Anders Linde

Introduktion til den internationale standard ISO/IEC 27005

En systematiseret tilgang til risikostyring og informationssikkerhed

14. November 2022

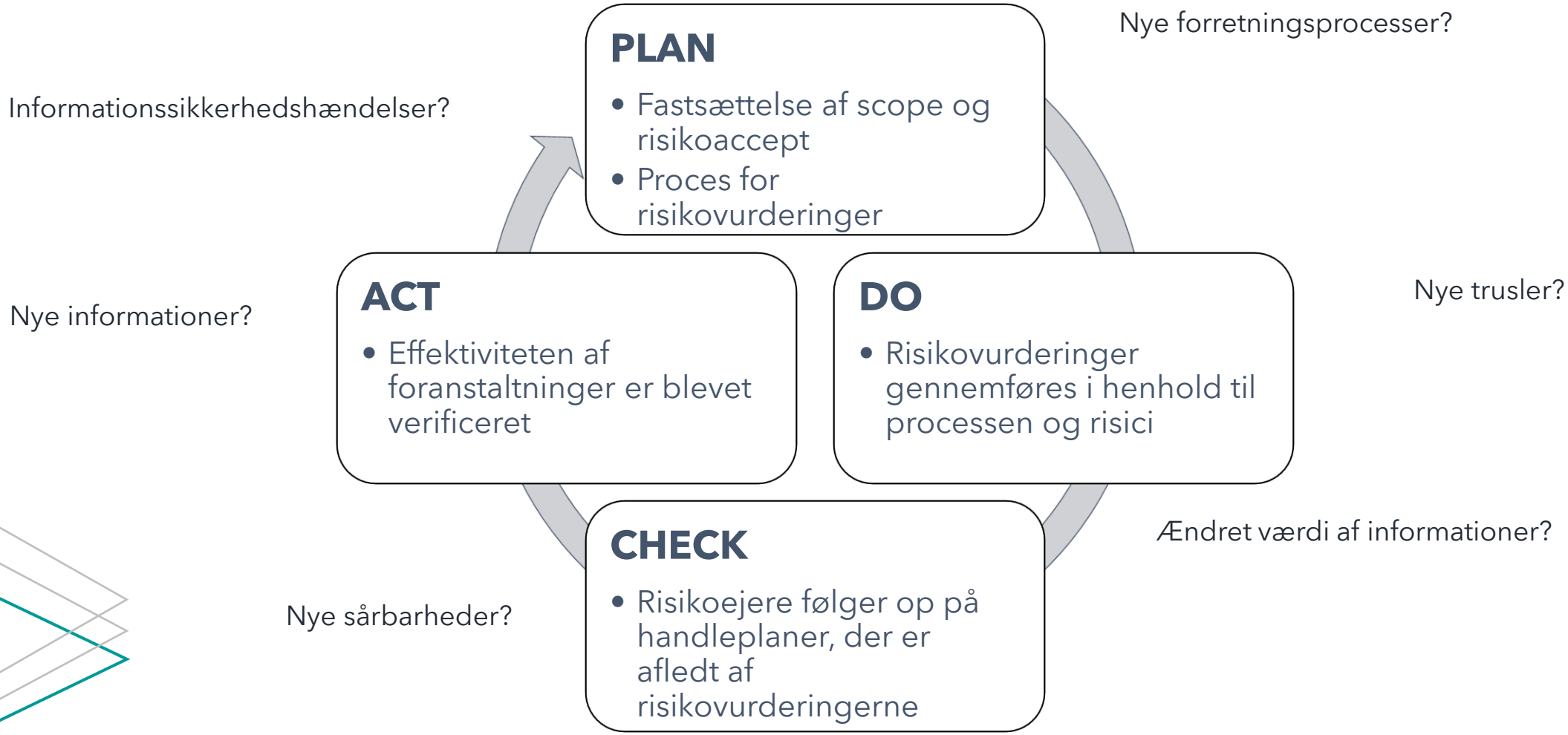
Risikostyring

ISO/IEC 27005's formål

I en kontekst af informationssikkerhed:

- Vurdering af risici
- Håndtering af risici
- Overvågning af risici
- Kommunikation af risici

