DS
DANSK STANDARD

Risikostyring og informationssikkerhed – ISO/IEC 27005

8. september 2022

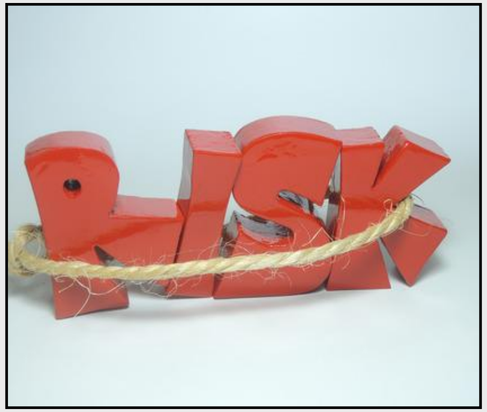
- Der er mulighed for at stille spørgsmål undervejs gennem chatten.
- Præsentationerne sendes ud efterfølgende
- Vi optager webinaret

Anders Linde

ISO/IEC 27005

Indblik i den nye vejledning i risikostyring for informationssikkerhed

Agenda



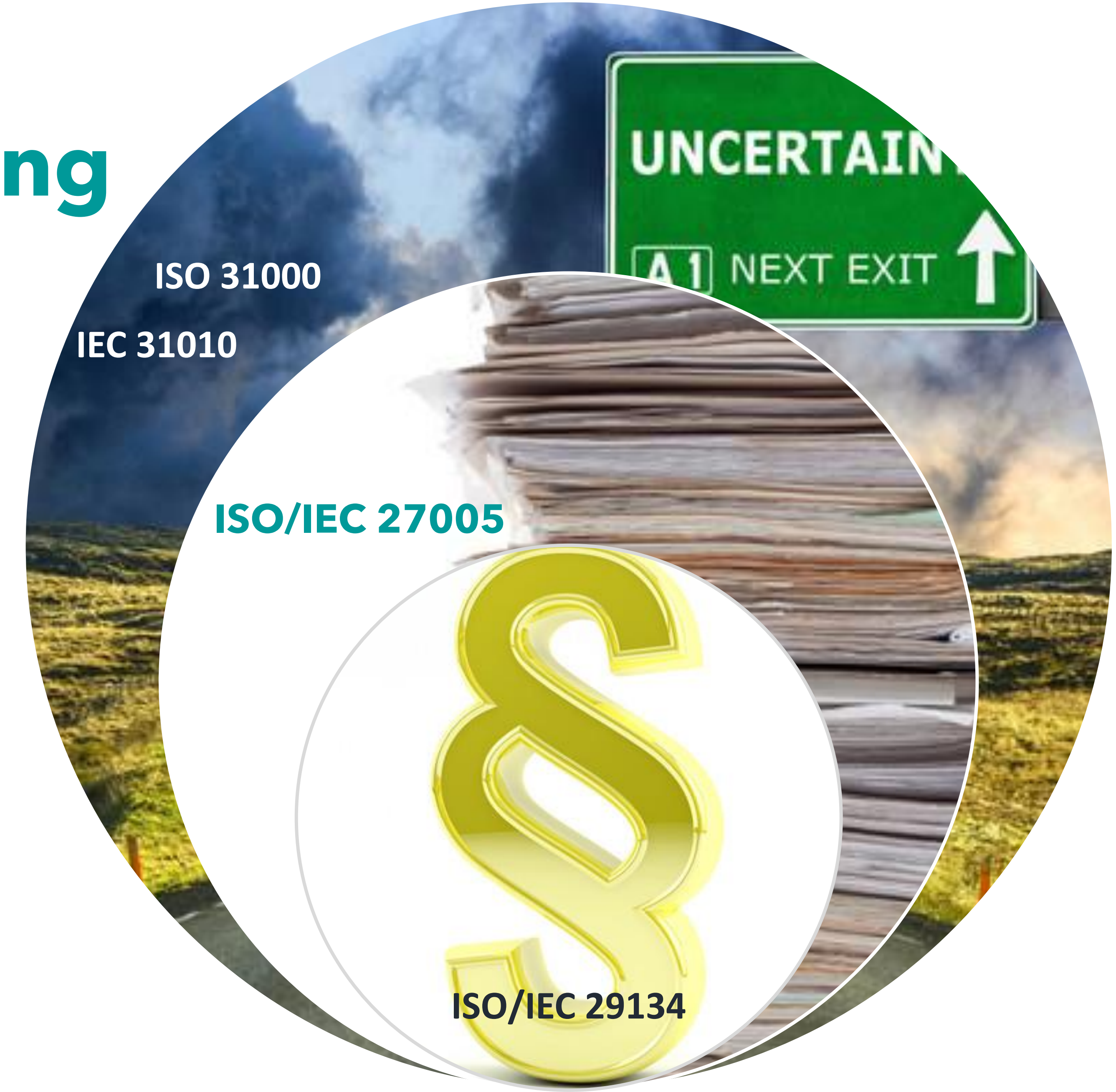
Introduktion

En ny ISO/IEC 27005

Inspiration

CISO27
Undervisning & rådgivning i
standarder for cybersikkerhed

Risikostyring



ISO 31000

IEC 31010

ISO/IEC 27005

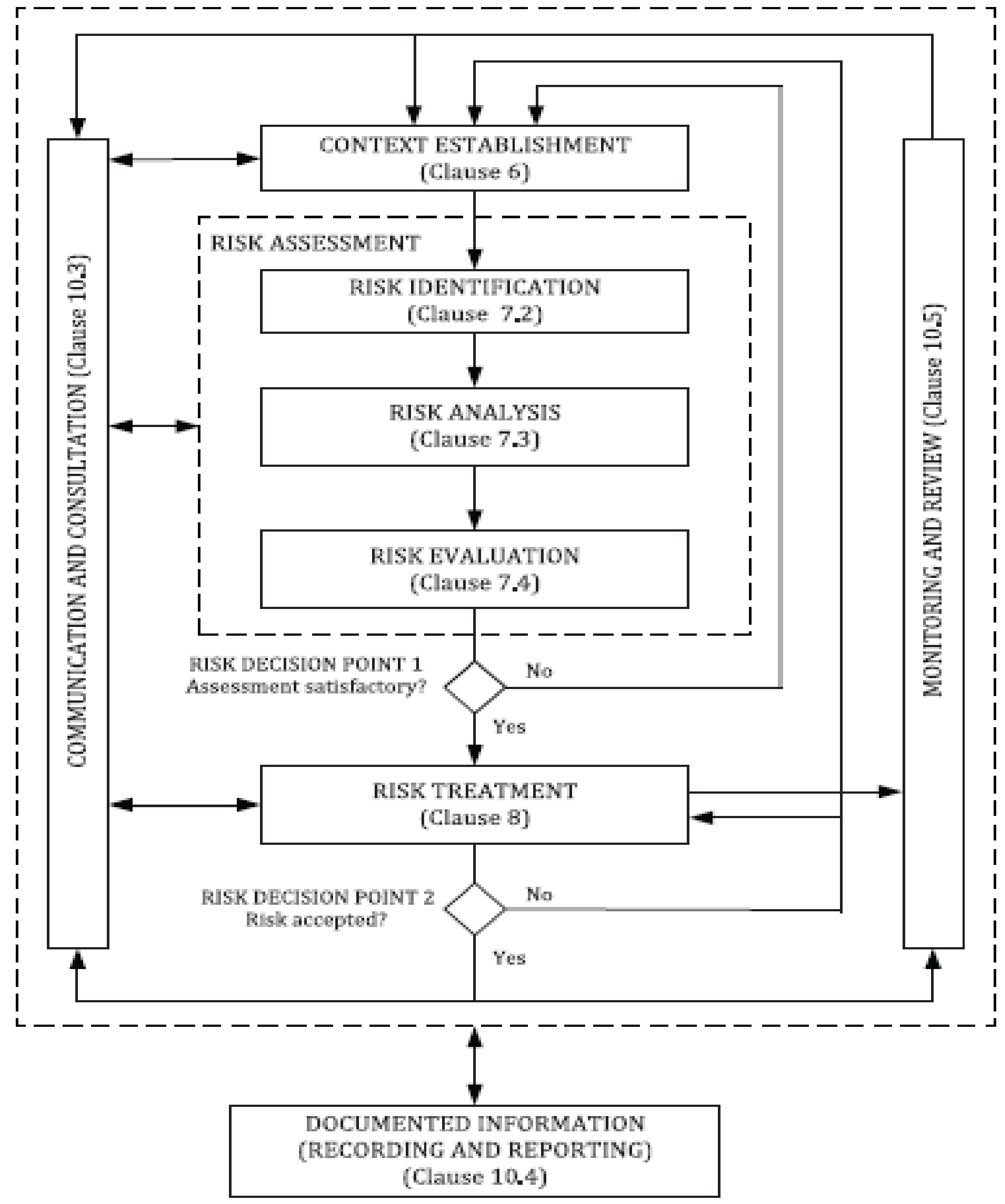
ISO/IEC 29134

ISO/IEC 27005's formål

I en kontekst af informationssikkerhed:

