28. november 2023

Risikostyring og informationssikkerhed

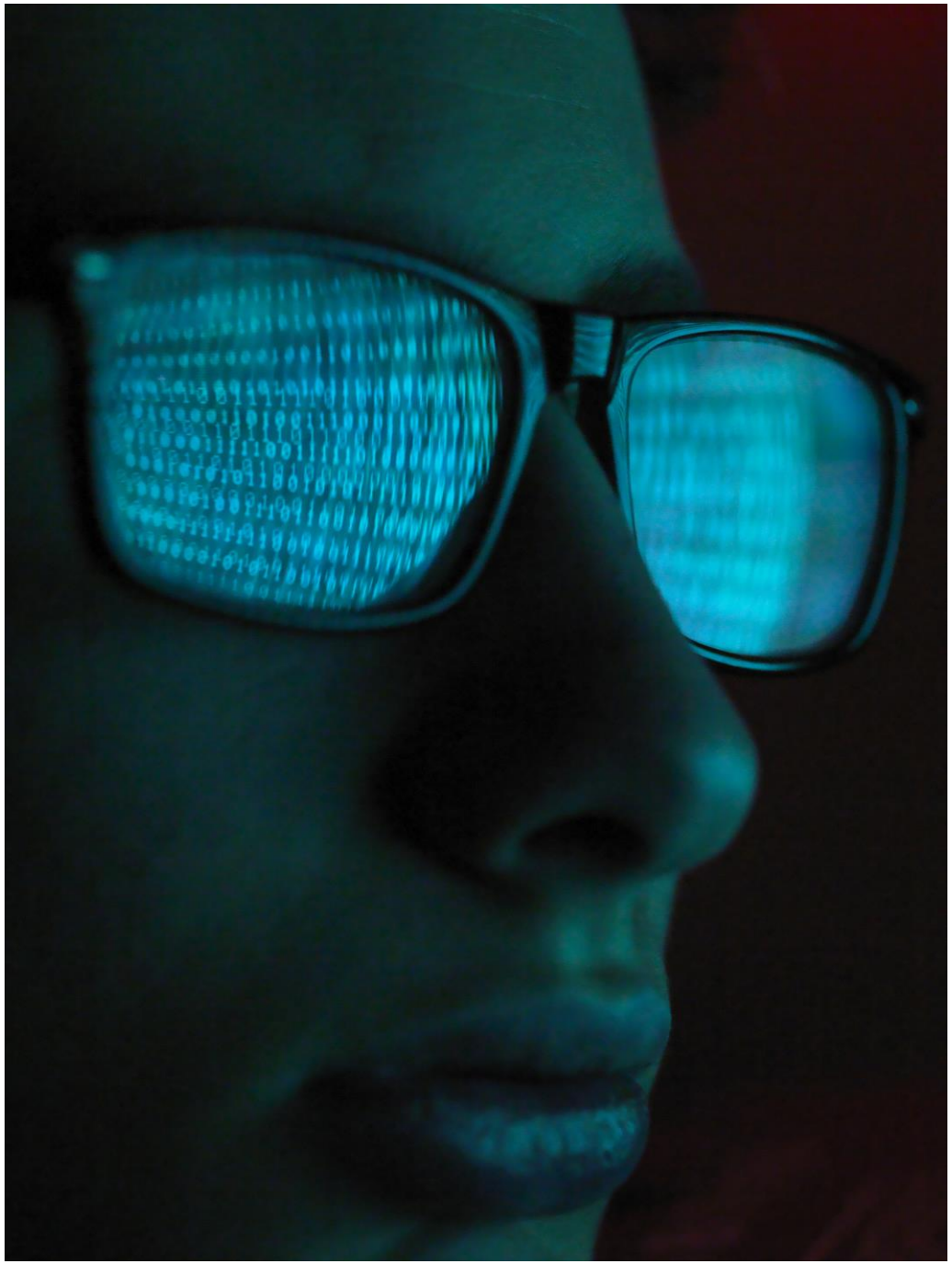
Inspiration til at imødegå kravene i NIS2

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- 196 medarbejdere (september 2023)
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