Det løbende forbedringshjul

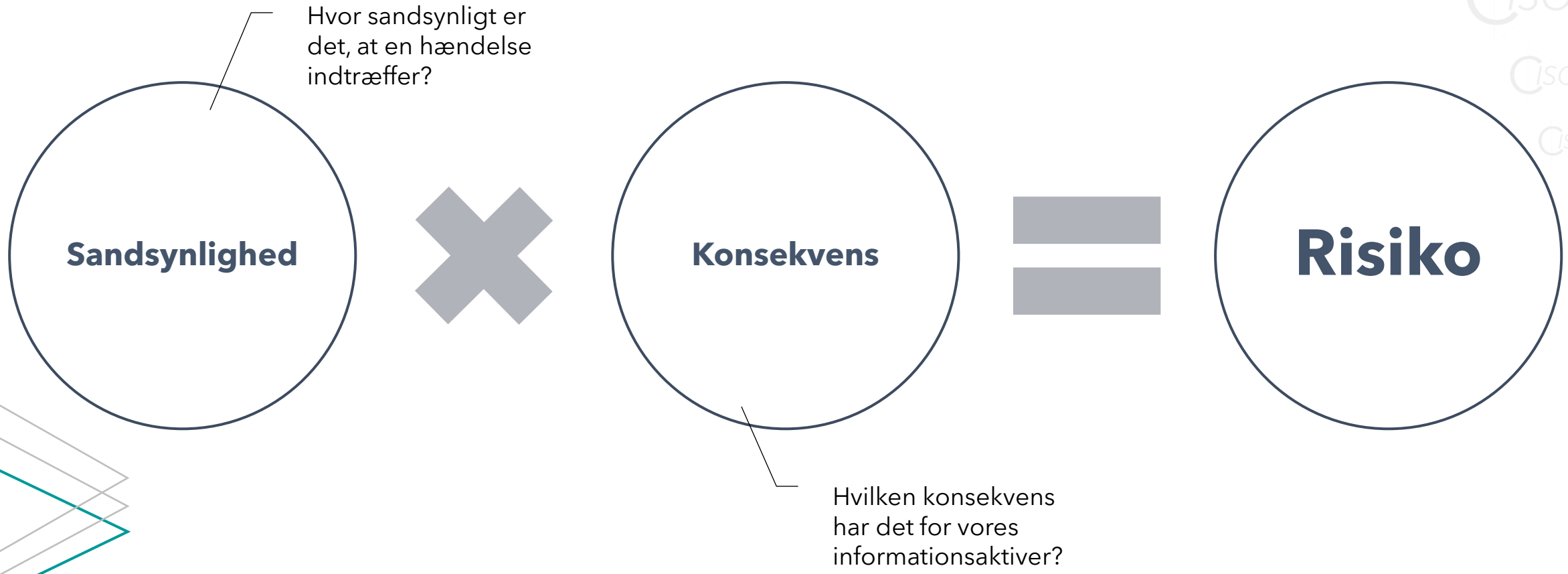


ISO/IEC 27001: metode

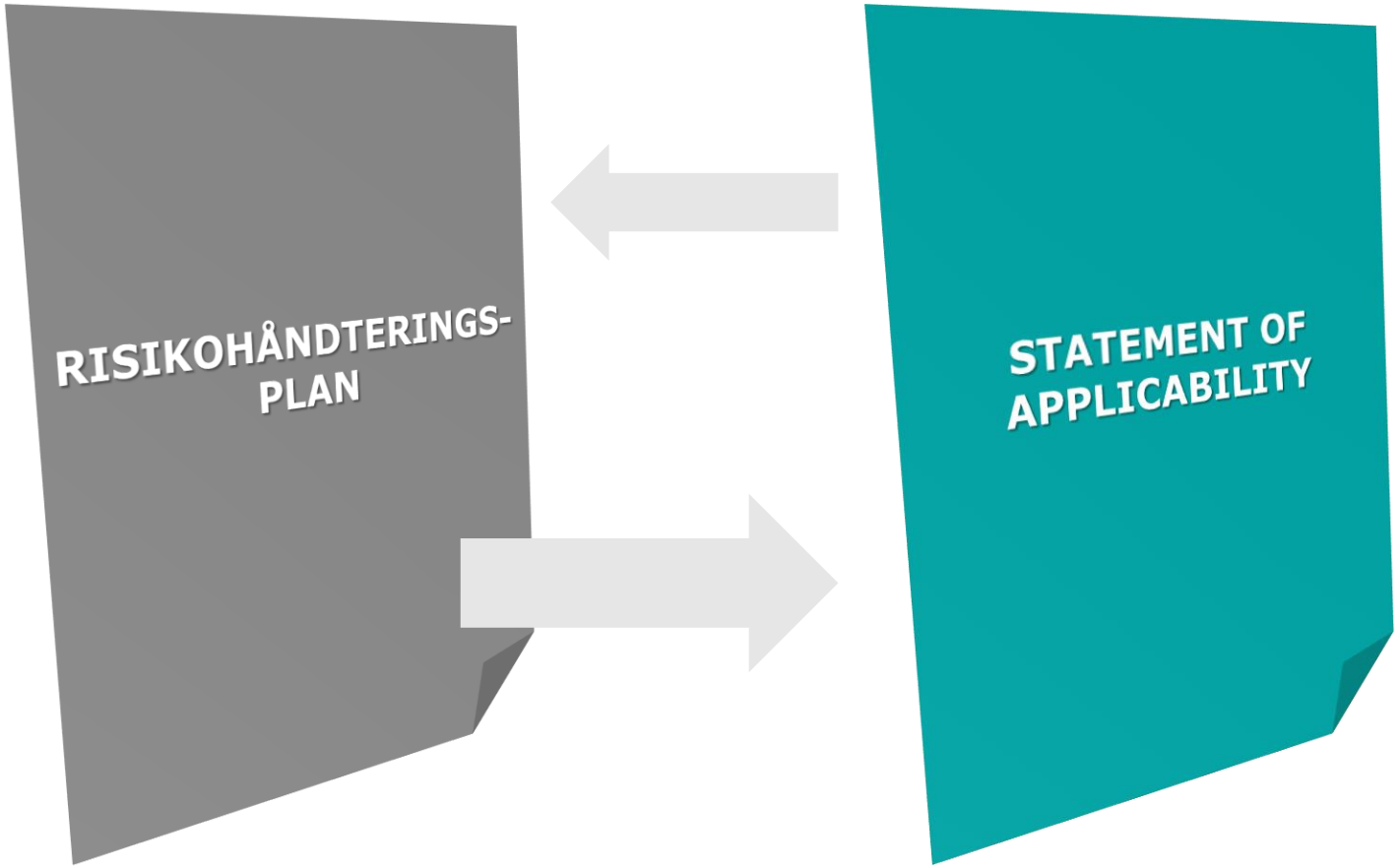
Fremgangsmåde:

- Metodevalg og beskrivelse, der muliggør sammenlignelige og reproducerbare resultater
- Kriterier for identifikation, analyse og evaluering
- Kriterier for accept af risici overensstemmelse med politikker, målsætninger og interessenter
- Risikovurdering med sandsynligheder og konsekvenser
- Organisatorisk setup, herunder udpegning af risikoejere