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

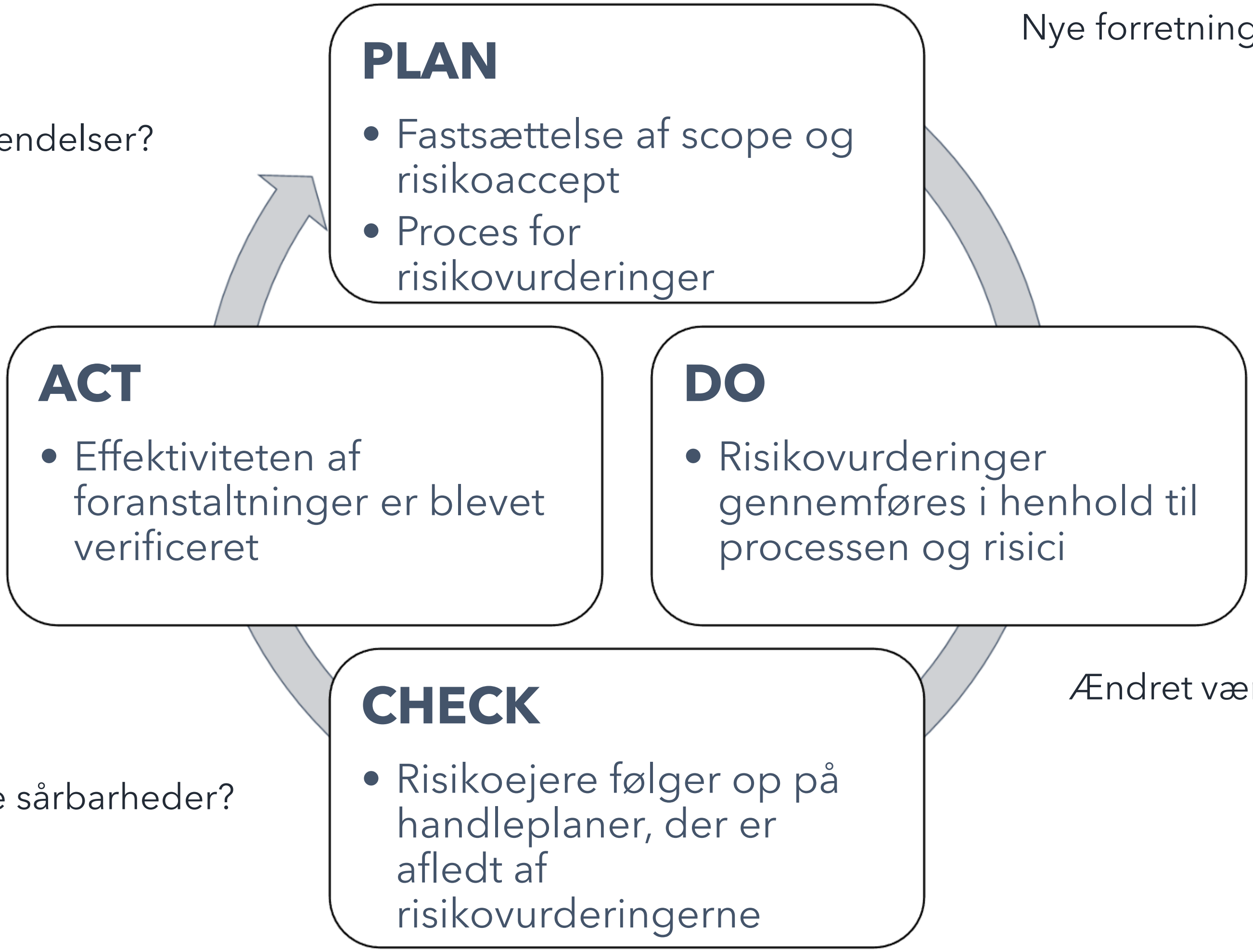
ISO 31000 som baggrund



Figur 1, jf. ISO/IEC FDIS 27005:2022, afsnit 5

CISO27
Undervisning & rådgivning i standarder for cybersikkerhed

Det løbende forbedringshjul



PLAN

- Fastsættelse af scope og risikoaccept
- Proces for risikovurderinger

DO

- Risikovurderinger gennemføres i henhold til processen og risici

CHECK

- Risikoejere følger op på handleplaner, der er afledt af risikovurderingerne

ACT

- Effektiviteten af foranstaltninger er blevet verificeret

Nye forretningsprocesser?

Informationssikkerhedshændelser?

Nye trusler?

Nye informationer?

Ændret værdi af informationer?

