Risikovurdering

– understøttet af modenhedsvurderinger

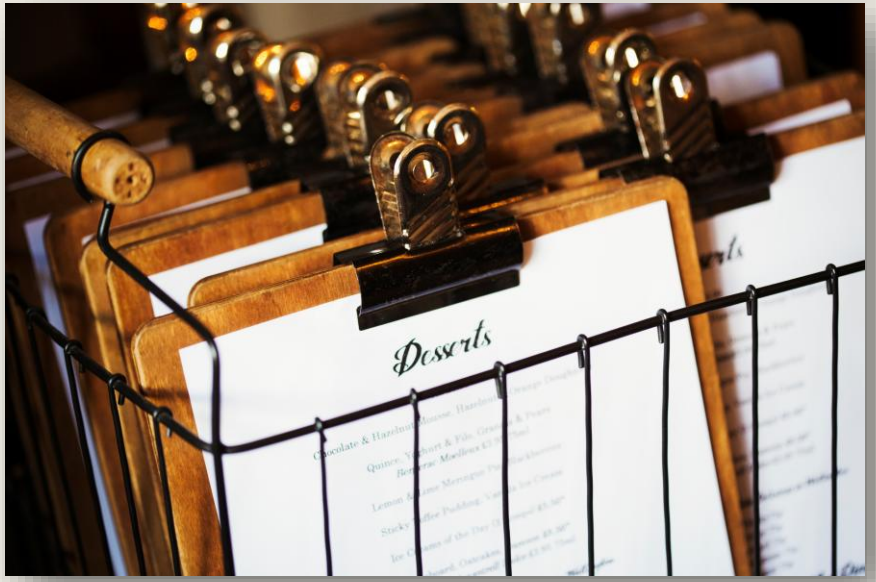
Jesper B. Hansen

14. April 2026

Webinar

Agenda

- Kort introduktion
  - Kort om Siscon & Jesper
- NIS2 fokusområder (eksempel)
  - Kortlægning
  - Modenhedsvurderinger
- Risikovurderinger
  - Perspektiver
  - Indarbejdelse af modenhedsvurderinger
- Afrunding



Spørgsmål er meget velkomne undervejs
Webinaret optages og fremsendes med slides

SISCON

Kort om Jesper

- Risikostyring
- IT-sikkerhedsstrategi
- Multidimensional compliance
  - ISO27001/2
  - NIS2, CIS, GDPR

- Baggrund
  - Nuværende
    - Chief Operating Officer, Siscon
    - Bestyrelsesmedlem Rådet for Digital Sikkerhed
  - Chief Technical Officer, Siscon
  - Chief Delivery Officer, Siscon
  - Leder af PFAs IT-Infrastrukturafdeling
  - IT-sikkerhedschef, PFA
  - Manager, PwC

Siscon - fakta

- Danskejet virksomhed
- Etableret i 2004
- Fagområde - informationssikkerhed og databeskyttelse
- Producent af GRC-værktøjet ControlManager
- 20 medarbejdere
- Hovedkontor i Søborg

CONTROL™ MANAGER by SISCON

ControlManager™

- Skaber **struktur** og skaber **overblik**.

- **Automatisering** af opgaverne **reducerer arbejdsbyrden** til et minimum
  - Årshjul
  - Sikrer kontinuert vedligehold

- Information **samlet ét sted**
  - **Risici**
  - **Kontroller**
  - **Gap-analyser**

Situationen i dag

Der kommer løbende mere og mere regulering

NIS2 hovedområder

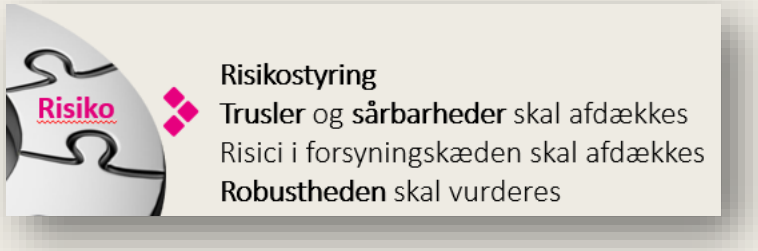
Ledelsesansvar
Topledelse, direkte ansvar:
- Kende og forstå direktivet
- Forstå de forretningsmæssige risici

Leverandørstyring
Risikovurdering
Screening
Tilsyn

Risikostyring
Trusler og **sårbarheder** skal afdækkes
Risici i forsyningskæden skal afdækkes
Robustheden skal vurderes

Hændelser
Hændelseshåndtering
Udveksling af trusselsinformation
Beredskab

Sikringsforanstaltninger
Grundlæggende computerhygiejne
People/processes/technology
Kontrol af sikringstiltags effektivitet
- Audit
- Kontroller



1

Overblik og GAP-analyser

BEK. 260 kredser omkring overblik og sårbarhedsstyring

BEK nr 260 af 06/03/2025 (Gældende)

Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren

11. §48. Fortegnelse over sofware- og hardware (1. Fuld efterlevelse)

Virksomheder skal have ajourførte fortegnelser over følgende software- og hardwareaktiver:

1) Servere, databaser og netværksudstyr, som anvendes i forbindelse med leveringen af virksomhedens tjenester.

2) Endpoints og virtuelle maskiner, der kan tilgå virksomhedens net- og informationssystemer.

3) Software- og hardwareaktiver i virksomhedens forsyningskritiske net- og informationssystemer.

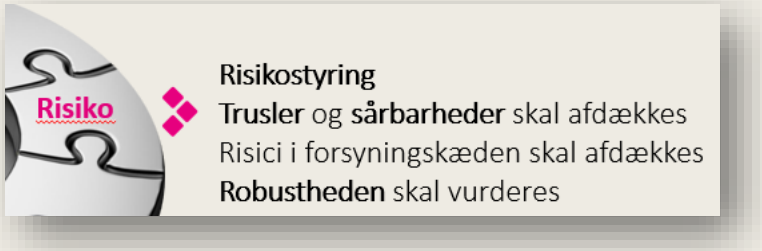
11. §48 stk 2. Detaljegrad i fortegnelser (1. Fuld efterlevelse)

Fortegnelserne skal være tilstrækkeligt detaljerede til at sikre hurtig identifikation af et aktiv, så eventuelle sårbarheder kan identificeres, vurderes og mitigeres, jf. § 47.

11. §47. Identifikation og mitigering af sårbarheder (1. Fuld efterlevelse)

Virksomheder skal være i stand til at identificere, reagere på og mitigere sårbarheder, som kan påvirke sikkerheden i virksomhedens net- og informationssystemer.

SISCON

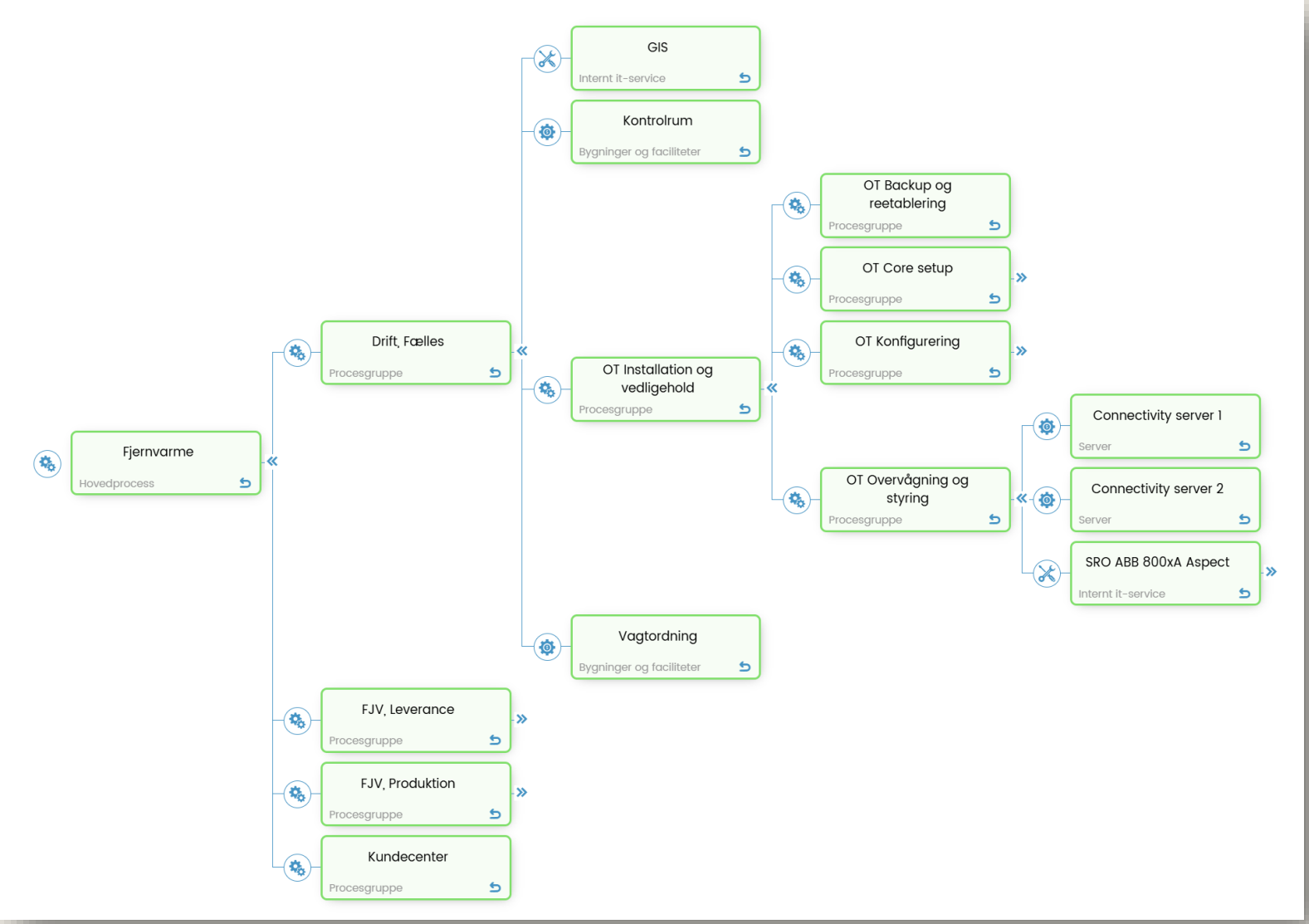


Skab overblik

- Forstå og **dokumenter** leverancer
  - Hvad er det virksomheden leverer?
  - Hvad er kravene til leverancen? (robusthed og beredskab)
  - Hvad er det for komponenter som understøtter leverancerne?
    - IT-/OT-Systemer
    - IT-/OT-Komponenter
    - Netværk
    - Leverandører