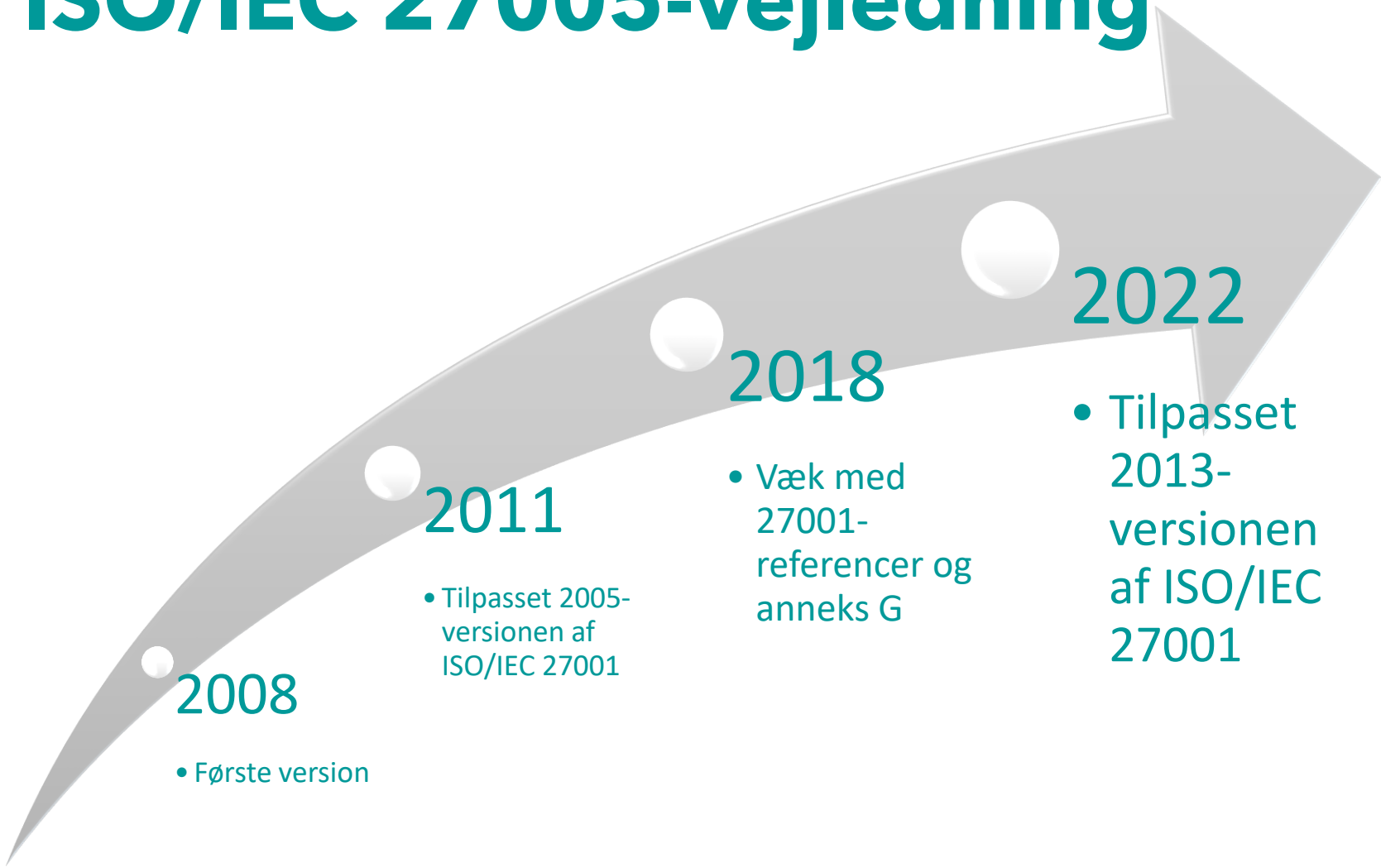
ISO/IEC 27001: risikovurdering



ISO/IEC 27001: risikohåndtering



En ny ISO/IEC 27005-vejledning



2008

- Første version

2011

