CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Robusthed i digitale forsyningskæder: Cybersikkerhed, cases og scenariearbejde

29. april 2026

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Styre- og referencegruppe

Styregruppen

Marianne Holmer Dekan, **SDU**, forperson i styregruppen

Pernille Kræmmergaard, CEO **DIX2**

Andreas Holbak Espersen, Branchedirektør **DI**

Kristian Fischer, **KFISCH**

Søren Vammen, CEO **Zoriac**

Referencegruppen

Henrik Findahl Brodersen, Acting Director, **SAMSIK**

Berit Aadal, Chefkonsulent, **Dansk Standard**

Morten Bjørn Hansen, CEO **Business Kolding**

Zaynab Al-Hussaini, Manager, **Capgemini Invent**

Joachim Finkielman, Underdirektør, **DI**

Tina Højrup Kjær Projektleder, **Odense Robotics**

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Action Call om cybersikre værdikæder

- Flere og flere angreb
- Internt fokus, ekstern trussel
- Voksende leverandørfokus (NIS2)
- SMV'erne kan blive de store tabere
- Komplekst område og få løsninger

Cyberportefølje

- Cybersikkerhed og Forretningskontinuitet, **SDU og Forsvarsakademiet**
- Cyber Safe Robotics, **Odense Robotics**
- Cybersikre Fødevareværdikæder, **Food & Bio Cluster Denmark**
- Styrket cybersikkerhed for SMV'er, **Erhvervshus Midtjylland**
- Cybersikre forsyningskæder, **CBS**

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Rusland mistænkes for cyberangreb mod Tysklands regering

Phishing-angreb var Der er tale om såkaldte phishing-an- ger fra en konto, der udgav sig for at af parlamentsmedlemmernes

Stigning i cyberangreb presser smv'erne

'Man føler sig dybest set misbrugt': Ny rapport sætter fokus på konsekvenserne ved svindel

Da hackerne angreb, stod han i et indkøbscenter

Kun hver tredje virksomhed øver sig i cyberberedskab – og det er for lidt

Det vil være uærligt at påstå, at AI ikke vil ændre noget inden for cybersikkerhed

Boyan Milanov, seniorforsker med speciale i cybersikkerhed, AI Now Institute

Russiske hackere har pillet ved nettrafik i Europa

Berygtet hackergruppe har omdirigeret internettrafikken til egne servere, så de kunne følge med og stjæle kodeord, lyder advarslen fra britiske og tyske sikkerhedsmyndigheder.

Topledere advarer om mangel på digital indsigt

Ledere frygter cyberangreb og efterspørger arbejdskraft

Når trusselsniveauet stiger hastigt, pålægges virksomhederne indirekte byrder.

Avanceret AI-model øger risikoen for målrettede cyberangreb

Baggrund: SMV'er, digitalisering og sårbarhed

- SMV'er er stærkt afhængige af IT til drift, samarbejde og outsourcing
- Digitalisering gør processer hurtigere og mere omkostningseffektive
- Øger samtidig risikoen for cyberangreb og digitale sårbarheder
- Mange SMV'er er eksportafhængige → påvirkes af geopolitik og forsyningskæder
- Begrænset cybersikkerhedsviden gør dem særligt udsatte (f.eks. ransomware og IP-tyveri)

Projektets formål og målsætninger

Formål

- At øge forståelsen af cybersikkerhed, og hvordan cybersikkerhed bidrager til at skabe og vedligeholde konkurrencefordele blandt danske produktions-SMV'er.
- At forbedre niveauet af cybersikkerhed for danske produktions-SMV'er ved at identificere og adressere sårbarheder i deres forsyningskæder og efterfølgende identificere de evner, der er nødvendige for at håndtere disse sårbarheder.

Målsætninger

- At udvikle open-source software til supply chain resilience
- At identificere trusselsscenarier for SMV’ers drift
- At udvikle operationelle værktøjer til at styrke cybersikkerhed

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Program

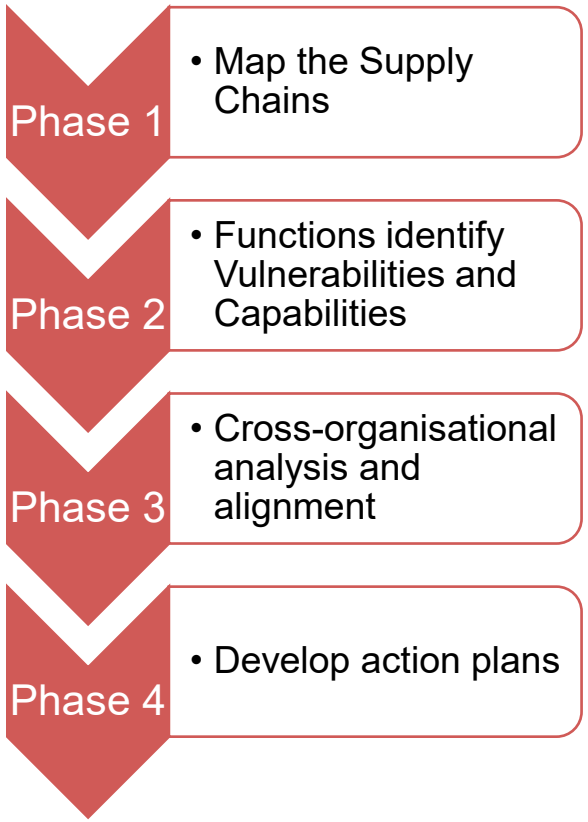
14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	**En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU**
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

Virksomhedsinvolvering i tre trin

Gennemført to runder med virksomhedsinvolvering

1. Supply Chain Resilience Process model
   → Formål: At skabe en tværorganisatorisk forståelse af virksomhedens forsyningskæder (fra kunder, lagrer, Distribution, produktion, indkøb og øvrige tredjeparter)
2. Træningsdage rundt i landet (Aalborg, Hobro, Brande, Vejle, Middelfart, Hvidovre og Kgs. Lyngby)
   → Formål: At afdække forståelser af cybersikkerhed og arbejde med fremtidsscenarier
3. Fælles træningsdag på SDU i Odense med fokus på cybersikkerhed, digitalisering og cloud computing, geopolitik, supply chain risk management og pentesting.

Process for Supply Chain Resilience



Main features of the process model

Stentoft, Mikkelsen & Kjær (2023)

→ Guides the creation of sound action plans to increase resilience based on cross-organisation alignment regarding supply-chain vulnerabilities and capabilities to mitigate them.

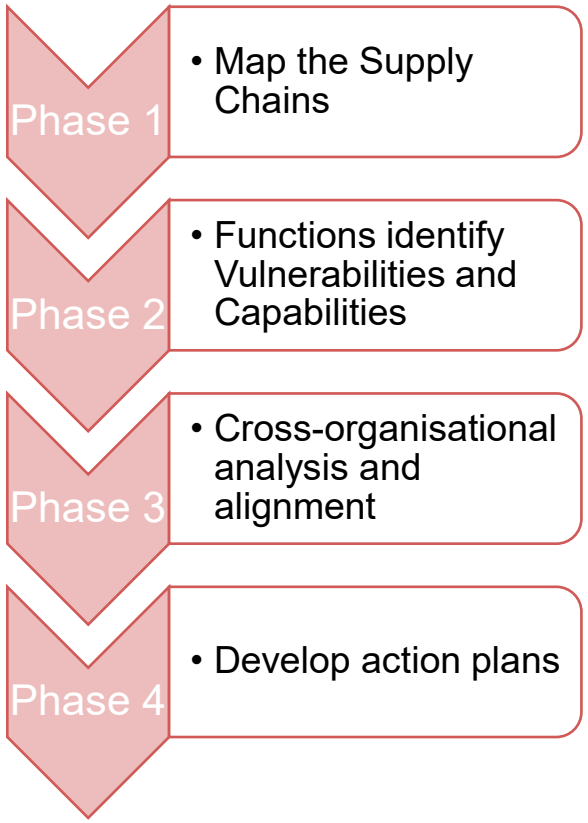
→ Designed to be lightweight and agile, tailored for small teams and SMEs

Terminology

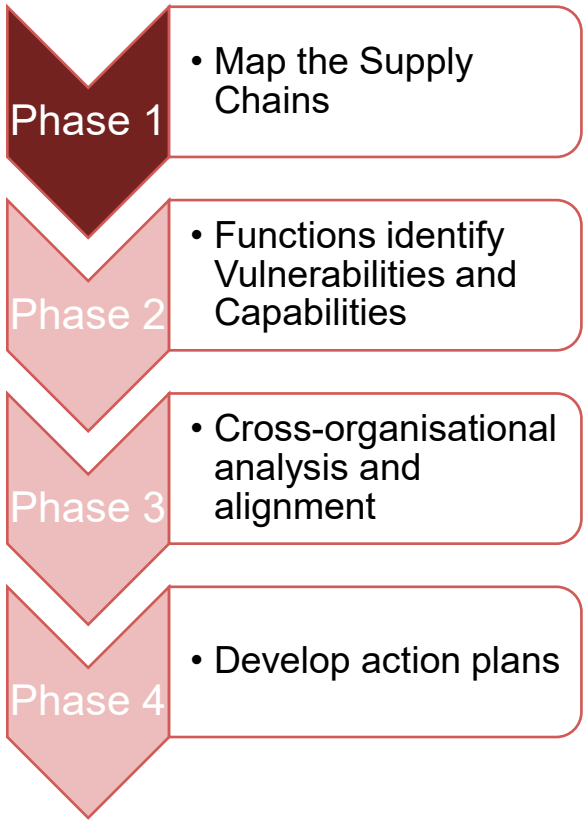
→ Vulnerabilities
- → Supply chain vulnerabilities refer to the risks that arise from disruptions within the supply chain due to inadequate security measures. (Jüttner et al. 2003)
- → These vulnerabilities constitute the fundamental factors that render a company susceptible to disruptions, including intentional threats and resource scarcity (Pettit et al., 2013).

→ Capabilities
- → Capabilities can be understood as the qualities that enable a company to anticipate and overcome disruptions (Pettit et al., 2010).
- → These capabilities can take various forms, such as preventing disruptions, mitigating their impact, and/or enabling the company to adapt.

Process for Supply Chain Resilience



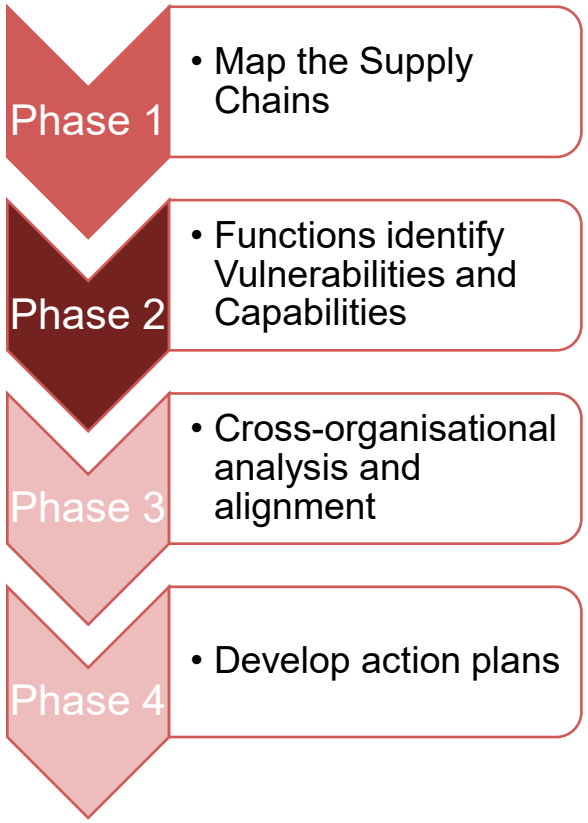
Process for Supply Chain Resilience



Phase 1

→ Map the company's supply chain based on concrete facts (e.g., customers, distribution channels, storage locations, order types, production methods, sourcing routes, suppliers, lead times and capital commitments).
→ Sales, production, purchasing, finance, IT and product development.
→ Individual preparation: reading material (e.g., frameworks), reflection on the function perspective
→ Joint discussion: mapping guided by questionnaires

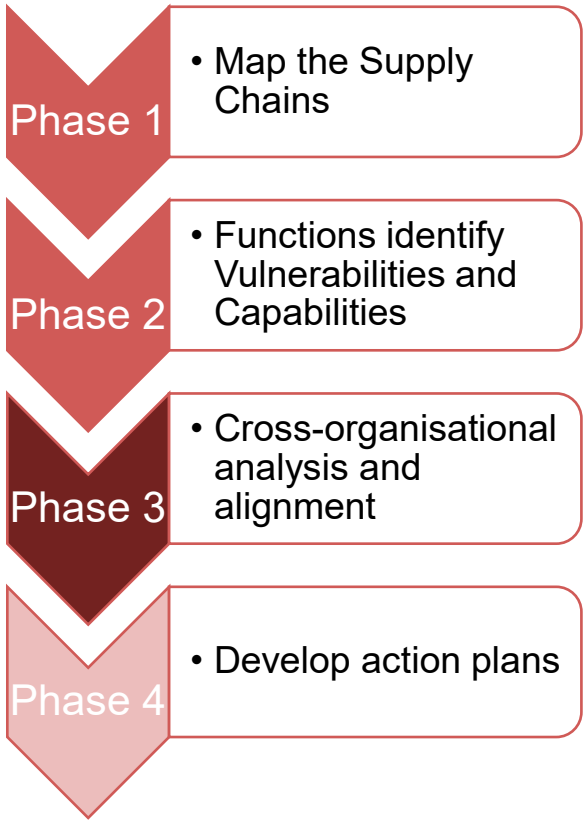
Process for Supply Chain Resilience



Phases 2 (function perspective)

→ Identify up to 10 vulnerabilities
→ Assess their perceived risk level (based on impact and likelihood)
→ For each vulnerability, identify up to 5 capabilities to mitigate it
→ For each capability assess the current and required capacity to mitigate

Process for Supply Chain Resilience



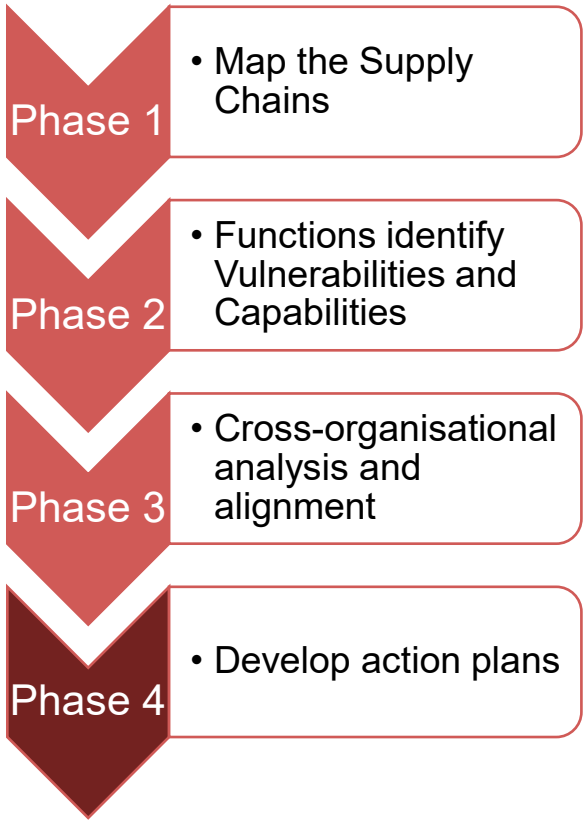
Phases 2 (function perspective)

→ Identify up to 10 vulnerabilities
→ Assess their perceived risk level (based on impact and likelihood)
→ For each vulnerability, identify up to 5 capabilities to mitigate it
→ For each capability assess the current and required capacity to mitigate

Phases 3 (cross-organisation alignment)

→ Representatives of each function jointly review the result of Phase 2
→ Repeat Phase 2 from a cross-organizational perspective to produce a joint assessment of the top vulnerabilities and the status of capabilities to mitigate them.

