



DevoTalks

Elementerne i velfungerende sikkerhedsledelse

- og hvorfor det er så svært at få til at fungere i praksis



Innovative technology consulting for business.



VELKOMMEN

DIGITALE
indspark

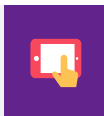
FORSKELLIGE
emner

SKIFTENDE
oplægsholdere

40 + 5
minutter



Lidt praktik inden start



Har du spørgsmål
kan du stille dem i chat-
funktionen, og de vil blive
besvaret efter 'talk'en'



Vil du gerne gense
slides bliver denne
DevoTalk optaget og
gjort tilgængelig på sitet
www.devotalks.dk



Vil du gerne se mere
så finder du en oversigt
over kommende
devotalks på sitet
www.devotalks.dk



COMPLIANCE

Mål eller milepæl?

EU GDPR

Datatilsynet

ISO 27001

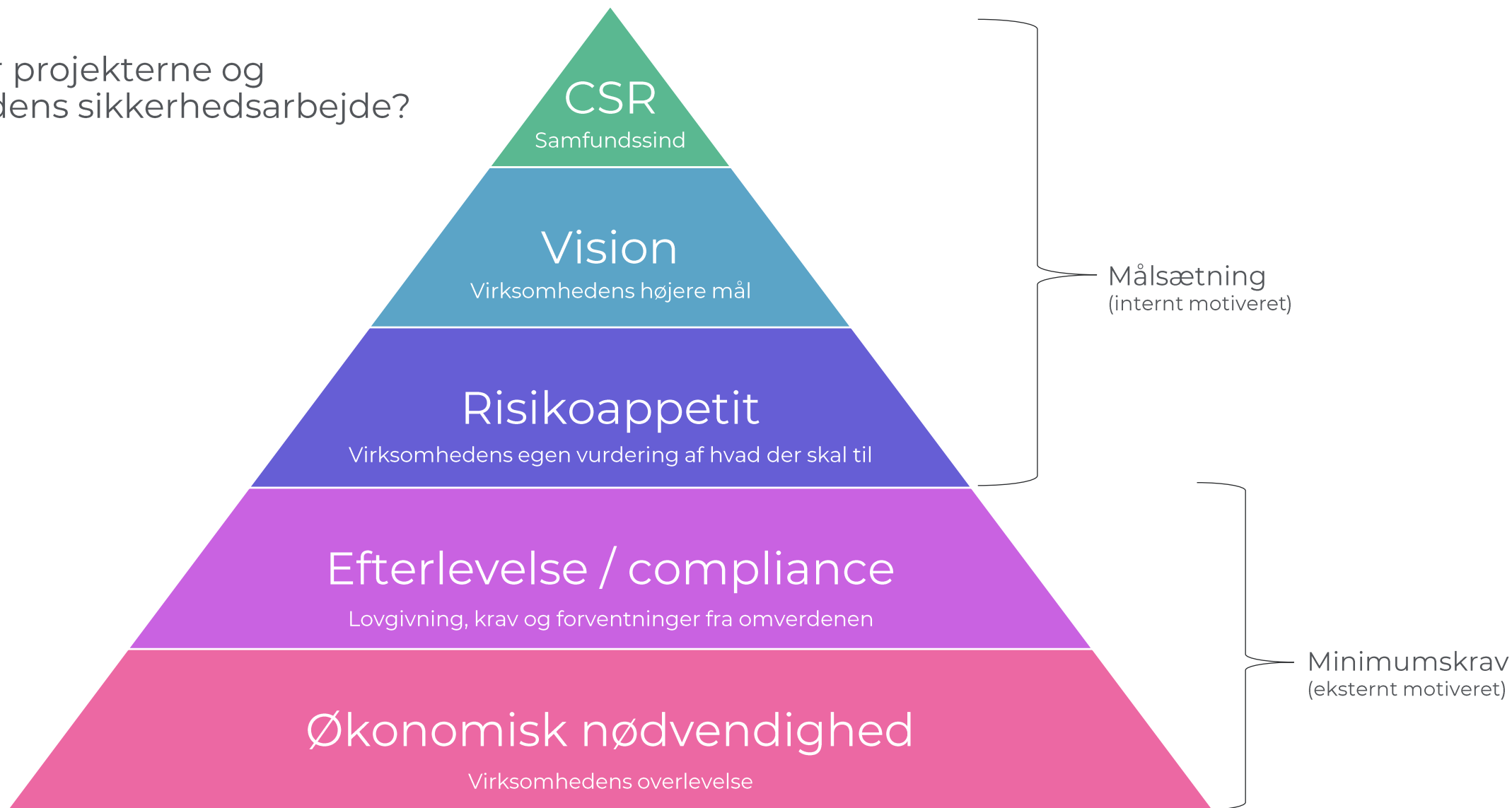
Finanstilsynet

NIS loven

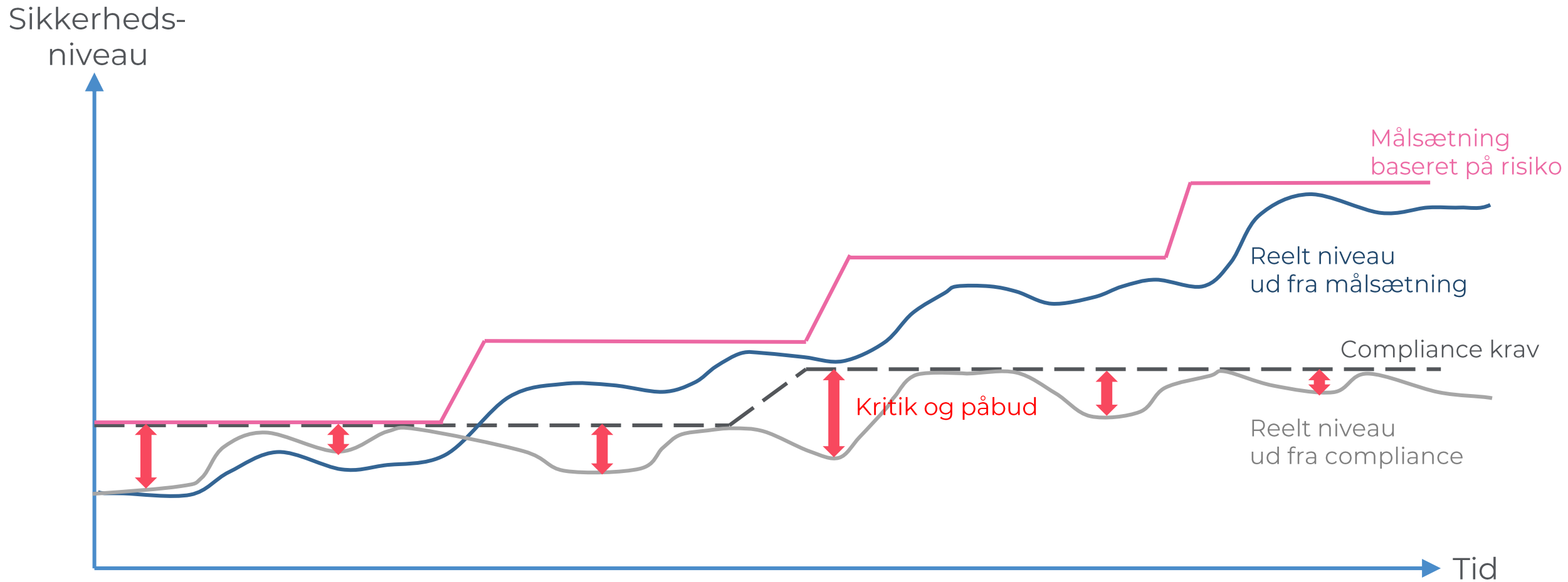
Rigsrevisionen

Behovspyramide for sikkerhedsledelse

Hvad driver projekterne og virksomhedens sikkerhedsarbejde?