- Tilpasset 2005-versionen af ISO/IEC 27001

2018

- Væk med 27001-referencer og anneks G

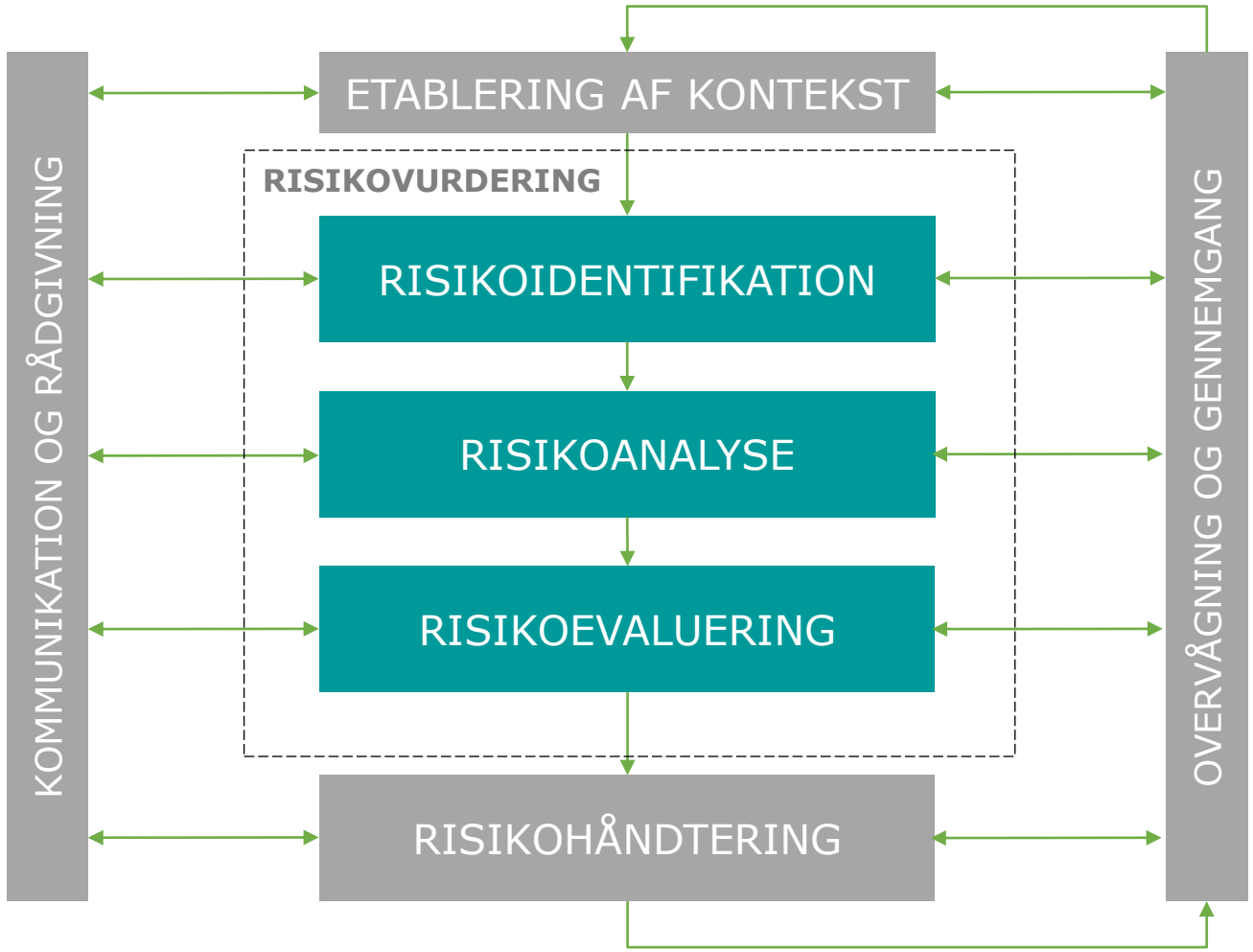
2022

- Tilpasset 2013-versionen af ISO/IEC 27001