Process for Supply Chain Resilience



Phase 4

→ Develop concrete action plans to eliminate or reduce the prioritized vulnerabilities.
→ Sales, production, purchasing, finance, IT and product development.
→ Reports from Phases 2 and 3, reading material, action plan templates

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Digital Tool for executing the SCR Process

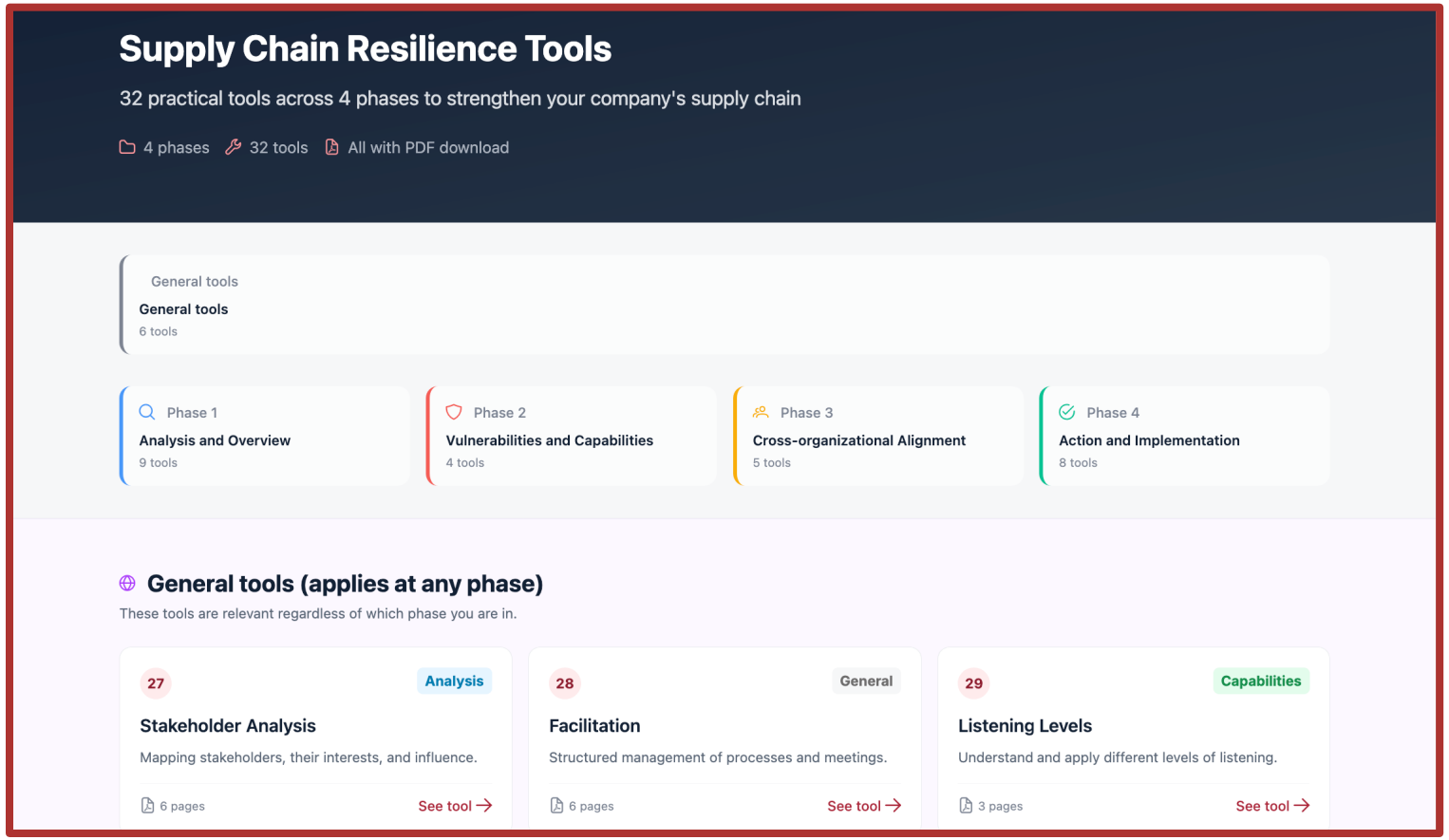
Phase 1
- Map the Supply Chains

Phase 2
- Functions identify Vulnerabilities and Capabilities

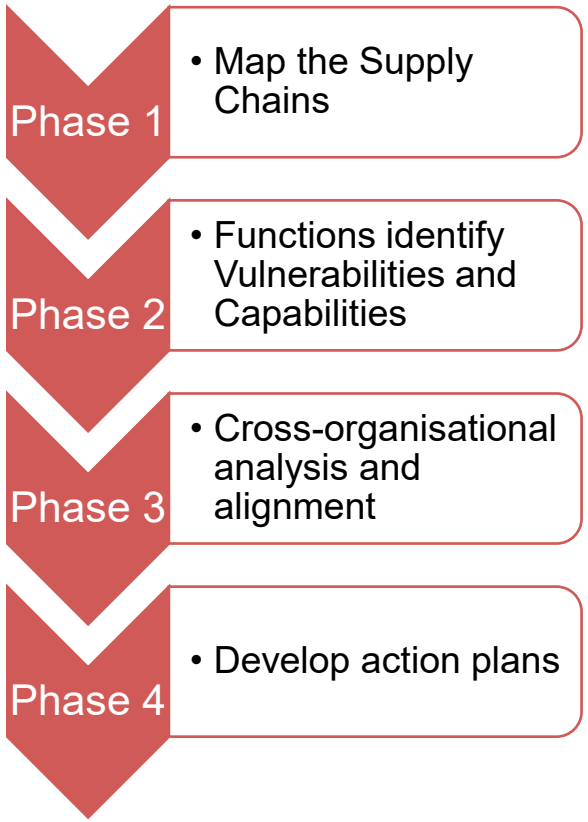
Phase 3
- Cross-organisational analysis and alignment

Phase 4
- Develop action plans

Web portal to support using the SCR Process Model



Digital Tool for executing the SCR Process



Web portal to support using the SCR Process Model

→ Templates, checklists, video tutorials, and preparatory reading material

→ Web application

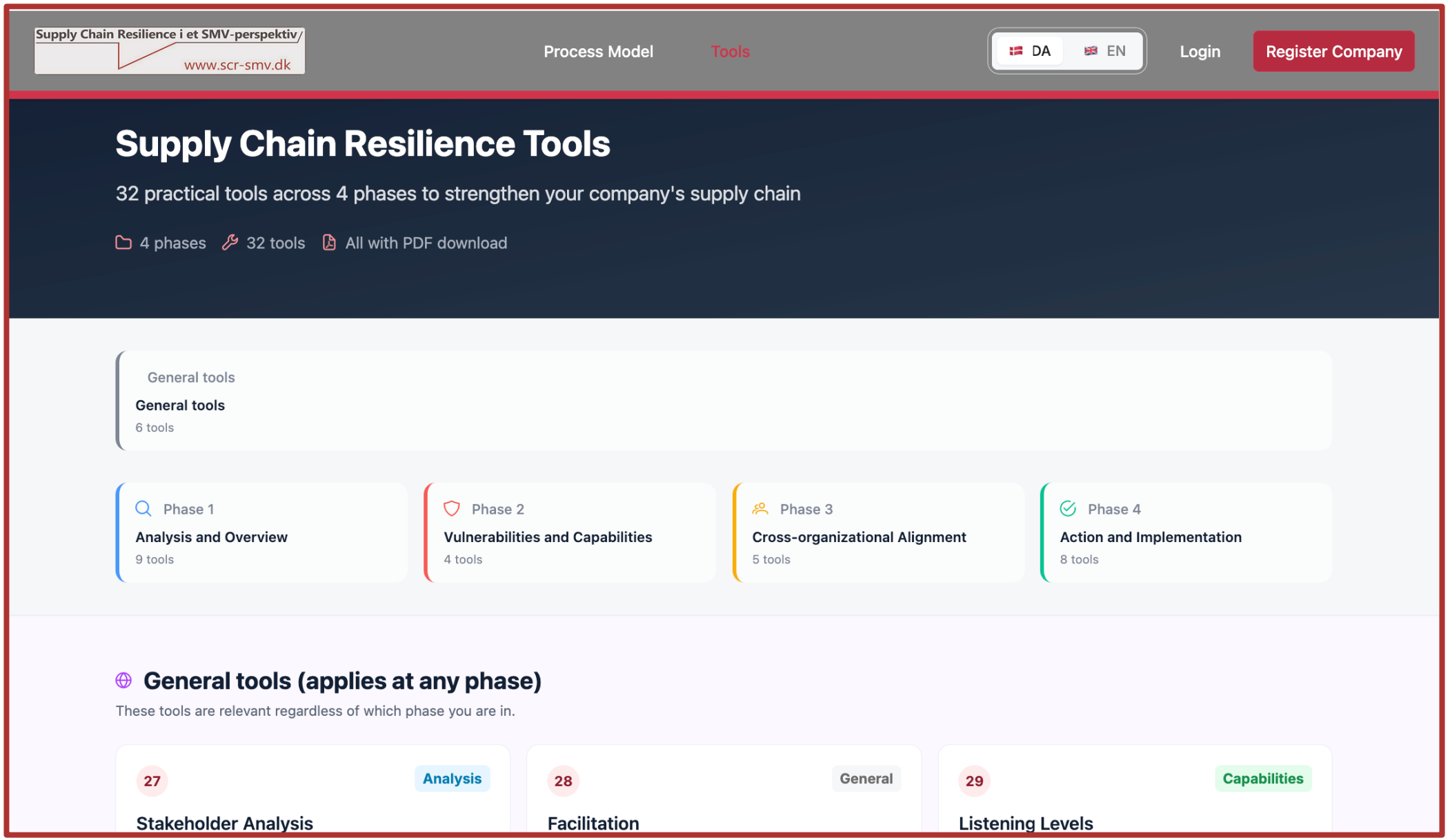
- → Automated digital workflow guiding the cross-function team progress
- → Structured surveys of vulnerabilities and capabilities
- → Interactive reports and analyses by function and organisation (cross-functional)
- → Allows to repeat the process periodically and track changes over time

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET



27 Analysis

Stakeholder Analysis

Mapping stakeholders, their interests, and influence.

6 pages — See tool →

28 General

Facilitation

Structured management of processes and meetings.

6 pages — See tool →

29 Capabilities

Listening Levels

Understand and apply different levels of listening.

3 pages — See tool →

30 General

Effective Meetings

Plan and conduct effective meetings.

7 pages — See tool →

31 Capabilities

Change Competence

Build the ability to handle change.

5 pages — See tool →

32 Risk Assessment

Decision Traps

Identify and avoid typical decision-making biases.

11 pages — See tool →

Phase 1 · 1 day workshop + preparation

Analysis and Overview

Strategic analysis of the company and its supply chain

9 tools

Phase 2 · 1 day workshop

Vulnerabilities and Capabilities

Identification and assessment of risks and strengths

4 tools

Phase 3 · 1 day workshop

Cross-organizational Alignment

Shared understanding and uncovering blind spots

5 tools

Register Your Company

Complete the form below to register your company for the Supply Chain Resilience program.

1 Company Information — 2 Address Information — 3 Personal Information

Company Information

Enter your company's basic details

Company Name *

Enter company name

Company name is required

CVR Number *

Enter 8-digit CVR number

Invalid CVR number (must be 8 digits)