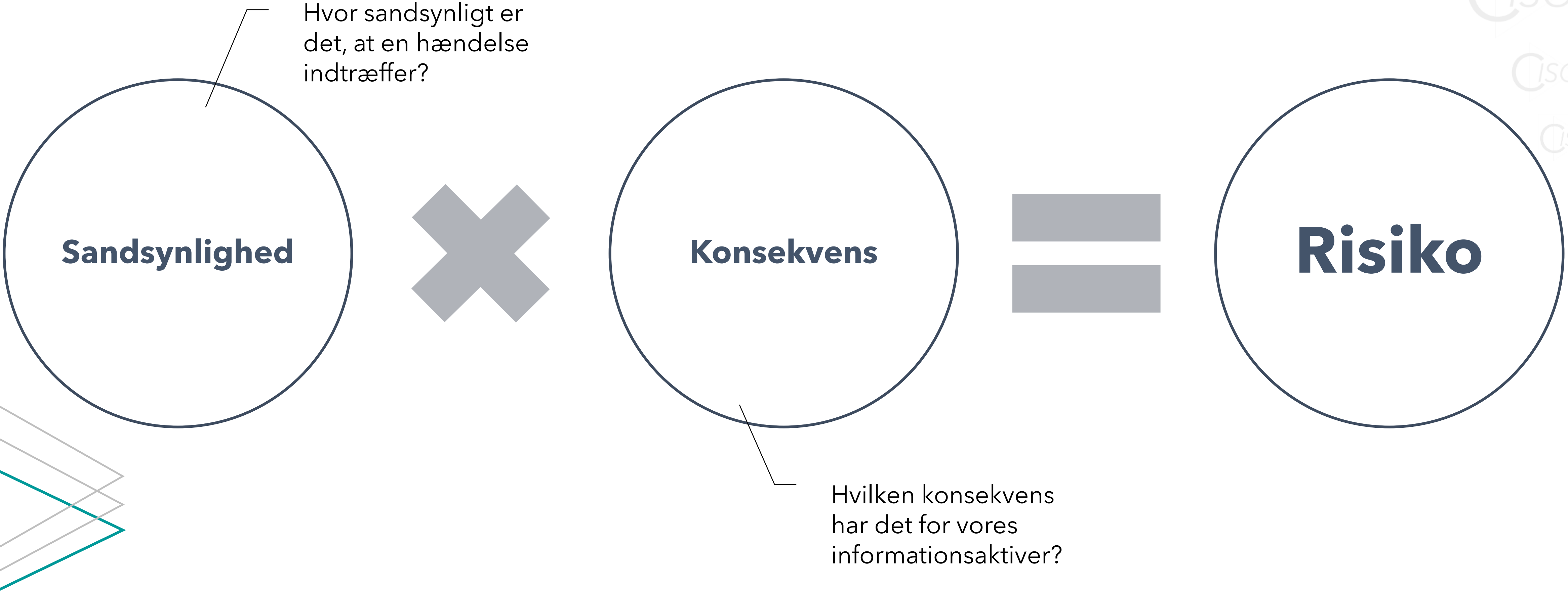
Nye sårbarheder?

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

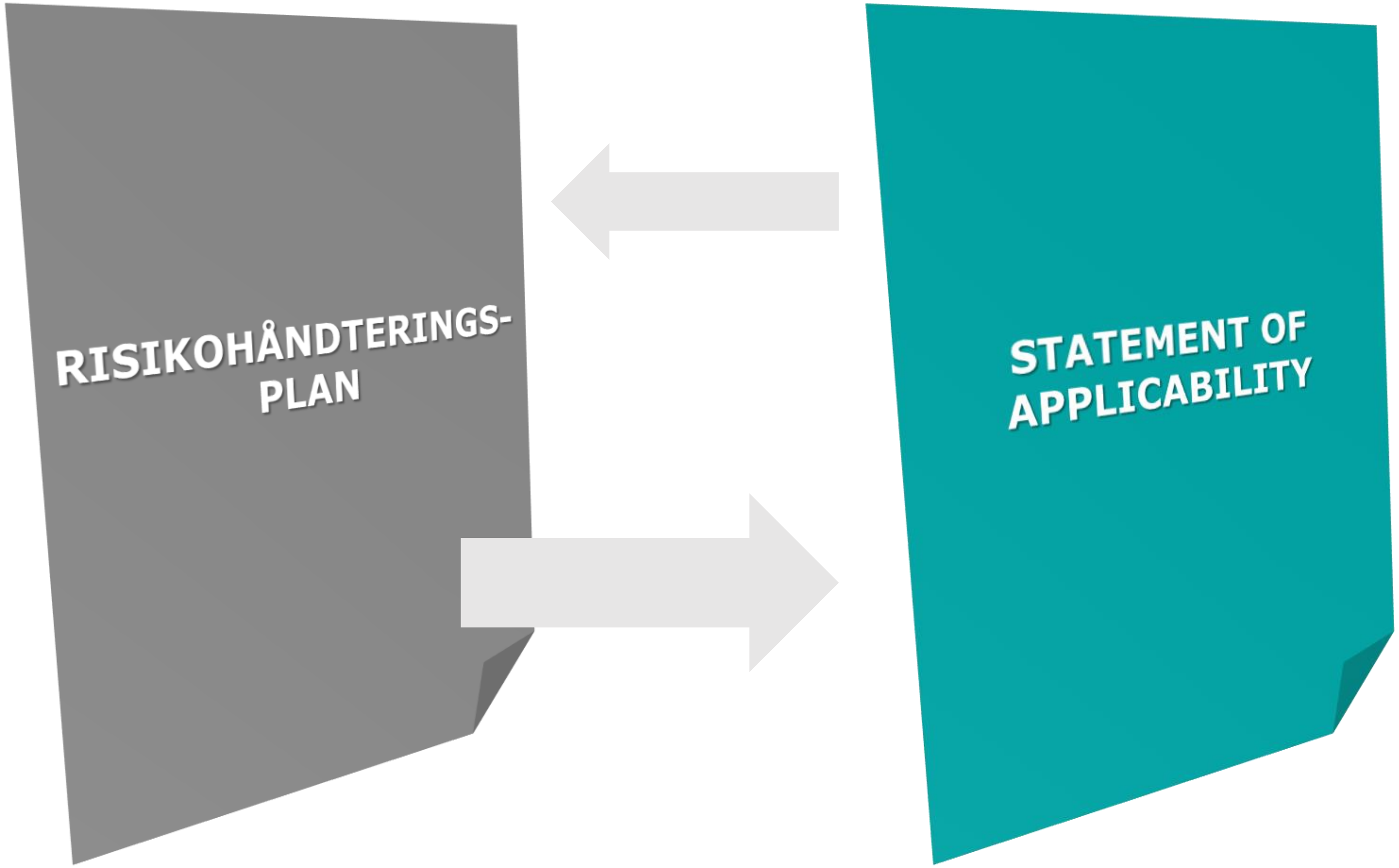


Hvor sandsynligt er det, at en hændelse indtræffer?