- Udgangspunktet er de kritiske leverancer
  (kræver dog man kan dokumentere hvad der er kritisk)

Kortlægning



- Overblik over kritisk i forhold til leverancer
- Skaber fundamentet for Risikovurderinger
- Struktur til GAP-analyser

CONTROL™ MANAGER by SISCON

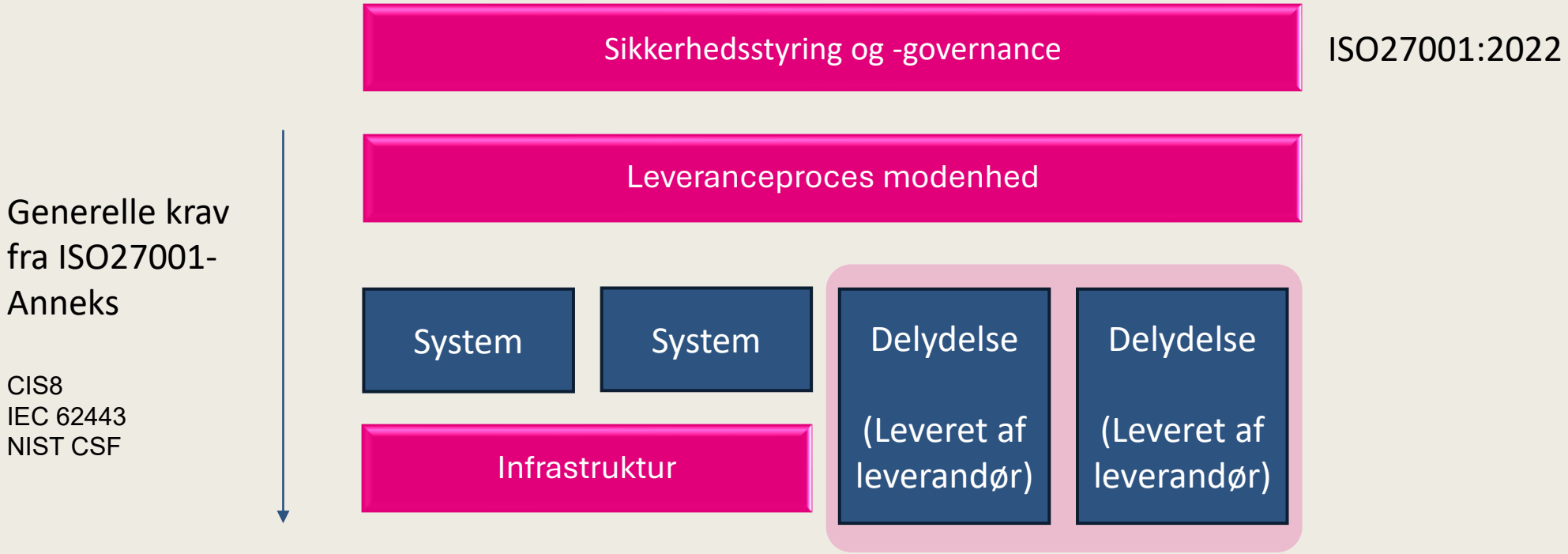
Struktur til GAP-analyser

- Kan bruges til at vurdere nuværende niveau i forhold til
  - en lovgivning
  - en standard (F.eks. ISO 27001)
  - kundekrav

- Kan anvendes som tilstandsrapport:
  - Overordnet
    - Hvor er jeg i dag generelt set?
  - Specifikt sikkerhedsmæssigt område
  - Specifikt organisatorisk område
  - På et givent system

Eksempel fra NIS2 projekt

- Bruger GAP/modenhedsanalyser
  - Som **temperaturmåling** det nuværende niveau
  - Som **løbende styrringsredskab** til gradvist at forbedre compliance/modenhed



CONTROL™ MANAGER by SISCON

Eksempel CIS18 GAP analyse

05. Account Management, Small Company

05. 5. Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

05. 5. 1. Establish and Maintain an Inventory of Accounts ! (50%)

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Compliance:
2 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
50%

05. 5. 2. Use Unique Passwords ! (75%)

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

Compliance:
3 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
75%

06. Access Control, Small Company

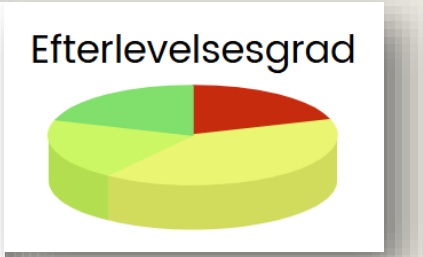
06. 6. Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

06. 6. 5. Require MFA for Administrative Access ✔

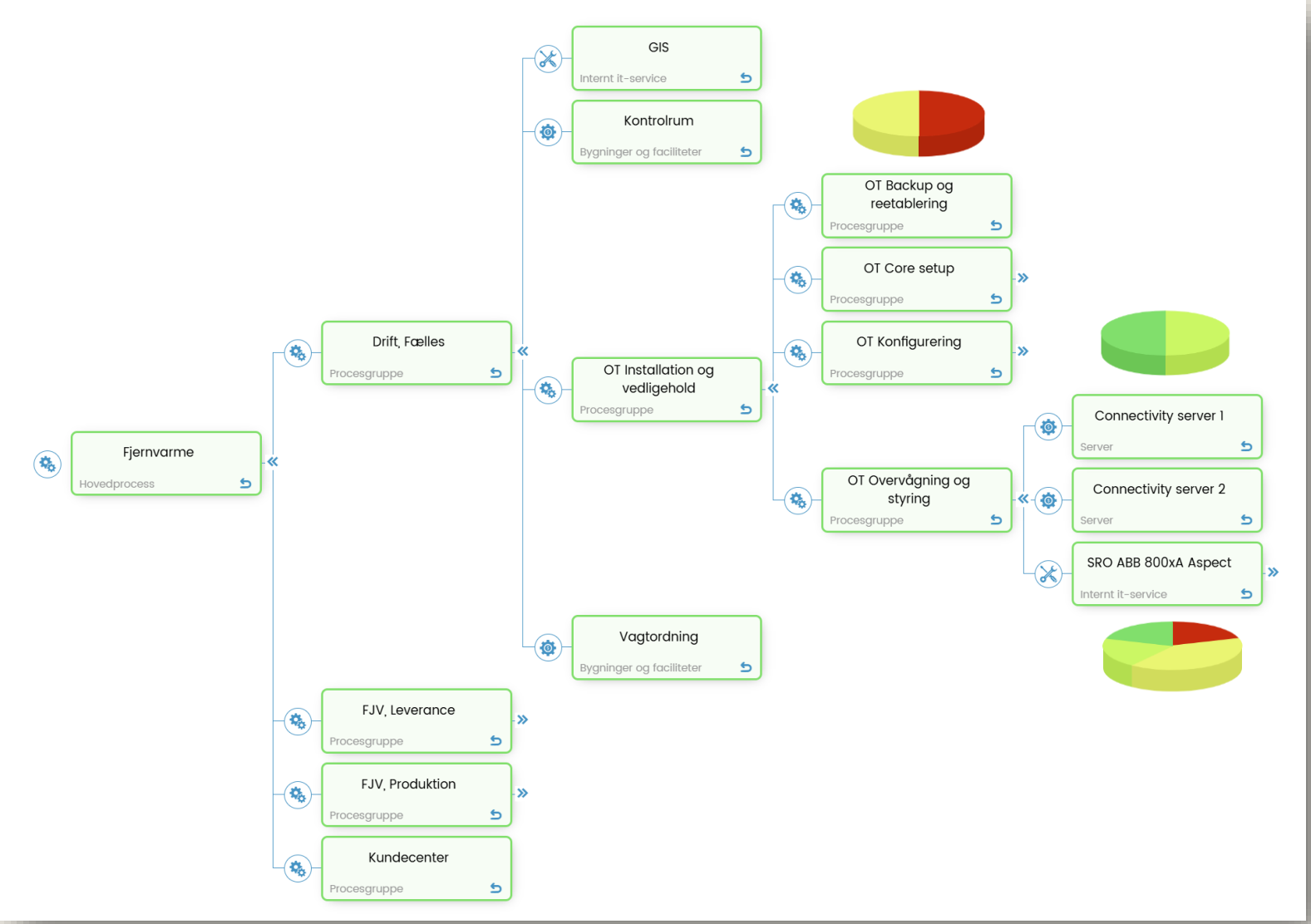
Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

Compliance:
4 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
100%



CONTROL™ MANAGER by SISCON

Kortlægning



- Overblik over kritisk i forhold til leverancer
- Skaber fundamentet for Risikovurderinger
- Struktur til GAP-analyser