Hvis du styrer efter compliance - så når du det aldrig



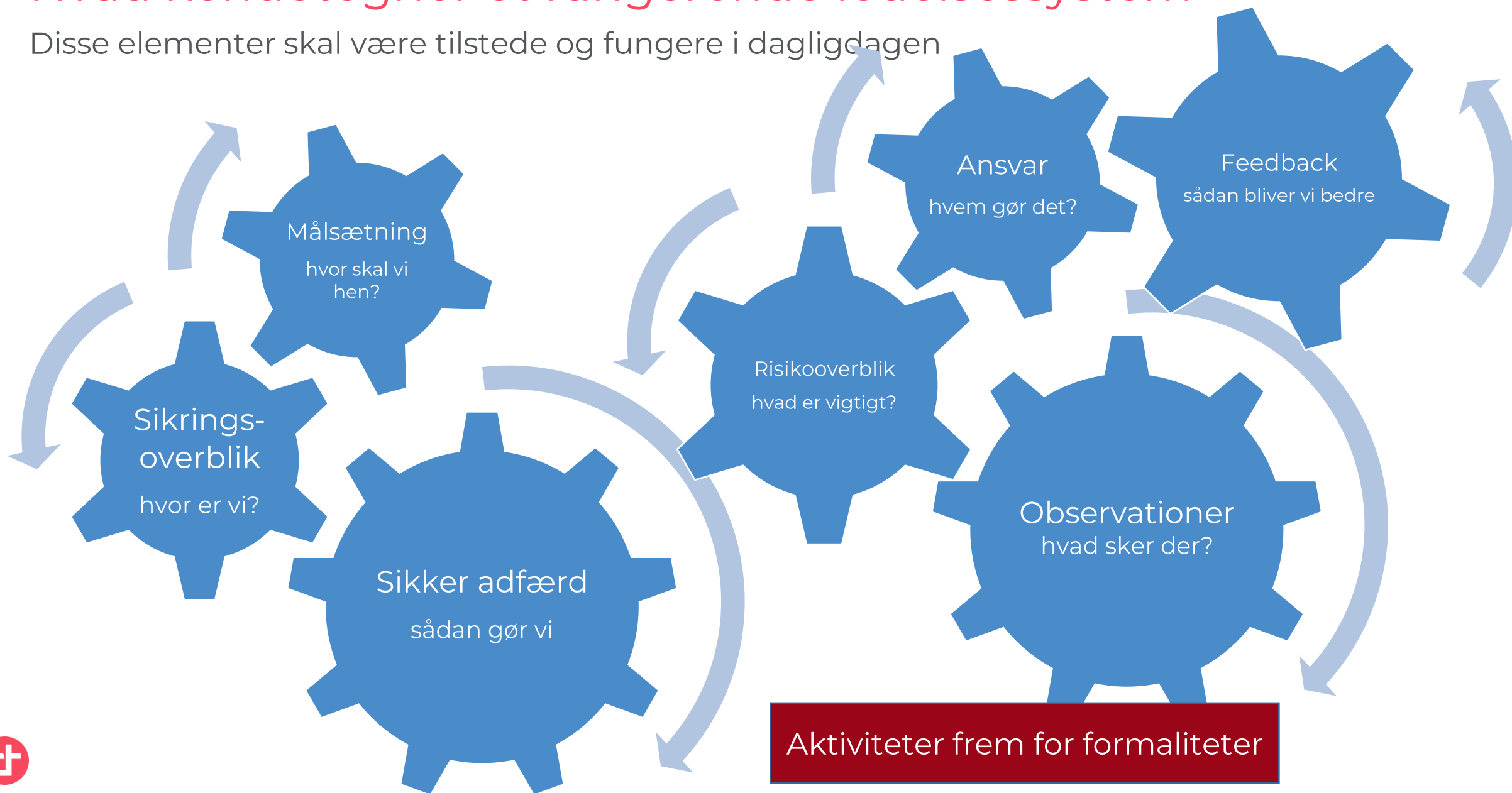
Fem klassiske problemstillinger

1. Vi **beskriver** formel sikkerhed – men **implementerer ikke** reel sikkerhed
2. Vi har ikke nogen velbegrundet **prioritering** at tiltag
3. Der er **for få interessenter** involveret
4. Det er uklart hvad sikkerhedsniveauet **kræver og koster**
5. **Ingen reel forandring** bliver implementeret



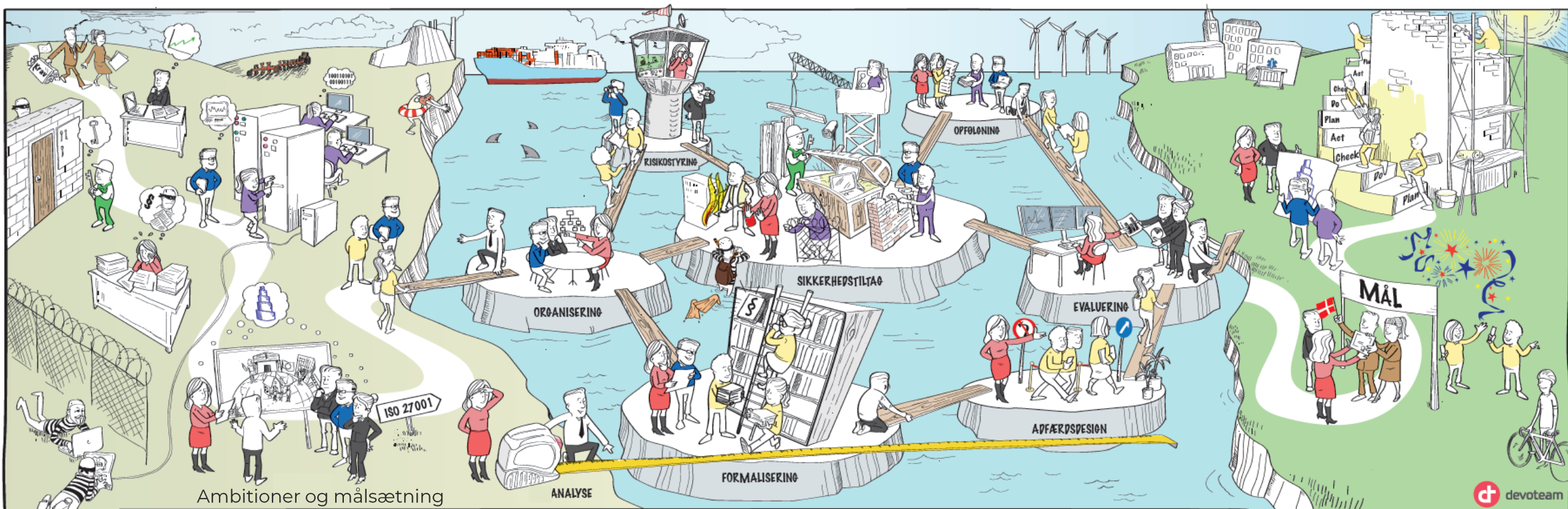
Hvad kendetegner et fungerende ledelsessystem