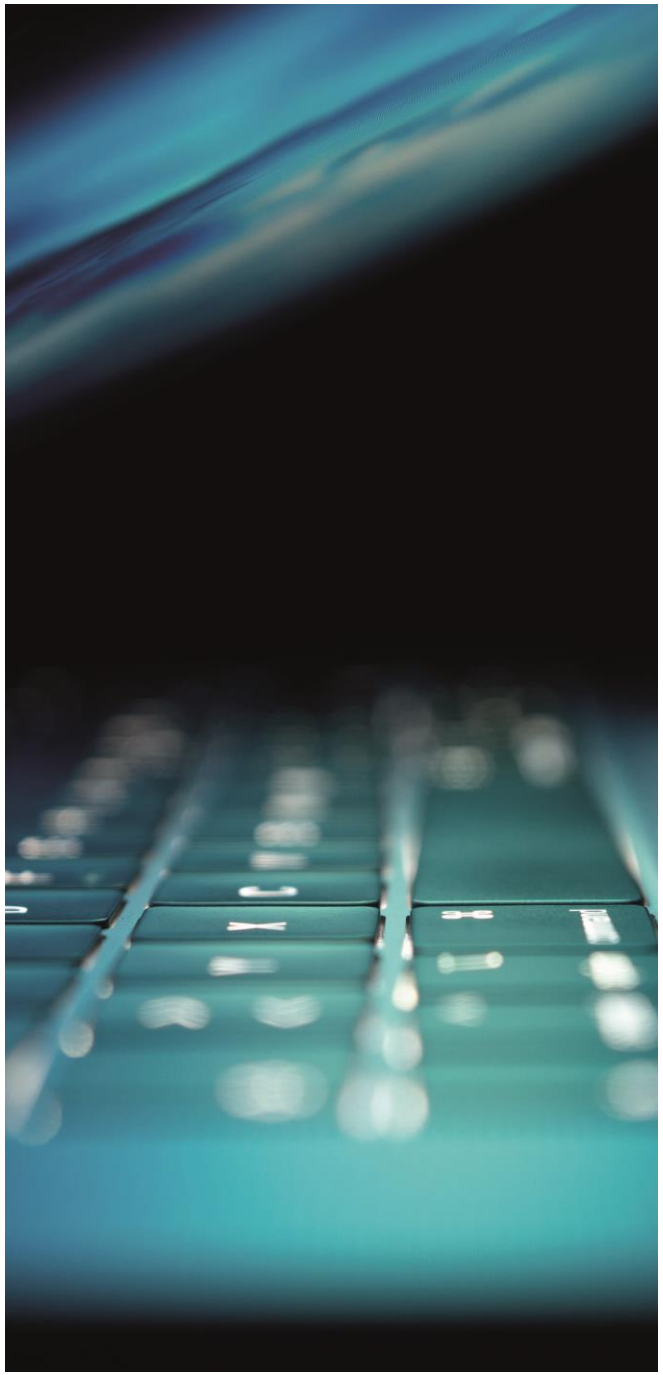
En stærk platform af solide brands:



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 februar 2023



Koblingen til NIS2

Med NIS2 fastsættes der en række minimumskrav til foranstaltninger, der bl.a. indebærer at udarbejde politikker for **risiko**analyse og informationssikkerhed, håndtere hændelser og sikre 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)

KMD
An NEC Company

HVORDAN KOMMER MAN I GANG MED AT ARBEJDE RISIKOBASERET?

HVAD FÅR MAN UD AF DET

PHILIPPE ROY

GRC SECURITY ADVISOR

KMD

INTRO

PHILIPPE ROY

- GRC Security Advisor i DTS
- Fokus på kundernes sikkerhed
- NIS2, modenhedsanalyser og generel Cyber-hygiejne

- Tidligere arbejdsgiver
  - Nordea
  - Danske Bank
  - Nordic Financial CERT
  - Fort Consult – Part of NCC Group
  - Combitech DK