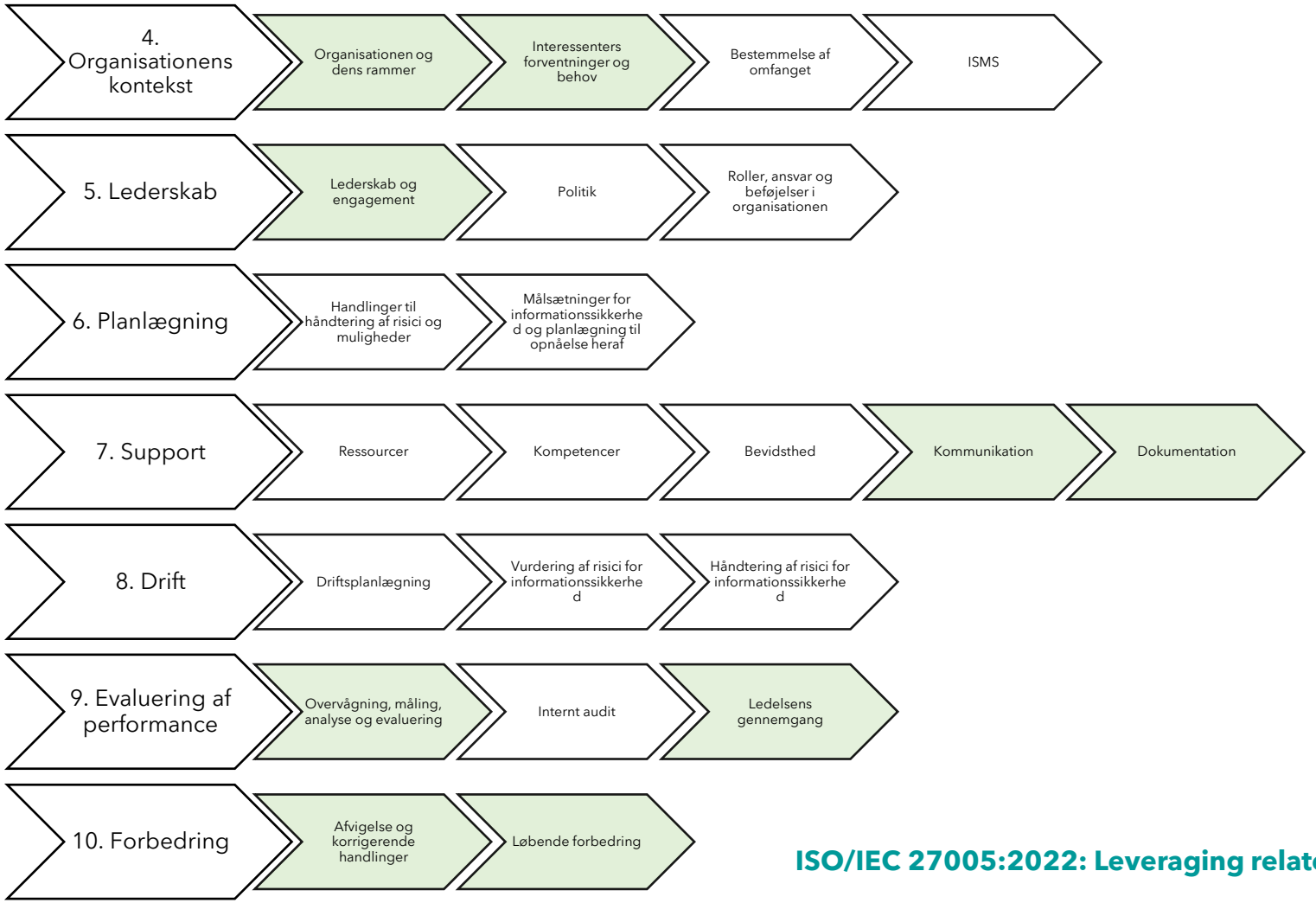
ISO/IEC 27001-tilpasning

"This document provides guidance on implementation of the information security risk requirements specified in ISO/IEC 27001:2022"

