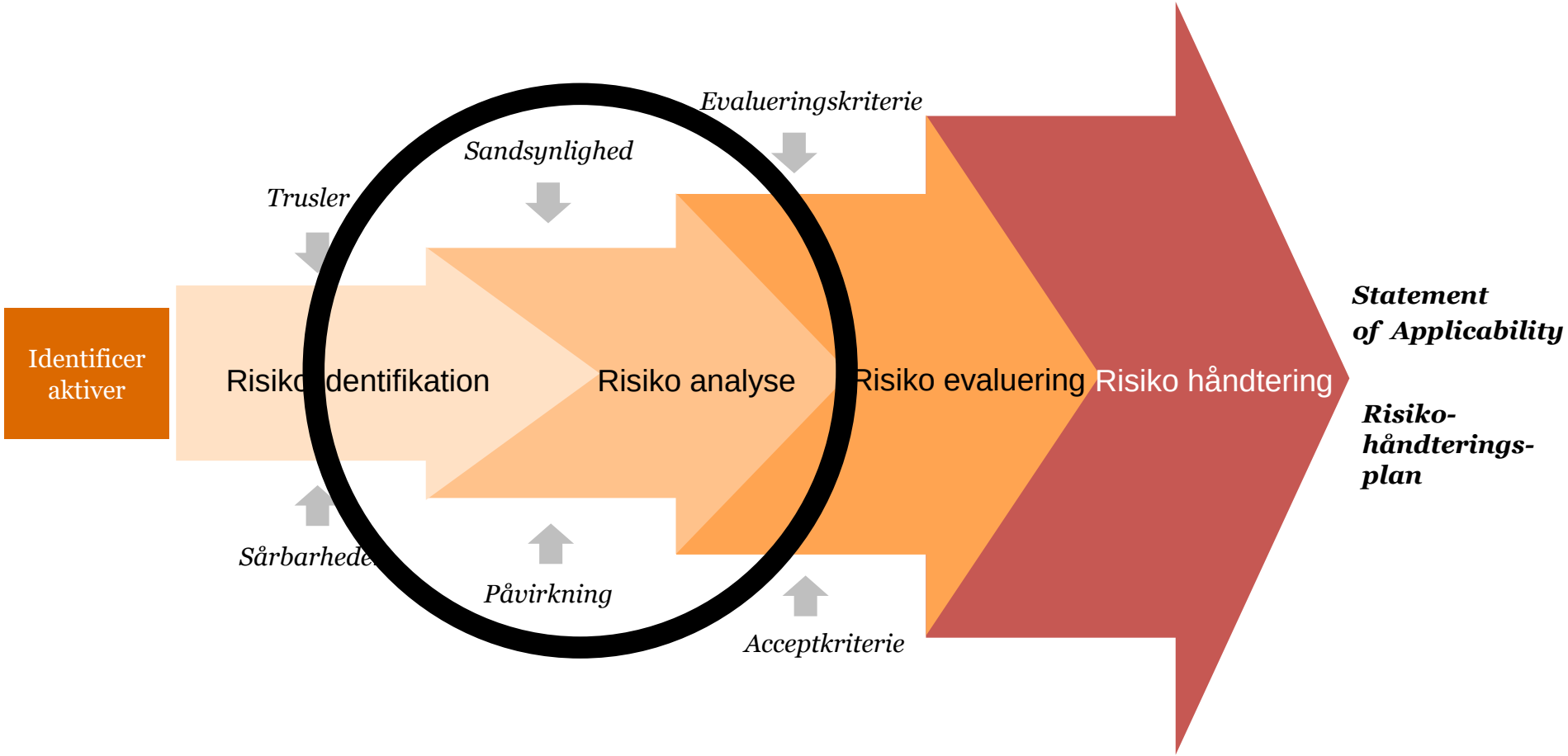
Praktisk tilgang til risikovurdering
Case Del 1
Risikoidentifikation