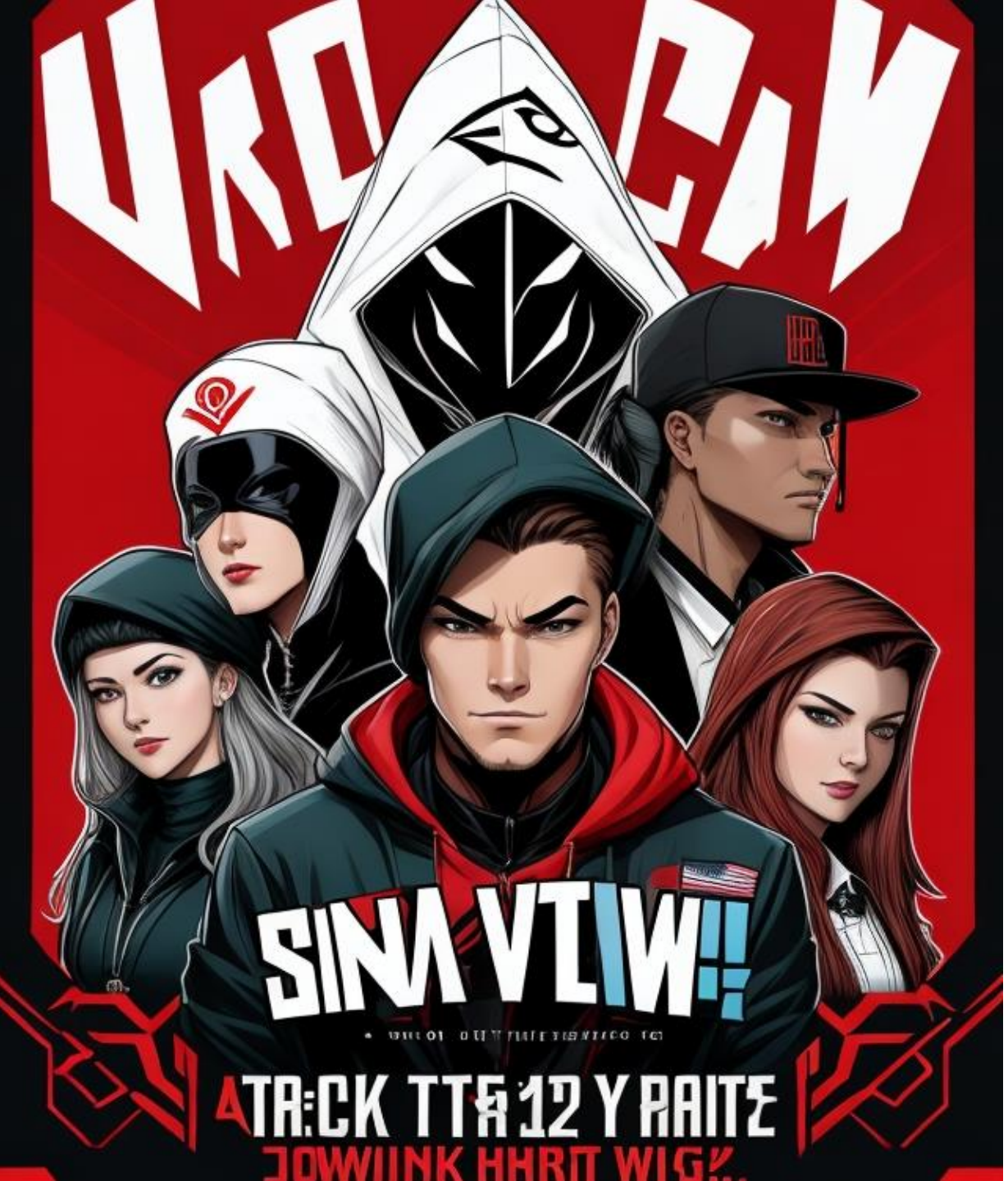
- Hvordan forklarer jeg mit arbejde?
  - Professionel Pessimist
    - Forbered på det uundgåelige
    - Forbered på at ting går galt
  - Sikre mig, at de værste scenarier ikke sker i virkeligheden.
  - Hvordan ser andre på os, når vi siger, at vi arbejder med IT risikostyring?

BETALT FOR AT VÆRE PESSIMIST

- Hvordan forklarer jeg mit arbejde?
  - Professionel Pessimist
    - Forbered på det uundgåelige
    - Forbered på at ting går galt
  - Sikre mig at de værste scenarier ikke sker i virkeligheden.
  - Hvordan ser andre på os når vi siger at vi arbejder med IT risikostyring?

BETALT FOR AT VÆRE PESSIMIST

- Hvordan forklarer jeg mit arbejde?
  - Professionel Pessimist
    - Forbered på det uundgåelige
    - Forbered på at ting går galt
  - Sikre mig at de værste scenarier ikke sker i virkeligheden.
  - Hvordan ser folk mig?



RISIKOVURDERING I PRAKSIS

- Risikovurdering og Trusselvurdering går hånd i hånd
- Trusselsvurderingen leder til hvem der vil jer ondt og er et input til en risikovurdering
- Risikovurderingen afdækker hvad der kan ske, ikke kun ved angreb, men ved mange faktorer, nogle er meget vage andre kan være meget specifikke:
  - Hacker
  - Fejlkonfigurationer
  - Oversvømmelse
  - Flystyrt
  - Pandemi
  - Manglende kontrol for jernindholdet i vandet for kølerørene i server rummene

BETALT FOR AT VÆRE PESSIMIST

- Risikovurdering kræver øvelse
  - Benytte eksisterende rammeværktøjer
    - Ingen grund til at genopfinde den dybe tallerken

Plan – Do – CHECK – ACT

- Identificere problemerne - Find passende sikkerhedsforanstaltningerne
- Implementerer sikkerhedsforanstaltningerne
- Kontroller at sikkerhedsforanstaltningerne virker
- Juster og forbedre sikkerhedsforanstaltningerne

https://www.creativesafetysupply.com/glossary/pdca-cycle/

RISIKOVURDERING I PRAKSIS

- Nogle gang kan en risikovurdering graves frem
  - Måske nogle kan huske tilbage på Marts 2006
    - Fugleinfluenza smitter kameler i Mellemøsten, potentiale for en pandemi i Europa

https://www.dr.dk/nyheder/fugleinfluenza-i-mellemoesten

RISIKOVURDERING I PRAKSIS

- Nogle gang kan en risikovurdering graves frem
  - Måske nogle kan huske tilbage på Marts 2006
    - Fugleinfluenza smitter kameler i Mellemøsten, potentiale for en pandemi i Europa
    - Ingenting, der var ingen pandemi, ingen nedlukning af samfundet