ISO/IEC 27005:2022, introduction

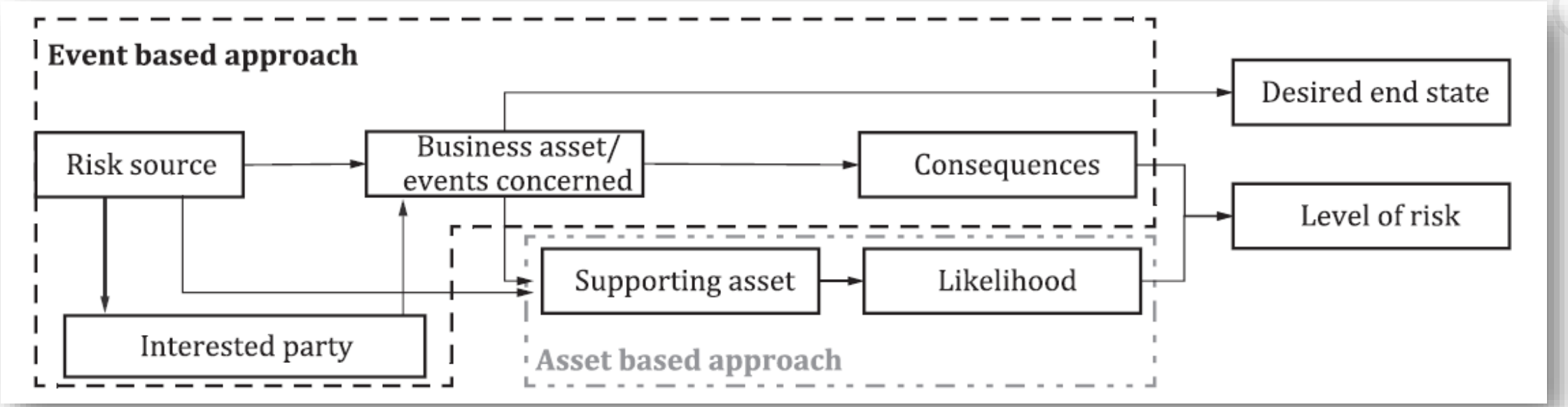


Risikostyring i et ISMS



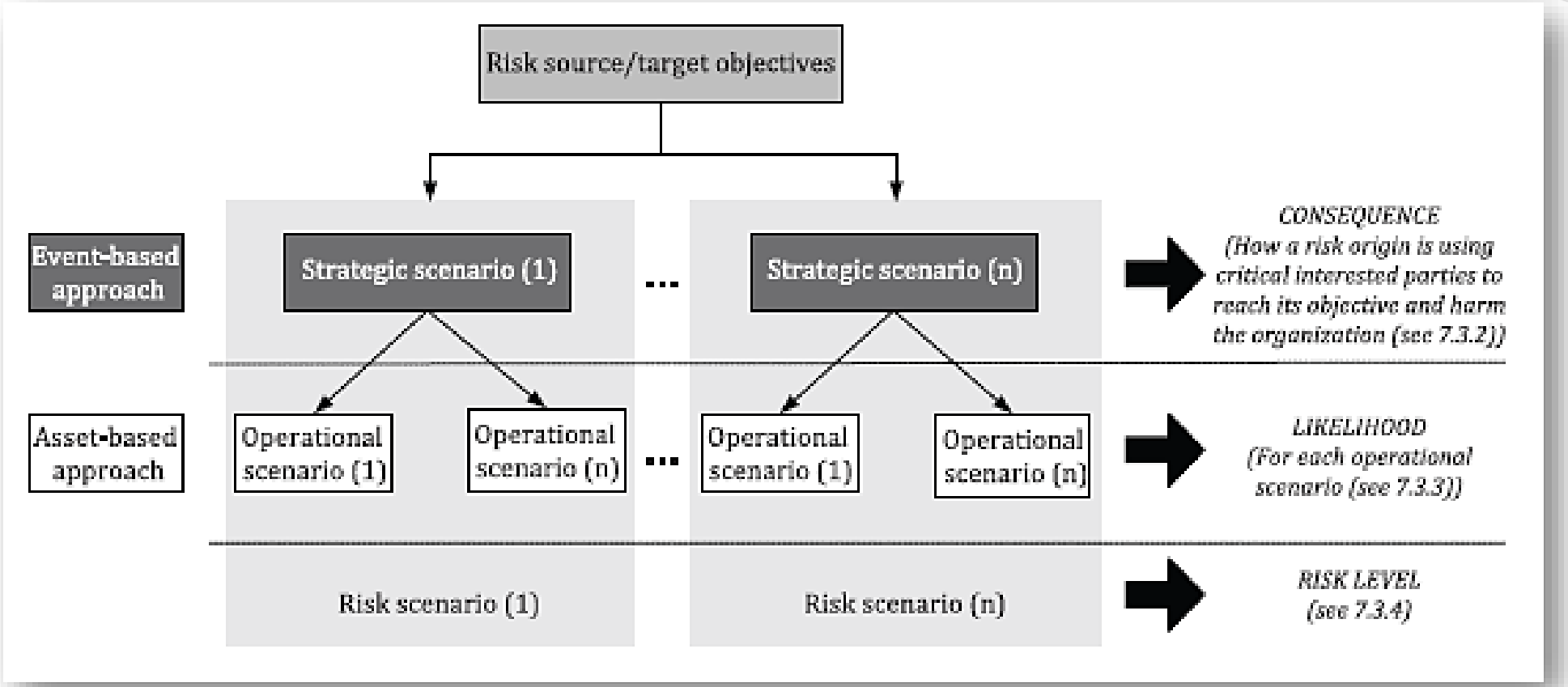
ISO/IEC 27005:2022: Leveraging related ISMS processes (clause 10)