Afkryds de hændelser og trusler som er relevante

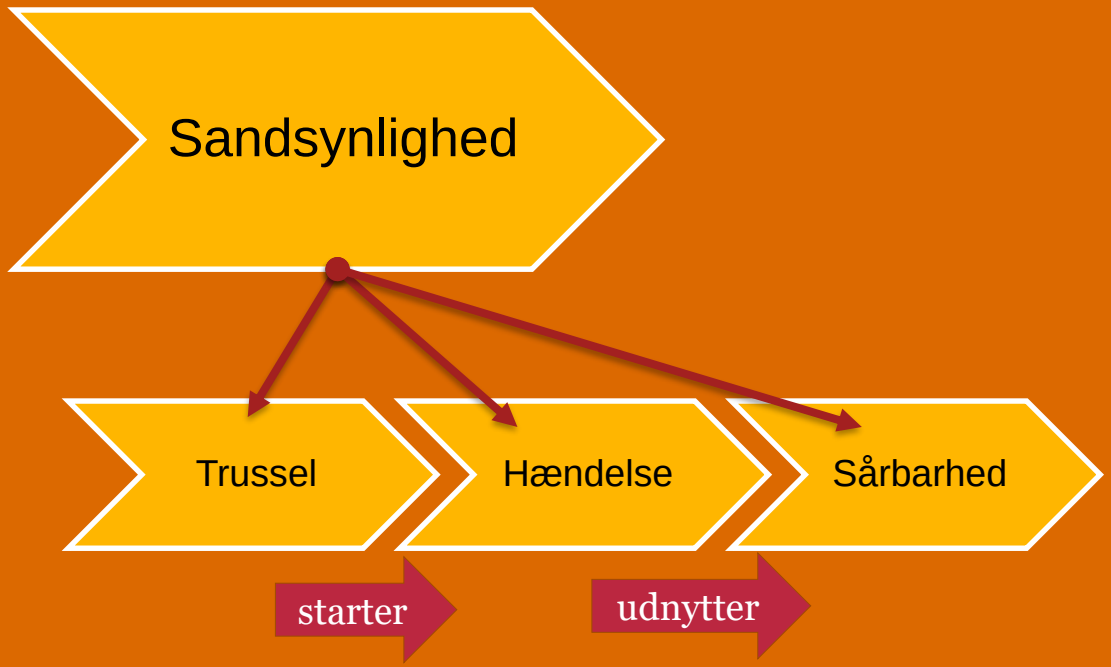
DOKUMENTER: Case Del 1

TID: 15 minutter

Risiko-vurdering og -håndtering



Sandsynlighed



Sandsynlighed for at hændelsen sker En fagteknisk vurdering

Sandsynlighed	Eksempel beskrivelse
1. Usandsynligt	Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme • Ingen erfaring med hændelsen • Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
2. Mindre sandsynligt	Hændelsen forventes ikke at komme • Ingen erfaring med hændelsen • Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark
3. Sandsynligt	Det er sandsynligt at hændelsen vil forekomme • Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder • Kendes fra andre offentlige og private virksomheder i Danmark (omtales årligt i pressen)
4. Forventet	Det ventes at hændelsen vil forekomme • Man har erfaring med hændelsen inden for de sidste 12 måneder • Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen)

Konsekvens
En ledelsesmæssig vurdering

- Konsekvens for brud på fortroligheden
- Konsekvens for brud på integritet
- Konsekvens for brud på tilgængelighed