CONTROL™ MANAGER by SISCON

Modenhedsrejsen

- Ved at gennemføre disse Gap/modenhedsvurderinger **regelmæssigt**, kan disse bruges til at løfte sikkerhedsniveauet for de systemer/områder som der analyseres

- Giver et **godt sprog** til at tale med **områdeeksperter:**
  - ISO 27001/2
  - CIS18
  - NIST CSF
  - IEC 62443
  - Branchespecifikke krav/frameworks

- **Konkrete målbare krav**

2

Risikovurderinger

NIS2 hovedområder

Ledelsesansvar
Topledelse, direkte ansvar:
- Kende og forstå direktivet
- Forstå de forretningsmæssige risici

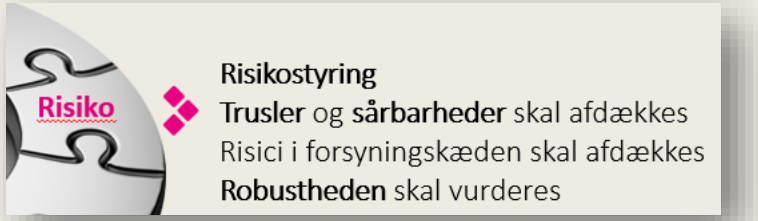
Leverandørstyring
Risikovurdering
Screening
Tilsyn

Risikostyring
Trusler og **sårbarheder** skal afdækkes
Risici i forsyningskæden skal afdækkes
Robustheden skal vurderes

Hændelser
Hændelseshåndtering
Udveksling af trusselsinformation
Beredskab

Sikringsforanstaltninger
Grundlæggende computerhygiejne
People/processes/technology
Kontrol af sikringstiltags effektivitet
- Audit
- Kontroller

Risikobaseret tilgang



- Krav om at forstå:
  - organisationen og **dennes leverancer** (i dybden)
  - it/ot-landskabet der **understøtter leverancerne**
  - **leverandørkæden** og deres understøttelse af systemer og leverancer
- gennemfør risikovurderinger
  - der illustrerer risikobilledet, både for **egne leverancer og på leverandørsiden**
- Implementere tilstrækkelige sikringsforanstaltninger
  - der sikrer den **kontinuerte leverance**
  - afbøder eventuelle hændelser

NIS2 - *Artikel 21*

Foranstaltninger til styring af cybersikkerhedsrisici

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

En ”klassiske” model

Afdækning af **forretnings**konsekvensen, hvis der sker brud på:
- Fortrolighed
- Integritet
- Tilgængelighed (flere tidshorisonter)

Oftest gennemført på processer/leverancer

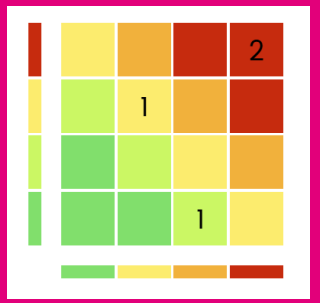
Hvad er **sandsynligheden** for en given trussel, der kan påvirke:
- Fortrolighed
- Integritet
- Tilgængelighed

Oftest gennemført på systemer/infrastruktur

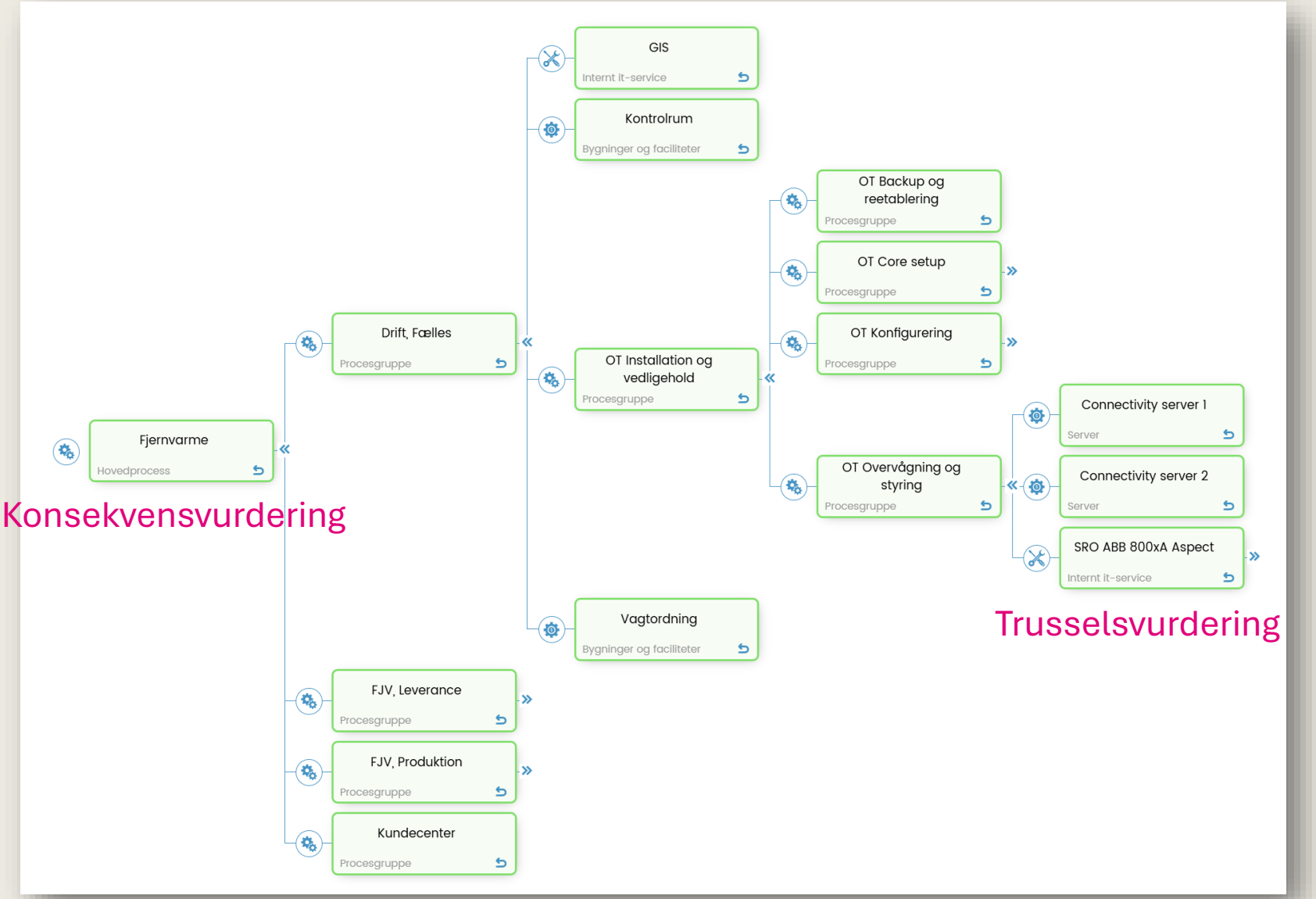
Konsekvens-analyse

Trussels-vurdering

Risikobilledet



Kortlægning – grundlaget for analyser



SISCON

Konsekvensvurdering

Organisationen							
Gennemførelse af arbejdsprocesser og ressourcetræk							
Omdømme							
Overholdelse af lovgivning							
Økonomi							
Samfundet (NIS2)							
Geografisk omfang							
Samarbejdspartneres forbundethed og afhængighed af services							
Sikkerhedshændelses negative konsekvenser for national sikkerhed							
Samlet							