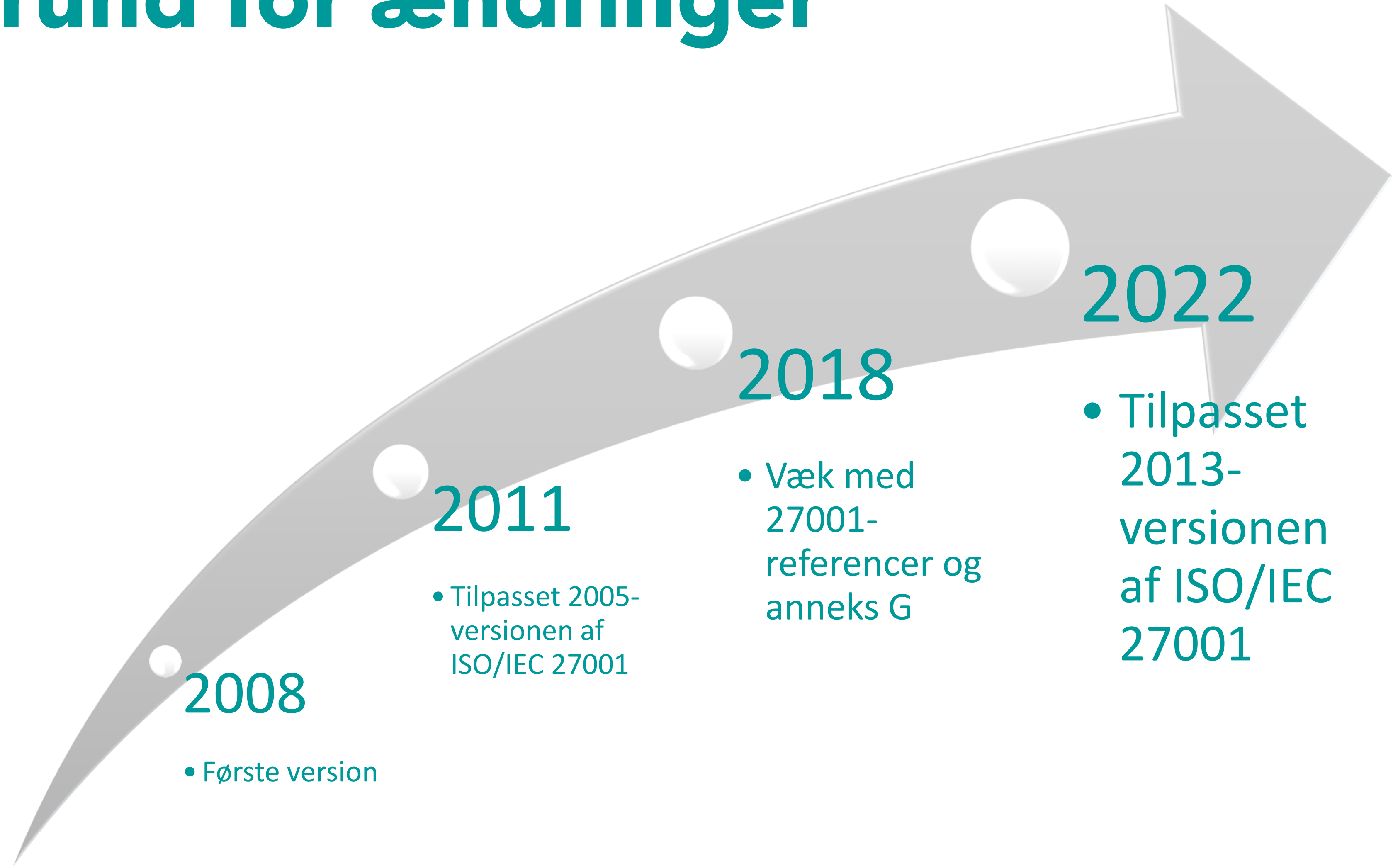
Sandsynlighed × **Konsekvens** = **Risiko**

Hvilken konsekvens har det for vores informationsaktiver?

ISO/IEC 27001: risikohåndtering



Baggrund for ændringer



2008

- Første version

2011

- Tilpasset 2005-versionen af ISO/IEC 27001

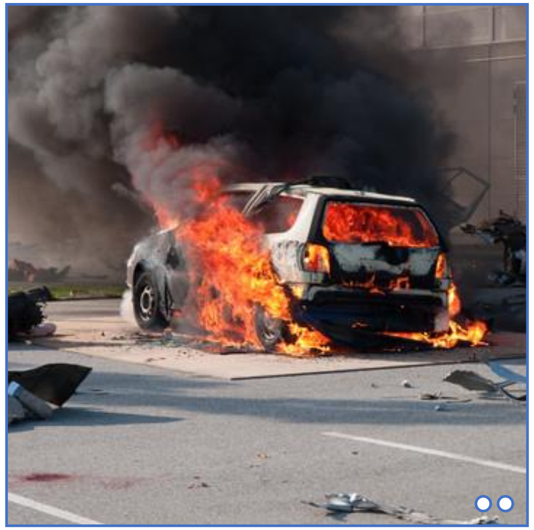
2018

- Væk med 27001-referencer og anneks G

2022

- Tilpasset 2013-versionen af ISO/IEC 27001

De største ændringer



Triggers

Input

Identificerer alle nødvendige oplysninger for at udføre aktiviteten

Action

Beskriver aktiviteten

Trigger

Giver vejledning om, hvornår aktiviteten skal startes, for eksempel på grund af en ændring i organisationen eller i henhold til en plan.

Output

Identificerer alle oplysninger, der følger udførelsen af aktiviteten, samt eventuelle kriterier, som et sådant output skal opfylde