Konsekvens
1. Lille
2. Medium
3. Stor
4. Meget stor

Risikoanalyse

Sandsynlighed
1. Usandsynligt
2. Mindre sandsynligt
3. Sandsynligt
4. Forventet

Konsekvens	1 Lille	2 Mediunm	3 Stor	4 Meget stor

Hands-on

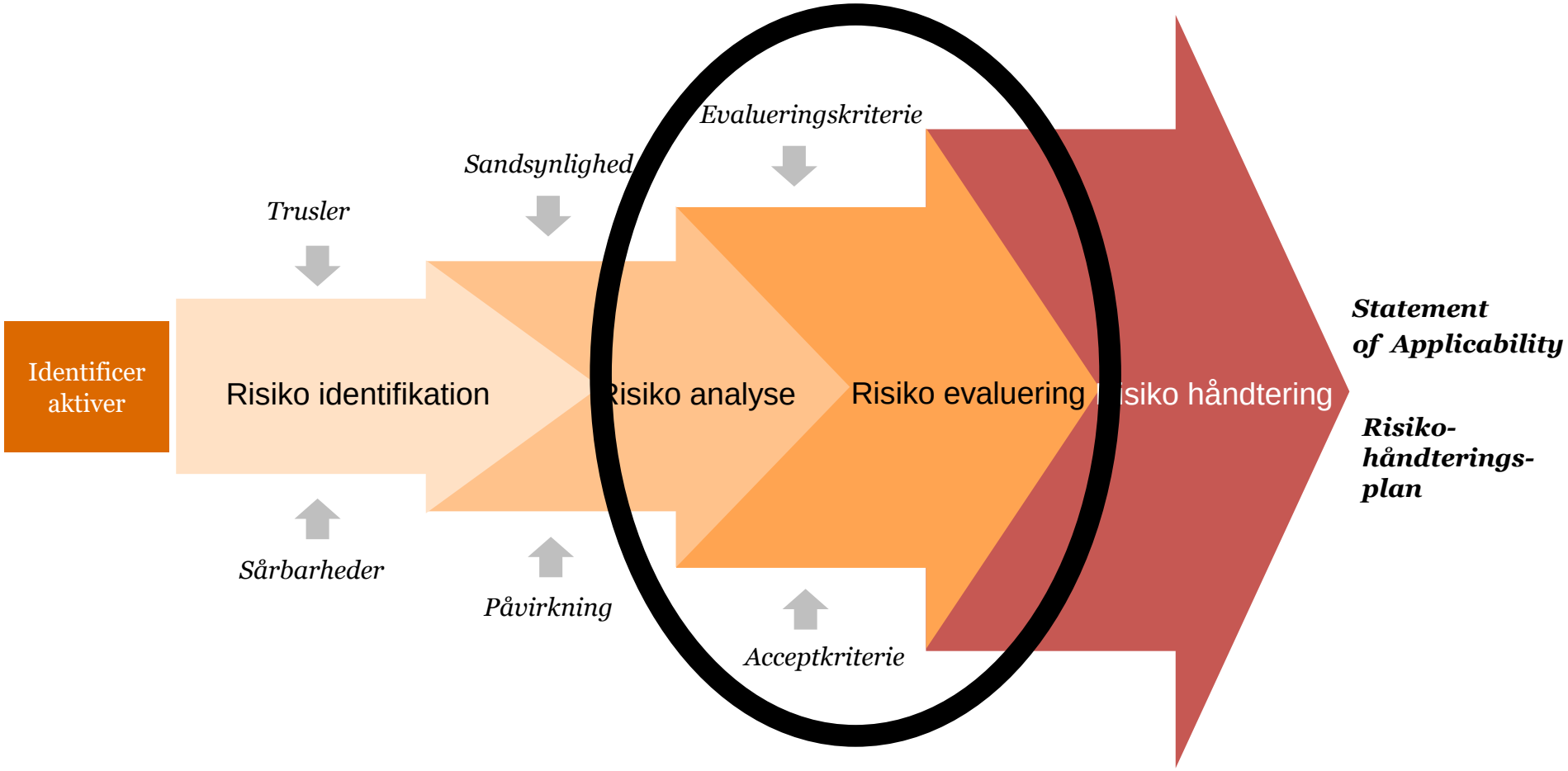
Praktisk tilgang til risikovurdering
Case Del 2
Risikoanalyse