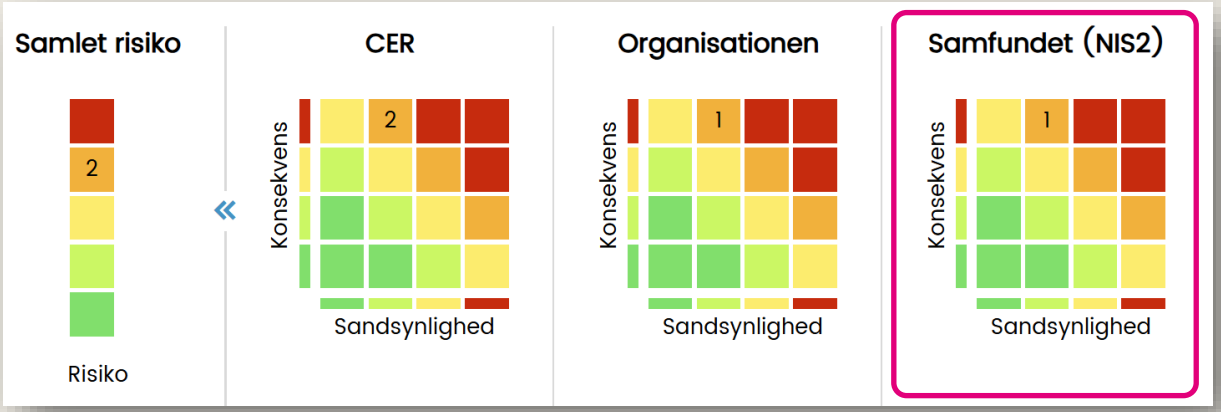
Trusselsvurderingen

Trusselstabel

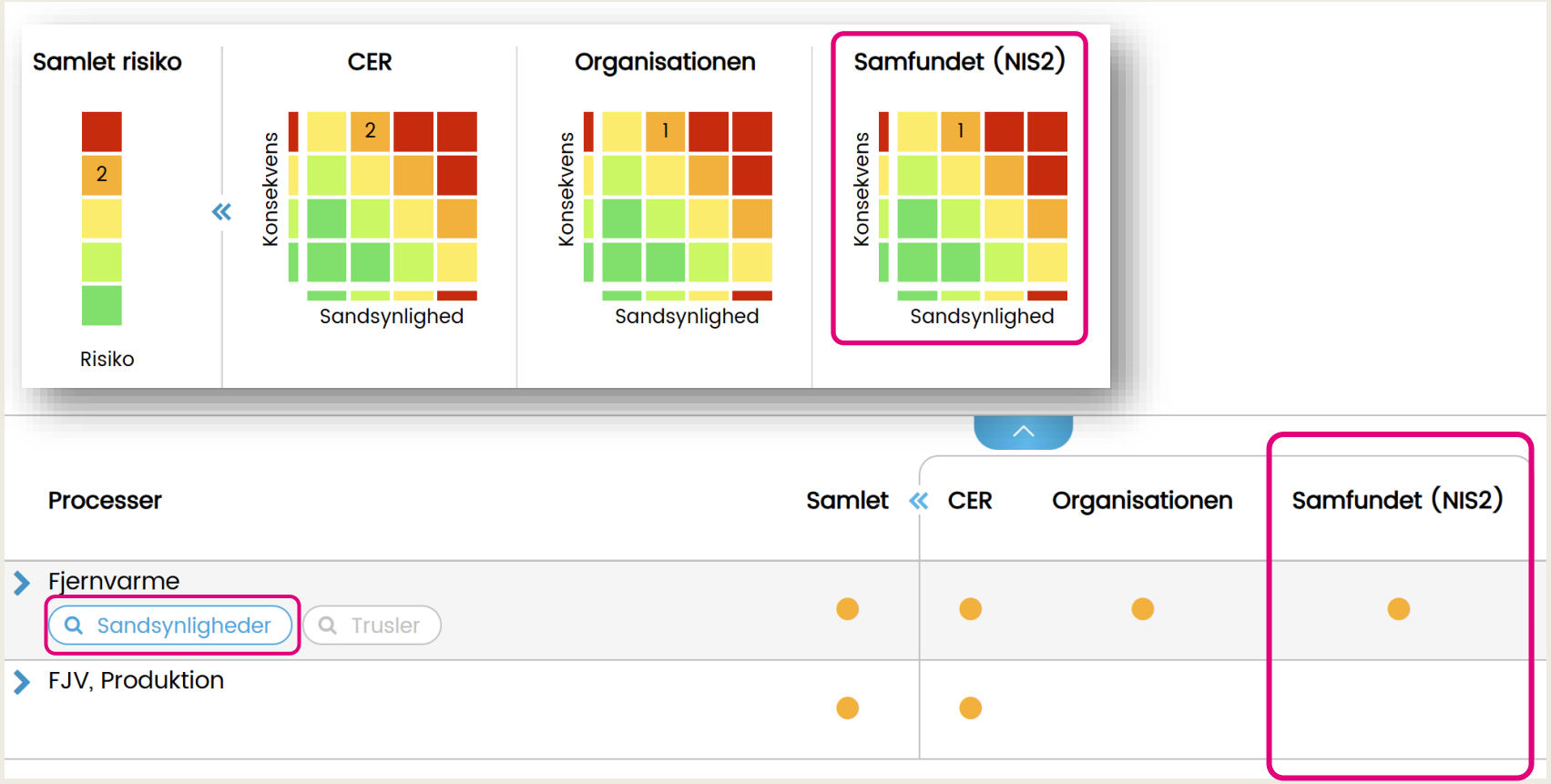
	F	I	T
Cyber-terror trusler	●	●	●
Hackerangreb (generelt) på systemet	●	●	●
Fejlede sikringsforanstaltninger	●	●	●
Backup er mangelfuld eller ikke eksisterende, hvorfor informationer ikke kan r...			●
For mange medarbejdere har superbruger - (administrative rettigheder til f...	●	●	●
Fratrådte medarbejderes adgang fjernes ikke, og vil derved kunne bruges til ...	●	●	●
Manglende eller mangelfulde organisatoriske sikringsforanstaltninger omkrin...	●	●	●
Medarbejdere har for mange rettigheder til forretningssystemet, eks. grundet ...			

Risikovurdering – ControlManager™

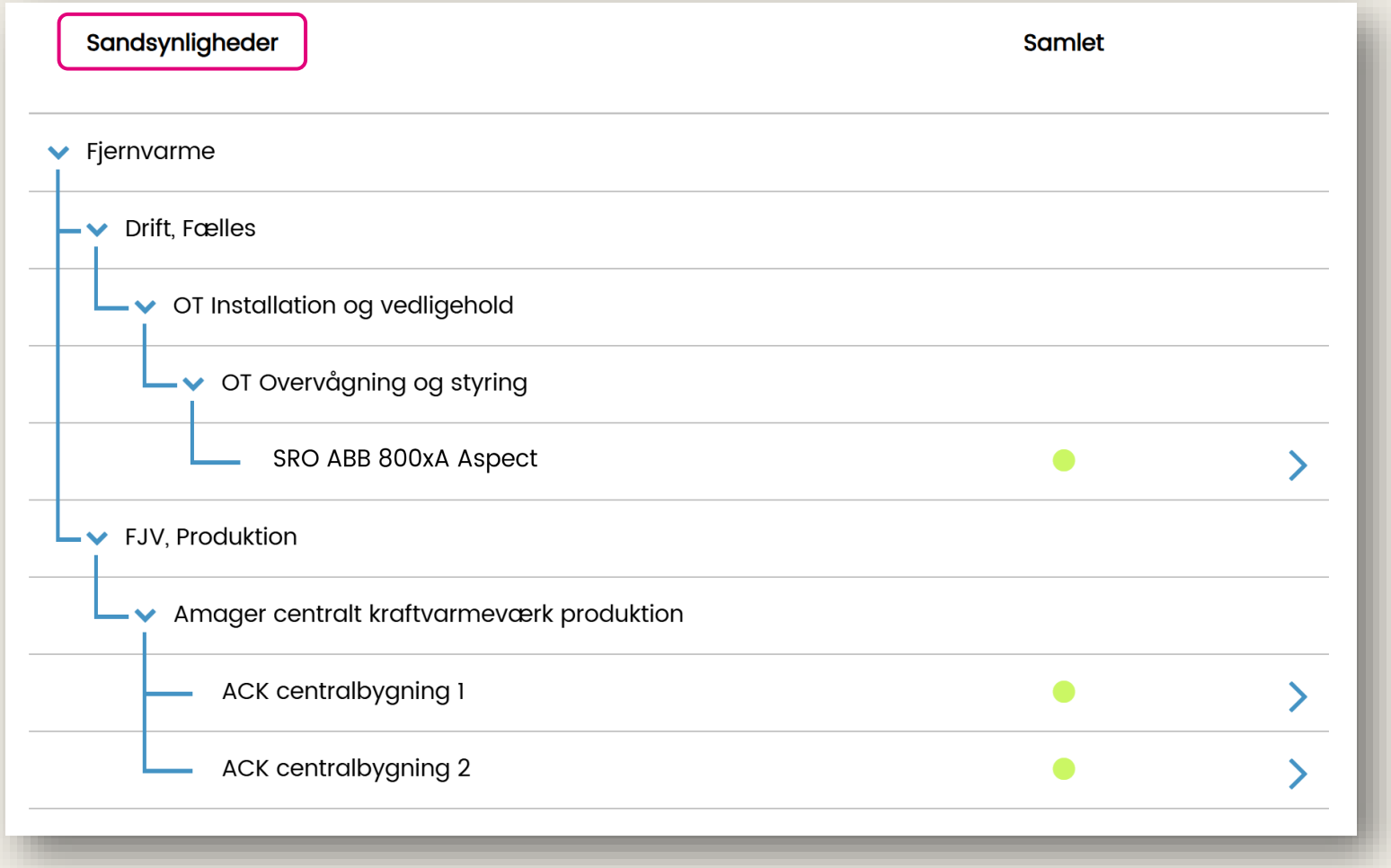
- I NIS2 er der fokus på at vurdere risici i et **samfundsmæssigt perspektiv**
- **Integrere** i de ”gængse” analyser
  - Hvad er risici for vores organisation?
  - Hvad er risici for den registrerede? (GDPR)
  - Hvad er risiciene mod vores infrastruktur? (CER)