https://www.dr.dk/nyheder/fugleinfluenza-i-mellemoesten

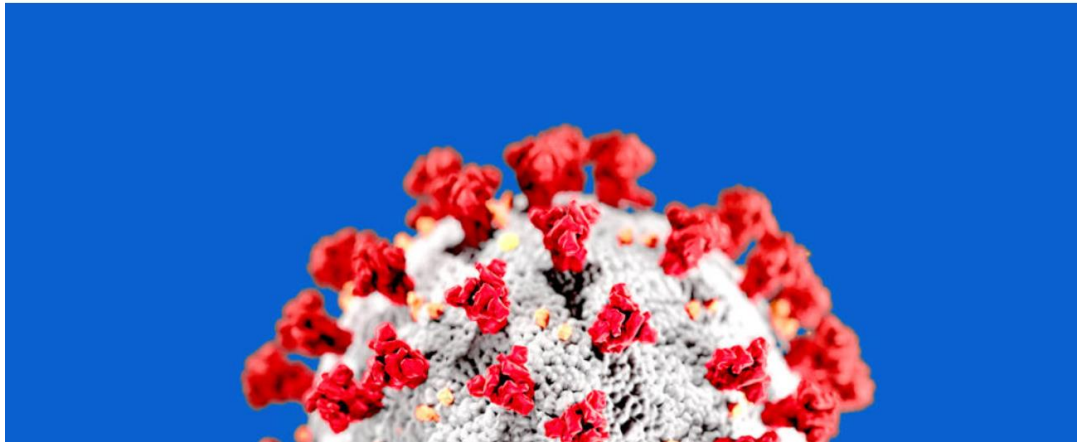
RISIKOVURDERING I PRAKSIS

- Nogle gang kan en risikovurdering graves frem
  - Måske nogle kan huske tilbage på Marts 2006
  - 2020…. Corona
    - Nedlukning
    - Hjemmeskole
    - Internetsupermarkedernes æra

INDLAND

Status på coronavirus lige nu

Se dagens coronatal og følg udviklingen i antallet af smittede, indlagte og døde.



https://www.dr.dk/nyheder/indland/status-paa-coronavirus-lige-nu

LESS IS MORE

- Alle skal kunne forstå risikovurderingen
  - Less is more
    - Der er ingen grund til at basere sin risikostyring på en alt for kompliceret proces
    - Kan det holdes simpelt, så gør det!
- Risikovurderingen fra to afdelinger skal kunne sammenlignes
  - Gør prioriteringen nemmere

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- **Unik ID**
- Hver risiko skal have et unikt nr
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- **Risk titel**

- Hver risko bør have en titel

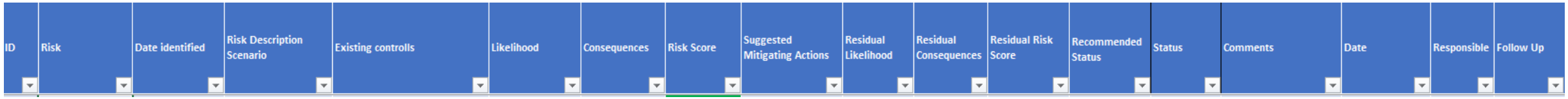
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- **Dato for identificering af risk**
- Hvornår er denne risiko identificeret?
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?



- Unik ID
- Risk titel
- Dato for identificering af risk
- **Beskrivelse af risk**
  - Kort beskrivelse, hvad kan gå galt?
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- **Eksisterende kontroller**

- Findes der eksisterende kontroller der kan minimere riskoen?

- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- **Sandsynlighed (Likelihood)**
- Hvor sandsynligt er det at det går galt?
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

RISIKOVURDERING I PRAKSIS

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- **Konsekvens**

- Hvad kan der ske, ved at det går galt?

- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- **Risiko score**
  - Sandsynlighed x Konsekvens
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- **Mitigirende handlinger**

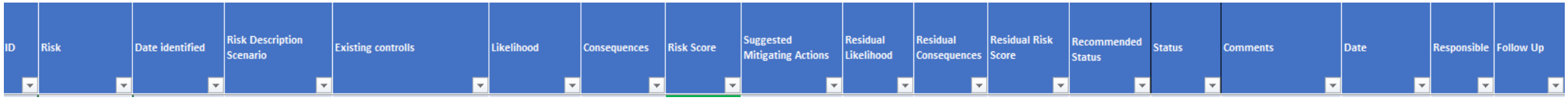
- Hvad kan vi gøre for at det ikke går galt?
  - Blivende sandsynlighed (Likelihood)
  - Blivende konsekvens
  - Blivende Risk Score
  - Stillingstagende til Risk
  - Status
  - Kommentarer
  - Dato
  - Ansvarlig
  - Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- **Blivende sandsynlighed (Likelihood)**
- Hvor sandsynligt efter vores forholdsregler
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?



- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- **Blivende konsekvens**
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

- Hvor stort et problem bliver risikoen?

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens

- **Blivende Risk Score**
  - Sandsynlighed x Konsekvens
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Stillingstagende til Risk
- **Status**

- Er dette en risiko vi acceptere, eller agter at gøre noget ved?