Vurder og nedskriv sandsynlighederne

DOKUMENTER: Case Del 2

TID: 30 minutter

Risiko-vurdering og -håndtering

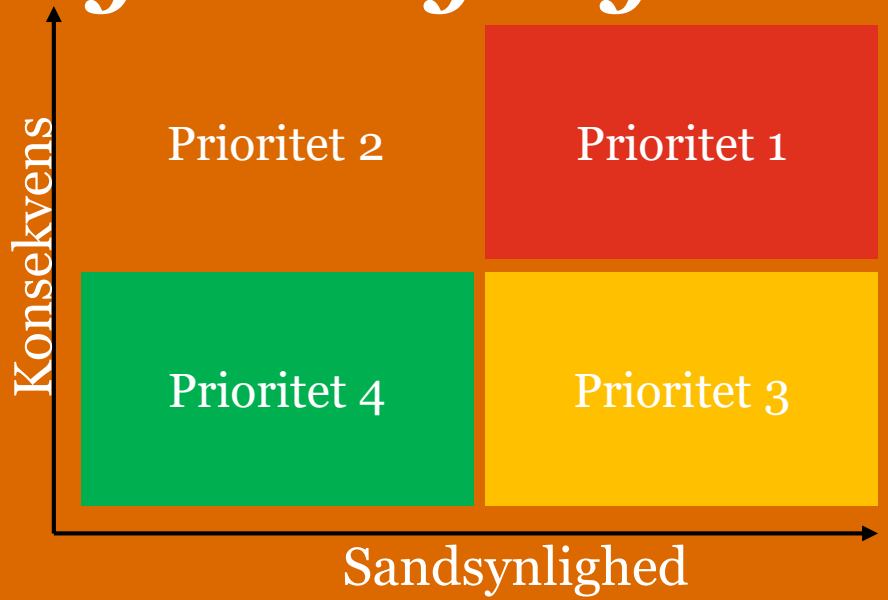


Risikoanalyse

Sandsynlighed
1. Usandsynligt
2. Mindre sandsynligt
3. Sandsynligt
4. Forventet

Konsekvens	1 Lille	2 Mediunm	3 Stor	4 Meget stor

Risikoevaluering
Risikobilledet i forhold til konsekvens og sandsynlighed



Trusselsscenarier, der kan medføre kompromittering af integriteten	*Risikoniveau*
Bruger sætter anden klient på netværket	12
Uautoriseret bruger får adgang til systemet, via manglende patching	6
Uautoriseret bruger opsætter sit eget transparente udstyr på netværket	6

Min foretrukne

SANDSYNLIGHED

KONSEKVENS

	Lille	**Medium**	**Stor**	**Meget stor**
Lille	1	2	3	4
Medium	2	4	6	8
Stor	3	6	9	12
Meget stor	4	8	12	16

Hands-on

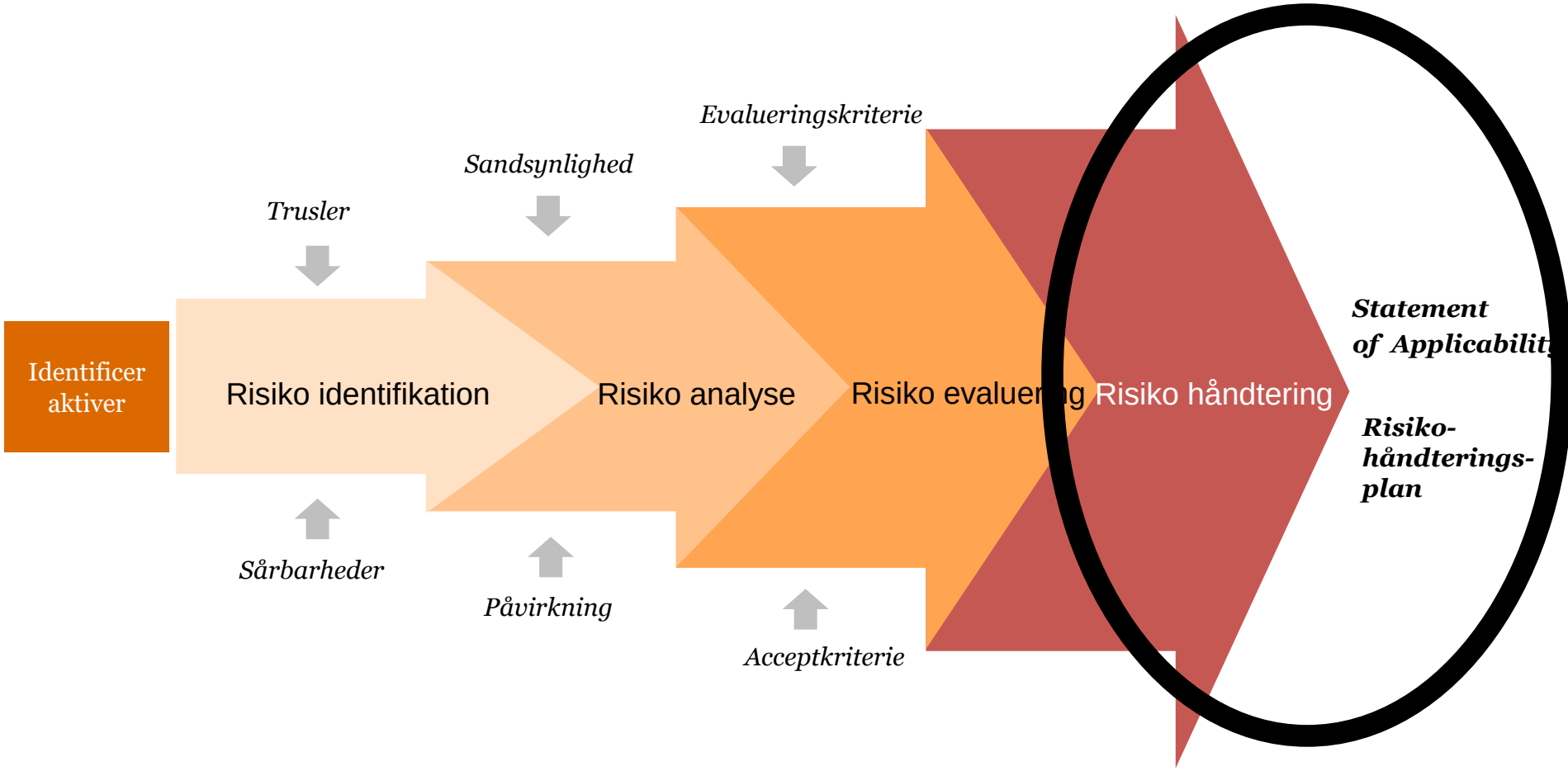
Praktisk tilgang til risikovurdering
Case Del 3
Risikoevaluering