Risikovurdering i forskellige perspektiver – ControlManager™



Drill-down



CONTROL™ MANAGER by SISCON

SRO ABB 800xA Aspect

Trusselstabel

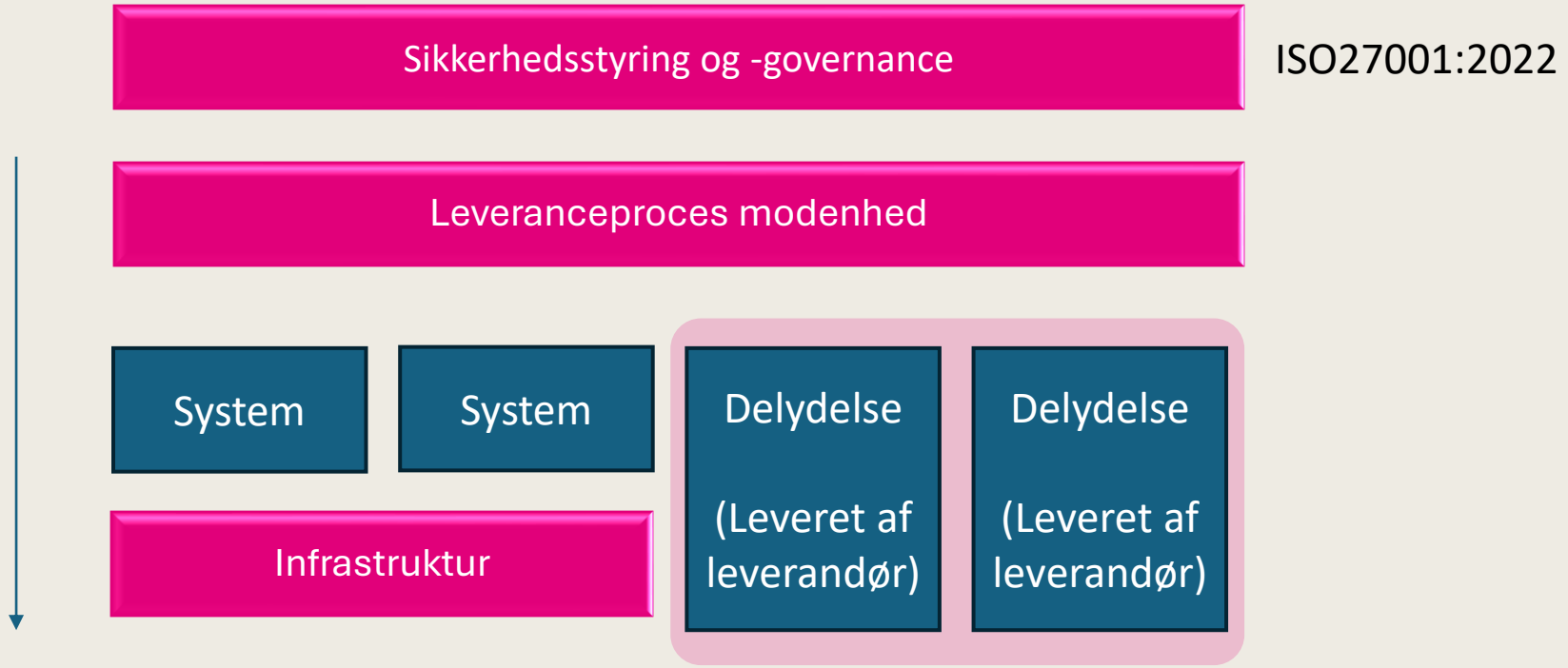
	F	I	T
Cyber-terror trusler	●	●	●
Hackerangreb (generelt) på systemet	●	●	●
Fejlede sikringsforanstaltninger	●	●	●
Backup er mangelfuld eller ikke eksisterende, hvorfor informationer ikke kan r...			●
For mange medarbejdere har superbruger - (administrative rettigheder til f...	●	●	●
Fratrådte medarbejderes adgang fjernes ikke, og vil derved kunne bruges til ...	●	●	●
Manglende eller mangelfulde organisatoriske sikringsforanstaltninger omkrin...	●	●	●
Medarbejdere har for mange rettigheder til forretningssystemet, eks. grundet ...			

Men hvad med gap/modenhedsanalyserne fra tidligere?

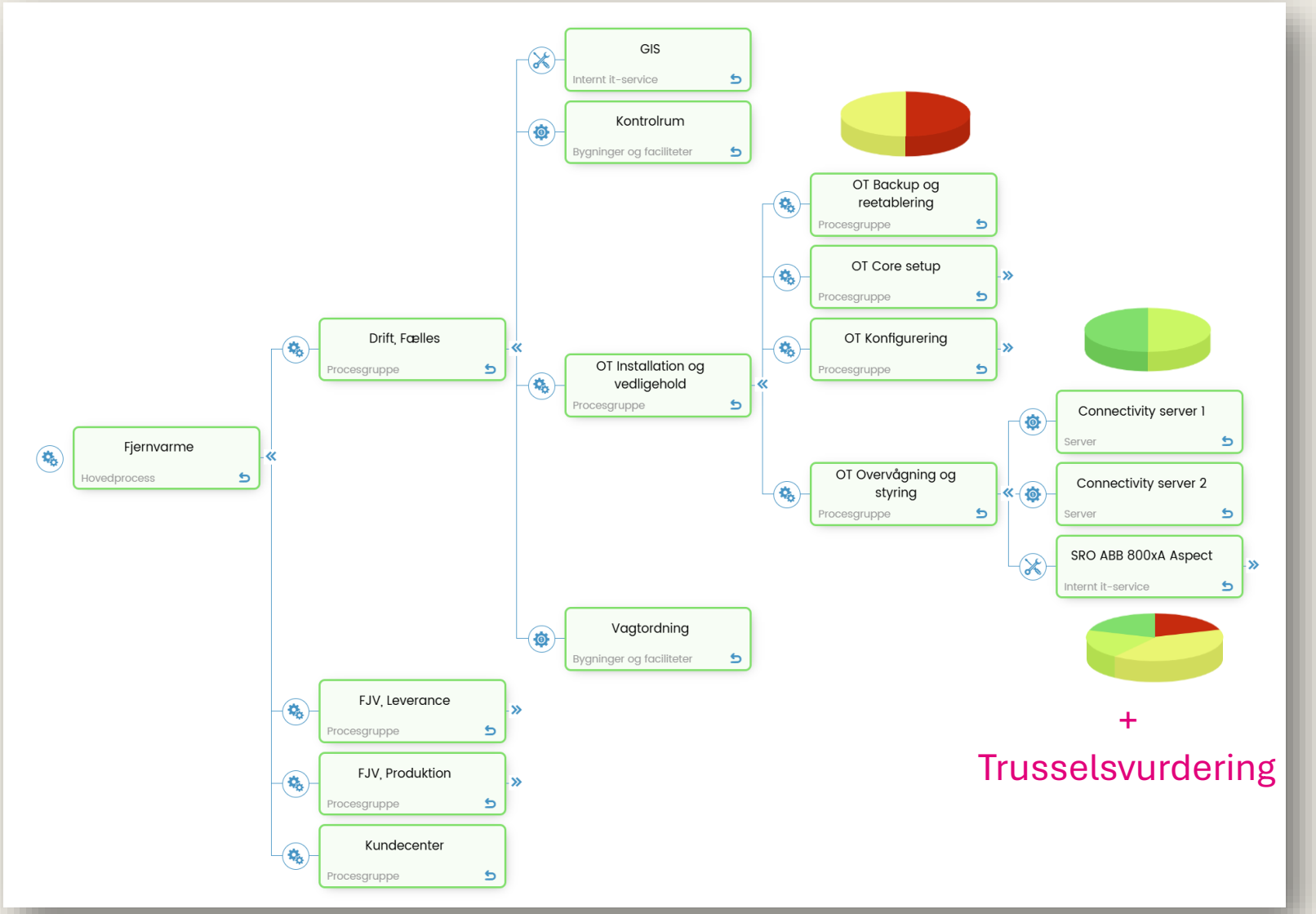
Gap-analyser

Generelle krav fra ISO27001-Anneks

CIS8
IEC 62443
NIST CSF



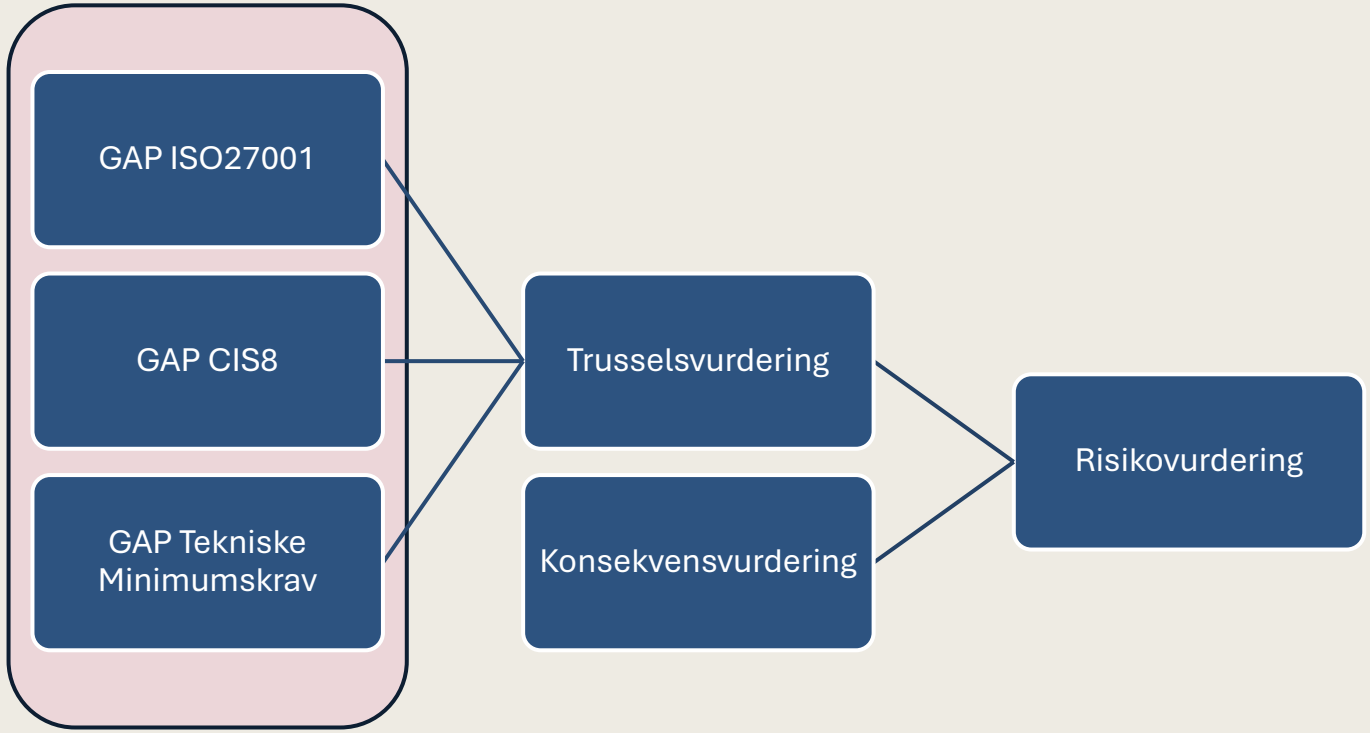
GAP-indlejret i trusselsvurdering?