- Kommentarer
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- **Kommentarer**
  - Kommentarer, hvad er sket siden sidst
- Dato
- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- **Dato**

- Hvornår har vi sidst besøgt denne risk

- Ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- **Ansvarlig**
- Hvilken afdeling og hvem er ansvarlig
- Opfølgning

HVAD BØR EN RISIKOVURDERING INDEHOLDE?

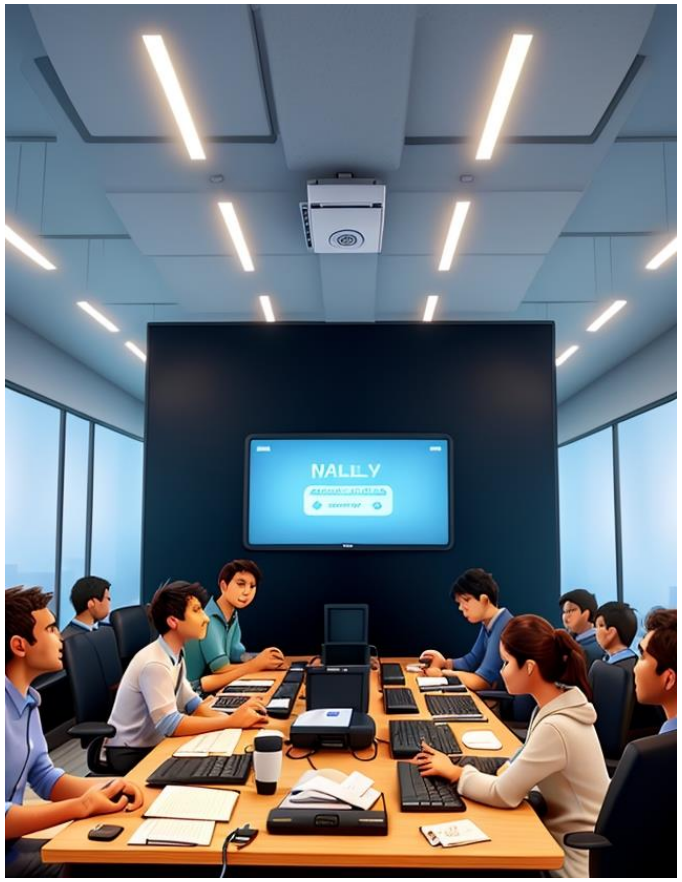
ID	Risk	Date identified	Risk Description Scenario	Existing controlls	Likelihood	Consequences	Risk Score	Suggested Mitigating Actions	Residual Likelihood	Residual Consequences	Residual Risk Score	Recommended Status	Status	Comments	Date	Responsible	Follow Up

- Unik ID
- Risk titel
- Dato for identificering af risk
- Beskrivelse af risk
- Eksisterende kontroller
- Sandsynlighed (Likelihood)
- Konsekvens
- Risiko score
- Mitigirende handlinger
- Blivende sandsynlighed (Likelihood)
- Blivende konsekvens
- Blivende Risk Score
- Stillingstagende til Risk
- Status
- Kommentarer
- Dato
- Ansvarlig
- **Opfølgning**

- Hvad er der sket siden risiko vurderingen sidst blev gennemgået

RISIKOVURDERING I PRAKSIS

- Less is more
  - Hold den gerne så simpel som muligt
- Forståeligt af alle
  - Sørg for at alle kan forstå vigtigheden af en risikovurdering
- Brug risikovurderingen aktivt
  - Kig på den mindst en gang om året



Q&A?

NYTTIGE LINKS OG KONTAKT OPLYSNINGER

- Er der ikke billede henvisninger er alle billeder i denne præsentation er dannet via https://app.leonardo.ai/ai-generations
  - En AI der omdanner tekst til et billeder

Philippe Roy

GRC Security Advisor

Mail: phr@kmd.dk

Telefon: +45 23 84 76 85

Introduktion risikostyring med afsæt i ISO/IEC 27005 og Dansk Standards guide for risikostyring

ISO/IEC 27005 – Vejledning i styring af informationssikkerhedsrisici

Standarden er en vejledning i implementeringen af de krav til **informationssikkerhedsrisici** som er specificeret i ISO/IEC 27001

Standarden henvender sig til:

- Organisationer, der har til hensigt at etablere og implementere et ledelsessystem for informationssikkerhed (ISMS) i overensstemmelse med ISO/IEC 27001
- Personer, der udfører eller er involveret i risikoledelse i forbindelse med informationssikkerhed (fx ISMS-specialister, risikoejere og andre interessenter)
- Organisationer, der har til hensigt at forbedre deres risikoledelsesproces for informationssikkerhed

Guide til risikostyring

Risikostyring ift. cyber- og informationssikkerhed for SMV'er

- Alexandra instituttet og Dansk Standard udgav guiden i 2023
- Formålet med guiden er at hjælpe danske smv'er i gang med at arbejde konkret og systematisk med risikostyring ift. cyber- og informationssikkerhed
- Guiden tager afsæt i den internationale standard *ISO/IEC 27005 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse - Vejledning i styring af informationssikkerhedsrisici*
- Guiden kan hentes her: https://www.ds.dk/risikostyring

Guiden benytter sig af tre virksomhedseksempler

VIRKSOMHED A
Autoværkstedet

Mindre autoværksted
Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer. Dog ikke kunder med særlige krav. Relativt få brugere.