Multiplicer konsekvens og sandsynlighed

DOKUMENTER: Case Del 3

TID: 15 minutter

Risiko-vurdering og -håndtering

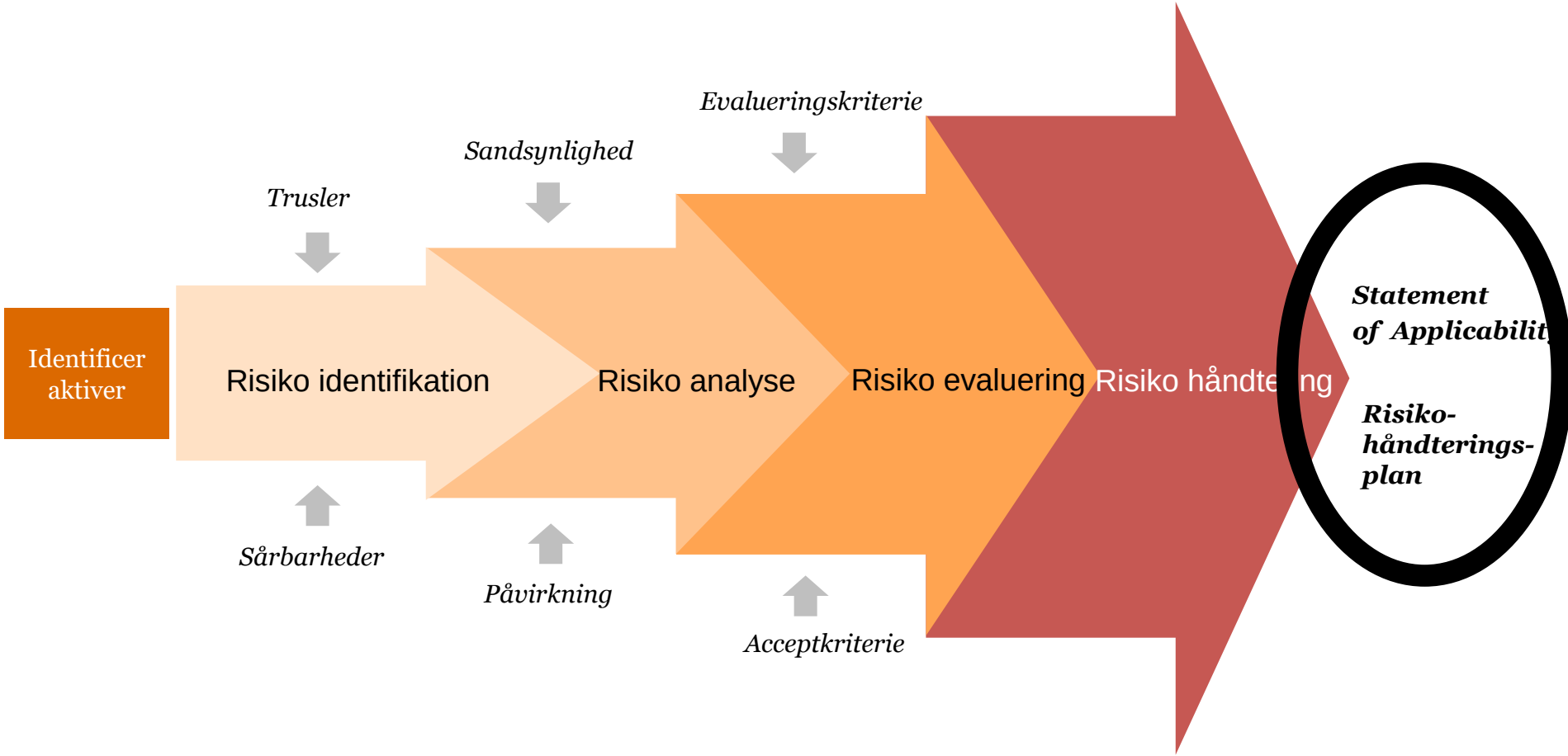


Risikohåndtering
Hvad gør vi nu?

- *Undgå (risikoundgåelse)*
- *Reducer (risikomodificering)*
- *Overfør (risikodeling)*