Guidance

Giver vejledning i udførelse af aktiviteten, nøgleord og nøglekonceptet

Termer

ISO/IEC 27005, 3.1.3, note 1

An effect is a deviation from the expected, positive or negative

ISO/IEC 27005, 3.1.3, note 6

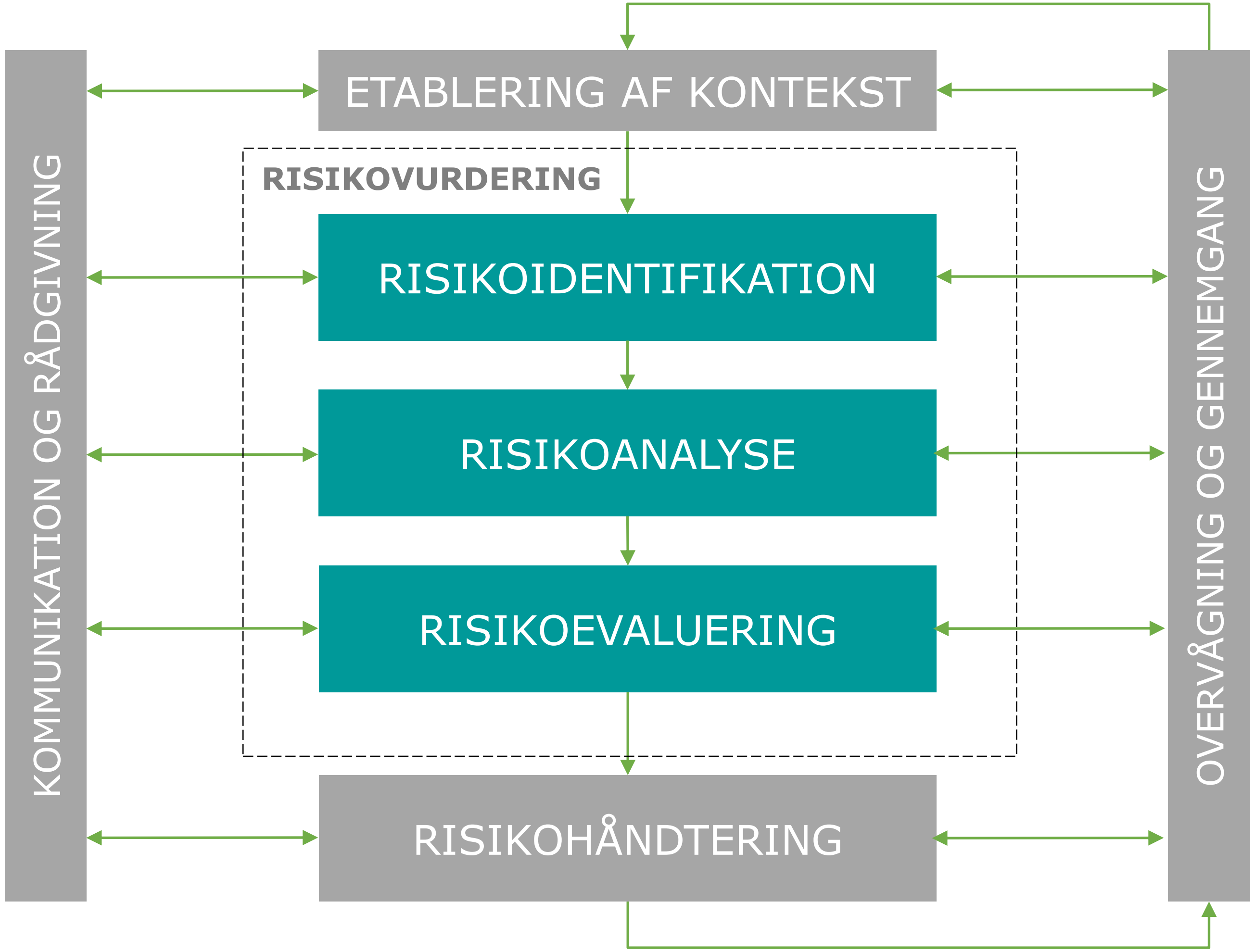
Information security risks are usually associated with a negative effect of uncertainty on information security objectives

ISO/IEC FDIS 27005:2022, afsnit 3

ISO/IEC 27001-tilpasning

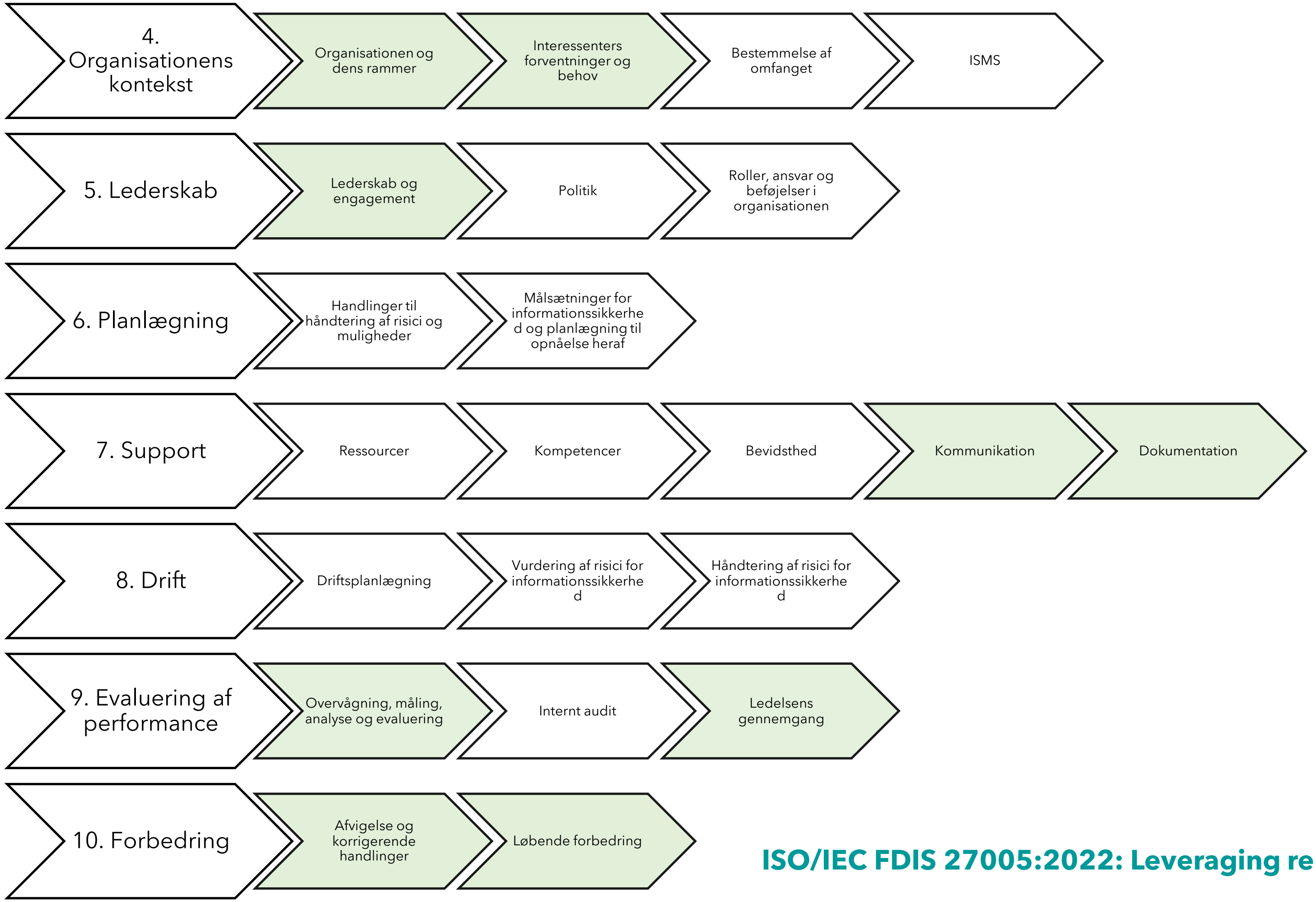
"This document provides guidance on implementation of the information security risk requirements specified in ISO/IEC 27001:2013"

ISO/IEC FDIS 27005:2022, introduction



Undervisning & rådgivning i standarder for cybersikkerhed

Risikostyring i et ISMS



4. Organisationens kontekst → Organisationen og dens rammer → Interessenters forventninger og behov → Bestemmelse af omfanget → ISMS

5. Lederskab → Lederskab og engagement → Politik → Roller, ansvar og beføjelser i organisationen

6. Planlægning → Handlinger til håndtering af risici og muligheder → Målsætninger for informationssikkerhed og planlægning til opnåelse heraf