VIRKSOMHED B
Produktionsvirksomheden

Mellemstor virksomhed
(omkring 85 ansatte), der producerer og installerer videoovervågningssystemer. Høj grad af digitalisering. Stor mængde fortrolige data. Stor snitflade med mange brugere; kunder, samarbejdspartnere, leverandører mm. Leverer til kritisk infrastruktur.

VIRKSOMHED C
Webshoppen

Lille virksomhed
(fire ansatte), der importerer vin. Høj grad af digitalisering (100 % webshop). Mange brugere af webshoppen. Nogen grad af fortrolige data. Benytter sig i høj grad af leverandører i forhold til IT-driften.

Figur fra guiden

Informationssikkerhed

Beskyttelse af informationer efter ISO/IEC 27001 – Ledelsessystem for informationssikkerhed

Tab af fortrolighed

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

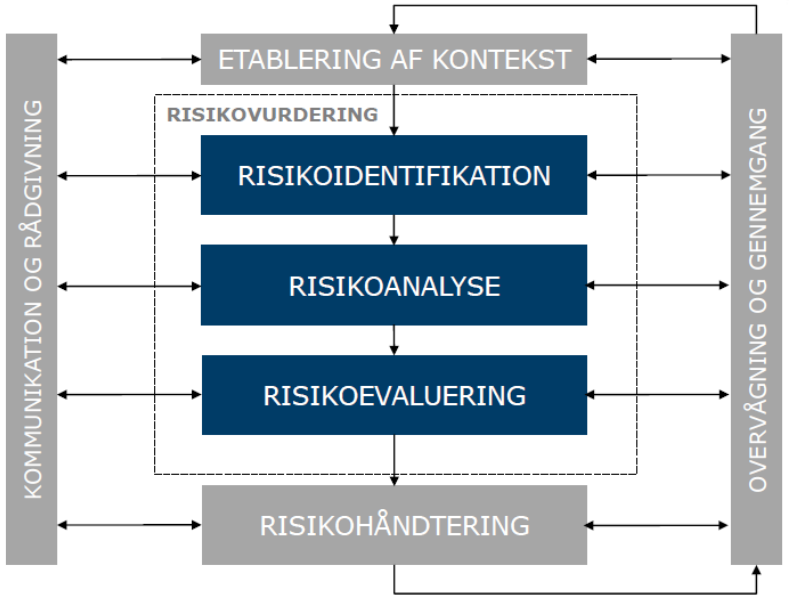
Tab af integritet

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

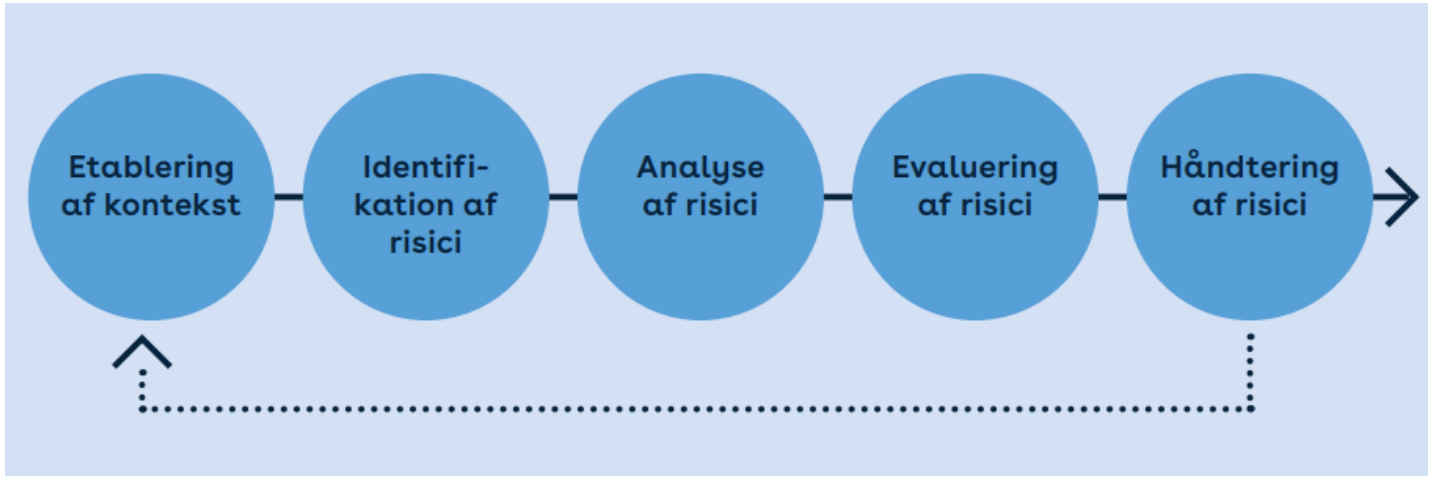
Tab af tilgængelighed

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

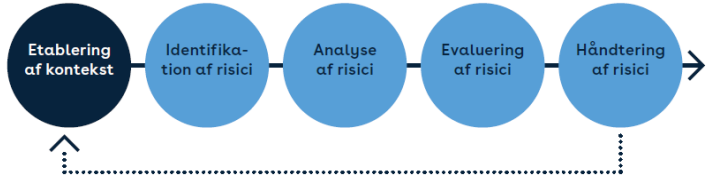
Risikostyringsprocessen efter ISO/IEC 27005



Figur fra ISO/IEC 27005:2022



Figur fra risikostyringsguiden



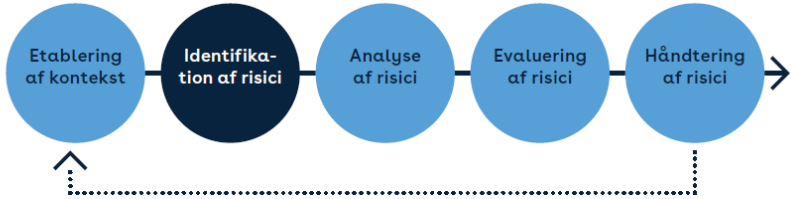
DS DANSK STANDARD

Etablering af rammer og vilkår (kontekst)

- Indblik i strategi, mål, vision og mission
- Fastlæggelse af risikovillighed og risikoaccept
- Definition af eksterne interessenter og deres krav
- Fastlægge rammer og metode for risikostyringsprocessen
- Identifikation af de forretningskritiske processer og informationer