- *Accept (risikofastholdelse)*

Risikoniveau	Strategi for håndtering	Tidshorisont
Lav		
Mellem		
Høj		

Risiko-vurdering og -håndtering



Statement of Applicability

Hvornår gør vi det?

Hvorfor gør vi det?

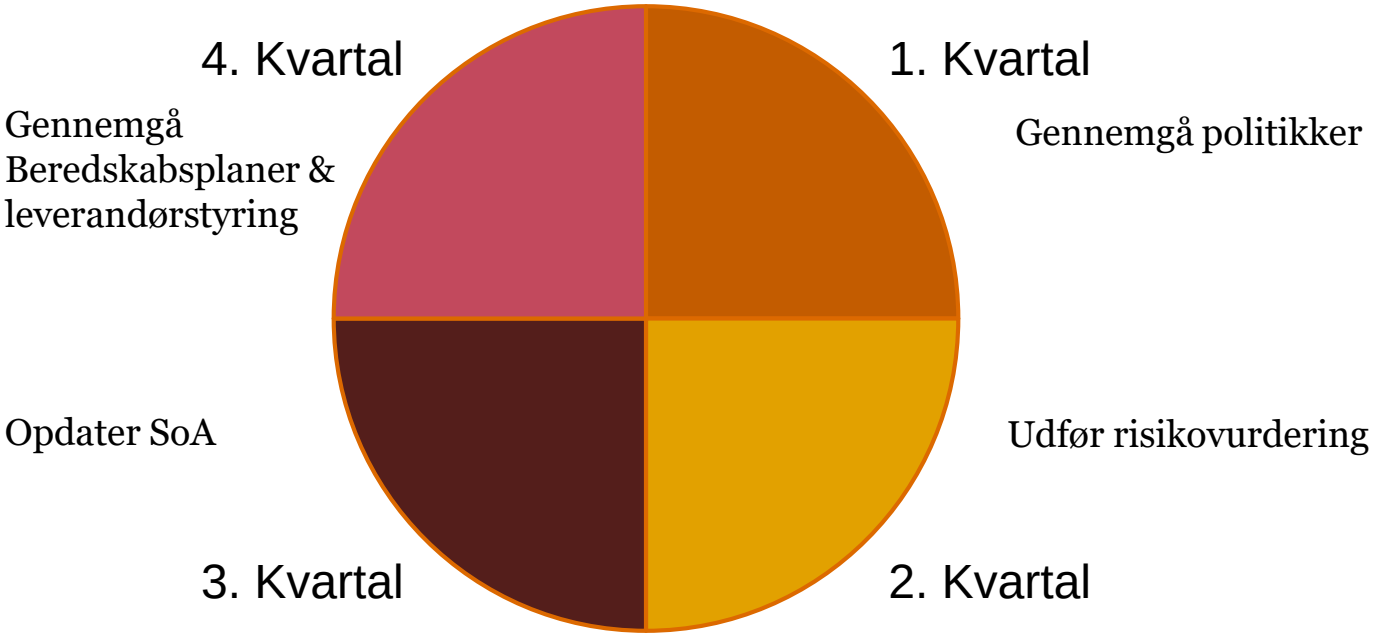
Hvad skal der være i den?

Hvordan gør vi det?