CONTROL™ MANAGER by SISCON

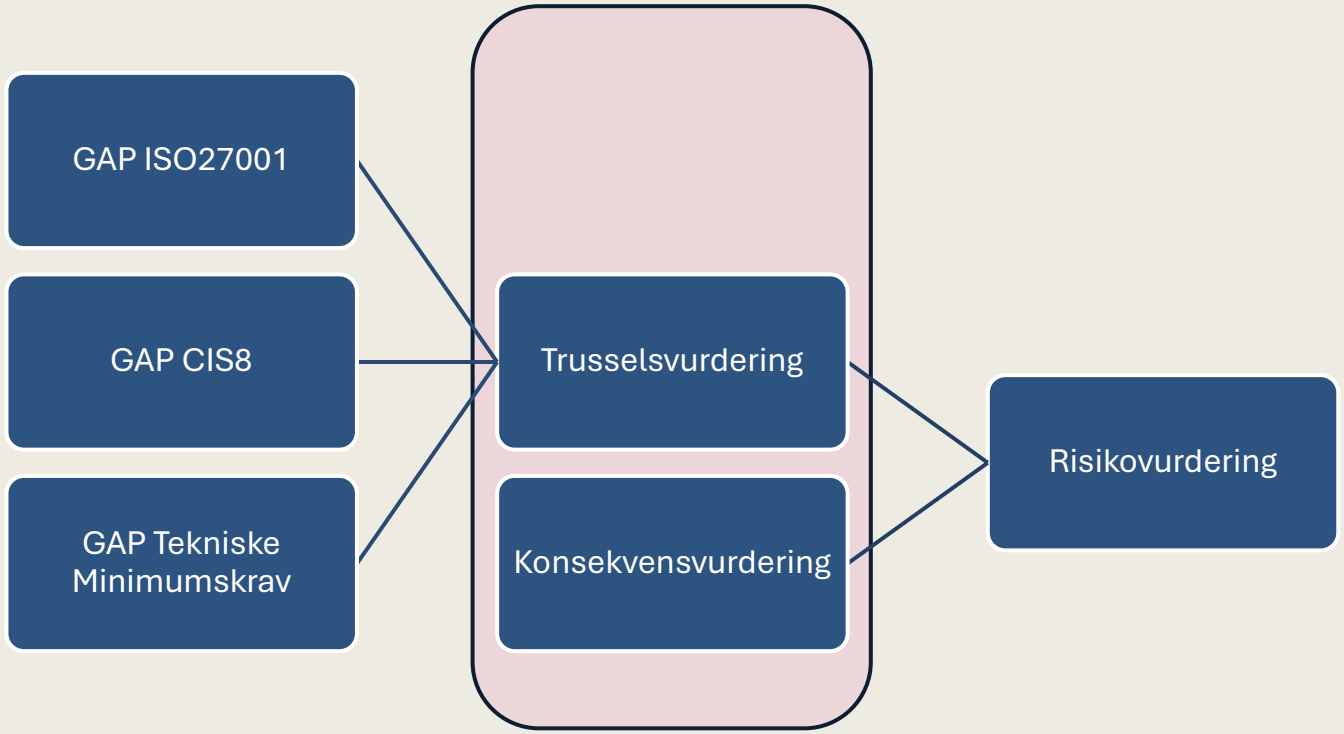
Genbrug af GAP-resultater til basisvurdering af trusler

Hvilke foranstaltninger
har vi implementeret?



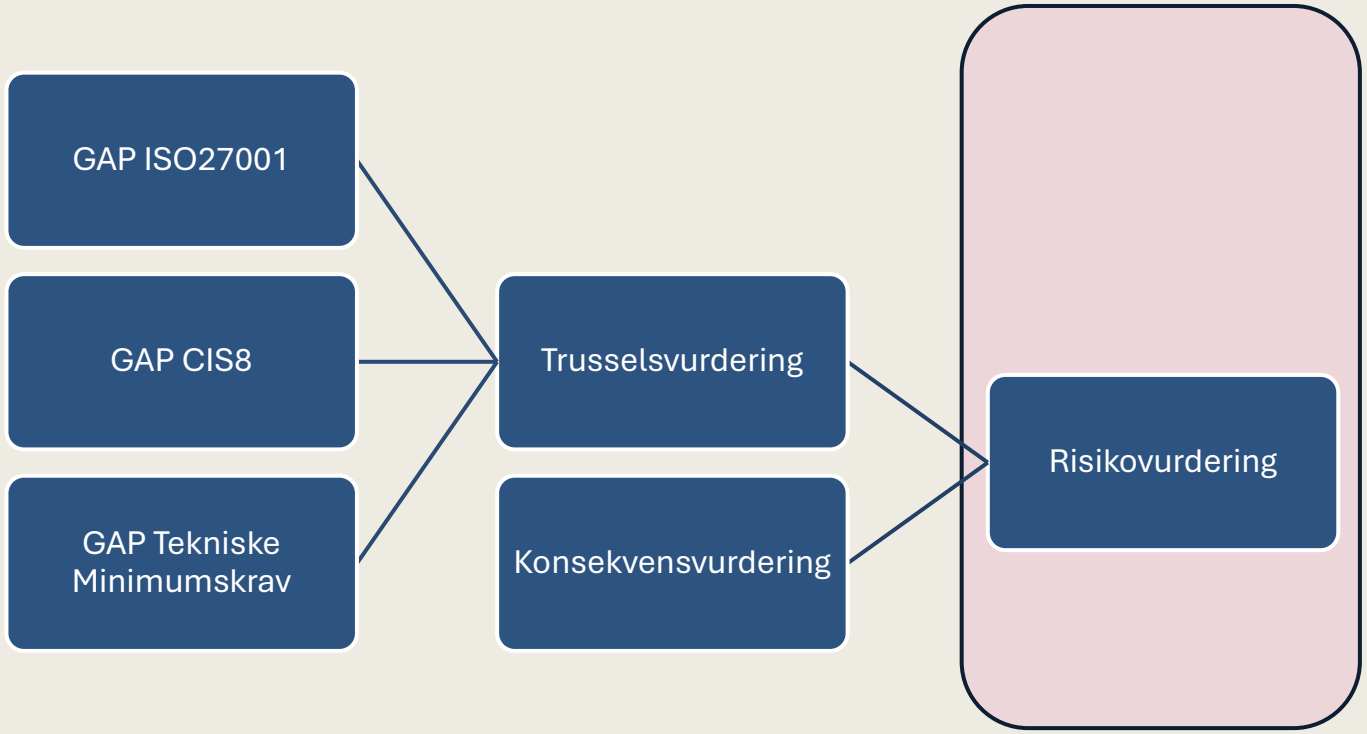
Genbrug af GAP-resultater til basisvurdering af trusler

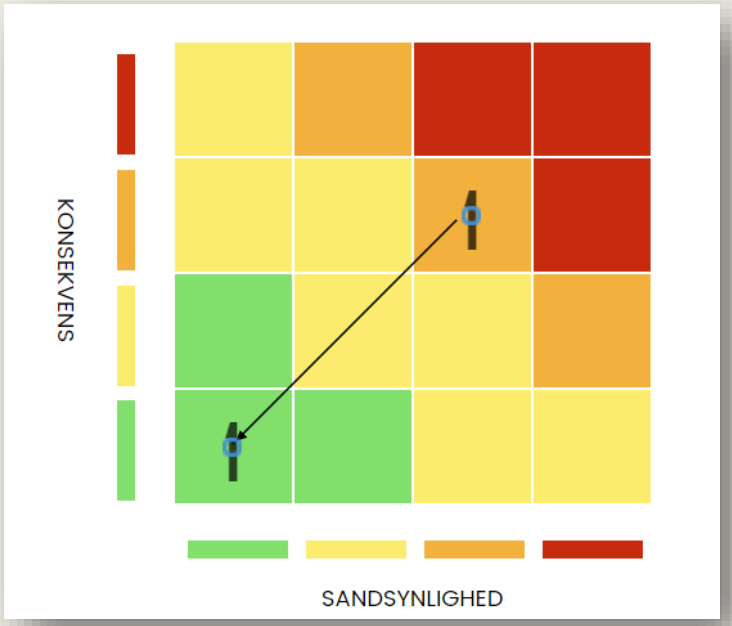
Hvilke trusler imødegår
vores sikringsforanstaltninger?