Disse elementer skal være tilstede og fungere i dagligdagen



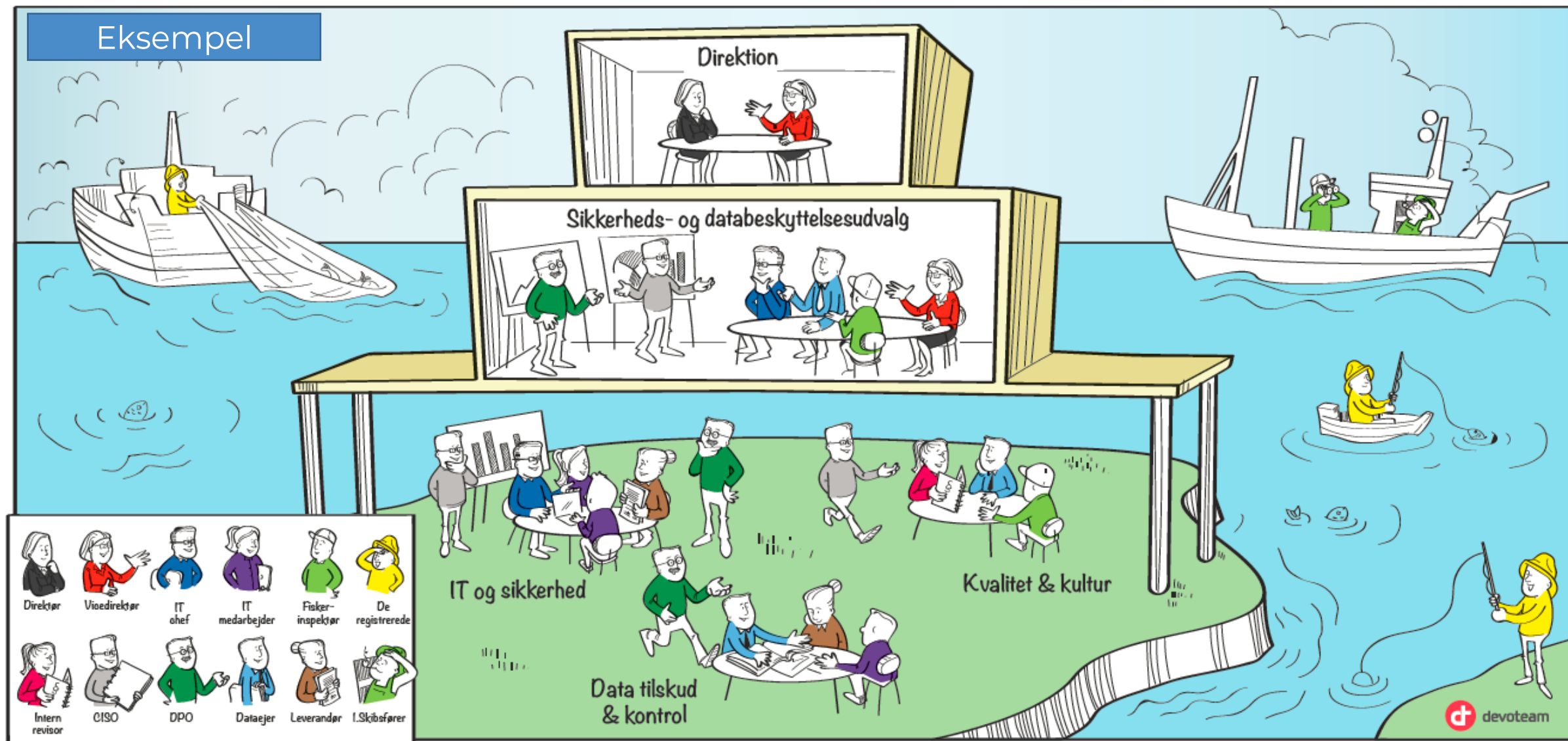
ISO 27001

Visualiseret i syv discipliner



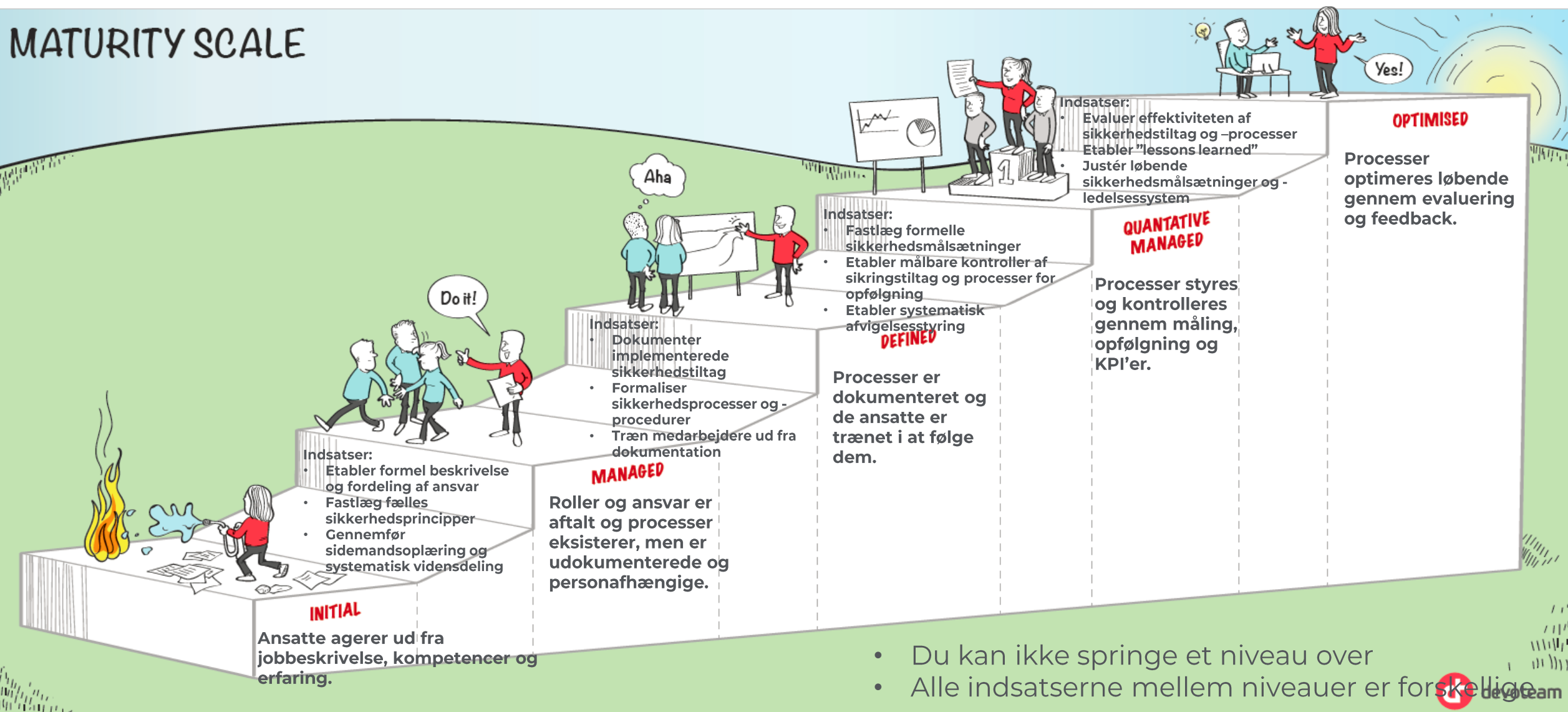
Start med organiseringen

Eksempel



Modenhedsskala for ledelsessystem

MATURITY SCALE



- Du kan ikke springe et niveau over
- Alle indsatserne mellem niveauer er forskellige

Modenhed og ambitionsniveau for implementering

Områder \ modenhed	Basis ISMS		ISO 27001 "compliant"	ISO 27001 certificering	
	Ad Hoc	Gentagelig	Defineret	Styret / Målbart	Optimerende
Organisering (Sikkerhedsorganisation)	Ansæt folk med de rette kompetencer og giv dem løbende efteruddannelse.	Fastlæg og dokumentér roller og ansvar formelt og sørg for at alt nødvendigt sikkerhedsansvar er delegeret og varetages.	Etablér og dokumentér formelle sikkerhedsledelsesprocesser og beslutningsorganer enten gennem udbygning af eksisterende strukturer eller ved etablering af nye. Vedtag og dokumentér en sikkerhedsstrategi.	Etablér processer, der sikrer at ledelsesbeslutninger dokumenteres i mødereferater, handlingsplaner og sikkerhedsstrategi. Etablér et årshjul for aktiviteter.	Etablér processer til evaluering af eksekvering på handlingsplaner og sikkerhedsstrategi og af konsekvens og effektivitet i organiseringen. Følg op på eksekvering af årshjul.
Formalisering (Dokumentation og politikker)	De ansatte vurderer selv, hvilke regler og hvilken dokumentation, der er behov for.	Definér sikkerhedsprincipper for virksomheden ud fra en overordnet vurdering af risiko og compliance-krav. Dokumentér principperne i en informationssikkerhedspolitik.	Etablér et Statement of Applicability (SoA), der dokumenterer de aktuelle sikringsforanstaltninger og kontroller. Udarbejd specifikke politikker, standarder og procedurer for områder, hvor det findes nødvendigt ud fra en formel risikovurdering.	Foretag målinger af, om de ansatte er trænet i, forstår og følger den dokumentation, de skal anvende.	Etablér processer til løbende evaluering og opdatering af dokumentation, herunder af sikkerhedspolitikker.
Risikostyring (Risikoidentificering, -vurdering og -håndtering)	Risici vurderes uformelt og løbende når de opdages af de ansatte og håndteres ud fra de ansattes viden og erfaring.	Vurdér risiko overordnet gennem GAP-analyse i forhold til et rammeværk for god praksis, fx. CIS 20 Critical Security Controls, ISF SoGP eller ISO 27002.	Identificér og dokumentér systematisk og regelmæssigt risici gennem vurderinger, der tager udgangspunkt i virksomhedens trusselsbillede, sårbarheder og forretningskonsekvenser. Dokumentér tiltag til risikohåndtering i handlingsplaner.	Foretag løbende opfølgning på risikovurderinger og -håndteringstiltag og rapportér på ændringer i risikobillede og fremdrift på handlingsplaner.	Etablér processer til evaluering af risikostyringen og dens effekt på sikkerheden gennem ledelsesgennemgang af risikobillede, risikohåndtering og trends for sikkerhedshændelser.