Industry *

Select industry

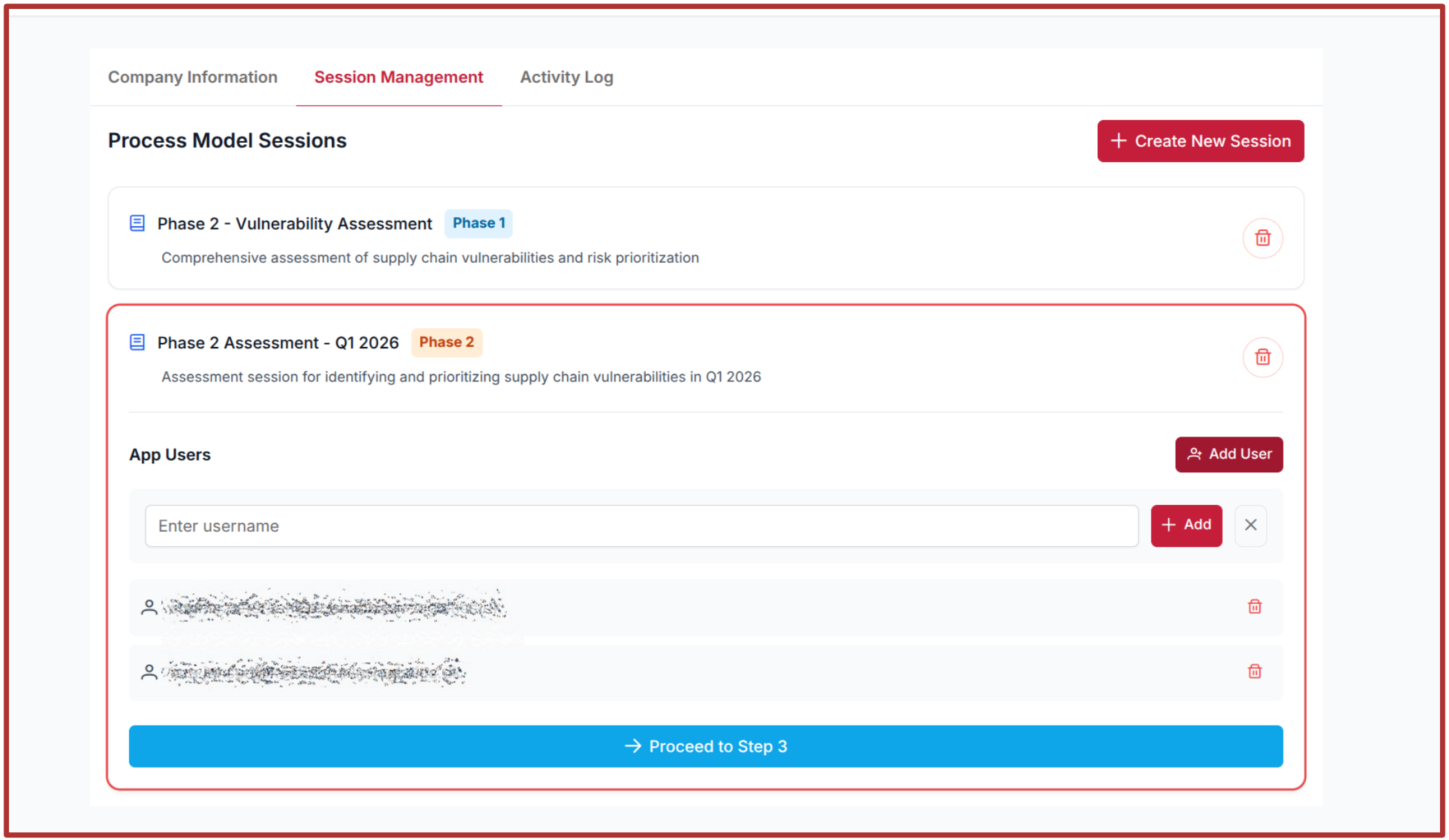
Industry is required

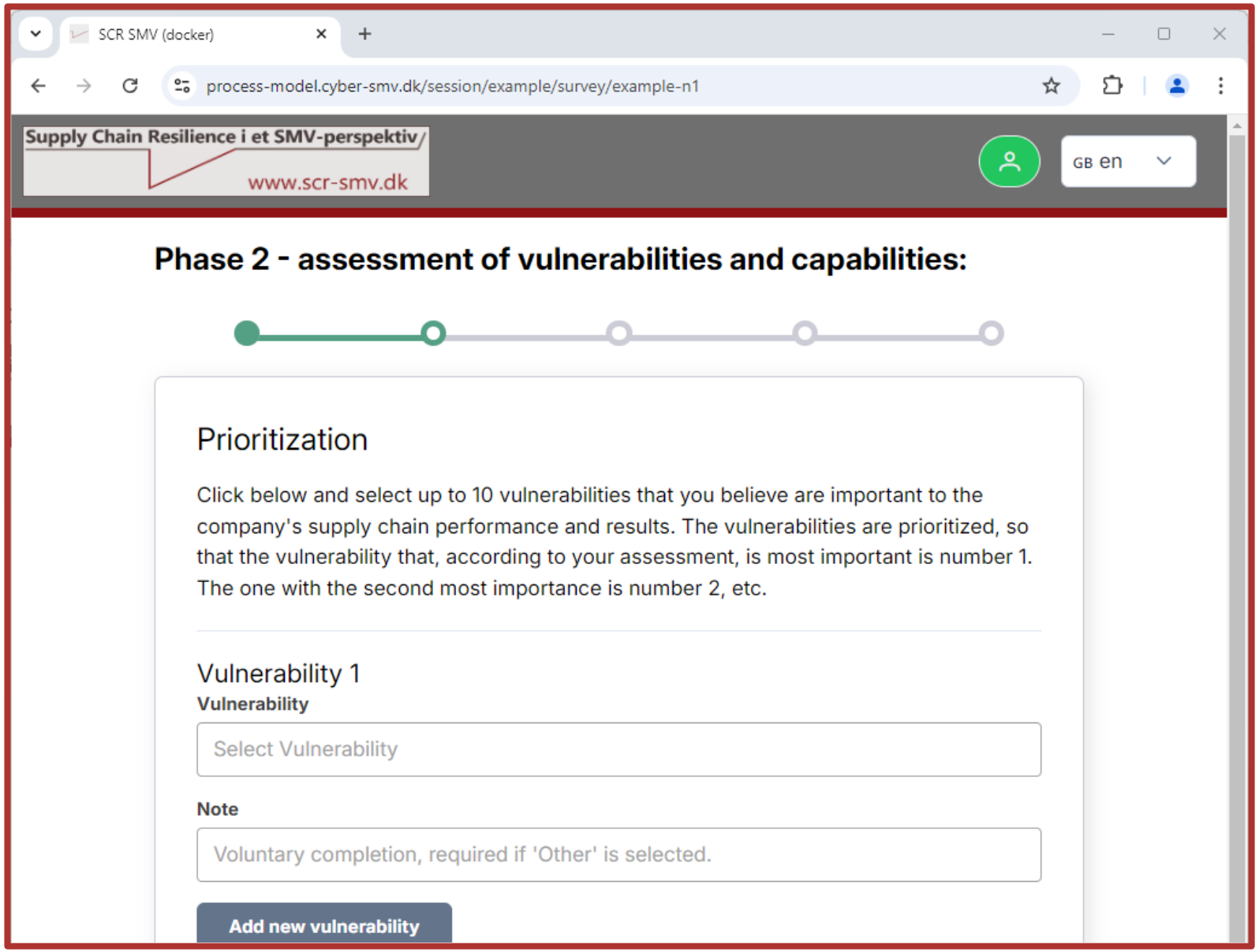
Company Size *

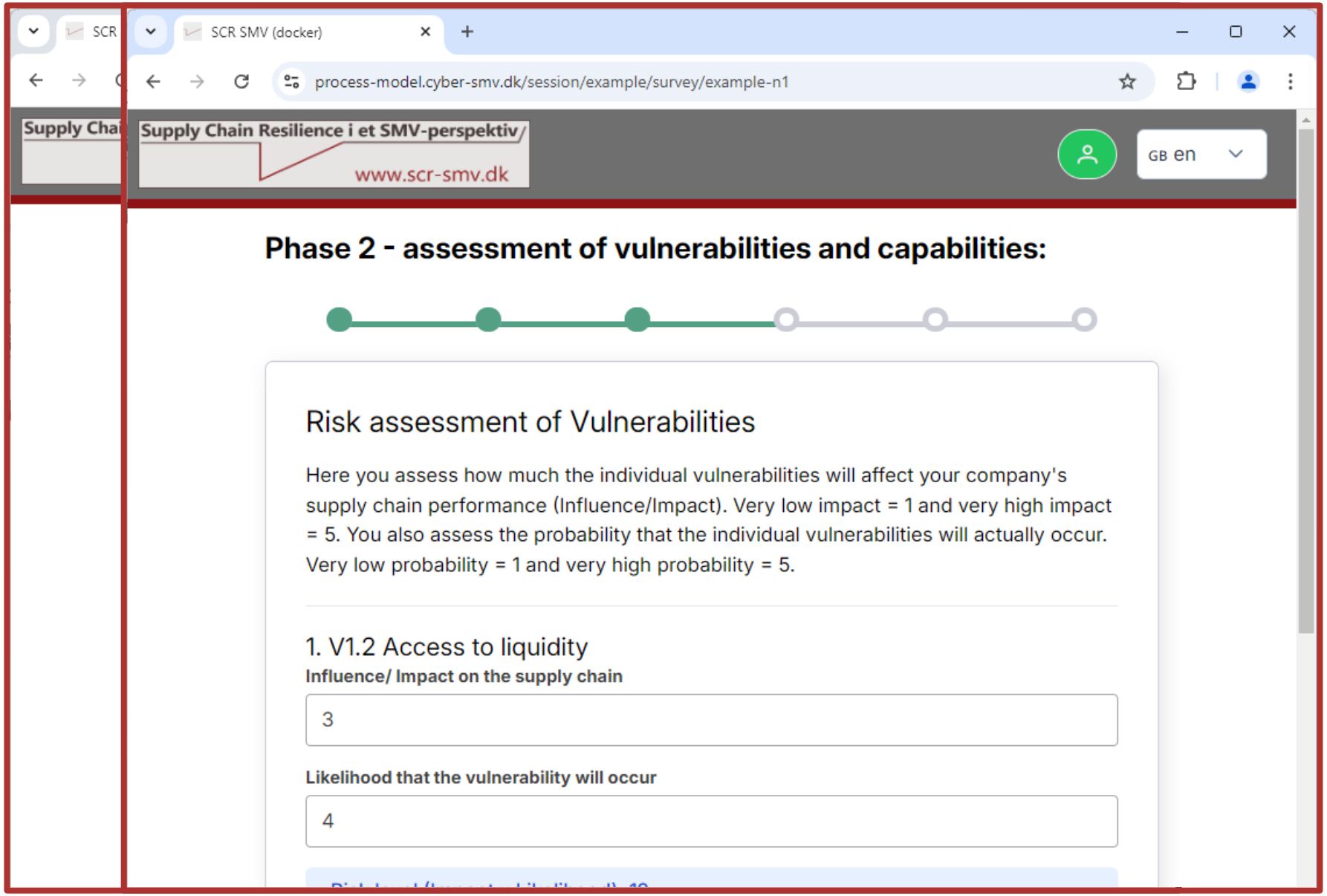
Select company size

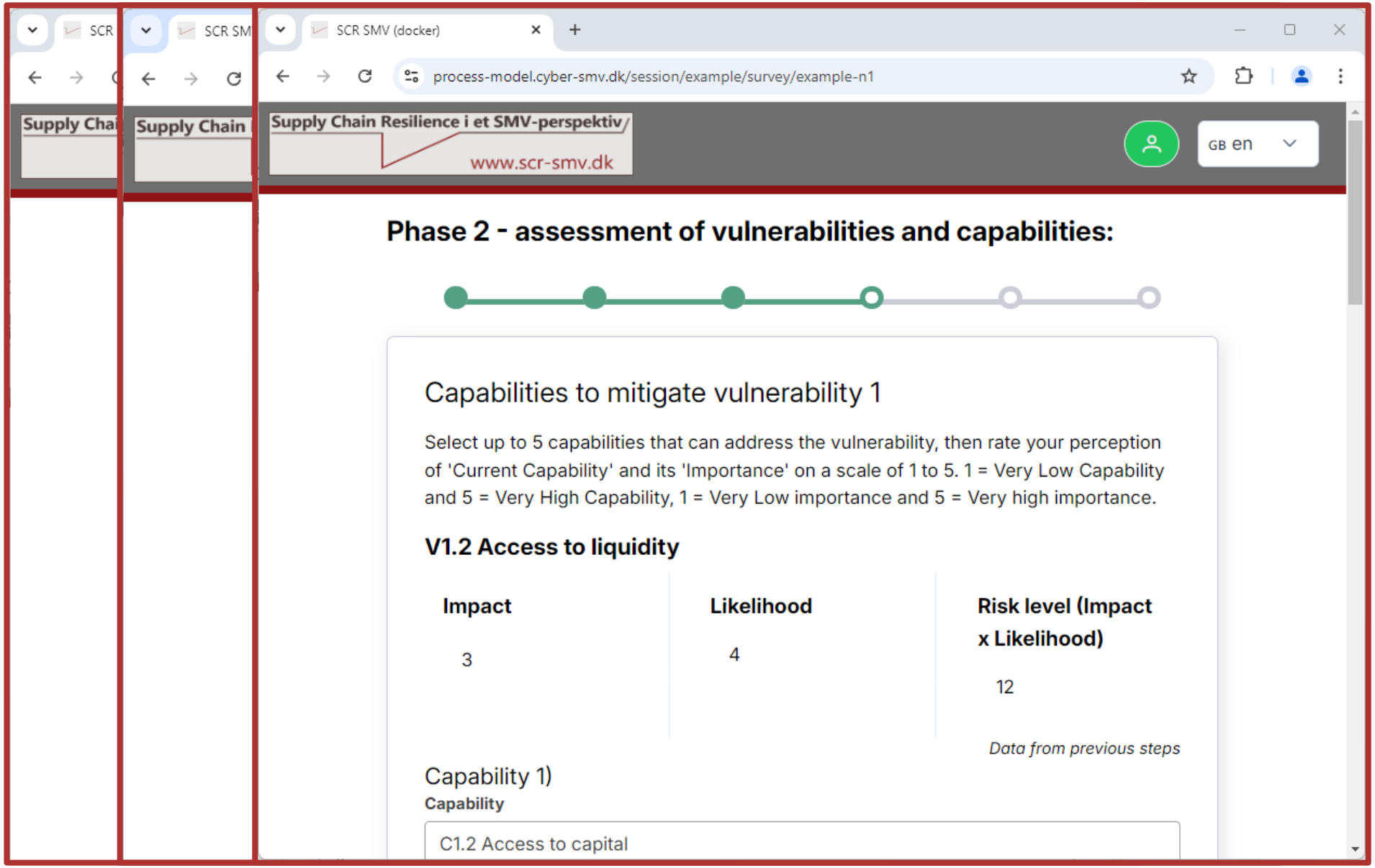
Company size is required

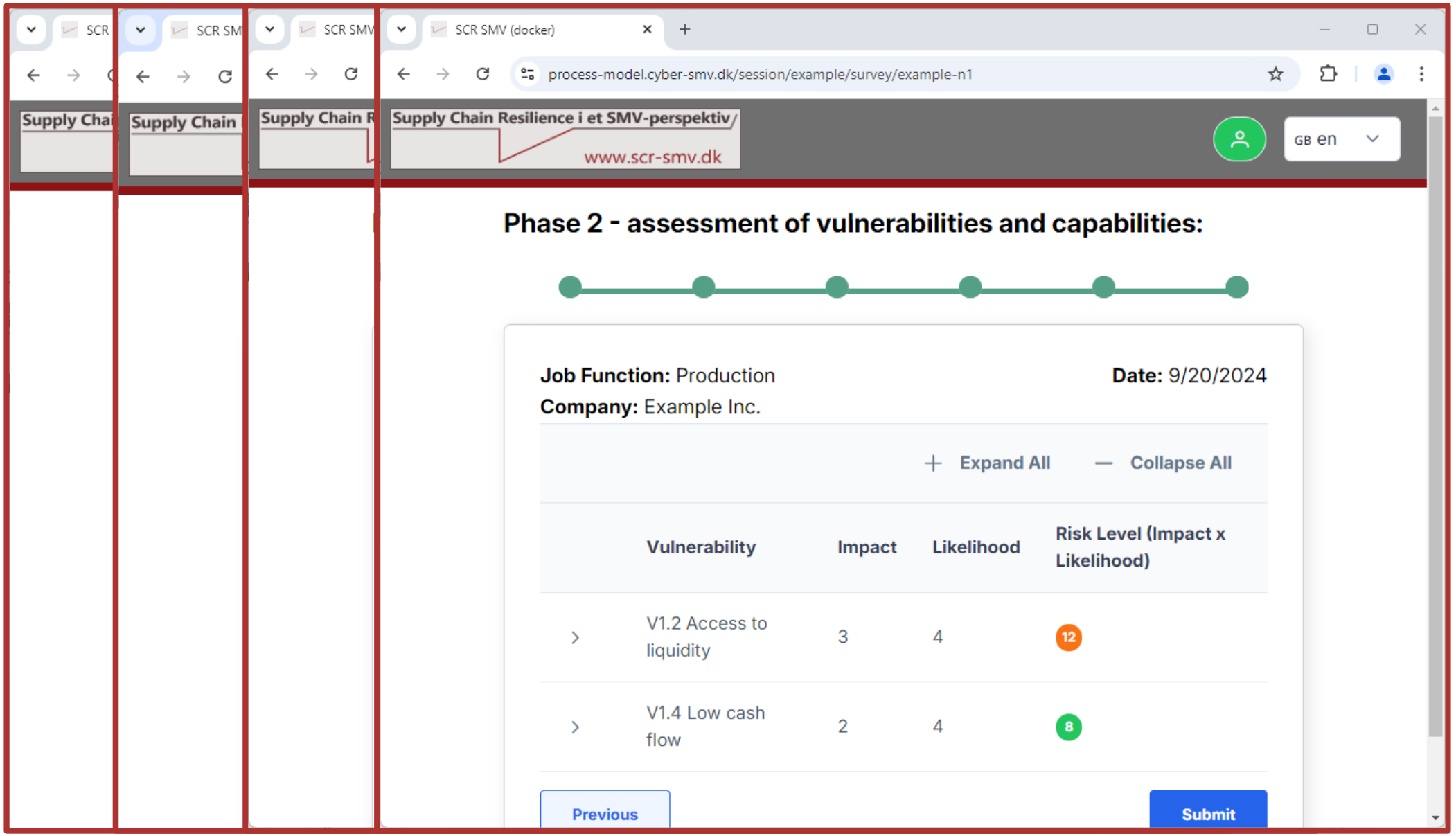
Cancel | Next


Company Information
Session Management
Activity Log
Process Model Sessions
Create New Session
Phase 2 - Vulnerability Assessment
Phase 1
Comprehensive assessment of supply chain vulnerabilities and risk prioritization
Phase 2 Assessment - Q1 2026
Phase 2
Assessment session for identifying and prioritizing supply chain vulnerabilities in Q1 2026
App Users
Add User
Enter username
Add
Proceed to Step 3


SCR SMV (docker)
process-model.cyber-smv.dk/session/example/survey/example-n1
Supply Chain Resilience i et SMV-perspektiv
www.scr-smv.dk
GB en
Phase 2 - assessment of vulnerabilities and capabilities:
Prioritization
Click below and select up to 10 vulnerabilities that you believe are important to the company's supply chain performance and results. The vulnerabilities are prioritized, so that the vulnerability that, according to your assessment, is most important is number 1. The one with the second most importance is number 2, etc.
Vulnerability 1
Vulnerability
Select Vulnerability
Note
Voluntary completion, required if 'Other' is selected.
Add new vulnerability


SCR SMV (docker)
process-model.cyber-smv.dk/session/example/survey/example-n1
Supply Chain Resilience i et SMV-perspektiv
www.scr-smv.dk
GB en
Phase 2 - assessment of vulnerabilities and capabilities:
Risk assessment of Vulnerabilities
Here you assess how much the individual vulnerabilities will affect your company's supply chain performance (Influence/Impact). Very low impact = 1 and very high impact = 5. You also assess the probability that the individual vulnerabilities will actually occur. Very low probability = 1 and very high probability = 5.
1. V1.2 Access to liquidity
Influence/ Impact on the supply chain
3
Likelihood that the vulnerability will occur
4


SCR
SCR SM
SCR SMV (docker)
process-model.cyber-smv.dk/session/example/survey/example-n1
Supply Chai
Supply Chain
Supply Chain Resilience i et SMV-perspektiv
www.scr-smv.dk
GB en
Phase 2 - assessment of vulnerabilities and capabilities:
Capabilities to mitigate vulnerability 1
Select up to 5 capabilities that can address the vulnerability, then rate your perception of 'Current Capability' and its 'Importance' on a scale of 1 to 5. 1 = Very Low Capability and 5 = Very High Capability, 1 = Very Low importance and 5 = Very high importance.
V1.2 Access to liquidity
Impact
3
Likelihood
4
Risk level (Impact x Likelihood)
12
Data from previous steps
Capability 1)
Capability
C1.2 Access to capital


SCR SMV (docker)
process-model.cyber-smv.dk/session/example/survey/example-n1
Supply Chain Resilience i et SMV-perspektiv
www.scr-smv.dk
GB en
Phase 2 - assessment of vulnerabilities and capabilities:
Job Function: Production
Date: 9/20/2024
Company: Example Inc.
Expand All
Collapse All
Vulnerability
Impact
Likelihood
Risk Level (Impact x Likelihood)
V1.2 Access to liquidity
3
4
12
V1.4 Low cash flow
2
4
8
Previous
Submit