- Kvalitativ vs. kvantitativ tilgang til at udregne risici
- Rollefordeling – risikoejere og ledelsens opbakning

Risikovurderingen bør hjælpe organisationen til at træffe beslutninger om styringen af de risici, der har indflydelse på opfyldelsen af dens mål.

ISO/IEC 27005:2022, 6.3



DANSK STANDARD

Identifikation af risici

- Vigtig proces der danner baggrund for den videre analyse, evaluering og håndtering af risici – kun de risici der identificeres som der arbejdes videre med
- **Hændelsesbaserede tilgang** (udgangspunkt i hændelser og deres konsekvenser). Find inspiration i trusselskataloger
- **Aktivbaserede tilgang** (udgangspunkt i virksomhedens aktiver; data, enheder og funktioner + vurdering af sårbarheder og trusler mod aktiverne). Kan være en fordel at tage udgangspunkt i noget velkendt

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

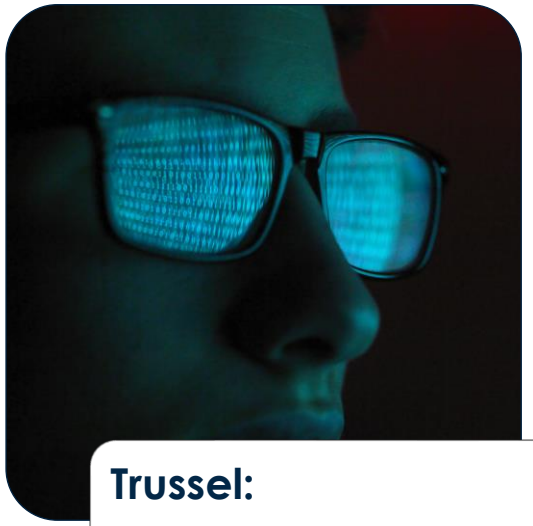
"Informationssikkerhedsrisici forbindes normalt med en negativ effekt af usikkerhed på målene for informationssikkerhed."

ISO/IEC 27005:2022, 3.1.3, note 6

Tilgange til risikostyring:
Aktivbaseret tilgang

Uønsket hændelse:

- fx brand i arkiv på kontoret



Trussel:

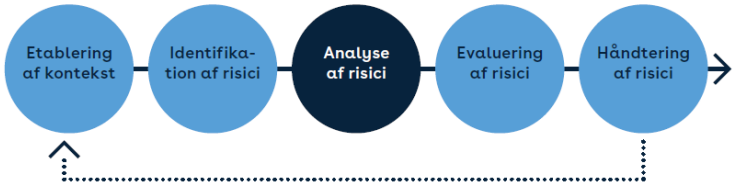
- fx Medarbejder-adfærd, teknisk installation mv.

Sårbarheder:

Fx opbevaring, manglende beredskabsplaner og sprinkleranlæg

"Informationssikkerhedsrisici kan være forbundet med den mulighed, at trusler vil udnytte sårbarhederne ved et informationsaktiv eller en gruppe af informationsaktiver og dermed forårsage skade i en organisation."