Sikkerhedstiltag (Sikringsforanstaltninger og kontroller)	Foranstaltninger implementeres ud fra de ansattes erfaring og faglige kompetencer.	Implementér foranstaltninger med baggrund i en prioriteret anvendelse af et rammeværk for god praksis, fx. CIS 20, ISF SoGP eller ISO 27002.	Implementér foranstaltninger med udgangspunkt i risikohåndteringsplaner og dokumentér dem løbende (som minimum) i SoA og desuden i nødvendige specifikke politikker, standarder og procedurer.	Etablér kontroller, der sikrer og verificerer effektiviteten af sikringsforanstaltninger definér effektivitetsmålinger og KPI'er for sikkerheden.	Etablér processer til evaluering af sikringsforanstaltningernes effektivitet og implementeringsgrad og til løbende effektivitetsforbedring.
Adfærdsdesign (Sikkerhedskultur og awareness)	Diskutér løbende emnet informations-sikkerhed på team- og afdelingsmøder.	Fastlæg et grundlæggende kodeks for adfærd på sikkerhedsområdet og etablér konsensus om det.	Udarbejd vejledninger til de ansatte i sikker / usikker adfærd og træn dem i det. Identificér områder, hvor adfærdsdesign eller tekniske foranstaltninger er mere effektive end vejledninger.	Gennemfør tests for at måle de ansattes forståelse af sikkerhedskodeks og -vejledninger. Gennemfør målinger af de ansattes faktiske adfærd.	Etablér processer til evaluering af virksomhedens sikkerhedskultur og de ansattes awareness og adfærd og gennemfør løbende justering af virkemidler.
Opfølgning (Kontrol af efterlevelse og behandling af afvigelser)	De ansatte beder hinanden om "peer review", når de finder det passende.	Beskriv i roller og ansvar, hvilke områder de ansatte skal føre kontrol med for hinanden.	Etablér og dokumentér en audit-proces og etablér et audit-program på baggrund af risikovurdering og compliance-krav. Dokumentér og rapportér audit-resultater.	Etablér en proces for registrering og behandling af afvigelser og dokumentation af korrigerende handlinger.	Etablér processer for evaluering af trends i auditresultater og opfølgning på afvigelseskorrigerende.
Evaluering (Ledelsens gennemgang og løbende forbedring)	Sæt "sikkerhed" på dagsordenen på eksisterende ledelsesmøder.	Fastlæg og beskriv ledelsens rolle i og ansvar for evaluering og forbedring af sikkerheden.	Etablér og dokumentér en formel proces for "ledelsens gennemgang" af risikostyring, efterlevelse og gennemførelse af hertil relaterede handlingsplaner.	Etablér en særskilt registrering af strategiske mål for ledelsessystemet og handlingsplaner, der er et resultat af "ledelsens gennemgang", og opstil KPI'er og deadlines for dem.	Foretag som del af "ledelsens gennemgang" en evaluering af ledelsessystemet og strategiske mål, KPI'er og deadlines og foretag derudfra justeringer af ledelsessystemet.



Hvor er du?
Hvor vil du hen?
Hvordan ser vejen ud?
Vær realistisk!