7. Support → Ressourcer → Kompetencer → Bevidsthed → Kommunikation → Dokumentation

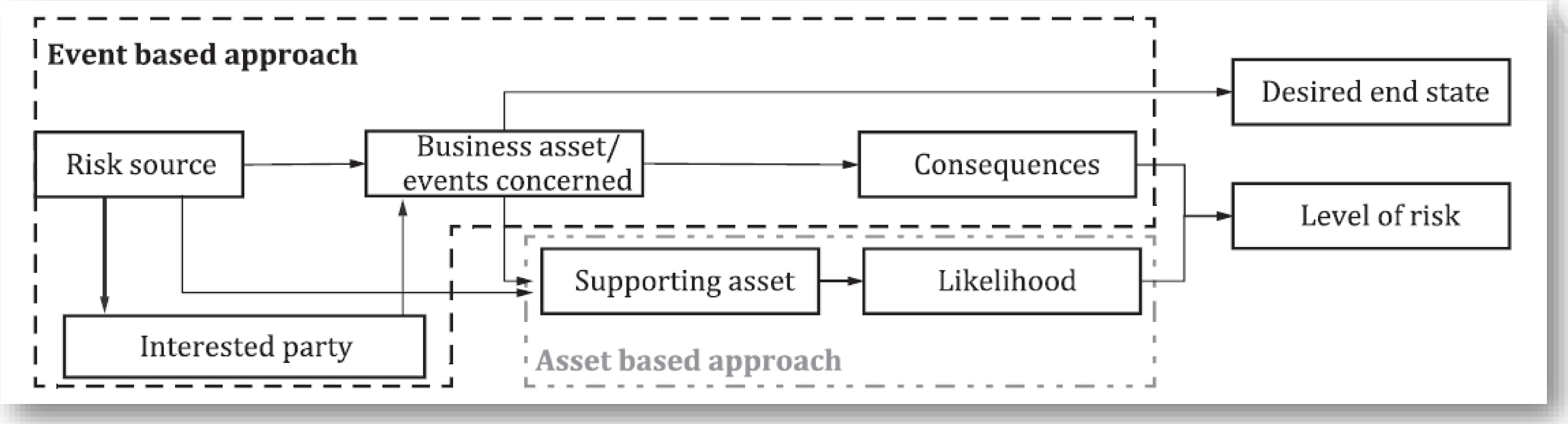
8. Drift → Driftsplanlægning → Vurdering af risici for informationssikkerhed → Håndtering af risici for informationssikkerhed

9. Evaluering af performance → Overvågning, måling, analyse og evaluering → Internt audit → Ledelsens gennemgang

10. Forbedring → Afvigelse og korrigerende handlinger → Løbende forbedring

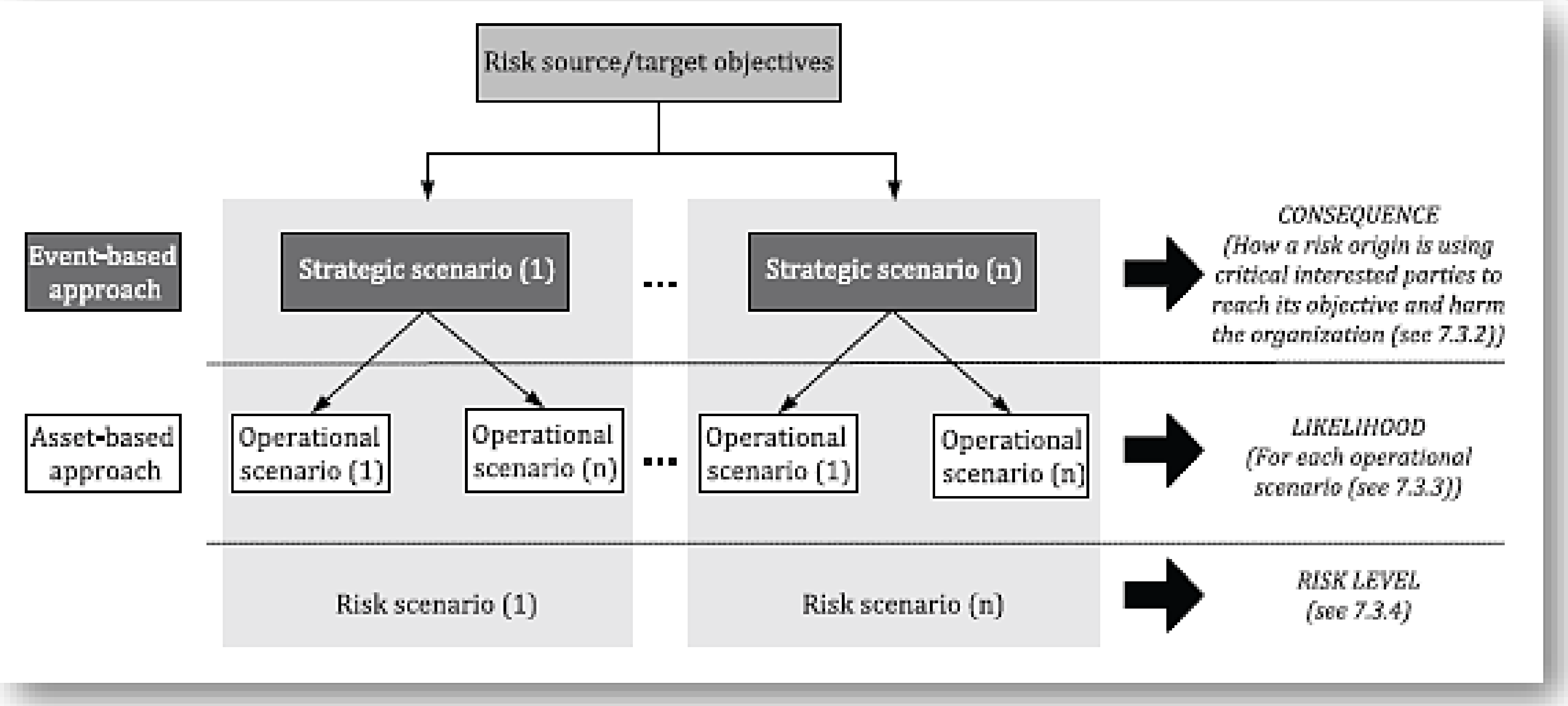
ISO/IEC FDIS 27005:2022: Leveraging related ISMS processes (clause 10)