Sådan kan vi gøre det

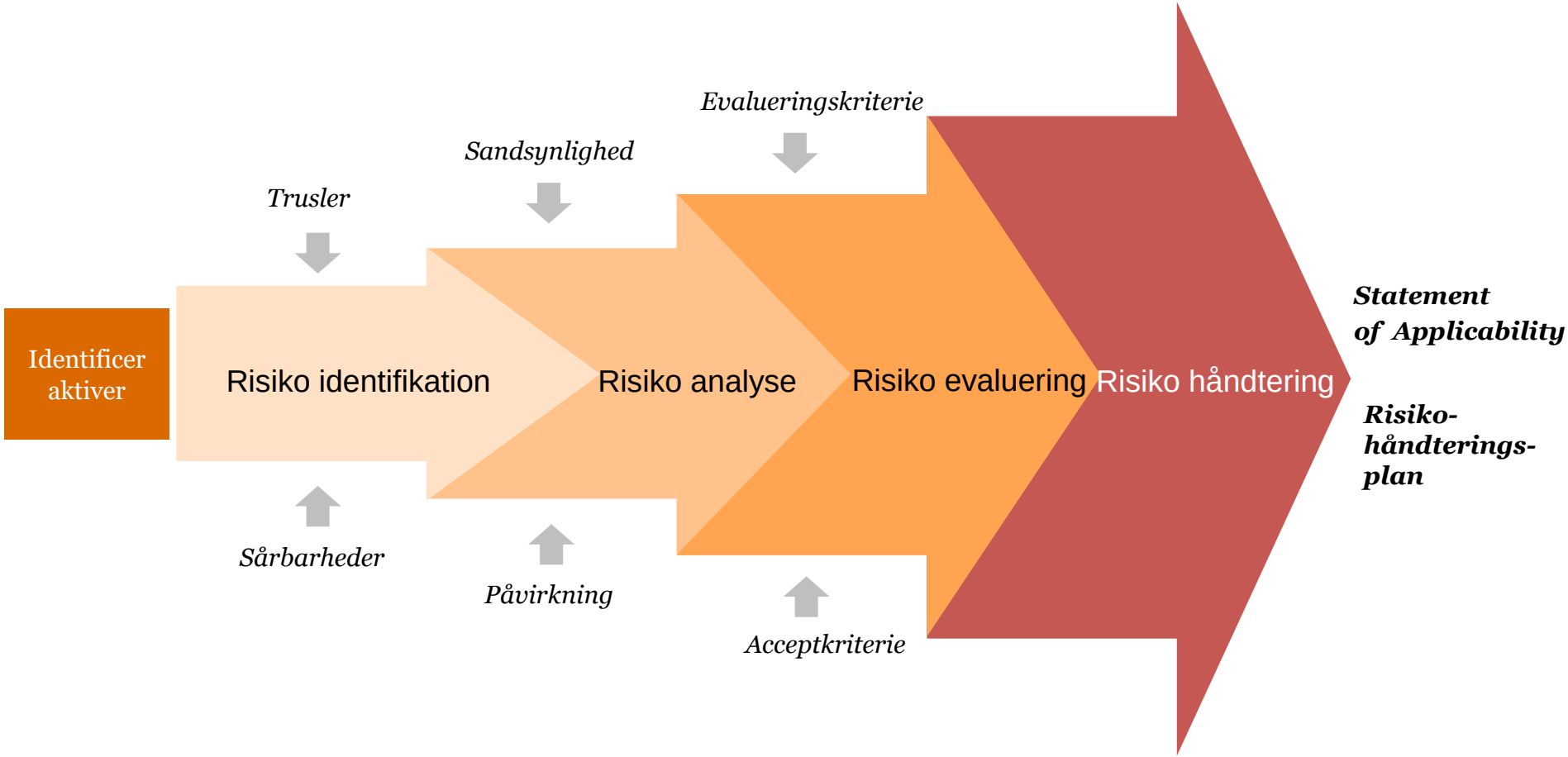
A.5.1.1. Politikker for informationssikkerhed	
kontrolbeskrivelse	
Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.	
Sikkerhedskrav	**Verifikation af sikkerhedskravsimplementering**
A.5.1.1.a [*Beskriv hvad*]	[*Beskriv hvordan*]
A.5.1.1.b [*Beskriv hvad*]	[*Beskriv hvordan*]
Dokumentation for implementering/håndtering af krav	Implementeret
[*Beskriv hvordan og evt. med link til dokumentationen*]	*[Ja/Nej/Delvis]*