Forudsætninger for implementering

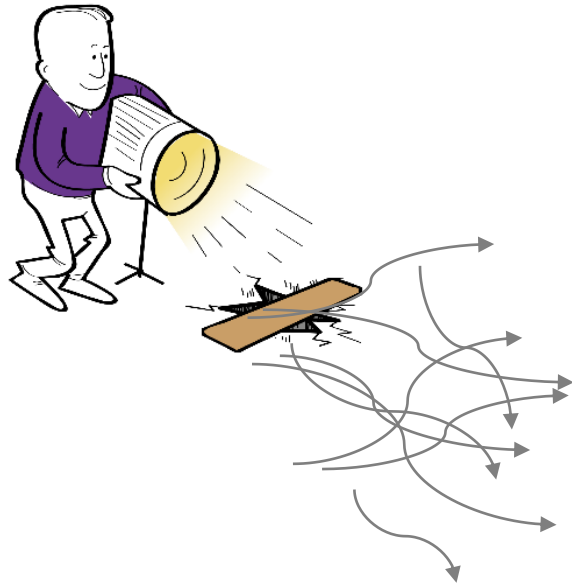


Vilje og lyst

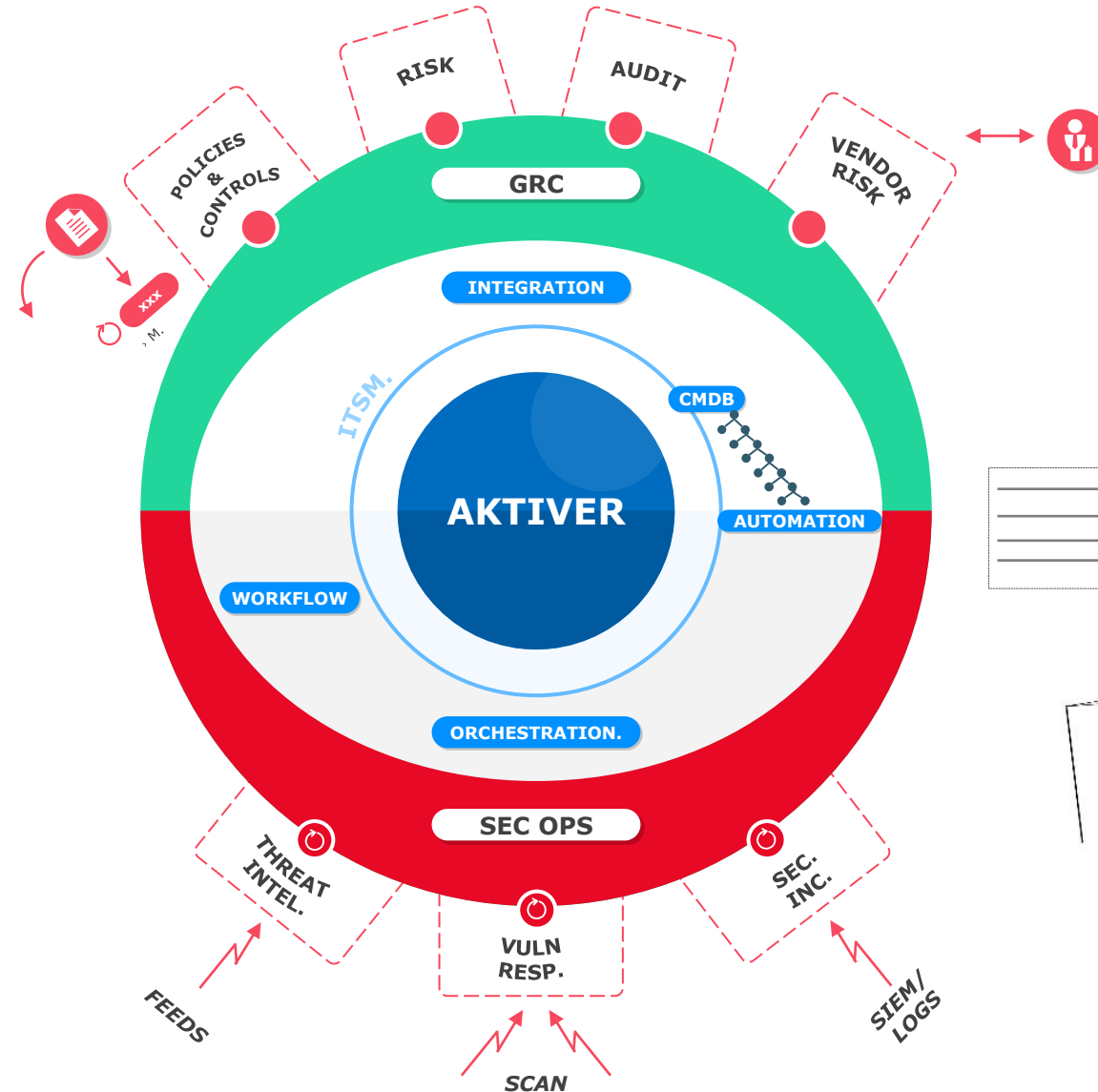
Ressourcer

Viden og kompetencer

Automatisering af ledelsessystemet



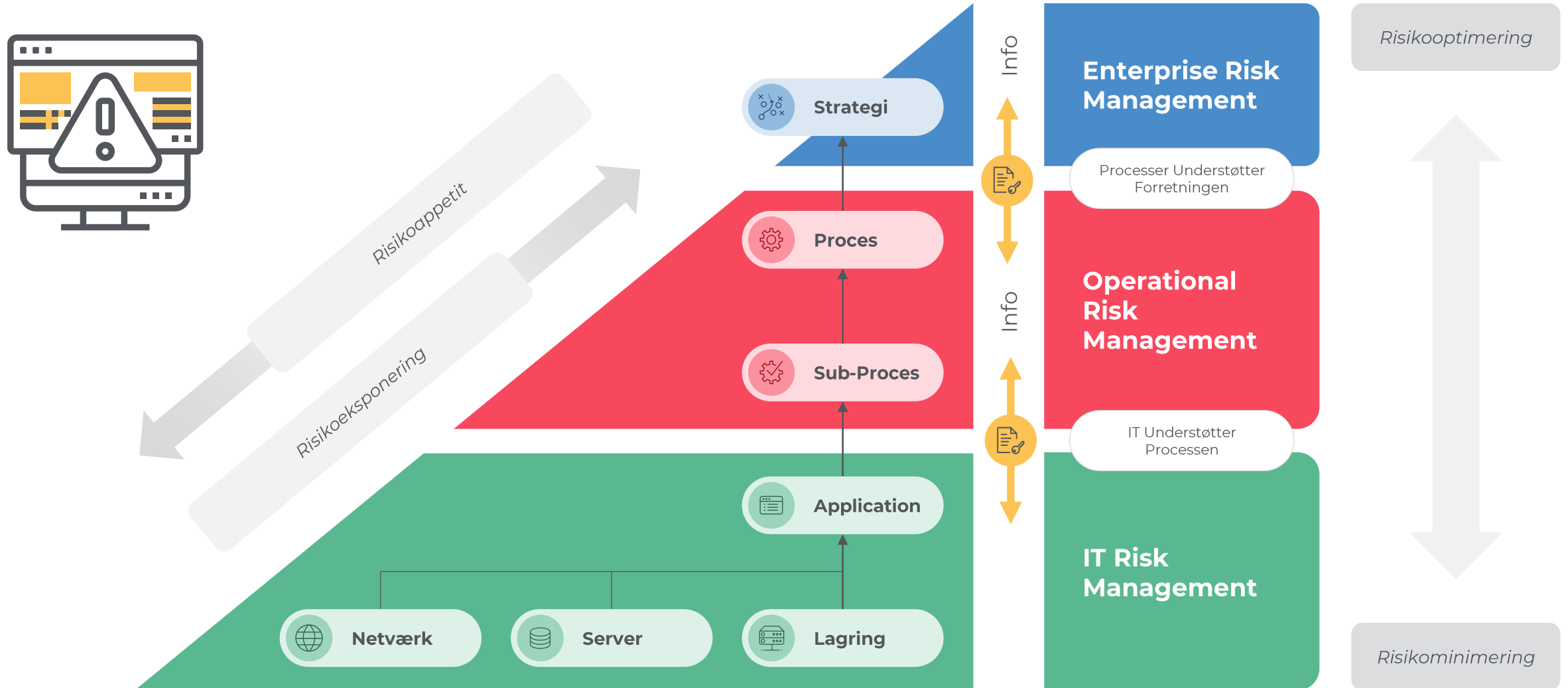
*Fragmenterede
processer og opgaver*



*Strømlinede og
integrerede processer*



Integrated Risk Management



Policy & Compliance i praksis

Input til
Proces

Generelle
procestrin

Output fra
Proces

Stadier
Servicenow

Sikkerhedspolitik

Policy

NIS-direktiv

Authority Documents

Vi opsætter mål for efterlevelse

- Hvordan efterlever vi politik og regulering?

Patching af kritisk systemer

Control Objectives

RISK

Patching af kritisk systemer

Control Objectives

System XYZ (NIS-Kritisk)

Entity

Vi etablerer sikkerhedstiltag

- Hvordan efterleveres dette i praksis?