Aktiv- vs. hændelsesbaseret tilgang



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

Strategi vs. drift



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

Undervisning & rådgivning i standarder for cybersikkerhed

Samling af annekser

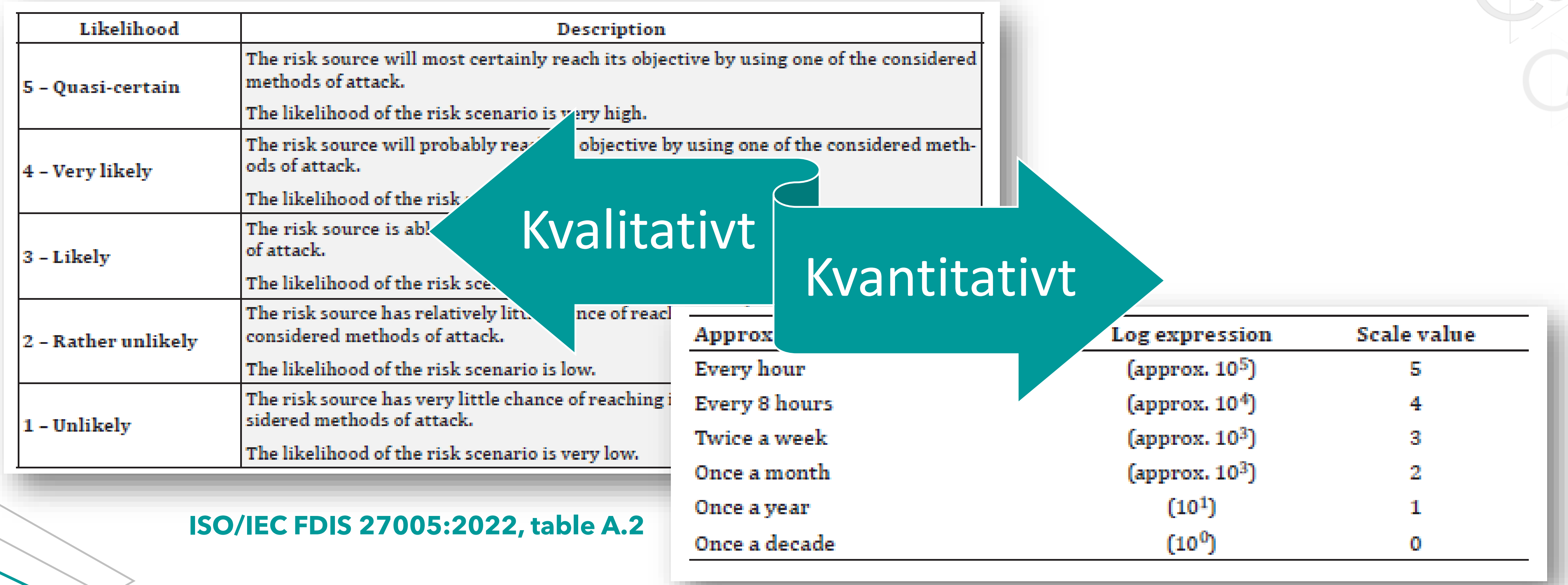
ISO/IEC 27005:2018

- 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 rea objective by using one of the considered methods of attack. The likelihood of the risk
3 – Likely	The risk source is abl of attack. The likelihood of the risk sce
2 – Rather unlikely	The risk source has relatively litt nce of reac considered methods of attack. The likelihood of the risk scenario is low.
1 – Unlikely	The risk source has very little chance of reaching i sidered methods of attack. The likelihood of the risk scenario is very low.

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 FDIS 27005:2022, table A.2

ISO/IEC FDIS 27005:2022, table A.4

Undervisning & rådgivning i standarder for cybersikkerhed

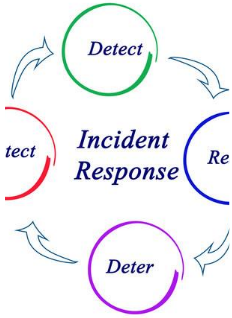
Opsummering

- 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

Trykprøv organisationen!

Er der tilstrækkelig sammenhæng mellem risikovurderingerne og SoA-dokumentet?

Giver vores fremgangsmåde mulighed for at prioritere de vigtigste risiko – eller drukner vi driftshensyn?



Kunne vi hente flere historiske eller finansielle data for en mere pålidelig beregning?

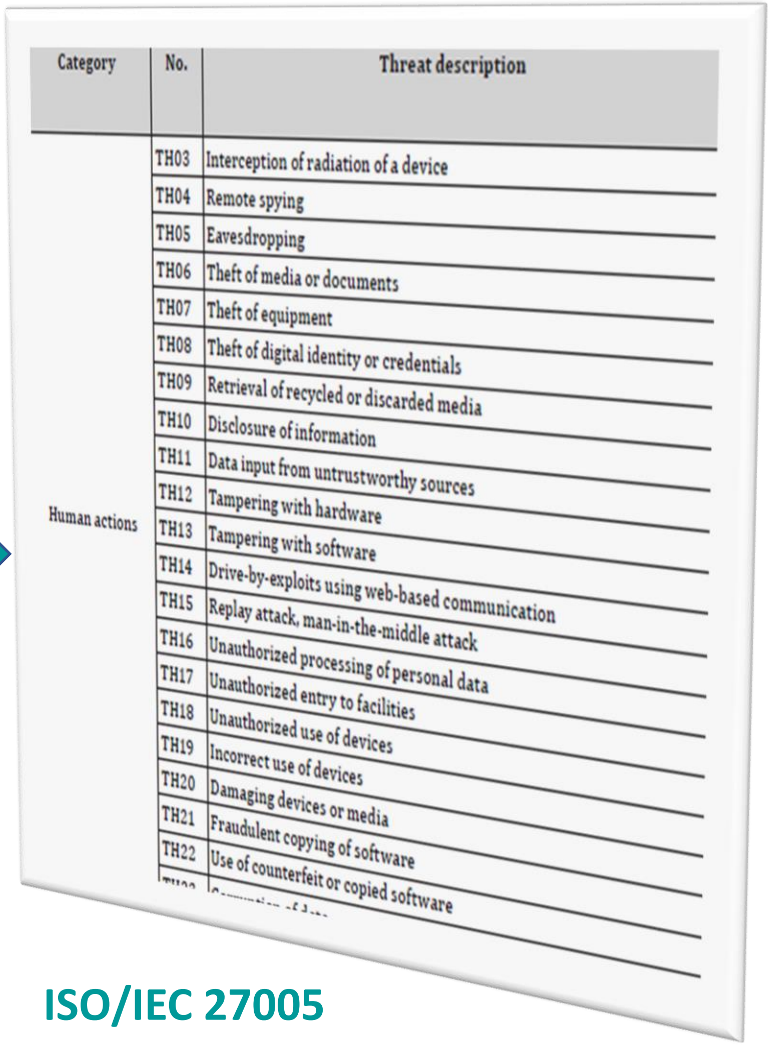
Ønsker for fremtiden

Organisatorisk

Adfærdsmæssig

Fysisk

Teknisk



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 27002

ISO/IEC 27005

Tak!