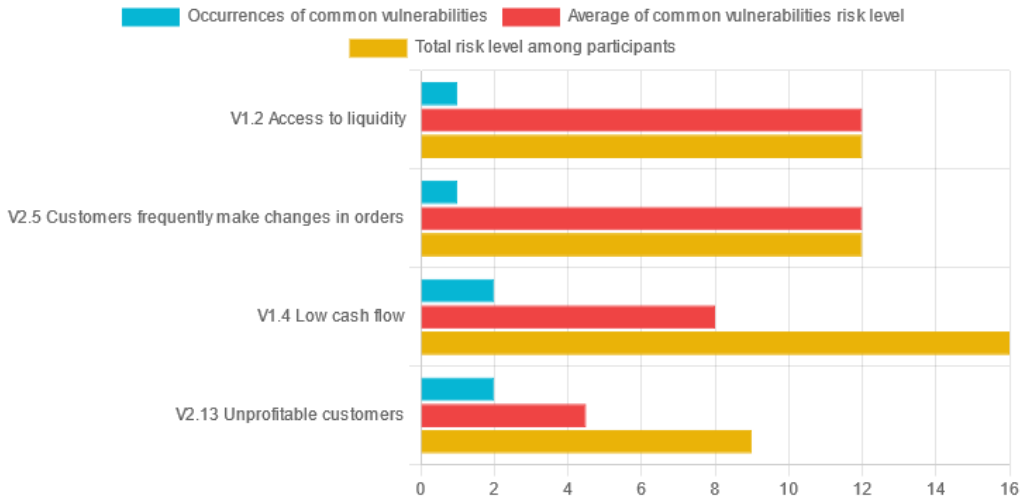
CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Summary of Selected Vulnerabilities



Vulnerability	Total risk level	Occurrences	Average risk level
V1.2 Access to liquidity	12	1	12.0
V2.5 Customers frequently make changes in orders	12	1	12.0
V1.4 Low cash flow	16	2	8.0
V2.13 Unprofitable customers	9	2	4.5

Summary Table

Functional Vulnerabilities

Job Function	Priority	Vulnerability
Production	1	V1.2 Access to liquidity 12
	2	V1.4 Low cash flow 8
Economy / IT	1	V2.13 Unprofitable customers 6
	2	V1.4 Low cash flow 8
Sales	1	V2.13 Unprofitable customers 3
	2	V2.5 Customers frequently make changes in orders 12

Summary Vulnerabilities

	Vulnerability	Count	Average
>	V1.2 Access to liquidity	1	12.0
>	V1.4 Low cash flow	2	8.0
>	V2.13 Unprofitable customers	2	4.5
>	V2.5 Customers frequently make changes in orders	1	12.0

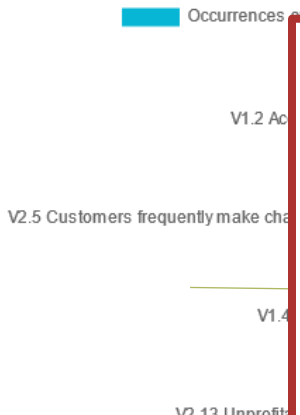
CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Summary of Selected Vulnerabilities



Vulnerability			
V1.2 Access to liquidity			
V2.5 Customers frequently make changes in orders	12	1	12.0
V1.4 Low cash flow	16	2	8.0
V2.13 Unprofitable customers	9	2	4.5

Summary Table

>	V2.13 Unprofitable customers	2	4.5

Capabilities:

Capabilities	Current Ability (avg.)	Importance (avg.)	Differ (avg.)
C1.4 Price margin Økonomi / IT	2	4	2.0
C2.10 Alternative distribution channels Salg	2	4	2.0
C2.1 Customer loyalty/retention			

to liquidity 12
sh flow 8
fitable customers 6
sh flow 8
fitable customers 3
ners frequently make changes in orders 12

		Count ↑↓	Average
>	V1.2 Access to liquidity	1	12.0
>	V1.4 Low cash flow	2	8.0
>	V2.13 Unprofitable customers	2	4.5
>	V2.5 Customers frequently make changes in orders	1	12.0

Digital Tool for executing the SCR Process

Phase 1
- Map the Supply Chains

Phase 2
- Functions identify Vulnerabilities and Capabilities

Phase 3
- Cross-organisational analysis and alignment

Phase 4
- Develop action plans

Web portal to support using the SCR Process Model

→ Templates, checklists, video tutorials, and preparatory reading material

→ Web application

- → Automated digital workflow guiding the cross-function team progress
- → Structured surveys of vulnerabilities and capabilities
- → Interactive reports and analyses by function and organisation (cross-functional)
- → Allows to repeat the process periodically and track changes over time

→ Free to use by Danish SMEs (starting mid-May)

→ Check https://cyber-smv.dk

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	**Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision**
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

Uerkendte sårbarheder vælter driften.
Erkendte sårbarheder kan ledes.

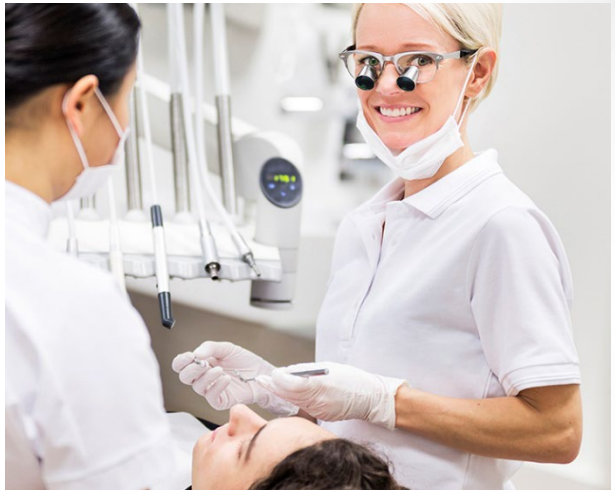
Fra model til driftsvirkelighed

Ole Anker Aagaard
Head of Legal & Compliance

Kliniske medicinsk udstyr fra… Samsø

- 3.617 indbyggere
- Flest solskinstimer i Danmark
- 863 virksomheder fordelt på 214 brancher
- En komprimeret motor med havudsigt

Det er vores DNA der skinner igennem alt hvad vi beskæftiger os med!



- Eget design, fabrik, salg og markedsunderstøttelse
- 75 ansatte
- 13 nationaliteter i én kantine
- Ca. 15 % årlig toplinevækst

Histore og stolte nedslag

Grundlagt i et baglokale i 2001

Vores hovedsæde på Industrivej 11, bygget i 2007, udvidet i 2013 og afslutte med 2 etage fabrik i 2024.

EN ISO 13485
(Iso 9001 for medicisnke udstyr)

reddot award winner

6 x RedDot Award

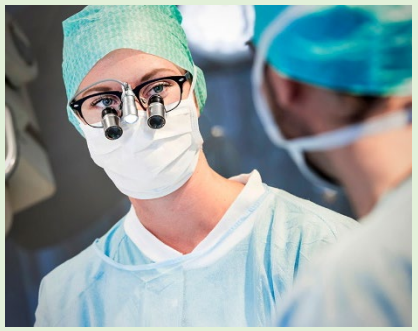
Danish Industry Initiative Award 2018

4 x Børsen Gazelle

Vi er vokset ind i kompleksitet

Personlige individuelle uniq-produkter, i den overvældende regulerede industri inden for produktion af medicinsk udstyr

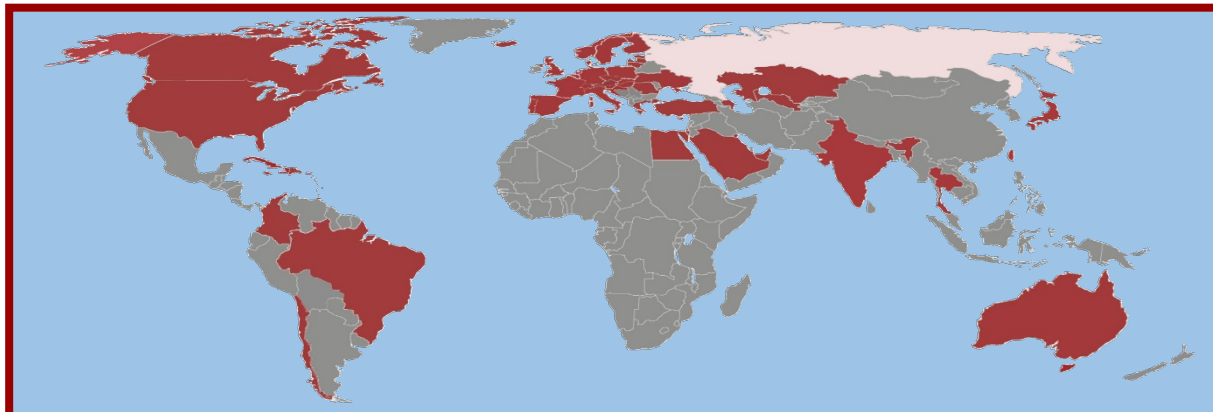
"Kompleks vej fra underleverandøre til slutbruger og med 10 års markeds levetid".



Medicin, hospitaler, dyrlæger, tandlæger, tandplejere, tandlægestuderende osv.

Repræsenteret på 6 kontinenter, forpligtet til normer og 600 kategorier af lovgivning og standarder.

"Udveksling af mere end 200.000 personlige identifikatoroplysninger på sundhedspersonale fra hele verden.

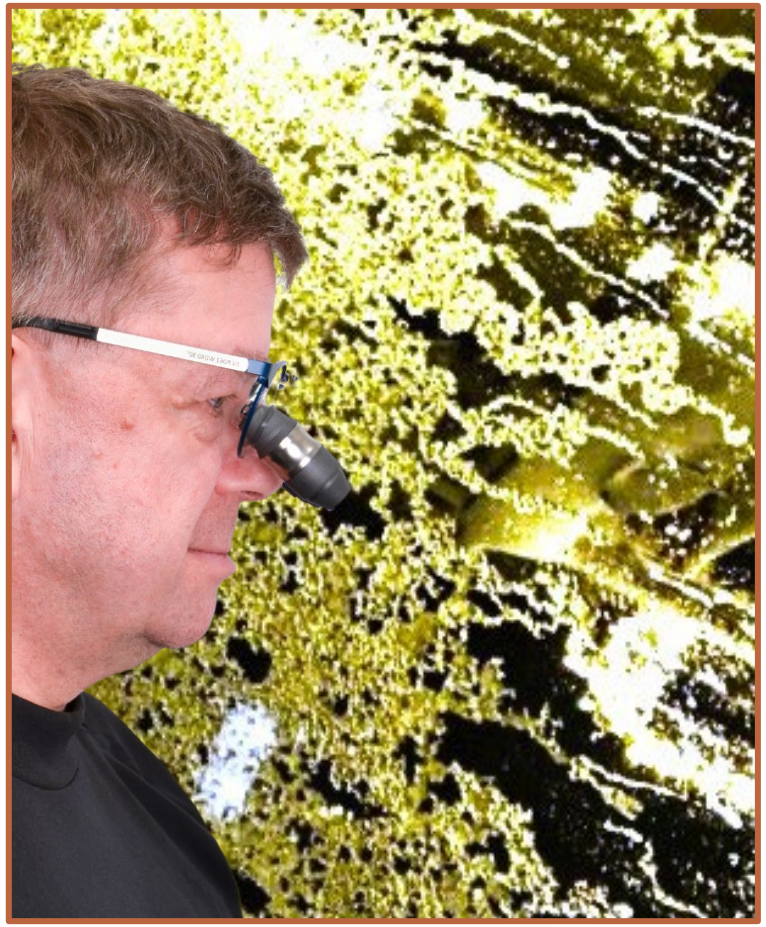


Distributører i ca. 50 lande

Udfordringerne er lette at nævne — svære at overskue

- ✓ Kompleksitet som følge af den globale reguleringer
- ✓ Personligt tilpasset udstyr, betyder mange person identificerbare informationer… på læger.
- ✓ Sprog, kultur og værdier variere … meget.
- ✓ Vækstfilosofi medføre, at investeringer i eks. cyber & compliance, kommer efter fokus på toplinjen.
- ✓ Vi har aldrig prøvet det før.

Fra analyse til organisatorisk bevægelse



Konferancens tema

- ✓ Risiko
- ✓ Sårbarhed
- ✓ Konsekvens
- ✓ Kapabiliteter
- ✓ Robusthed

Min vinkel i dag

Det svære efter analysen
Er Ikke at forstå ordene

Men at motivere til
- modtagelighed
- Prioritering
- Ejerskab
- Bevægelse

Mit budskab i dag

U-erkendte sårbarheder vælter driften.

Det farlige er sjældent kun teknologi.
Det er afhængigheder, overgange, tavs viden og langsom erkendelse.

Erkendte sårbarheder kan ledes.

Robusthed kræver fælles virkelighed
og et team, som får lov at forstyrre den.

Og du er kapaciteten der få det til at ske.

Indsigt giver plads til erkendelse

Arrangørens formulering

"Vigtigheden af en tværorganisatorisk faciliteret proces til cybersikkerhed".

Korrekt.

Men dødbringende kedeligt.

Fordi det bliver *for svagt i praksis.*

Tarvorix fra udstilling på MOMU "*Kelternes verden – Europas urkraft*"
Foto: Ole Anker Aagaard.

Facilitering bør være ganske konkret.

De brugbare observationer fremkaldes, når nogen faktisk tvinger trusselsbillederne sammen.

Din opgave er at hjælpe organisationen med at opdage sine egne blinde vinkler, før hændelsen gør det

Forebyggelse handle om dig

Risiko er hændelser, der endnu ikke er indtruffet

Handler cybercrime kun om tekniske nedbrud og angrebsforebyggelse?
Nej, ikke alene

For de fleste organisationer handler det også om:
uklarhed om ansvar, leverandørafhængighed, skjulte integrationer, tavs viden, og porøse overgange mellem funktioner.

Optimistisk rapportering er dit varselssignal

Hvis virksomheden først under pres opdager,
- hvem der ejer hvad,
- hvilke processer der kun lever i bestemte hoveder,
- og hvor support- eller dataafhængigheder faktisk ligger,

så er skaden allerede begyndt at forplante sig.

Langsom erkendelse = flere ubudgetterede omkostninger end selve hændelsen

Min væsentligste fejl

De tre vigtigste fejl, jeg har erfaret.

"Jeg ville bruge det vi allerede gjorde så godt , og fejlede".

Følelse af orden er ikke en organisatorisk evne.
Det er en behagelig tilstand.
Mit nye fokus er, at de tværgående funktioner hele tiden spørger:
Indsigt. Dokumentation. Realitets-test.

1 at forveksle teknisk aktivitet med organisatorisk modenhed

2 at intern forståelse auto-matisk er dokumenteret kontrol

3 at antage, at en plan i sig selv er beredskab.

Fakta kræver intern klarhed.

De spørgsmål robuste organisationer tør stille

- Indsigt
  - ❑ **Hvor er vi reelt sårbare?**
  - ❑ Hvilke afhængigheder kan stoppe os?
- Dokumentation
  - ❑ Hvad lever kun i bestemte menneskers hoveder?
  - ❑ Hvor har vi byttet dokumentation ud med tradition?
- Realitetstest
  - ❑ Hvilke leverandører er vores skjulte single points of failure?
  - ❑ **Hvad ser elegant ud i PowerPoint, men er skrøbeligt i praksis?**

Vil du have robusthed, - opsøg tværgående erkendelse.

Overgange mellem driftsområder

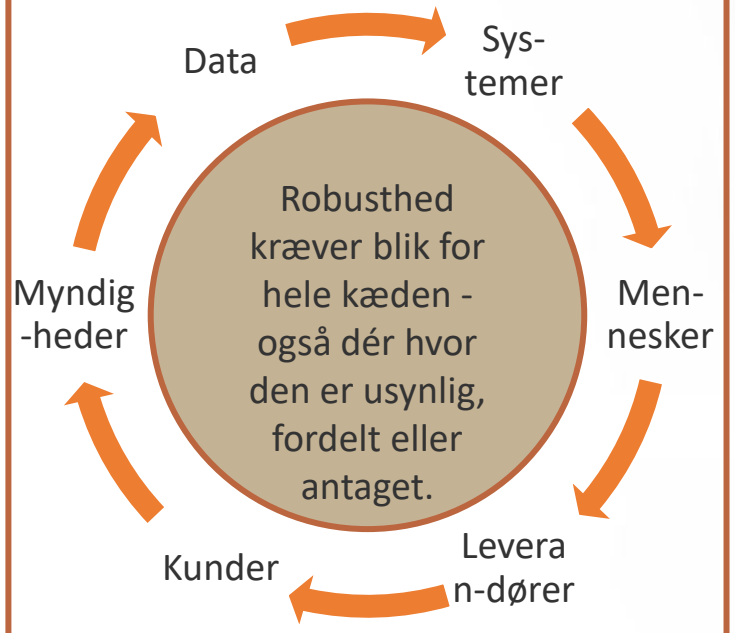
Facilitering skaber fælles blik

- IT ser noget,
- drift noget andet,
- ledelsen et tredje billede.

Det er op til dig at facilitere den tværgående erkendelse.

Når de ukendte mangler bliver synlige, kan organisationen styrke sikkerheden i tide

Digitale forsyningskæde



We have made a serious effort to make this presentation worth your attention.
If anything remains unclear, or if you wish to continue the dialogue,
- please contact us at
COMPLIANCE@EXAMVISION.COM
Thank you.