Patching af Serverer for System XYZ (NIS-Kritisk)

Control

Spørgsmål: Er foranstaltningen på plads?

Attestations

Valider at kritiske serverer for System XYZ patches

Control Indicator

Vi udfører og måler effektivitet

- Er der effekt bag vores handlinger

Valider at kritiske serverer for System XYZ patches i Januar

Indicator Task

RISK

Valider at kritiske serverer for System XYZ patches i Januar

Indicator Task

Patching er ikke foretaget

Issues

Vi opdager og håndterer afvigelser

- hvad gør vi ved det?

Der findes ikke en patch, bed om kravundtagelse

Remediation Task

Bed om undtagelse ift. Sikkerhedspolitik

Policy Exceptions

Vi overvåger

- Har vi et samlet overblik og håndterer vi afvigelser

Reports and Dashboards

Draft

Attest

Review

Monitor

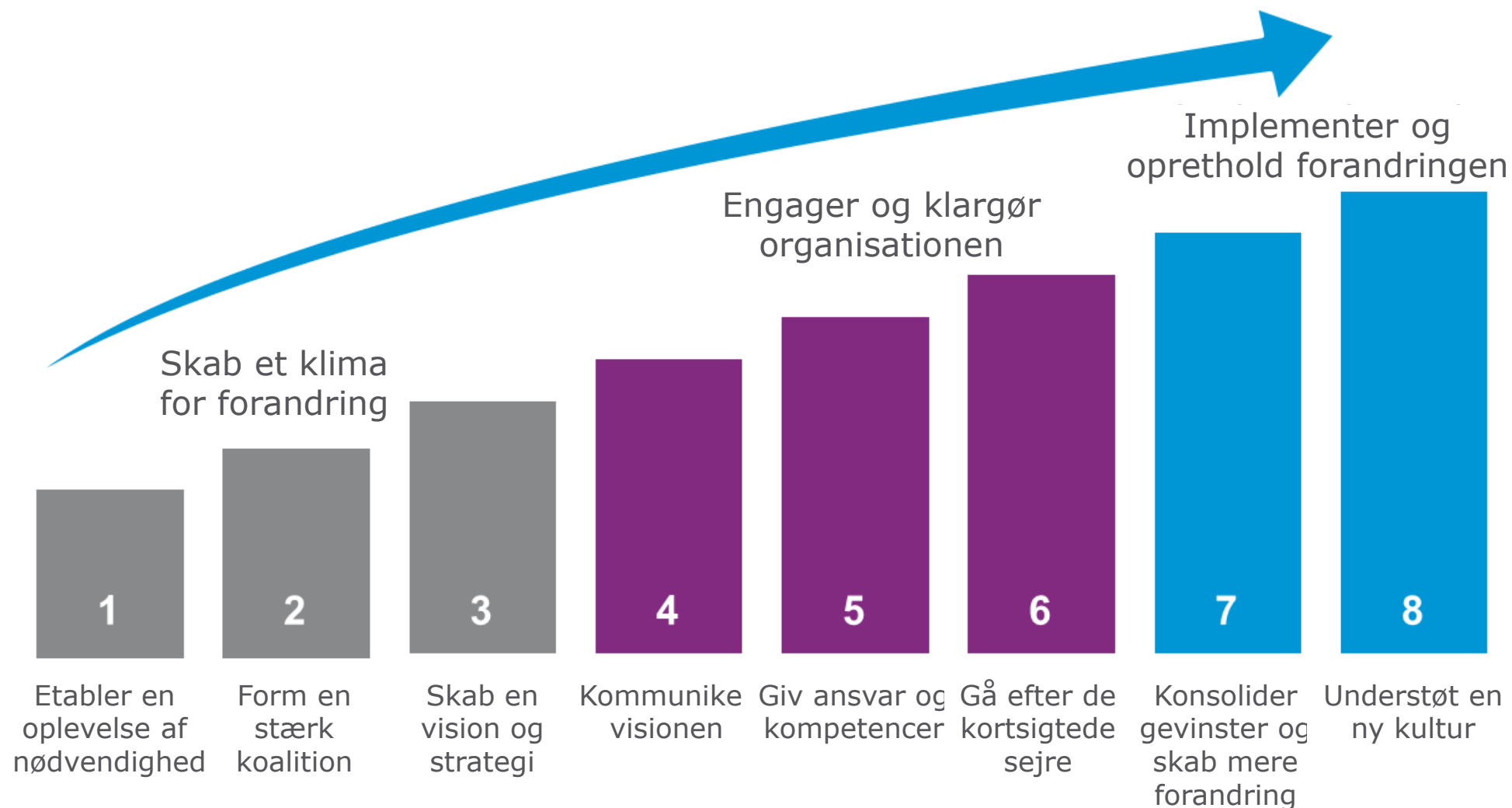


INFORMATION
OM REGLER ER
IKKE
FORANDRING
-
GØR NOGET!



