8. november 2023

Effektiv risikostyring med ISO/IEC 27005

DEIC Konference 2023

Dansk Standard

Agenda

DS
DANSK STANDARD

- **Introduktion**
- **Baggrund for risikostyring**
- **Risikostyring efter ISO/IEC 27005**
  Kontekst, identifikation, analyse, evaluering og håndtering
- **Tilgange til risikovurdering**
  Aktivbaseret og scenariebaseret
- **Udfordringerne i risikostyring**
- **Spørgsmål og Tak for i dag**

Baggrunden for risikostyring

Cybertruslen mod Danmark

- Truslen fra cyberspionage er **MEGET HØJ**
- Truslen fra cyberkriminalitet er **MEGET HØJ**
- Truslen fra cyberaktivisme er **HØJ**
- Truslen fra destruktive cyberangreb er **LAV**
- Truslen fra cyberterror er **INGEN**

Kilde: CFCS trusselsvurdering maj 2023

NIS2 krav

Samfundskritiske sektorer - herunder uddannelse og forskning - er omfattet af NIS2-direktivet.

Med NIS2 fastsættes der en række minimumskrav til foranstaltninger, der bl.a. indebærer udarbejdelse af politikker for **risiko**analyse og informationssikkerhed, håndtering hændelser og sikring driftskontinuitet.

"En risikostyringskultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles." (betragtning 77)

Beskyttelse af informationer efter ISO/IEC 27001 –
Ledelsessystem for informations-sikkerhed

Tab af fortrolighed

- Læk af interne strategier
- Ledere deler oplysninger om ansattes sygdomsforløb
- Ansatte taler åbent om sagsbehandling

Tab af integritet

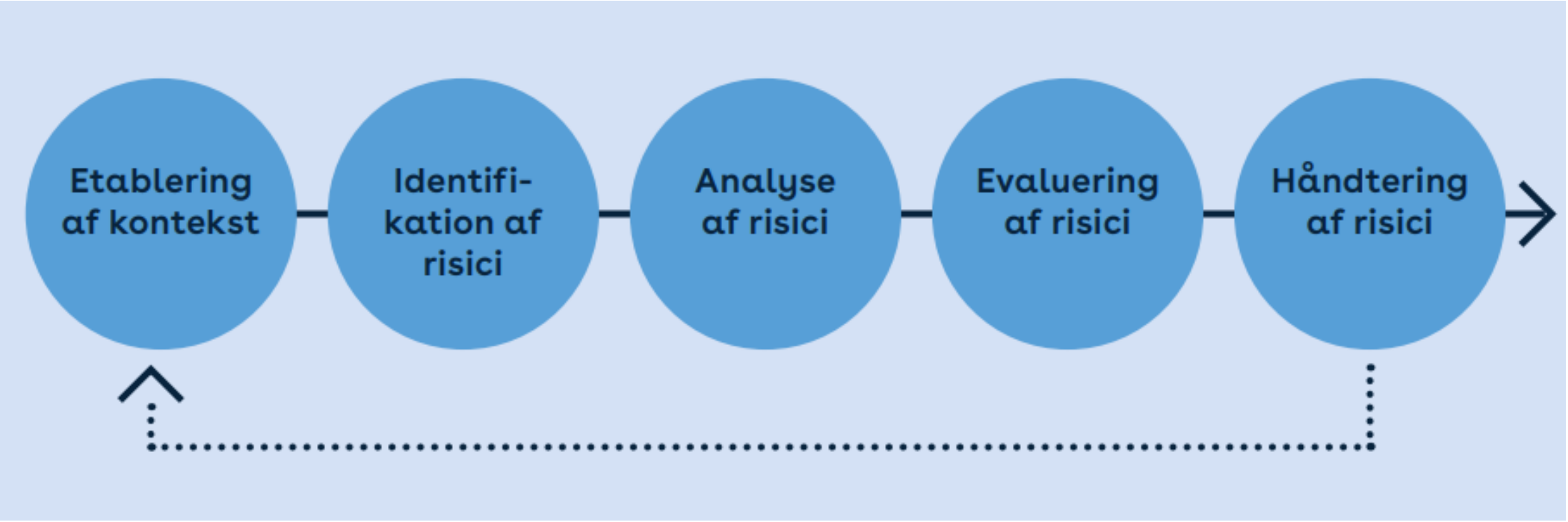
- Fejlbehæftet opdatering af systemer
- Fejl i udprint af filer
- Hackers ændring af kundedata

Tab af tilgængelighed

- Oversvømmelse af arkiver i kælderen
- Overbelastningsangreb
- Ransomware rammer sagsbehandlingssystem

DS
DANSK STANDARD

Risikostyring efter ISO/IEC 27005



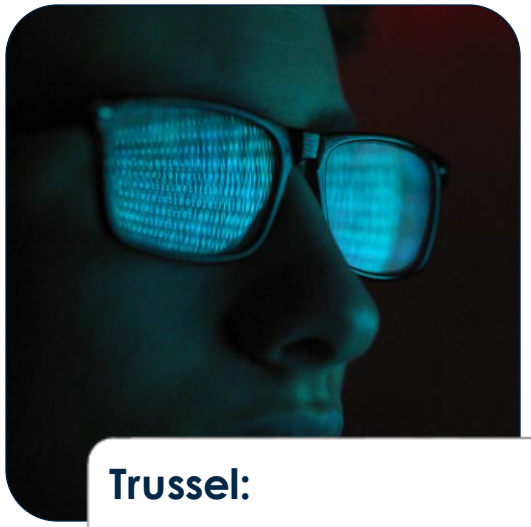
Figur fra guiden

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

Tilgange til risikostyring:
Aktivbaseret tilgang

Uønsket hændelse:

- fx brand i arkiv på kontoret



Trussel:

- fx Medarbejder-adfærd, teknisk installation mv.

Sårbarheder:

Fx opbevaring, manglende beredskabsplaner og sprinkleranlæg

"Information security risk can be associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization."

ISO/IEC 27005, 3.1.3, note 7

Tilgange til risikostyring:
Hændelsesbaseret tilgang

Uønsket hændelse:

- fx ingen adgang til forretningen

Informations-sikkerhedsprincip:

- fx tab af tilgængelighed

Konsekvens for forretningen:

- fx tab af service

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

ISO/IEC 27005, 3.1.3, note 6

Udfordringer i arbejdet med risici og informationssikkerhed

Komplekst samspil med risici for it-systemer og forretningen

Svag kobling mellem informationsrisici og organisationens øvrige risikovurderinger

Informationer er svære at definere og værdiansætte

Trussels- og sårbarhedsbilledet er uigennemsigtigt og foranderligt

Q&A

Tak for i dag!

Majken Prip
E-mail:MPR@ds.dk