Pause

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	**Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU**
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

Working with Future Scenarios

How to Work with Future Scenarios

Purpose of Future Scenarios: for situations framed by uncertainty rather than risk

- Risk can be forecasted (probabilities add up to 100%)
- Uncertainty cannot be forecasted (incomplete knowledge – cannot calculate “rational” action)

Situations that are uncertain require different techniques

- Uncertain situations tend to lead to conservative thinking – we rely on past procedures and practices

One way to break out of this conservative thinking is to engage in scenarios

- Scenarios are meant to be “predictive,” but are a tool to help us consider contingency in uncertain situations

Building Future Scenarios

1. Workshops with experts in defense and foreign affairs to identify and define geopolitical crises in the next 5 years
   - Mapping each potential crisis with PESTEL variables (political, economic, social, technological, legal)
   - Work through which of the created scenarios are both most *uncertain* and most *severe* to Denmark

2. Creation of 5 scenarios that were in the most uncertain and severe quadrant
   - Narrative style to engage the reader into the problems faced by the hypothetical business

3. Acid testing of the 5 scenarios with industry groups to ensure sensibility and consider what business effects might be missing from the existing scenarios to deepen their impact

SDU

5 Scenarios

Scenario 1: USA’s Withdrawal from Europe

Scenario 2: USA-China Confrontation over Taiwan

Scenario 3: Cascading Climate Crises

Scenario 4: The Strain of Economic Polarization

Scenario 5: When AI Goes Rogue

Working with Future Scenarios

In workshops, we had the leadership of individual businesses read the scenarios and engage with them through a set of guiding questions

- They were instructed not to “solve” the dilemma in the scenario, but reflect on what the general problem would mean for their business

Business are encouraged to synthesize the more critical vulnerabilities and insights that emerge from the exercises to map their potential resilience gaps

- Follow up with an impact/effort prioritization matrix to find “quick wins” (High Impact, Low Effort) and “major projects” (High Impact, High Effort)

Guiding Scenario Questions

1. What are the key risk factors and vulnerabilities in this scenario?
2. What risks does this scenario pose to Danish businesses?
3. What vulnerabilities affect your business?
4. What mitigation, if any, has your business considered or implemented?

SDU

Scenario 1: USA's Withdrawal from Europe

The Story: Following a shift in U.S. foreign policy, America dramatically reduces its security commitments to Europe, pulling troops out of the region and creating a leadership vacuum in NATO. To compensate, European nations, including Denmark, are forced to significantly increase defense spending, leading to cuts in other areas. The global trade environment becomes more hostile.

The Shocks to Your Business:

→ *Supply Chain Shock*: The U.S. implements a new universal trade tariff, significantly increasing the cost of your exports to the American market and the components you import from U.S. suppliers

→ *Cyber Threat*: With the U.S. security umbrella diminished, Russia launches a constant, low-level campaign of sophisticated cyberattacks targeting European infrastructure and their suppliers, including companies like yours

Scenario 1: USA's Withdrawal from Europe

Guided Discussion (The Tabletop Exercise – Detailed Example):

→ **Detection & Assessment**: How would we first learn about the new tariffs? Who in our company is responsible for monitoring international trade policy? How would our current IT security systems distinguish a state-sponsored cyberattack from a common criminal one?

→ **Immediate Response**: What are our first three actions in the 24 hours after the tariff announcement? Who is on our immediate response team for a major cyber intrusion? Do we have contact information for legal counsel and forensic experts readily available?

→ **Business Continuity**: Can our business model survive a 20% tariff on our main export product? How long can we operate if our primary logistics partner is crippled by a cyberattack? Do we have vetted alternative suppliers outside the U.S. for critical components?

→ **Vulnerabilities Exposed**: How does this scenario exploit specific weaknesseses? What new vulnerabilities does it reveal?

Scenario 3: Cascading Climate Crises

The Story: A series of extreme weather events causes widespread disruption. A major flood in Germany severs key European transport arteries for weeks. In response to climate goals, the EU implements new energy-saving regulations that have unintended consequences for digital infrastructure.

The Shocks to Your Business:

- → *Supply Chain Shock*: Your primary land route for European distribution is impassable. Simultaneously, a key supplier, already stressed by the climate event, is hit by a ransomware attack and goes offline.

- → *Cyber Threat*: The new EU regulations limit the use of computation-intensive AI, forcing your cloud security provider to disable its most advanced threat detection systems. This makes your company more vulnerable to attack precisely when cybercriminals are exploiting the chaos.

→ **Guided Discussion Example:** Does our business continuity plan account for simultaneous physical and digital disruptions? Is our insurance coverage adequate for climate-related business interruptions? How do we assess the second-order consequences of new regulations that seem unrelated to our core business?

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	**Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S**
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

GOMSPACE

Cybersikkerhed som en driftsdisciplin

WE MAKE SPACE YOURS

Søren Lind Therkildsen | COO GomSpace

Søren Lind Therkildsen

COO & Head of Quality (2025 -)

CITO / CMO / Senior Director Business Transformation (2021–2025)

Head of ERP & Planning / Manufacturing Engineer (2018–2021)

Master (OIM) – industrialisering af nanosatellitter

Ledelse & transformation
Opbygget og ledet centrale funktioner fra drift til strategisk niveau
Gennemført større organisatoriske og kulturelle transformationer

Manufacturing & industrialisering
Nøglespiller i industrialiseringen af nanosatellitter
Design og etablering af moderne, skalerbar produktion (cleanroom, microsatellite fabrik)

ERP, data & styring
Ledet ERP-implementering og videreudvikling (ERP, IT, planning)
Skabt bedre beslutningsgrundlag gennem struktur, data og governance

Strategi & kvalitet
Drevet strategisk business transformation på tværs af organisationen
I dag ansvarlig for både COO-området og kvalitet, inkl. informationssikkerhed og compliance

GOMSPACE

Cybersikkerhed som en driftsdisciplin

- Ikke et IT-projekt

Søren Lind Therkildsen

Kompleksitet

Vi ved ikke, hvilket scenarie der vil ramme os.
Men vi ved, at når det gør – skal vi være forberedt.

Beredskabsst

Mellemstore

omheder (SMV)

Kompleksitet

Kompleks

Hvad er det:

- Mange indbyrdes afhængige variable
- Fremtiden kan ikke beregnes præcist
- Årsag–virkning kan først ses bagudrettet
- Problemer løses ved at eksperimentere, lære og tilpasse

Kompliceret

Hvad er det:

- Flere korrekte svar
- Kræver analyse, specialister eller modeller
- Årsag–virkning findes, men er ikke åbenlys
- Problemer løses ved at analysere og optimere

Kaotisk

Hvad er det:

- Alt er ustabilt
- Høj turbulens, sammenbrud og forstyrrelser
- Ingen mønstre – ingen forudsigelighed
- Problemer løses ved at handle øjeblikkeligt for at stoppe kaos
- – og derefter bevæge sig mod det komplekse domæne

Simpel

Hvad er det:

- Stabile og gentagelige situationer
- Ét korrekt svar
- Best practice kan anvendes
- Problemer løses ved at standardisere

Kompleksitet

x = beslutningsvektor (fx kapacitetsplan, leverandørallokering, lagerpolitikker)
ω = tilfældige fremtidige udfald (efterspørgsel, fejl, forsinkelser, priser …)
C(x, ω) = samlet omkostning / “regret” hvis beslutning x træffes og udfald ω indtræffer

Kompleks

Konceptuel forecasting
x* = argmin_x ∑_{s=1}^S p_s · C(x, ω_s)

Hvorfor kompleks?
Eksponentiel vækst i tidshorisont og usikkerhed
Eksplotion i scenarier – fuld optimering kan tage år at beregne

Kompliceret

Euler’s

Euler’s Formula

$$e^{i\phi} = \cos\phi + i\sin\phi$$

Euler’s identity

$$e^{i\pi} + 1 = 0$$

Hvorfor kompliceret?
Kræver eksperter og modeler, stadig deterministisk,
Løsningen finds – men ikke trivielt.

Kaotisk

“En kritisk leverandør bliver ramt af cyberangreb eller konkurs”
Non-linear dynamics: x_{t+1} = r x_t (1 – x_t)

Beregningen pr. trin er trivial – **Men forudsigelseshorisonten er ekstremt kort**

Det er ikke et problem, man regner sig ud af
Det er et problem, man designer robusthed imod.

Simpel

Egenkapitalafkast (ROE) =
(Nettoresultat / Omsætning) x (Omsætning / Aktiver) x (Aktiver / Egenkapital)

Hvorfor simpel?
Kendt, Lineær, Kan løses på et øjeblik
(Klassisk finansielt forhold (ingen usikkerhed)

“Når en forsyningskæde bliver ramt af cyberangreb, leverandørsvigt eller systemnedbrud, så er vi ikke i et IT-problem.
Vi er i kaos.
Og i kaos hjælper analyser og planer ikke – der skal handles hurtigt for at genskabe stabilitet.
Først derefter kan vi begynde at lære og forbedre.”

Forsyningskæden

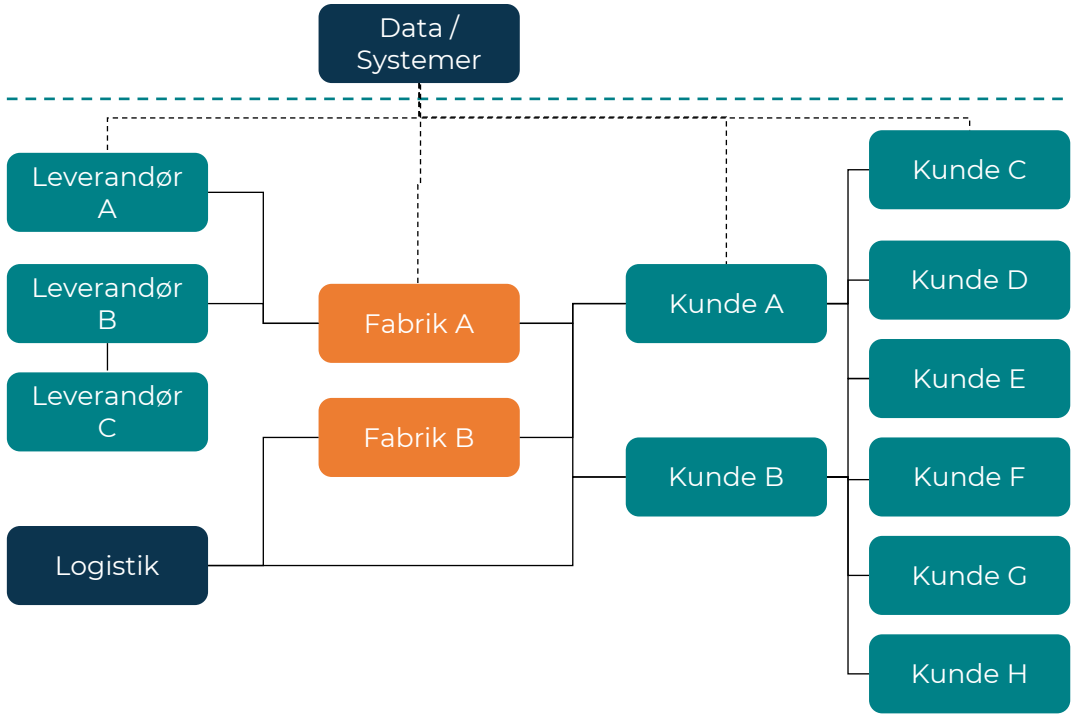
LEAN

Leverandør – Fabrikation – Lager/logistik – Kunde

"Når vi tænker LEAN, ser vi ofte forsyningskæden som **et flow**. Vi fjerner spild, reducerer variation og optimerer gennemløb.

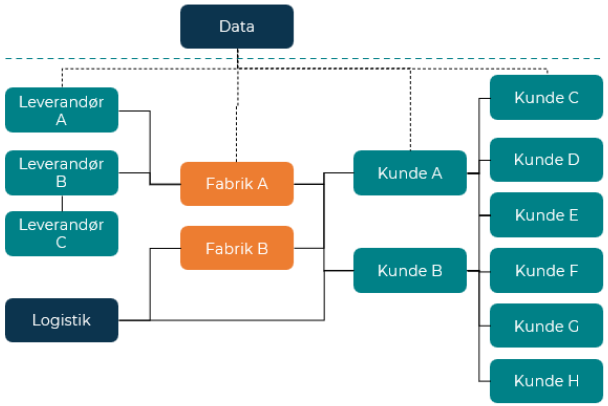
I **stabile og forudsigelige** verdner virker det framragende."

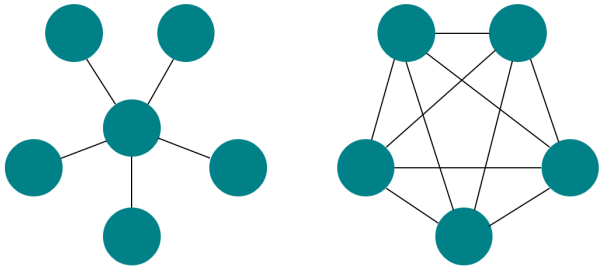
Virkeligheden er mere kompleks!



Enhver kritisk leverance i forsyningskæden må aldrig være afhængig af én sti, ét system eller én leverandør.

Fra flow til netværk – hvor skabes robusthed?





Traditionelt LEAN-fokus

- Ét primært flow
- Optimering af gennemløb
- Minimering af variation
- Høj effektivitet – lav redundans

Moderne virkelighed

- Forsyningskæden er et netværk af afhængigheder
- Systemer, data, mennesker og partnere er tæt koblet
- Forstyrrelser opstår sjældent i selve flowet – men i forbindelserne omkring det

Robusthed opstår, når:

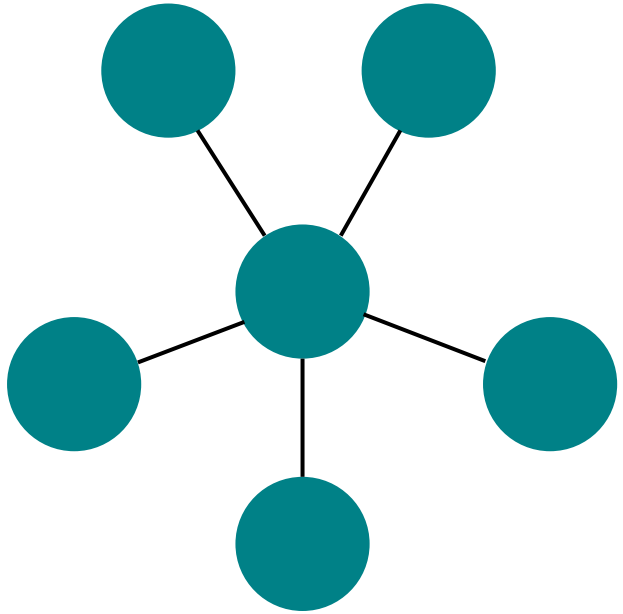
- Kritiske leverancer har mere end én vej
- Systemer kan erstattes eller omgås midlertidigt
- Beslutninger kan træffes lokalt under forstyrrelser
- Organisationen kan skifte fra effektiv drift → stabilisering

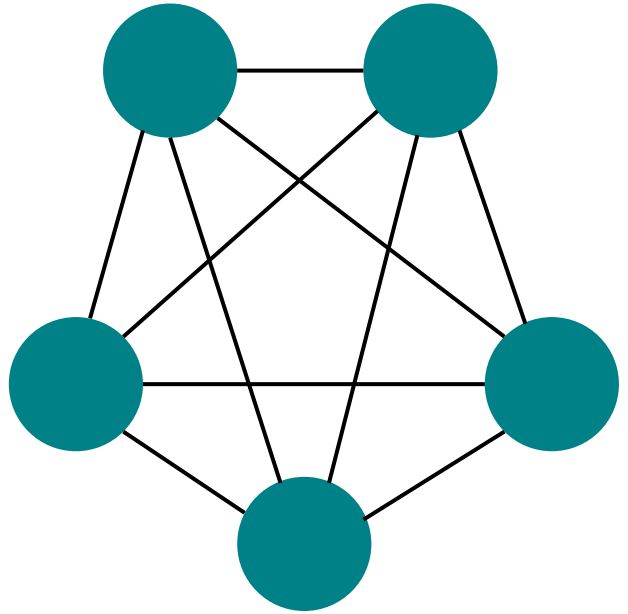
Et netværk fejler sjældent ét sted

Det fejler der hvor:

- Der kun er én vej
- Der kun er én beslutningstager
- Der kun er én sandhed / ét system

Robusthed er et designvalg





Netværk kan designes:

- Med single point of failure
- Eller med alternative stier

Robusthed handler om:

- Struktur
- Valg
- Prioriteringer **før** hændelsen sker

Robusthed som et ledelses tema

- Højteknologisk produktion med lange leveringstider
- Mange afhængigheder på tværs af:
  - leverandører
  - produktion og test
  - IT-systemer og data
  - mennesker og samarbejdspartnere
- Små forstyrrelser kan få meget store konsekvenser

I komplekse industrivirksomheder kan vi ikke eliminere hændelser – kun eliminere deres effekt

Konkrete initiativer

1. Samarbejde med SDU-projektet

- Fælles sprog for kompleksitet og forsyningsnetværk
- Scenarier fremfor forecasting
- Fokus på kapabiliteter – ikke kun risici

2. Struktur og governance (NIS2 som ramme)

- Klart ejerskab af kritiske afhængigheder
- Leverandør- og systemsyn uden silotænkning
- Fokus på beslutningsevne under forstyrrelser

Konkrete initiativer

3. Fra analyse til drift

- Øvelser og scenarier
- Prioritering af alternative stier
- Robusthed ind i daglige beslutninger

Hvad ændre det I hverdagen?