De 8 trin mod forandringen

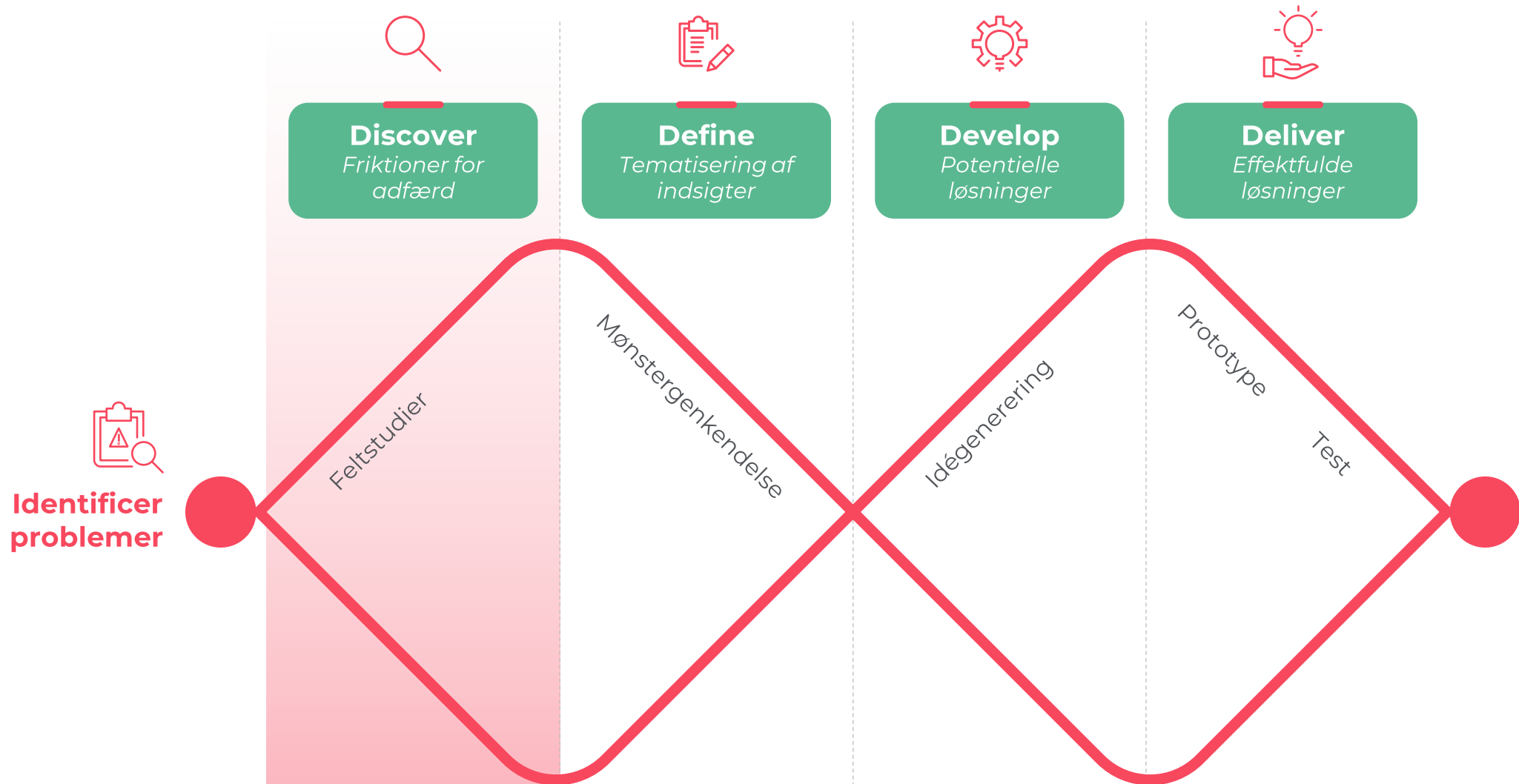
Hvordan du forbereder dig...



**The 8-Step Process for Leading Change – Dr. John Kotter*

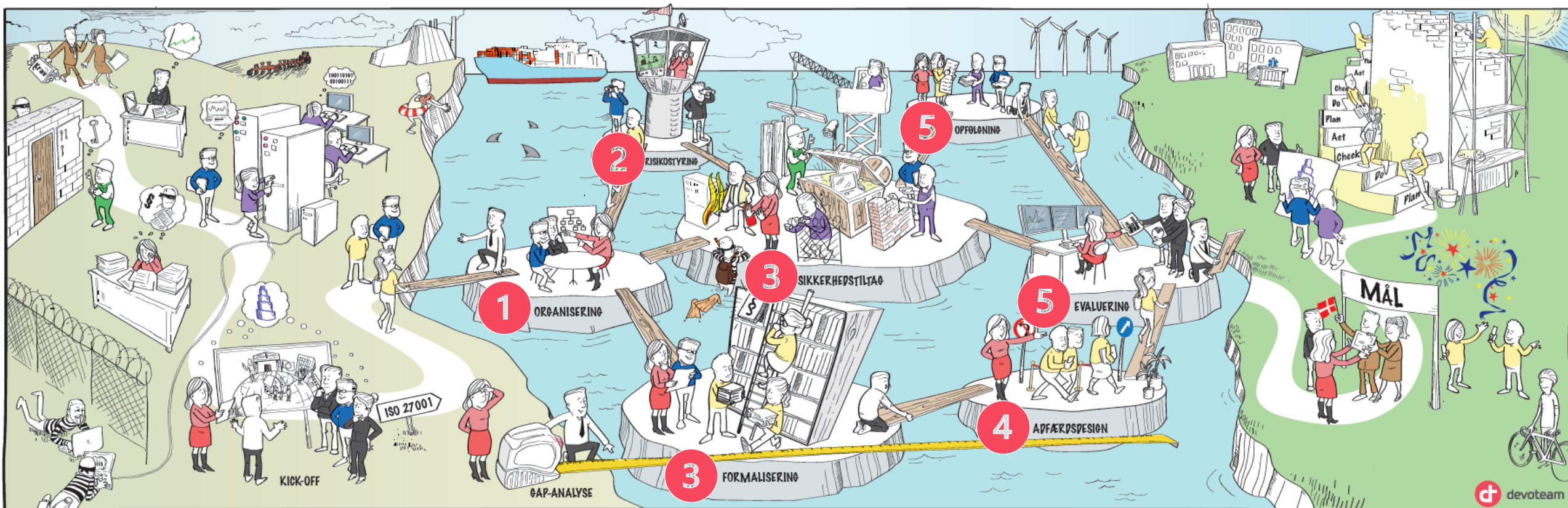


Adfærdsdesign starter med at gå på opdagelse



Start her...