Genbrug af GAP-resultater til basisvurdering af trusler

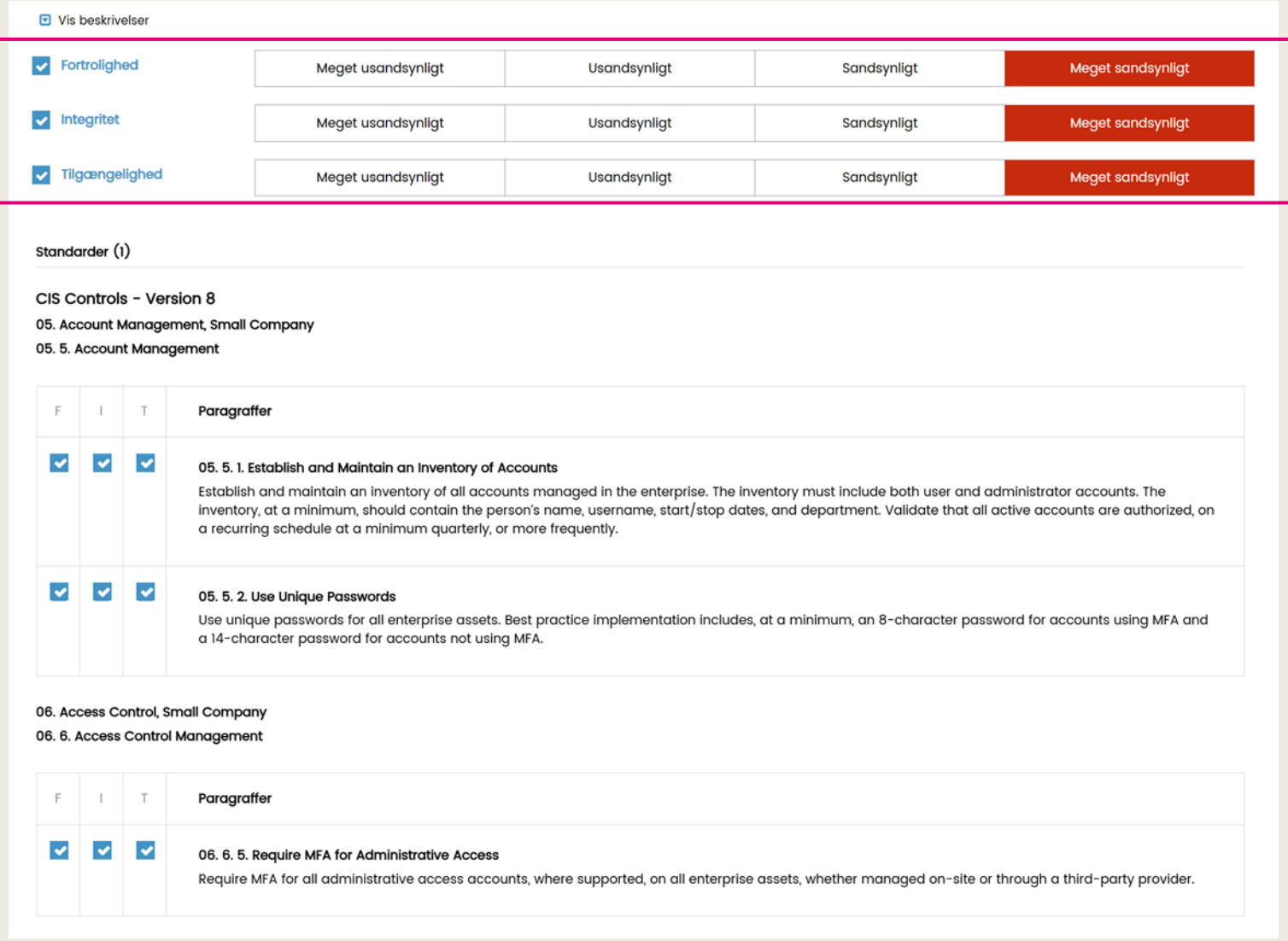
Hvordan påvirker det Risikovurderingen?





Trussel – ”Hackerangreb (generelt) på systemet”

Initial/iboende sandsynlighed



Trussel – ”Hackerangreb (generelt) på systemet”

Initial/iboende sandsynlighed

Vis beskrivelser

Fortrolighed	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt
Integritet	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt
Tilgængelighed	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt

Mitigerende sikringsforanstaltninger

Standarder (1)

CIS Controls - Version 8

05. Account Management, Small Company

05. 5. Account Management

F	I	T	Paragraffer
☑	☑	☑	**05. 5. 1. Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
☑	☑	☑	**05. 5. 2. Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

06. Access Control, Small Company

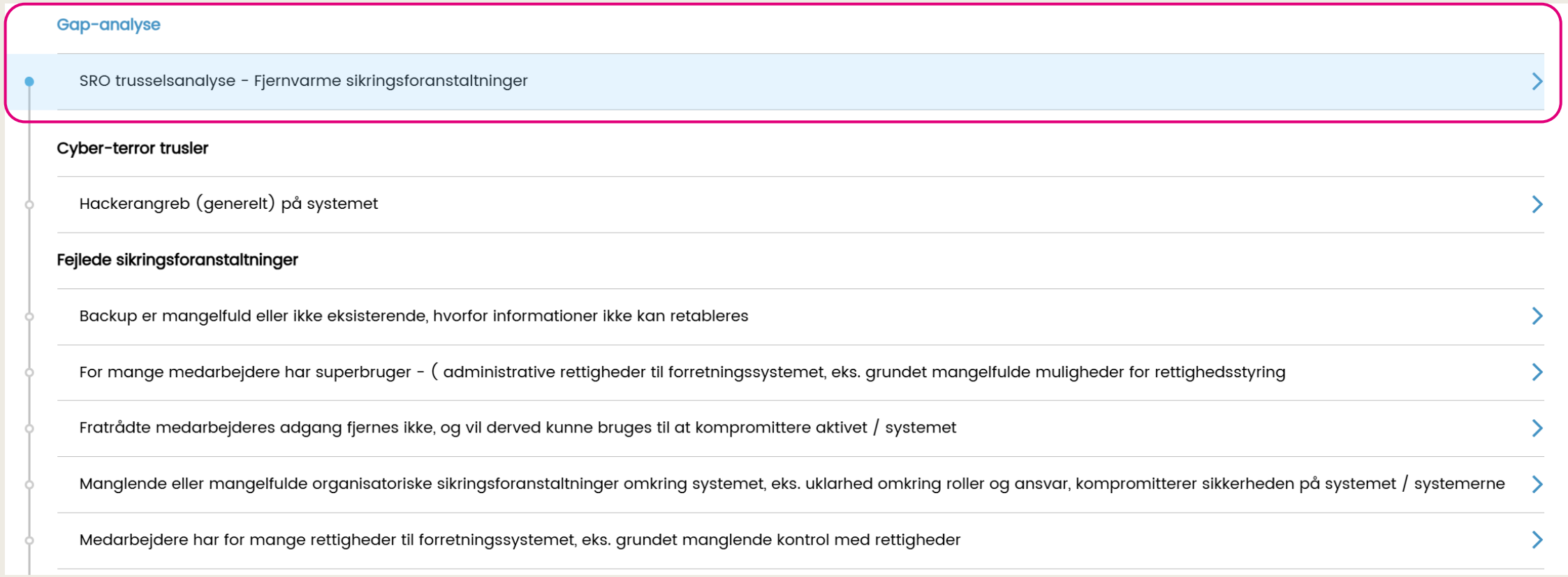
06. 6. Access Control Management

F	I	T	Paragraffer
☑	☑	☑	**06. 6. 5. Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

SISCON

Trusselsbesvarelsen består af to dele

GAP



GAP analyse

05. Account Management, Small Company

05. 5. Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

05. 5. 1. Establish and Maintain an Inventory of Accounts ! (50%)

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Compliance:
2 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
50%

05. 5. 2. Use Unique Passwords ! (75%)

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.

Compliance:
3 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
75%

06. Access Control, Small Company

06. 6. Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

06. 6. 5. Require MFA for Administrative Access ✔

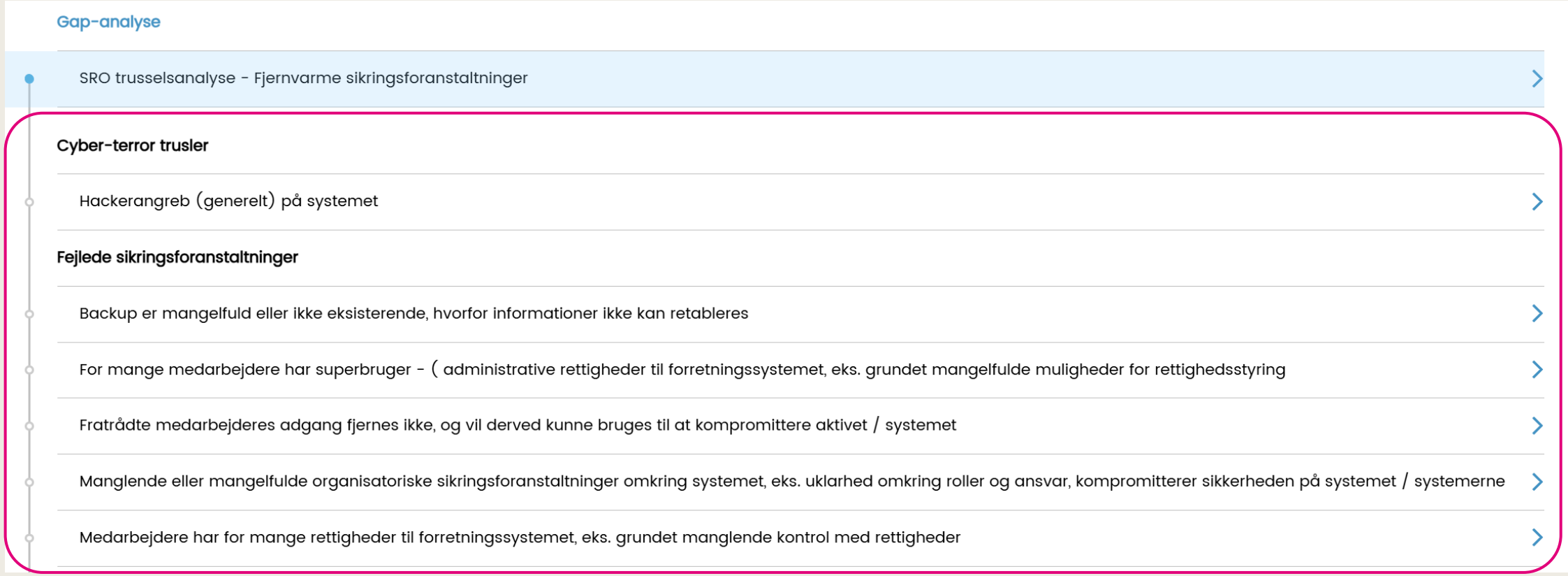
Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

Compliance:
4 of following: Policy, Implemented, Automated, Reported
Efterlevelsesgrad:
100%

CONTROL™ MANAGER by SISCON

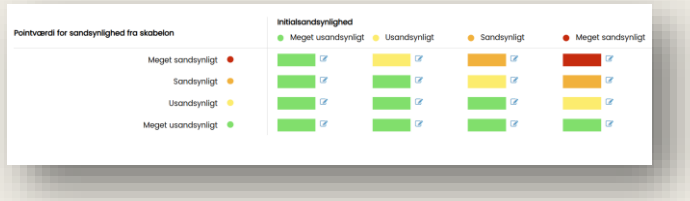
Trusselsbesvarelsen består af to dele

Trussels-vurdering



En gennemført analyse

Beregnet sandsynlighed



Gap-analyse svar (point)

Hackerangreb (generelt) på systemet

Initial sandsynlighed

Fortrolighed ?