- Mindre afhængighed af enkeltpersoner og enkelt-systemer
- Hurtigere beslutninger, når noget går galt
- Bedre dialog mellem:
  - drift
  - IT
  - ledelse
- Cybersikkerhed flyttede fra “kontrol” til muliggørelse

Hvad kan I andre tage med hjem?

- **Behandl forsyningskæden som et netværk – ikke et flow**
- Sårbarhed opstår i forbindelserne.

- **Design robusthed før hændelsen sker**
- Alternativer slår perfektion.

- **Gør cybersikkerhed til en del af driften**
- Ikke et IT-projekt – et ledelsesansvar.

LEARN MORE

THANK YOU

WE MAKE SPACE YOURS

www.gomspace.com

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	**Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva**
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

ineva
VIDEN TIL UDVIKLING

EKSTERN EVALUERING

'CYBERSIKKERHED OG FORRETNINGSKONTINUITET I DANSKE PRODUKTIONS-SMV'ER'

- EVALUERINGENS FOKUS
- VIRKSOMHEDERNES UDGANGSPUNKTER
- DET MEST LÆRERIGE
- ET NYT MINDSET

DE SAMLEDE KONKLUSIONER

EVALUERINGENS FOKUS

Projektets formål

- At styrke danske produktions-SMV'ers cybersikkerhed
- At identificere og adressere cybersikkerhedsmæssige sårbarheder
- At udvikle kapabiliteter til at håndtere nuværende og fremtidige cybertrusler
- At koble cybersikkerhed tættere til forretningskontinuitet og forsyningskæder

Den eksterne evaluering følger op på, om projektet har bidraget til:

- Identifikation af relevante sårbarheder og kapabiliteter
- Styrket resiliens over for nuværende og fremtidige cybertrusler
- Øget tværorganisatorisk forståelse for cybersikkerhed
- Ændret mindset: fra cybersikkerhed som omkostning til strategisk investering
- Tilførsel af viden, kompetencer og anvendelige værktøjer

Evalueringens datagrundlag

- Kvalitative interviews med deltagende virksomheder
- Fokus på erfaringer, læringspunkter og oplevet udbytte

VIRKSOMHEDERNES UDGANGSPUNKTER

Virksomhederne deltog med forskellige forudsætninger:

- Forskellig modenhed i arbejdet med cybersikkerhed
- Forskellige organisatoriske setups
- Forskellige erfaringer med risikostyring og sårbarhedsanalyser

Det betød, at projektets værdi antog forskellige former:

- For nogle: ny viden, struktur og systematik
- For andre: kvalificering, validering og nye perspektiver
- For de mere modne: bekræftelse af, at de var på rette vej

> Vi kunne blive klogere, og vi kunne også blive bekræftet i, at vi er på rette vej. Og det synes jeg egentlig har stor værdi, fordi det jo også handler om tryghed. (Projektdeltager)

ineva
VIDEN TIL UDVIKLING

DET MEST LÆRERIGE

Virksomhederne fremhæver især den strukturerede tilgang

- Projektet skabte en ramme, hvor virksomhederne blev ført systematisk gennem centrale spørgsmål om sårbarheder, risici og konsekvenser.
- Den faste metode gjorde det lettere at få taget de nødvendige drøftelser - også dem, der ellers kan være svære at få prioriteret i hverdagen.
- Flere oplevede, at strukturen hjalp dem med at omsætte brede bekymringer til mere konkrete problemstillinger og handlemuligheder.

De scenariebaserede øvelser gjorde cybersikkerhed mere konkret

- Realistiske scenarier gav virksomhederne mulighed for at afprøve, hvordan de ville reagere i en presset situation.
- Øvelserne tydeliggjorde, at cybersikkerhed ikke kun handler om teknologi, men også om beslutninger, kommunikation, ansvar og beredskab.
- Scenarierne gjorde det lettere at koble cybersikkerhed til virksomhedens drift, kritiske funktioner og forretningskontinuitet.

> Det er nogle gange denne her meget stramme metodefremgang, der gør, at man ligesom bliver trukket igennem og får taget de rigtige drøftelser på det rigtige tidspunkt. (Projektdeltager)

ineva
VIDEN TIL UDVIKLING

ET NYT MINDSET

Et centralt udbytte er et bredere syn på cybersikkerhed

- Cybersikkerhed forstås i højere grad som mere end et teknisk IT-anliggende.
- Projektet har koblet cybersikkerhed til ledelse, drift, medarbejdere og forretningskontinuitet.
- Flere virksomheder har fået et fælles sprog for at tale om cyberrisici på tværs af organisationen.

Medarbejdere, leverandører og arbejdsgange fylder mere

- Medarbejderadfærd og awareness mere bredt ses som en vigtig del af risikobilledet.
- Leverandører og samarbejdspartnere er blevet tydeligere som en brik i cybersikkerhedsarbejdet i virksomhederne.
- Cybersikkerhed handler derfor også om ansvar, procedurer og daglige arbejdsgange.

> Bevidstheden om, at 70% af cyberangreb kommer ind gennem medarbejdere, det gør jo nok, at det er et oplagt sted for et indsatsområde, hvor vi skal bruge lidt mere systematisk kontrol. (Projektdeltager)

DE SAMLEDE KONKLUSIONER

Projektet har samlet set bidraget positivt

- Virksomhederne har fået styrket deres refleksioner om sårbarheder, risici og handlemuligheder.
- Projektet har skabt mere struktur i arbejdet med cybersikkerhed.
- Flere virksomheder har fået et bedre grundlag for at prioritere og følge op på konkrete indsatser.

Den væsentligste værdi ligger i den organisatoriske forankring

- Cybersikkerhed er i højere grad blevet koblet til ledelse, drift og forretningskontinuitet.
- Projektet har bidraget til øget tværorganisatorisk forståelse og et mere fælles sprog.
- For flere virksomheder er cybersikkerhed blevet et mere strategisk anliggende.

Hovedkonklusion

Projektets mest vedvarende værdi ligger i, at cybersikkerhed i højere grad forstås som en del af virksomhedens samlede robusthed og konkurrenceevne - ikke kun som et IT-anliggende. Og at virksomhederne har metoder og strukturer til det konkrete arbejde med cybersikkerhed.

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	**Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU**
17.55 – 18.00	Afrunding v/Jan Stentoft, professor, SDU

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Rapporten er baseret på dataindsamling fra december 2025 til februar 2026.

Rapporten er tilgængelig her.

25% af virksomhederne har indenfor de seneste to år oplevet cyberangreb (i 2024 undersøgelsen var dette 20%).

Formålet med undersøgelsen er *at afdække danske små og mellemstore produktionsvirksomheders praksis med cybersikkerhed* med henblik på at analysere, om virksomhedernes praksis er blevet styrket sammenholdt med 2024-undersøgelsen (tilgængelig her).

Cybersikker supply chain risk management

- Cybersecurity Supply Chain Risk Management (C-SCRM) kan forstås som en systematisk tilgang til at *identificere*, *vurdere* og *afbøde* cyberrisici, der opstår gennem leverandører, IT/OT-produkter, tjenester og andre tredjepartsrelationer på tværs af hele livscyklussen (f.eks. design, indkøb, implementering, drift, vedligeholdelse og udfasning).
- I en produktionsvirksomhed er C-SCRM særligt relevant, fordi "forsyningskæden" ikke kun består af fysiske materialer, men også af digitale afhængigheder:
  - ERP-systemer
  - Cloud-tjenester
  - EDI-/kundeportaler
  - Fjernservice af maskiner
  - Softwareopdateringer til OT-udstyr
  - Dataudveksling med kunder og leverandører.

Cybersikker supply chain risk management: 10 praksisser fra NIST (1 af 2)

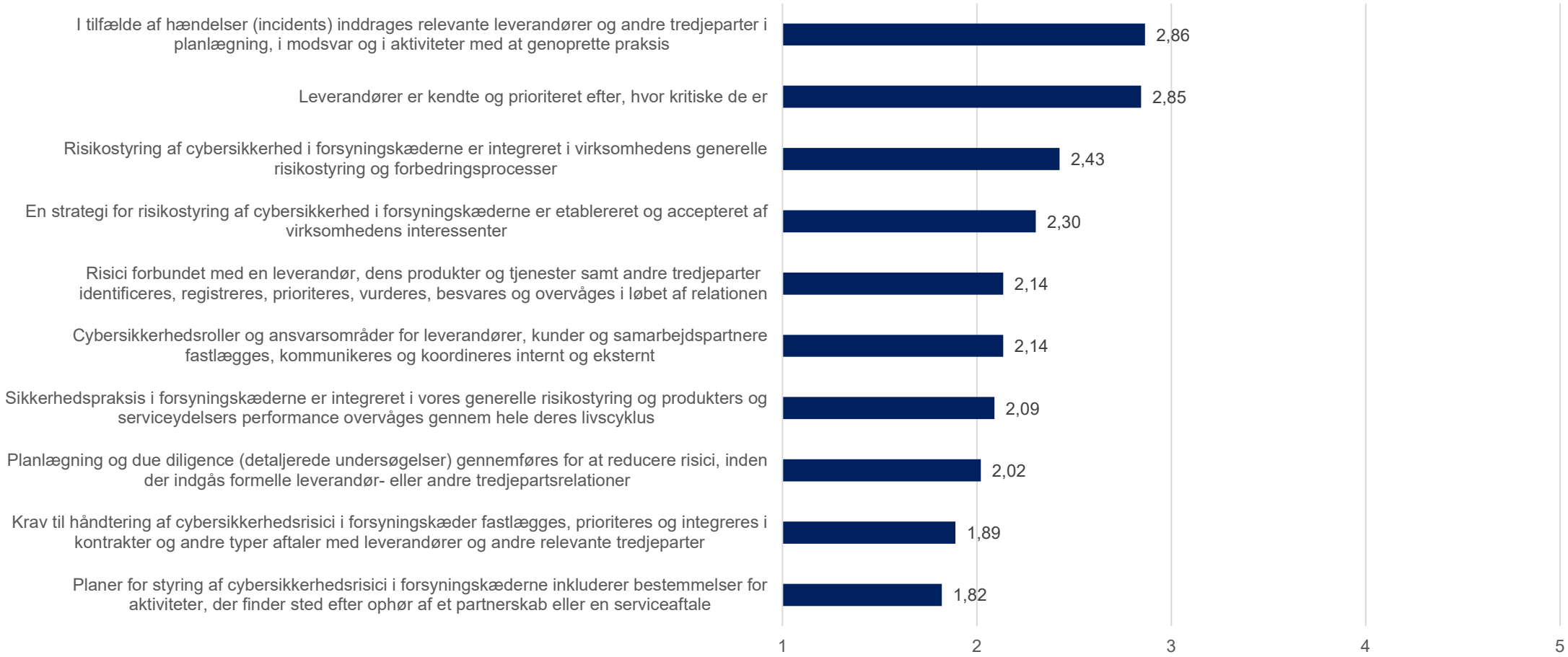
1. En **strategi for risikostyring** af cybersikkerhed i forsyningskæderne er etableret og accepteret af virksomhedens interessenter.
2. **Cybersikkerhedsroller** og ansvarsområder for leverandører, kunder og samarbejdspartnere fastlægges, kommunikeres og koordineres internt og eksternt.
3. **Risikostyring af cybersikkerhed** i forsyningskæderne er **integreret** i virksomhedens generelle risikostyring og forbedringsprocesser.
4. Leverandører er kendte og **prioriteret** efter, hvor kritiske de er.
5. **Krav** til håndtering af cybersikkerhedsrisici i forsyningskæder fastlægges, prioriteres og **integreres i kontrakter og andre typer aftaler** med leverandører og andre relevante tredjeparter.

NIST = National Institute of Standards and Technology – som har udgivet et Cybersecurity Framework (CSF)

Cybersikker supply chain risk management: 10 praksisser fra NIST (2 af 2)

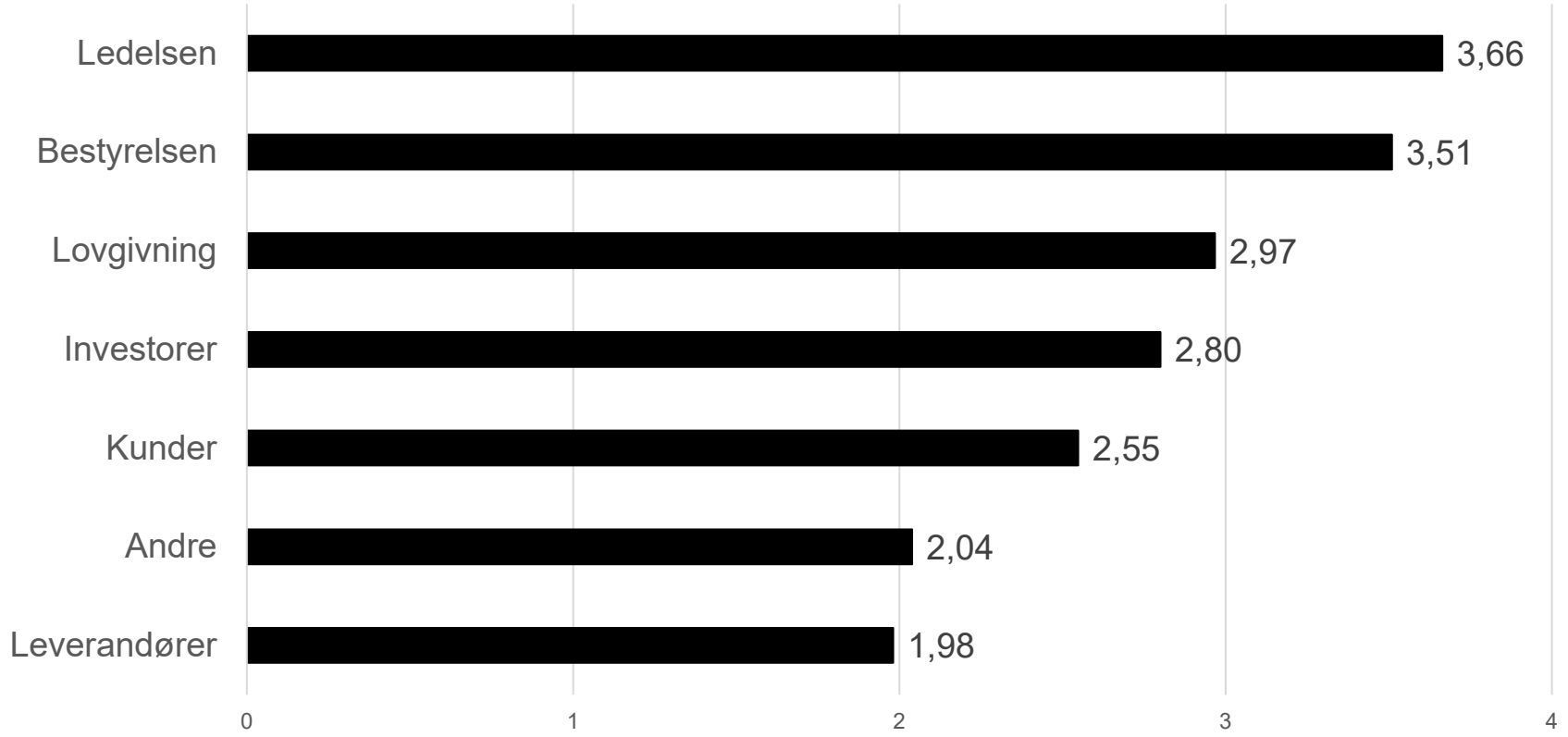
6. **Planlægning og due diligence** (detaljerede undersøgelser) gennemføres for at reducere risici, inden der indgås formelle leverandør- eller andre tredjepartsrelationer.
7. **Risici** forbundet med en leverandør, dens **produkter og tjenester** samt andre tredjeparter identificeres, registreres, prioriteres, vurderes, besvares og overvåges i løbet af relationen.
8. **I tilfælde af hændelser** (incidents) inddrages relevante leverandører og andre tredjeparter i planlægning, i modsvar og i aktiviteter med at genoprette praksis.
9. **Sikkerhedspraksis** i forsyningskæderne er integreret i vores generelle risikostyring og produkters og serviceydelsers performance overvåges gennem hele deres livscyklus.
10. **Planer for styring af cybersikkerhedsrisici** i forsyningskæderne inkluderer bestemmelser for aktiviteter, der finder sted **efter ophør af et partnerskab** eller en **serviceaftale**.