anders@ciso27.dk
Tlf. 6162 1500

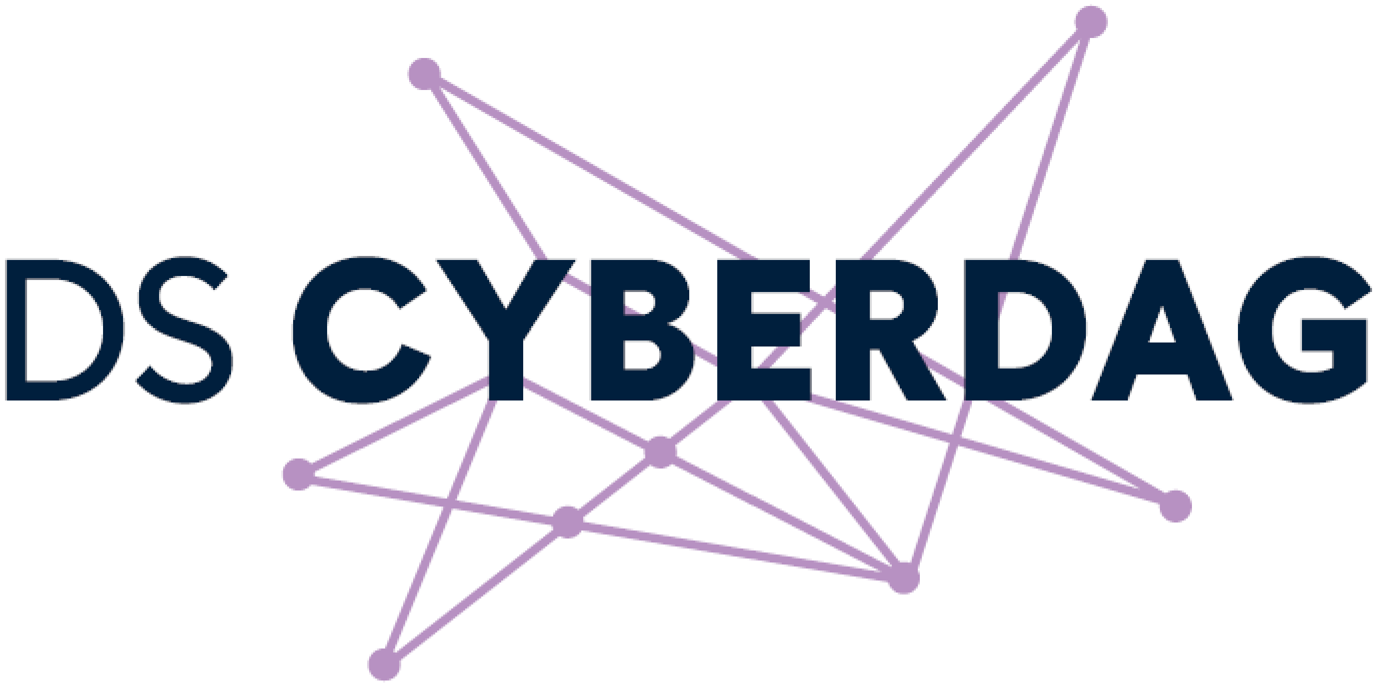
Nyt whitepaper om ISO/IEC 27005

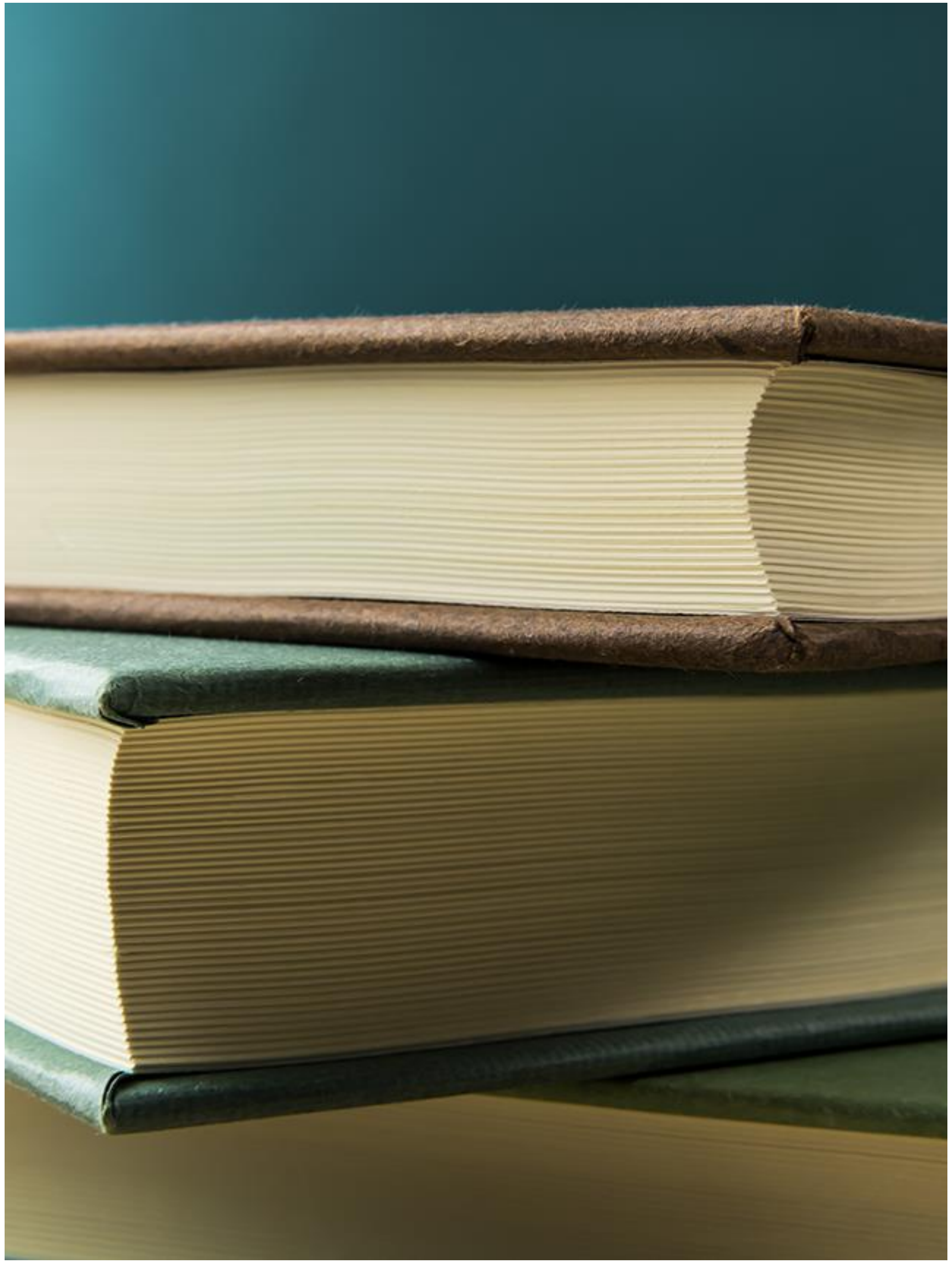
https://www.ds.dk/whitepaper-27005

Spørgsmål

Dansk Standard afholder DS Cyberdag den 29. september

https://www.ds.dk/ds-cyberdag





DANSK STANDARD

Ny guide for risikostyring ift. cyber- og informationssikkerhed på vej

- Guiden udarbejdes af Alexandra Instituttet og Dansk Standard
- Guiden skal primært inspirere danske SMV'er til at komme i gang med risikostyring
- Guiden udgives i starten af 2023