ISO/IEC 27005:2022, 3.1.3, note 7



DANSK STANDARD

Analyse af risici

- Formål at fastsætte en risikoværdi - ofte udgangspunkt i sandsynlighed og konsekvens

- Kvalitativ tilgang (f.eks. lav, middel, høj) eller kvantitativ tilgang (skala med f.eks. numeriske værdier som økonomiske omkostninger, frekvens eller sandsynlighed for forekomst)

- Målet med denne fase er at ende ud med en række lister:
  - over potentielle konsekvenser i relation til risikoscenarier med tilhørende konsekvenser for aktiver eller hændelser (afhængig af anvendt metode)
  - over hændelser eller risikoscenarier suppleret med sandsynligheden for at de opstår
  - over risici med de tildelte niveauværdier

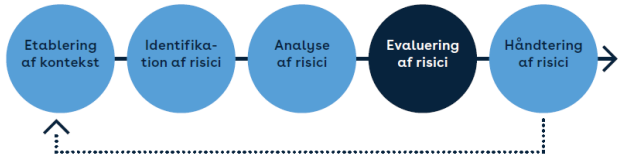
Eksempler på analyse af risici

Sandsynlighedsanalyse

RISIKOSCENARIE/TRUSSEL	SÅRBARHEDER	FORANSTALTNINGER	SCORE
Skybrud medfører oversvømmelse i kælderen	• It-udstyr og arkiv placeret på gulvet • Ingen pumper • Beliggenhed nær havn	• Sensorer • Beredskabsplaner	**3**
Virus installeres via USB-stick	• Ingen retningslinjer • Manglende awareness	• ID-kort • Reception	**4**
Nøglemedarbejder siger op	• Få trivselssamtaler • Lavt lønniveau	• Vejledninger til brugerne • Eksternt rekrutteringsbureau	**4**

Konsekvensanalyse

RISIKOSCENARIE/TRUSSEL	FORTROLIGHED	INTEGRITET	TILGÆNGELIGHED	SCORE
Skybrud medfører oversvømmelse i kælderen			Vand i kælderen ødelægger server og arkiv	**3**
Virus installeres via USB-stick		Tabte data i forbindelse med back-up proces	Systemnedbrud: større adgangstab til forretningsprocesser	**3**
Nøglemedarbejder siger op			Tab af specialistviden til at drive vigtige systemer	**4**



DANSK STANDARD

Evaluering af risici

- Formålet med dette trin er at forholde sig til om den enkelte risiko er en risiko man vil leve med i forhold til forretningens målsætninger og politikker
- Prioritering af de identificerede risici
- Træffe beslutninger om hvilke og om alle risici skal håndteres

Tabel C4

KONSEKVENS \ SANDSYNLIGHED	Lav	Middel	Høj
Lav	**Lav/Lav**	Middel/Lav	Høj/Lav
Middel	Lav/Middel	Middel/Middel	**Høj/Middel**
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Brug af persondata

DDoS-angreb

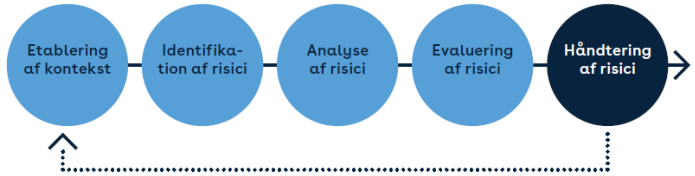
Tabel B4

KONSEKVENS \ SANDSYNLIGHED	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	**10**	15	**20**	25

Manglende ekspertise ifm. et cyberangreb

Manglende validering af hvor data stammer fra

Eksempler fra risikostyringsguiden



DANSK STANDARD

Håndtering af risici

I risikohåndteringen opereres der med fire valgmuligheder for at håndtere én risiko:

- Acceptere risikoen
- Undgå risikoen (stoppe eller ændre den aktivitet, der forårsager risikoen)
- Flytte/dele risikoen (outsourcing, forsikring)
- Forøge/minimere risikoen (foranstaltninger der kan mindske sandsynligheden eller konsekvensen og dermed nedbringe risikoen til et acceptabelt niveau).

Plan for håndtering af informationssikkerhedsrisici – statement of applicability (SoA). Find inspiration i ISO/IEC 27002

Hvad skal der til for at lykkedes med en risikostyringsproces?

- **Ledelsesforankring**
- Afsætte nødvendige ressourcer til arbejdet
- Rollefordeling på plads
- Få delt arbejdet op i overkommelige 'bidder'
- Kommunikation om vigtigheden til resten af organisationen
- Forstå at der er tale om en løbende proces og at ens risikobillede hurtigt kan ændre sig

DANSK STANDARD

ISO/IEC 27005 er nu oversat til dansk!

Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse
– Vejledning i styring af informationssikkerhedsrisici

Link til webshop

Q&A

Stil dit spørgsmål i chatten

Tak for i dag

Berit Aadal

E: baa@ds.dk

M: 26 22 46 96