Cybersikker supply chain risk management

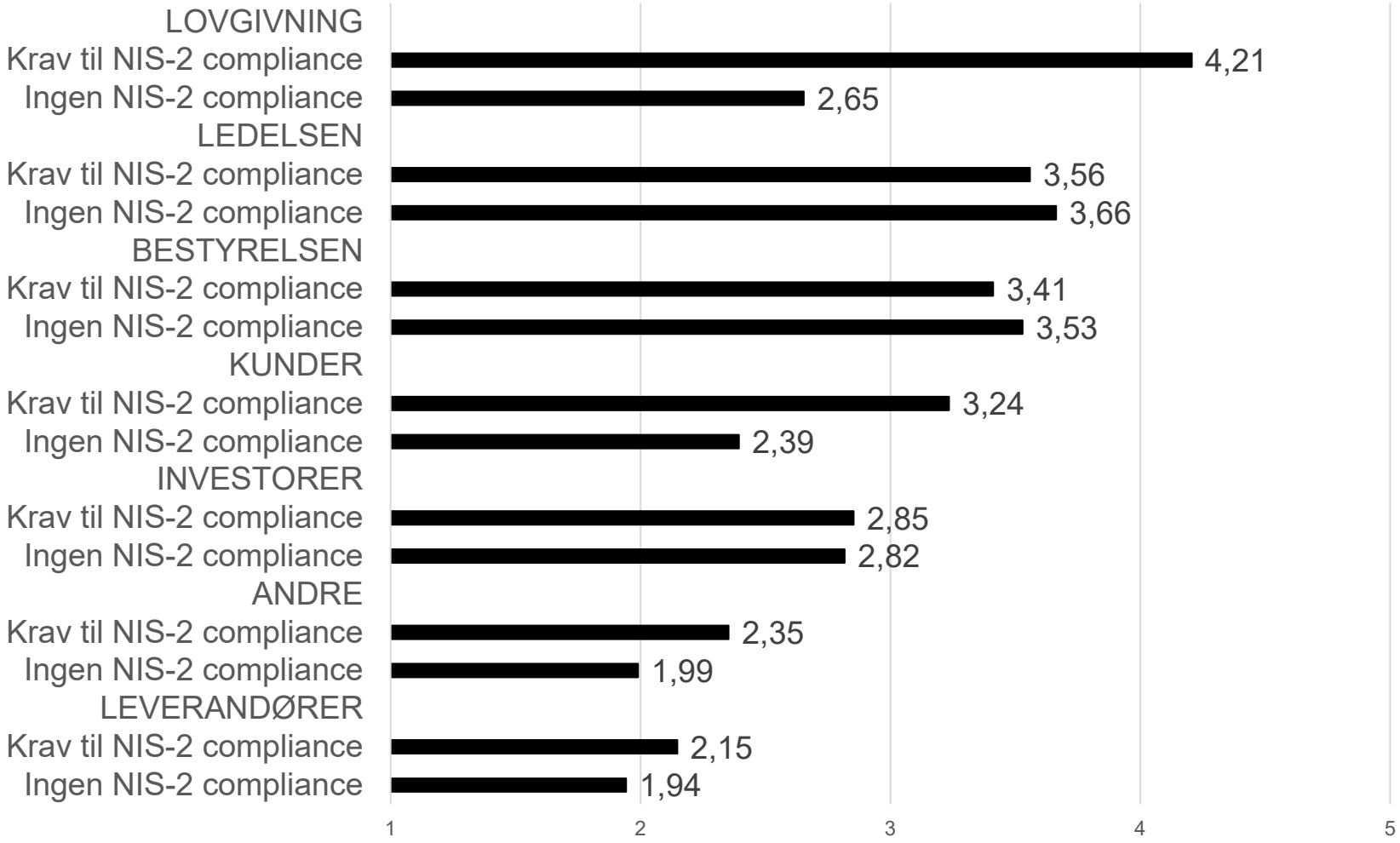


Kilde: Stentoft et al. (2026)

Krav til cybersikkerhed fra virksomhedens interessenter



Krav til cybersikkerhed fra virksomhedens interessenter

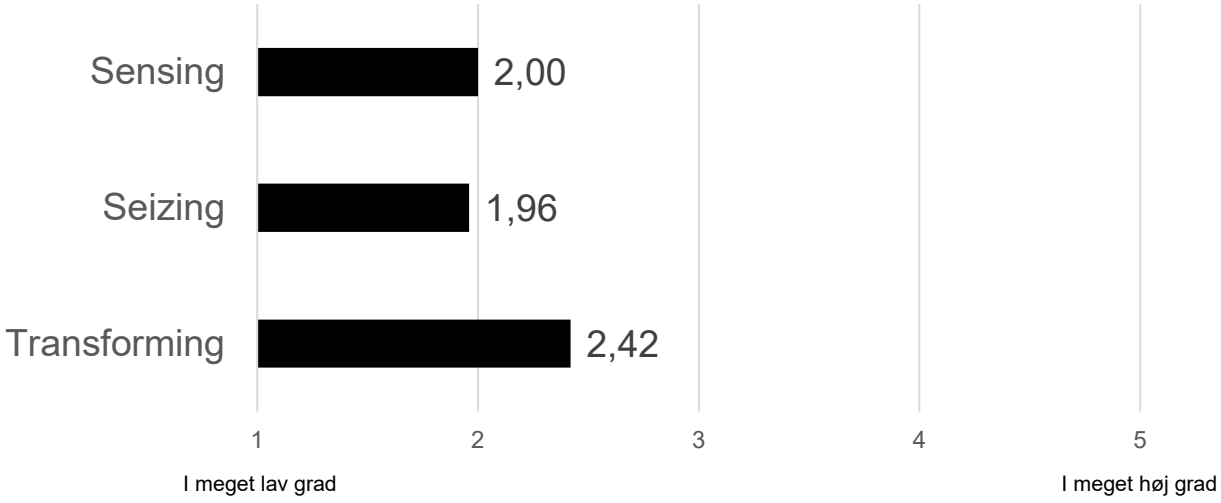


Dynamiske kapabiliteter

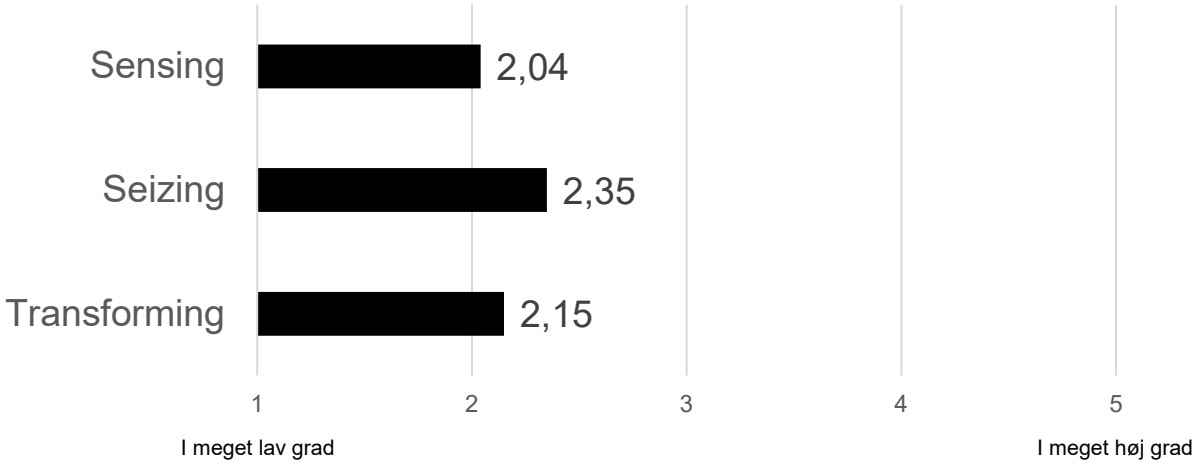
- I en verden præget af teknologiske forandringer, geopolitisk usikkerhed og stigende cybertrusler er det ikke længere tilstrækkeligt, at virksomheder blot er effektive i deres daglige drift.
- Virksomheder skal også kunne **tilpasse sig**, **omstille sig** og **løbende forny sig**. Dette er kernen i teorien om dynamiske kapabiliteter.
- Dynamiske kapabiliteter kan defineres som en virksomheds *evne til at integrere, opbygge og omkonfigurere interne og eksterne kompetencer som reaktion på hurtigt foranderlige omgivelser*.
- Hvor ordinære kapabiliteter handler om at "gøre tingene rigtigt" i den daglige drift (f.eks. producere effektivt og levere til tiden), handler dynamiske kapabiliteter om at "gøre de rigtige ting", når omgivelserne ændrer sig.

Dynamiske kapabiliteter

Cybersecurity dynamiske kapabiliteter



Geopolitiske dynamiske kapabiliteter



Geopolitiske markedskræfter

Geopolitisk risikostyring

Sammenfatning

- 25 % har oplevet cyberangreb
- NIS2: 22 % omfattet, 67 % ikke, 11 % ved ikke
- Krav drives primært af ledelse – næstmest fra bestyrelse
- Lav modenhed i værdikæden → få krav til kunder/leverandører
- Svagt fokus på supply chain risk management → stort udviklingsbehov
- Lave dynamiske kapabiliteter (sensing, seizing, transforming) → risiko for langsom reaktion
- Geopolitik påvirker i nogen grad (især cybertrusler og krig)
- Generelt lavt niveau af geopolitisk risikostyring

- **Konklusion:** SMV'er har styr på grundlæggende cybersikkerhed, men mangler strategisk fokus og robusthed – især i værdikæder og ift. eksterne risici.

Cyberværktøjer

Udviklede værktøjer

Værktøjer til cybersikkerhed i SMV'er

- Praktiske værktøjer til at styrke cybersikkerhed (teknisk, organisatorisk og menneskeligt)
- Udviklet til SMV'er med begrænsede ressourcer og komplekse risici

Værktøjskassen gør det muligt at:

- Forstå cyberrisici
- Sikre forsyningskæder og drift
- Kombinere teknologi, organisation og adfærd
- Omsætte sikkerhed til konkrete handlinger
- Består af skabeloner, tjeklister og processer med klare trin
- Hvert værktøj har formål, deltagere og anvendelsesvejledning

Overblik over værktøjer

Supply Chain Resilience procesmodel

Fase 1
Kortlæg forsyningskæden

Fase 2
Individuel vurdering af sårbarheder og kapabiliteter

Fase 3
Fælles vurdering af sårbarheder og kapabiliteter

Fase 4
Udvikling af handleplaner

Cyberrelaterede sårbarheder og kapabiliteter

1 værktøj

Fremtidsscenarier

1: USA's tilbagetrækning fra Europa
2: USA-Kina konfrontation om Taiwan
3: Klimaforandringer
4: Økonomisk polarisering
5: Når AI går amok

1 værktøj

Cyber risikostyring i forsyningskæderne

11 værktøjer

Forretningskontinuitet

7 værktøjer

Cyber mindset

6 værktøjer

Cyber resiliens

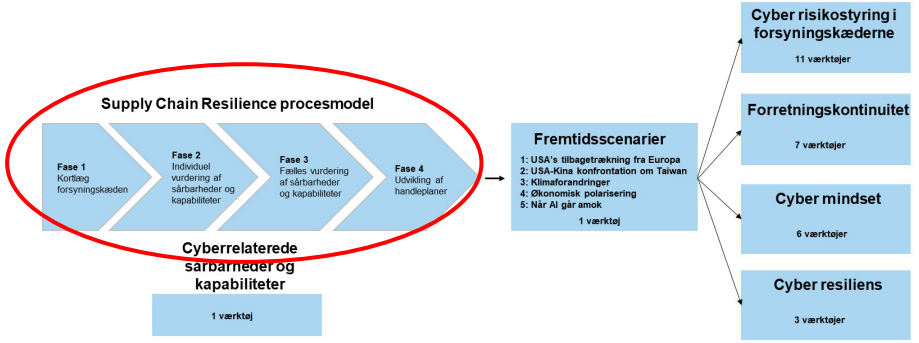
3 værktøjer

www.cyber-smv.dk

Supply Chain Resilience procesmodellen

Et tværorganisatorisk team fra virksomheden deltager, som typisk består af repræsentanter fra:

- Salg
- Produktion
- Indkøb
- Produktudvikling
- Økonomi
- IT



Processen gennemføres i fire faser:

1. Kortlægning af forsyningskæder
Overblik over leverandører, afhængigheder og kritiske forbindelser.

2. Individuel vurdering
Medarbejdere vurderer sårbarheder og kapabiliteter ved hjælp af software.

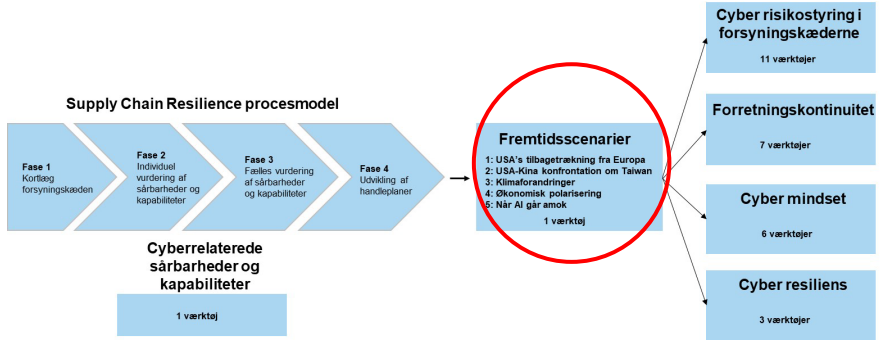
Fælles vurdering
3. Teamet samler og diskuterer vurderingerne i et fælles, softwareunderstøttet overblik.

4. Handleplaner
Konkrete og prioriterede indsatser, der styrker robusthed og reducerer risiko.

Formålet er at skabe **fælles forståelse, bedre beslutninger og målrettede handlinger**.

Fremtidsscenarier

Scenariearbejde – cybersikkerhed i en usikker verden
Det andet værktøj arbejder med **strategiske scenarier**, der viser, hvordan ændringer i det globale forretningsmiljø kan øge virksomheders sårbarhed over for cyberangreb.



Vejledning: Sådan gennemføres øvelsen

De fem scenarier er:
USA's tilbagetrækning fra Europa
USA-Kina-konfrontation om Taiwan
Klimaforandringer
Økonomisk polarisering
Når AI går amok

Scenarierne bruges til at:
Teste virksomhedens robusthed identificere nye typer cyberrisici understøtte strategisk dialog og ledelsesbeslutninger

Spørgsmål til scenarierne
1. Hvad er de vigtigste risikofaktorer og sårbarheder i dette scenarie?
2. Hvilke risici udgør dette scenarie for danske virksomheder?
3. Hvilke sårbarheder påvirker jeres virksomhed?
4. Hvilke mitigeringsinitiativer, hvis nogen, har jeres virksomhed overvejet eller implementeret?

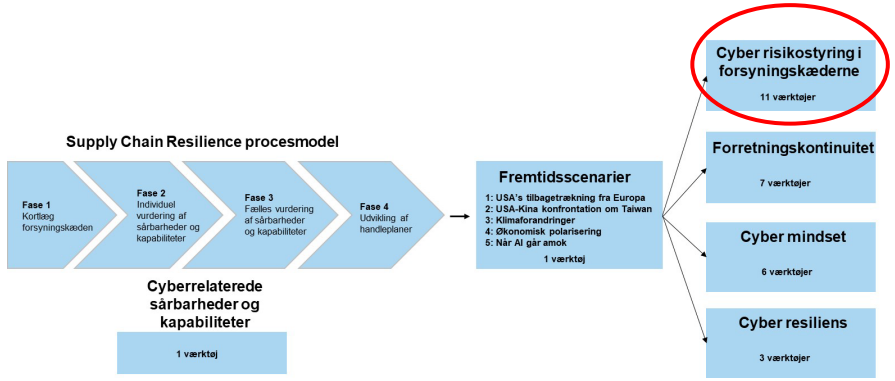
Cyber risikostyring i forsyningskæden

Det tredje sæt består af **10 operationelle værktøjer**, der adresserer cybersikkerhed i et forsyningskædeperspektiv.