og pas på ambitionsniveauet



Konklusioner



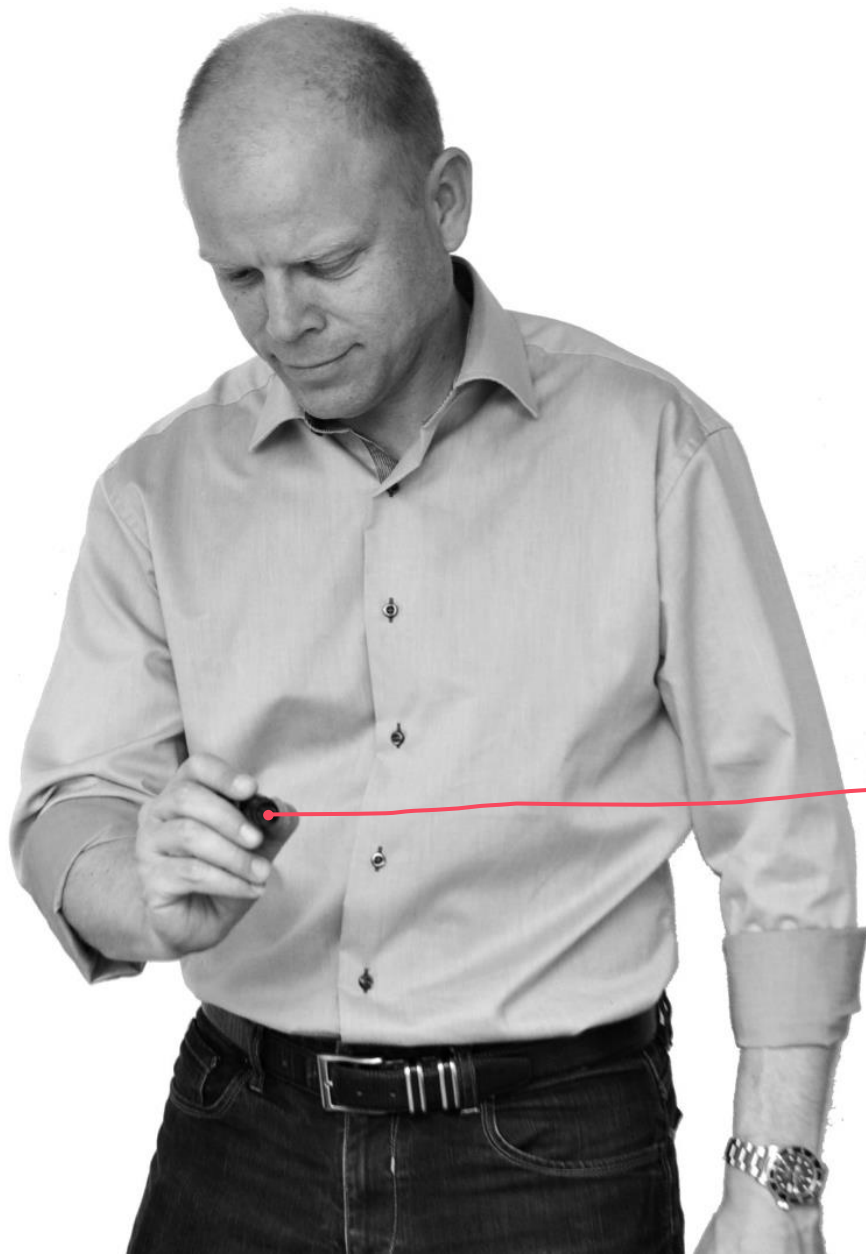
Tre hovedbudskaber

- **Vær realistisk.**
 - Sæt ikke niveauet højere end du kan gennemføre aktiviteterne.
- **Vær autentisk.**
 - Håndhæv og gennemfør beslutningerne.
- **Vær konsekvent.**
 - Hold fast i fremdriften.



Spørgsmål

- Er jeres sikkerhedspolitik et billede af virkeligheden?
- Løfter jeres organisation opgaverne i samarbejde?



Spørgsmål...

Frederik Helweg-Larsen

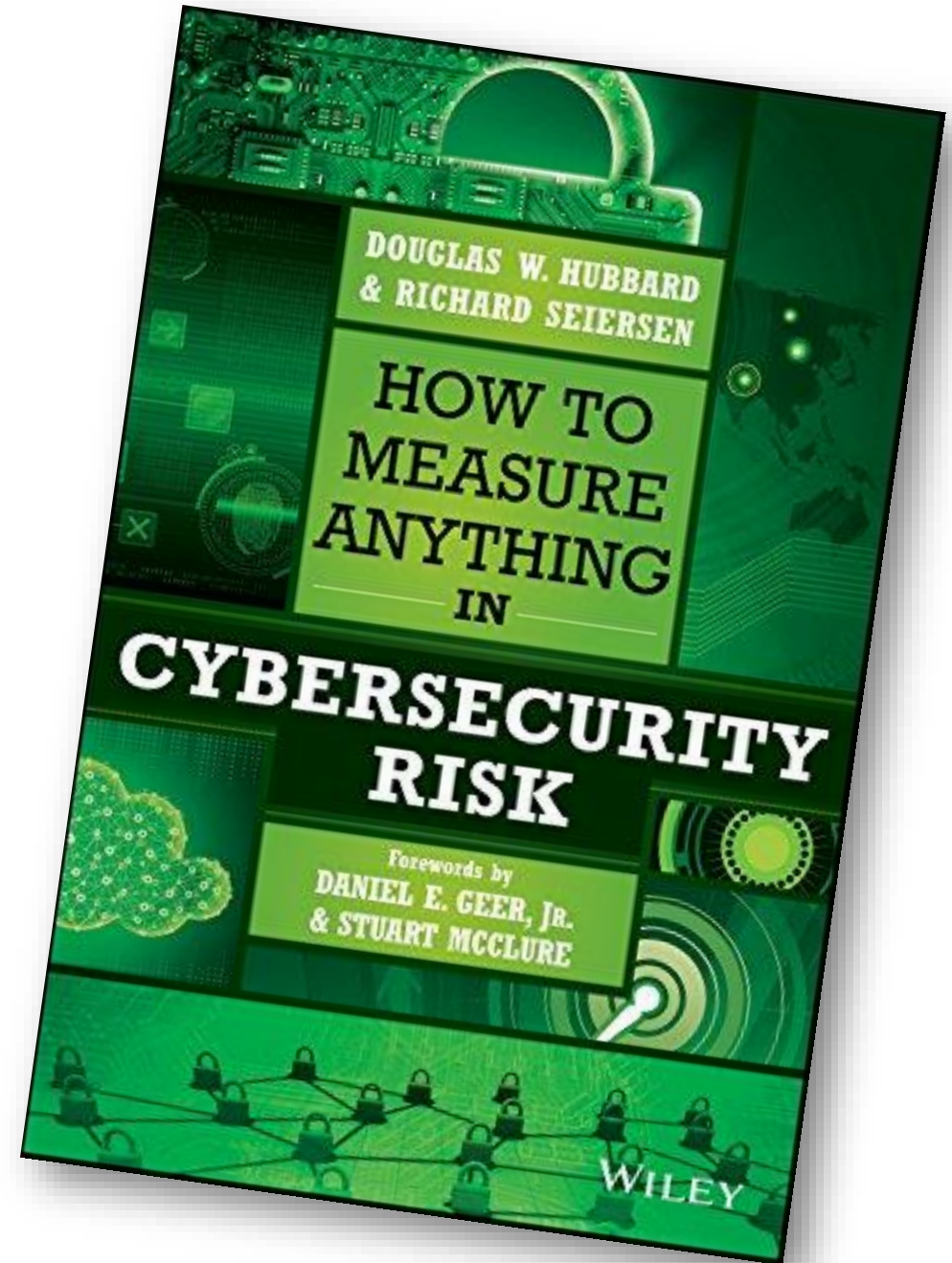
Expert Director, Risk & Security

fhl@devoteam.com

T: +45 4057 6828







Boganbefaling