Aktiv- vs. hændelsesbaseret tilgang



Samspil mellem en hændelses- og aktivbaseret tilgang, jf. ISO/IEC 27005:2022, figure A.1

Strategi vs. drift



Risikoscenarier ud fra en hændelses- eller aktivbaseret tilgang, jf. ISO/IEC 27005:2022, figure A.4

Samling af annekser

ISO/IEC 27005:2018

- Annex A (informative) Defining the scope and boundaries of the information security risk management process
- Annex B (informative) Identification and valuation of assets and impact assessment
- Annex C (informative) Examples of typical threats
- Annex D (informative) Vulnerabilities and methods for vulnerability assessment
- Annex E (informative) Information security risk assessment approaches
- Annex F (informative) Constraints for risk modification

ISO/IEC 27005: 2022

- Annex A (informative) Techniques in support of the risk assessment process:
  - **A.1 Information security risk criteria**
    - A.1.1 Criteria related to risk assessment
    - A.1.2 Risk acceptance criteria
  - **A.2 Practical techniques**
    - A.2.1 Information security risk components
    - A.2.2 Assets
    - A.2.3 Risk sources and desired end state
    - A.2.4 Event-based approach
    - A.2.5 Asset-based approach
    - A.2.6 Examples of scenarios applicable in both approaches
    - A.2.7 Monitoring risk-related events

Beregningsmodeller

Likelihood	Description
5 – Quasi-certain	The risk source will most certainly reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very high.
4 – Very likely	The risk source will probably reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is high.
3 – Likely	The risk source is able to reach its objective by using one of the considered methods of attack. The likelihood of the risk scenario is moderate.
2 – Rather unlikely	The risk source has relatively little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching its objective by using one of the considered methods of attack. The likelihood of the risk scenario is very low.

ISO/IEC 27005:2022, table A.2

Kvalitativt

Kvantitativt

Approx	Log expression	Scale value
Every hour	(approx. 10^5)	5
Every 8 hours	(approx. 10^4)	4
Twice a week	(approx. 10^3)	3
Once a month	(approx. 10^3)	2
Once a year	(10^1)	1
Once a decade	(10^0)	0

ISO/IEC 27005:2022, table A.4

Opsummering

- Mere anvendelig i forhold til ISO/IEC 27001's krav
- Vigtig sondring mellem en aktiv- og hændelsesbaseret tilgang
- Mere konkret vejledning i risikostyringsteknikker via flere eksempler

Ønsker for fremtiden

Organisatorisk

Adfærdsmæssig

Fysisk

Teknisk

ISO/IEC 27002

Category	No.	Threat description
Human actions	TH03	Interception of radiation of a device
	TH04	Remote spying
	TH05	Eavesdropping
	TH06	Theft of media or documents
	TH07	Theft of equipment
	TH08	Theft of digital identity or credentials
	TH09	Retrieval of recycled or discarded media
	TH10	Disclosure of information
	TH11	Data input from untrustworthy sources
	TH12	Tampering with hardware
	TH13	Tampering with software
	TH14	Drive-by-exploits using web-based communication
	TH15	Replay attack, man-in-the-middle attack
	TH16	Unauthorized processing of personal data
	TH17	Unauthorized entry to facilities
	TH18	Unauthorized use of devices
	TH19	Incorrect use of devices
	TH20	Damaging devices or media
	TH21	Fraudulent copying of software
	TH22	Use of counterfeit or copied software

ISO/IEC 27005

Anders Linde

Tak!

anders@ciso27.dk
Tlf. 6162 1500