Så ofte kan vi gøre det
Eksempel på årshjul for risikovurdering

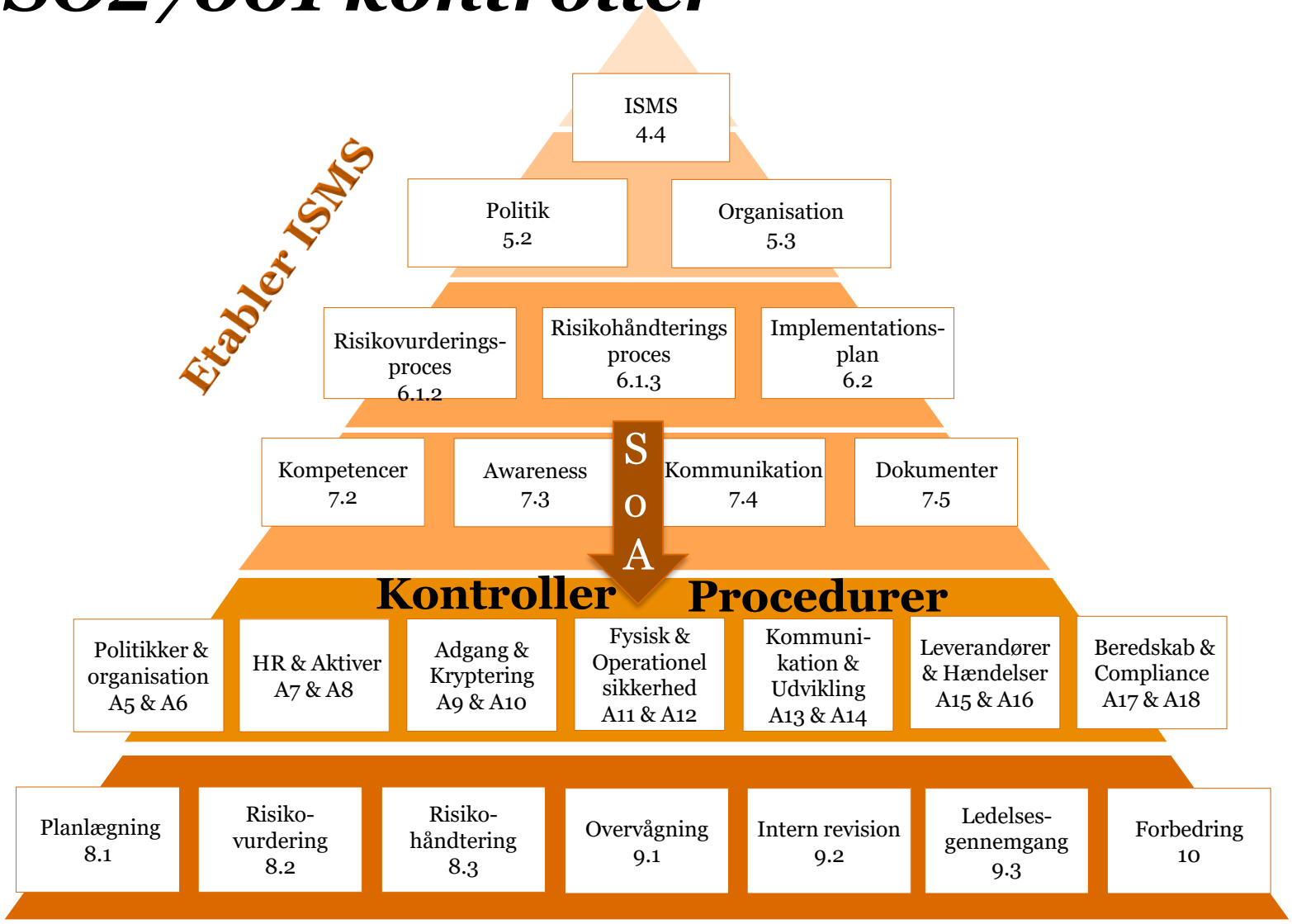


Opsummering

Risiko-vurdering og -håndtering



ISO27001 kontroller



Spørgsmål?

Klaus Hansen Ravn
Manager - Security & Technology
T: 8932 5683
E: kxy@pwc.dk