Initialsandsynlighed				Meget sandsynligt
Beregnet sandsynlighed		Usandsynligt		
Vurderet sandsynlighed	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt

Kommentarer

Manuelt angivet sandsynlighed

Integritet ?

Initialsandsynlighed				Meget sandsynligt
Beregnet sandsynlighed		Usandsynligt		
Vurderet sandsynlighed	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt

Kommentarer Tilføj kommentarer...

Tilgængelighed ?

Initialsandsynlighed				Meget sandsynligt
Beregnet sandsynlighed		Usandsynligt		
Vurderet sandsynlighed	Meget usandsynligt	Usandsynligt	Sandsynligt	Meget sandsynligt

Kommentarer Tilføj kommentarer...

Gap-analyse: SRO trusselsanalyse - Fjernvarme sikringsforanstaltninger Åbn

Standard: CIS Controls - Version 8

05. Account Management, Small Company

05. 5. Account Management

- **05. 5. 1. Establish and Maintain an Inventory of Accounts** (2 of following: Policy, Implemented, Automated, Reported)
- **05. 5. 2. Use Unique Passwords** (3 of following: Policy, Implemented, Automated, Reported)

06. Access Control, Small Company

06. 6. Access Control Management

- **06. 6. 5. Require MFA for Administrative Access** (4 of following: Policy, Implemented, Automated, Reported)

07. Vulnerabilities, Small Company

07. 7. Continuous Vulnerability Management

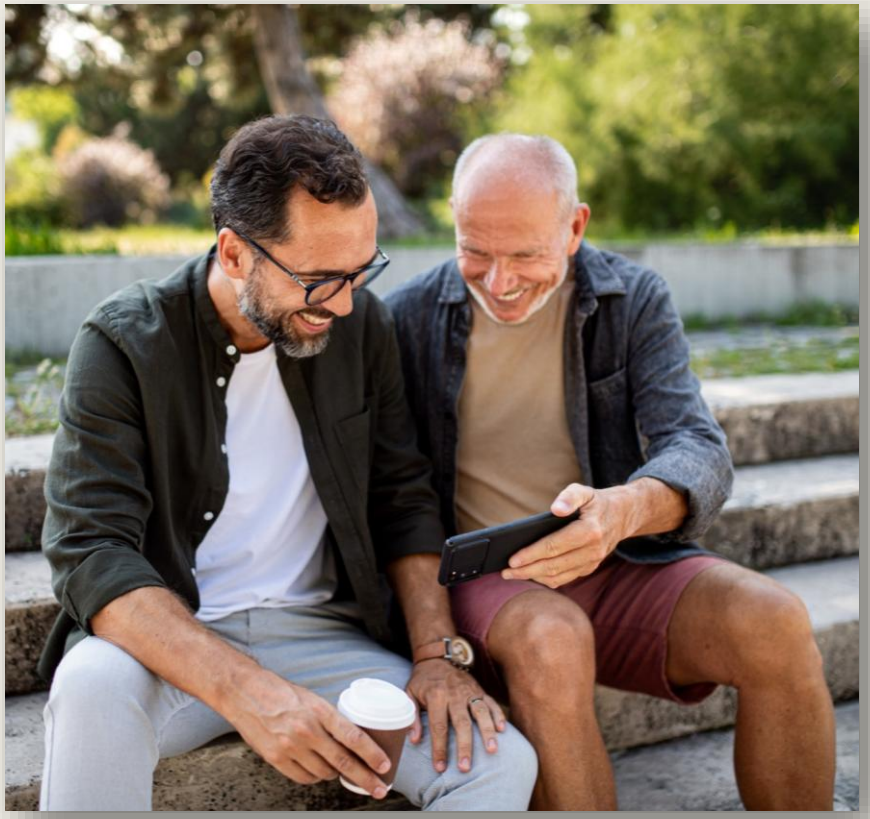
- **07. 7. 1. Establish and Maintain a Vulnerability Management Process** (2 of following: Policy, Implemented, Automated, Reported)
- **07. 7. 3. Perform Automated Operating System Patch Management** (3 of following: Policy, Implemented, Automated, Reported)

Fordele

- Systemejer
  - fortsætter med at tale et **"sprog"** som systemejer/-ansvarlig forstår
    - **Ingen sandsynligheder**
    - **Vurdering** af **implementerede foranstaltninger**
  - **Genbrug** af analyser, som de måske alligevel skal bruge

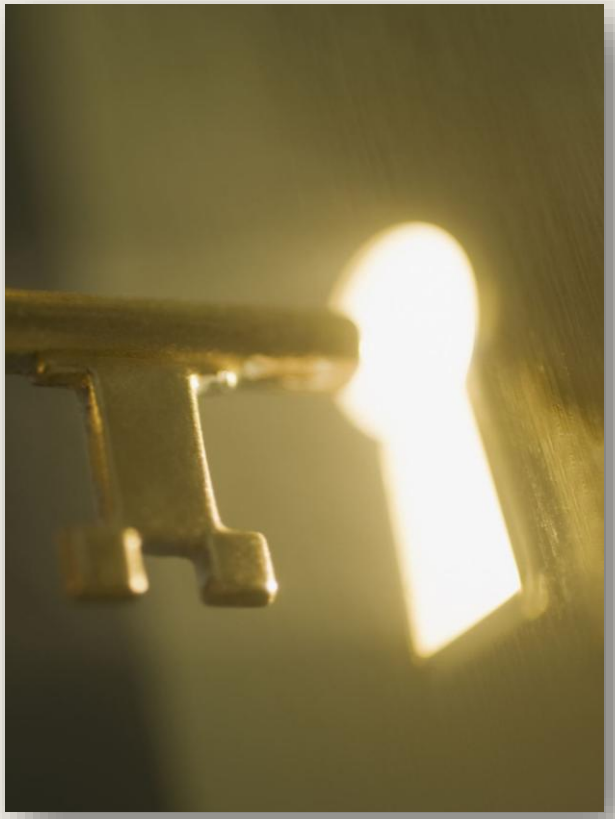
- Risikomanager/Sikkerhedsansvarlig
  - bedre vurderinger, da sikringstiltag dokumenteres
  - godkende/afvise trusselsbilledet eller tilføje manuel værdi

- Vi kan løbende følge udviklingen i styrken af de implementerede sikringsforanstaltninger



Key takeaways

Key Takeaways



- Modenhedsvurderinger er et stærkt værktøj OG kan indarbejdes i risikovurderinger, enten **indlejret** eller **standalone**
- **Fokusér** på det kritiske og **skab overblik**
  - over **leverancer** og **it-/ot-understøttelsen**
- **Brug modenhedsvurderinger som sprog** sammen med systemansvarlige, det **kan give fordele** frem for sandsynlighedsvurderinger
- Tænk **genbrug og perspektiver** når der gennemføres risikovurderinger

SISCON

GRC - samlet i én løsning

ControlManager™
- Organisering
- Styring
- Drift og opfølgning
- Overblik og årshjul

ISMS
- Politikker – ISO27xxx
- Roller og ansvar
- Kontroller
- Efterlevelse (SOA)

EU-GDPR
- Art. 30 fortegnelse
- Risikoanalyse/DPIA
- Tilsyn med databehandlere

Risikovurdering
- Konsekvensanalyse
- Sårbarhedsanalyse
- Operational risk
- Overblik over risici

Opfølgning
- Kontroller
- Indsatser
- Hændelser
- Revision

Beredskab
- Beredskabsplan
- Forretningsberedskab
- IT-beredskab
- Beredskabstest

SISCON
... styrker din position

NIS2 / ISO27001 implementering - Det vi hjælper vores kunder med

- Modenhedsvurderinger
  - Udarbejdelse af projektplan(er)
  - Design og implementering af NIS2 sikringstiltag (Ikke-tekniske)
- ISO27001
  - Design og Implementering af ledelsessystem
  - Design og Implementering af kontrolkatalog
- Risikostyring
  - Risikovurderinger
  - Enterprise Risk Management
- Beredskab
  - Beredskabsplaner
  - Nød- / Genetalberingsplaner
  - Beredskabstest
- Opbygning af **multidimensional compliance** ☺

TAK FORDI I LYTTEDE

Få mere information på:

succes@siscon.dk

www.siscon.dk

Tlf.: +45 70 232 231

... styrker din position