Værktøjerne er:

- Struktureret efter **NIST-rammeværket**
- Oversat til konkrete handlinger, der kan bruges i hverdagen
- Målrettet samarbejde med leverandører og partnere

Fokus er på at gøre cybersikkerhed **praktisk, prioriterbar og anvendelig**.



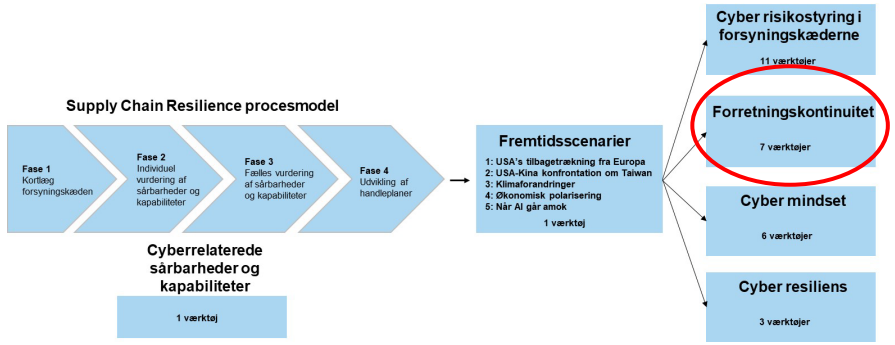
Værktøjer til cyber risikostyring i forsyningskæden:

0: Overblik
1: Strategi for risikostyring og interessentanalyse
2: Cybersikkerhedsroller og ansvarsområder
3: Integration af cybersikkerhed i risikostyring og forbedringsprocesser
4: Leverandørprioritering
5: Cybersikkerhed i kontrakter
6a: Cybersecurity due dilligence mod nye kunder
6b: Cybersecurity due dilligence mod nye leverandører
7: Cybersikkerhedsregister
8: Involvering af partnere ved cyberhændelser
9: Integrering af supply chain cybersikkerhed gennem hele produktlivscyklussen
10: Tjekliste for ophør af samarbejde

Forretningskontinuitet

Det fjerde sæt indeholder **7 værktøjer til forretningskontinuitet**, der handler om virksomhedens evne til at:

- Opretholde eller hurtigt genoptage kritiske funktioner
- Håndtere alvorlige forstyrrelser som:
  - IT-nedbrud
  - Cyberangreb
  - Brand
  - Leverandørsvigt



Værktøjerne udgør tilsammen en pragmatisk tilgang, der hjælper produktions-SMV'er med at beskytte drift, leverancer og forretning.

Værktøjerne er bevidst opbygget, så man:

- Forstår forretningen
- Identificerer risici
- Prioriterer afhængigheder
- Planlægger handling
- Træner beslutninger

De 7 værktøjer er:

1. Business Impact Analysis (BIA)
2. Risiko- og sårbarhedsanalyse
3. Leverandørkritikalitetsanalyse
4. Kontinuitetsplaner
5. Scenarieplanlægning
6. Cyberberedskabsplanlægning
7. Tabletop-øvelser

Cyber mindset

Mentale modeller for cybersikkerhed – mennesket i centrum
Det femte sæt fokuserer på **mentale modeller og adfærd** og består af **6 værktøjer** udviklet til awareness-træning.

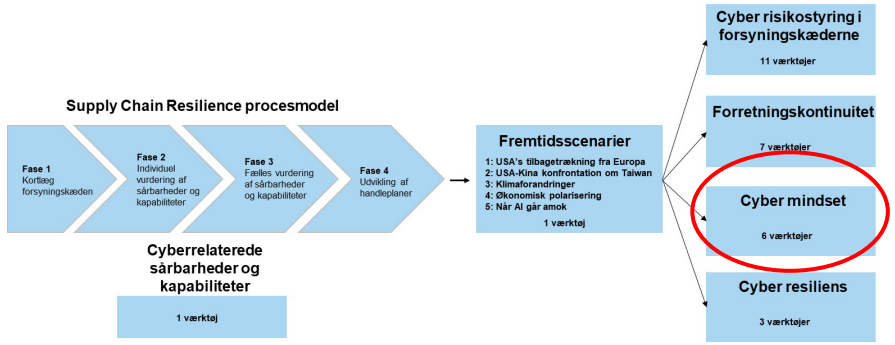
Cybersikkerhed handler ikke kun om teknologi og politikker – det handler i høj grad om **menneskelig adfærd** i en hverdag præget af:

- Travlhed
- Kompleksitet
- Konstante afbrydelser

De fleste cyberangreb lykkes ikke, fordi teknologien fejler, men fordi mennesker presses til at handle hurtigt, ureflekteret eller i god tro.

Værktøjerne giver medarbejdere:

- Enkle og genkendelige tankeprincipper
- Støtte til at stoppe op og tænke sig om
- Hjælp til konkrete situationer, **før der klikkes, deles, betales eller reageres**



Værktøjerne er:

Antag komprimittering
Angriberens perspektiv
Lag på lag (Defense in Depth)
Pause-knappen (Slow Down)
Normalisering af fejl (Just Culture)
Signal vs støj (Attention Economics)

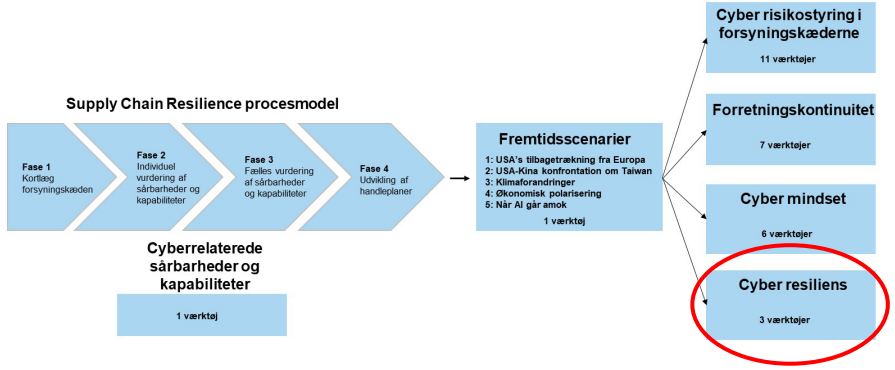
Cyber resiliens

Dette sjette sæt værktøjer understøtter organisationer i at øge deres cyberrobusthed ved at forstå, reducere og håndtere digitale trusler på tværs af interne processer, produkter og eksterne relationer.

Mere specifikt hjælper værktøjerne organisationer med at:

- Forudse, modstå og tilpasse sig cybertrusler og -forstyrrelser
- Beskytte kritiske aktiver såsom immaterielle rettigheder og følsomme data
- Håndtere afhængigheder af leverandører og samarbejdspartnere gennem hele produkt- og/eller servicelevetiden

Værktøjerne har fokus på forebyggelse, beredskab og løbende forbedringer, hvilket gør det muligt for organisationer at reducere deres eksponering for cyberhændelser og opretholde deres sikkerhed i et trusselsbillede under konstant forandring.



Værktøjerne er:

Beskyttelse af intellektuel ejendomsret
Risikoreduktion ved indgåelse af leverandør eller andre tredjepartsrelationer
Sikkerhedspraksisser i forsyningskæden set fra et produkt og tjenestelivscyklusperspektiv

Øh, hvor skal vi starte? Et bud på en proces

- Se den skitserede proces i fire faser som en praktisk guide
- Identificér og anvend de vigtigste værktøjer i hvert step
- Gennemfør konkrete handlinger løbende over de første 60 dage
- Tilpas tempo og omfang efter virksomhedens prioriteter
- Implementér øvrige værktøjer efter de første 60 dage

Fase 1 – dag 1-15: Skab overblik, ejerskab og forretningskritikalitet

Step	Værktøj (VT)	Hvad virksomheden gør	Ejerskab og output
1	VT. 1. Supply Chain Resilience-procesmodellen VT. 3.1: Strategi for risikostyring og interessentanalyse VT. 3.2: Cybersikkerhedsroller og ansvarsområder	Direktionen nedsætter et lille tværgående team (fx drift, indkøb, økonomi og IT/ekstern IT). Fastlæg scope, beslutningsrum, møderytme og hvilke forretningsområder der er med i første bølge.	Ejerskab: xx Output: Ejerskab, mandat, team, scope og mødeplan
2	VT. 3.0: Overblik VT. 4.1: Business Impact Analyse (BIA)	Kortlæg de 5-10 mest kritiske processer, systemer, data, nøglekunder og leverandører. Beslut hvad der maksimalt må være nede, og hvad der først skal genstartes ved et nedbrud.	Ejerskab: xx Output: Liste over kritiske processer, maksimal nedetid og afhængigheder
3	VT. 4.2: Risiko- og sårbarhedsanalyse	Vurder de mest realistiske hændelser: Phishing/Business E-mail Compromise, ransomware, kompromitterede konti, nedbrud hos IT-leverandør, ERP eller mail nede og eventuel OT/produktionspåvirkning. Prioritér de 10 største risici.	Ejerskab: xx Output: Prioriteret risikoliste

- Man bør starte med disse værktøjer, fordi ledelsen ellers ikke ved, hvad der er forretningskritisk, hvem der ejer indsatsen, eller hvor de største risici ligger.
- Formålet er at give ledelsen et reelt greb om cybersikkerhedsopgaven, før virksomheden begynder på en lang liste af tekniske tiltag.

Fase 2 – dag 16-30: Prioritér leverandører og byg styring

Step	Værktøj (VT)	Hvad virksomheden gør	Ejerskab og output
4	VT. 4.3: Leverandørkritikalitetsanalyse	Del leverandører i A/B/C efter betydning for drift, data og leveringsevne. Identificér de få leverandører, hvor en cyberhændelse reelt kan stoppe virksomheden eller skabe større tab.	Ejerskab: xx Output: Prioriteret leverandørliste
5	VT. 3.7: Cybersikkerhedsregister VT. 3.3: Integration af cybersikkerhed i risikostyring og forbedringsprocesser	Omsæt risici til et samlet register med risiko, ejer, handling, deadline og status. Indbyg registeret i ledelsesmøder, tavler, forbedringsarbejde eller eksisterende risikostyring, så cybersikkerhed bliver et fast ledelsespunkt.	Ejerskab: xx Output: Aktivt register og månedlig opfølgningsrytme
6	VT. 3.5: Cybersikkerhed i kontrakter VT. 3.6b: Due diligence mod nye leverandører	Definér minimumskrav til de vigtigste leverandører og nye leverandører: MFA, backup, adgangsstyring, hændelsesvarsling, kontaktpunkter, underleverandører og adgang ved ophør. Brug et kort minimumssæt – ikke et tungt compliance-program.	Ejerskab: xx Output: Minimumskrav og standardspørgsmål til leverandører

- Disse værktøjer omsætter analysen til styring og minimumskrav.

Fase 3 – dag 31-45: Byg minimumsberedskab og adfærdsregler

Step	Værktøj (VT)	Hvad virksomheden gør	Ejerskab og output
7	VT. 4.4: Kontinuitetsplaner	Lav 3-5 korte planer for de mest sandsynlige afbrydelser, fx mail nede, ERP utilgængelig, ransomware, tab af filadgang eller leverandørsvigt. Beskriv manuelle workarounds, prioriterede aktiviteter og hvem der beslutter hvad.	Ejerskab: COO/driftschef Output: Korte kontinuitetsplaner pr. scenarie
8	VT. 4.6: Cyberberedskabsplanlægning VT. 3.8: Involvering af partnere ved cyberhændelser	Saml alarmkæde, eskalation, roller, ekstern bistand, kundekommunikation, leverandørkontakt og beslutningspunkter i én operativ beredskabsplan. Aftal hvem der kontaktes først internt og eksternt.	Ejerskab: xx Output: Cyberberedskabsplan og kontaktliste
9	VT. 5.4: Pause-knappen VT. 5.1: Antag kompromittering	Gennemfør en kort leder- og medarbejderbriefing. Indfør få adfærdsregler med høj effekt: stop-op ved betalings- og kontoskift, rapportér fejl hurtigt, og gå ud fra at konti kan kompromitteres.	Ejerskab: xx Output: 3-5 fælles adfærdsregler og rapporteringsvej

- Her går virksomheden fra analyse til handlingsplaner, der kan bruges under en reel hændelse.

Fase 4 – dag 46-60: Test, justér og vælg næste modenhedstrin

Step	Værktøj (VT)	Hvad virksomheden gør	Ejerskab og output
10	VT. 2: Fremtidsscenarier	Brug ét eller to relevant scenarie til at udfordre planerne, f.eks. AI-misbrug, geopolitisk uro eller væsentlig leverandørforstyrrelse. Test om de valgte prioriteringer holder under pres.	Ejerskab: XX Output: Justerede antagelser og ekstra tiltag Ledelsesmæssigt fremadblik
11	VT. 4.5: Scenarieplanlægning VT. 4.7: Tabletop-øvelser VT. 5.2: Angriberens perspektiv VT. 5.3: Lag på lag (Defense in Depth)	Afhold en 1,5-2 timers tabletop-øvelse med ledelsen og nøglefunktioner. Gennemspil et realistisk angreb trin for trin og test beslutninger, samarbejde, kommunikation og genopretning. F.eks. kompromitteret mailkonto med efterfølgende ransomware eller nedbrud hos kritisk leverandør. Notér alle brud i ansvar og plan.	Ejerskab: xx Output: Øvelsesnotat, læringspunkter og korrigerende handlinger
12	VT. 3.3: Integration af cybersikkerhed i risikostyring og forbedringsprocesser VT. 5.5: Normalisering af fejl	Beslut faste rutiner: Månedlig registergennemgang, kvartalsvis leverandøropdatering, årlig tabletop og rapportering af fejl og næsten-fejl uden skyldkultur.	Ejerskab: xx Output: Varig ledelsesrytme
13	VT. 6: Cyber Resiliens-værktøjerne VT. 3.10: Tjekliste for ophør af samarbejde	Brug de sidste dage til at beslutte næste kvartals modning: Beskyttelse af intellektuel ejendomsret, risikoreduktion ved nye tredjepartsrelationer, sikkerhedspraksisser i produkt-/tjenestelivscyklus og tjekliste ved ophør af samarbejde. Vælg kun de 3-5 næste tiltag, der reducerer mest risiko.	Ejerskab: xx Output: Næste 90 dages modenheds-roadmap

- Disse værktøjer giver størst værdi, når virksomheden allerede har et minimum af overblik, roller og planer.

Hvad ledelsen bør stå med ved dag 60

- Et navngivet cyberteam med tydelige roller og fast møderytme.
- En light *Business Impact Analysis* med prioriterede kritiske processer, maksimal nedetid og afhængigheder.
- En prioriteret risiko- og sårbarhedsliste, samt et aktivt cybersikkerhedsregister.
- En liste over kritiske leverandører samt korte minimumskrav til kontrakter og nye leverandører.
- Korte kontinuitetsplaner, en operativ cyberberedskabsplan.
- Mindst én gennemført Tabletop-øvelse med læringspunkter og en fast ledelsesrytme
- Et besluttet næste 90-dages modenheds-roadmap med få, prioriterede tiltag.

CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Program

14.30 – 15.00	Ankomst med kaffe og te
15.00 – 15.10	Velkomst v/Jan Stentoft, professor, SDU
15.10 – 15.40	En digitaliseret supply chain resilience-model med cyberrelaterede sårbarheder og kapabiliteter v/Jan Stentoft, professor, SDU og Marco Peressotti, lektor, SDU
15.40 – 16.00	Uerkendte sårbarheder vælter driften. Erkendte sårbarheder kan ledes v/Ole Anker Aagaard, Head of Legal and Compliance, ExamVision
16.00 – 16.15	Pause
16.15 – 16.45	Sådan arbejder du med fremtidsscenarier v/Vincent Keating, lektor, SDU
16.45 – 17.05	Cybersikkerhed som en driftsdisciplin – ikke et IT-projekt v/COO Søren Lind Therkildsen, GomSpace A/S
17.05 – 17.15	Ekstern projektevaluering v/Amalie Therkelsen Agerbæk, chefkonsulent, Ineva
17.15 – 17.55	Resultater fra landsdækkende cyberundersøgelse og præsentation af cyberværktøjer v/Jan Stentoft, professor, SDU
17.55 – 18.00	**Afrunding v/Jan Stentoft, professor, SDU**

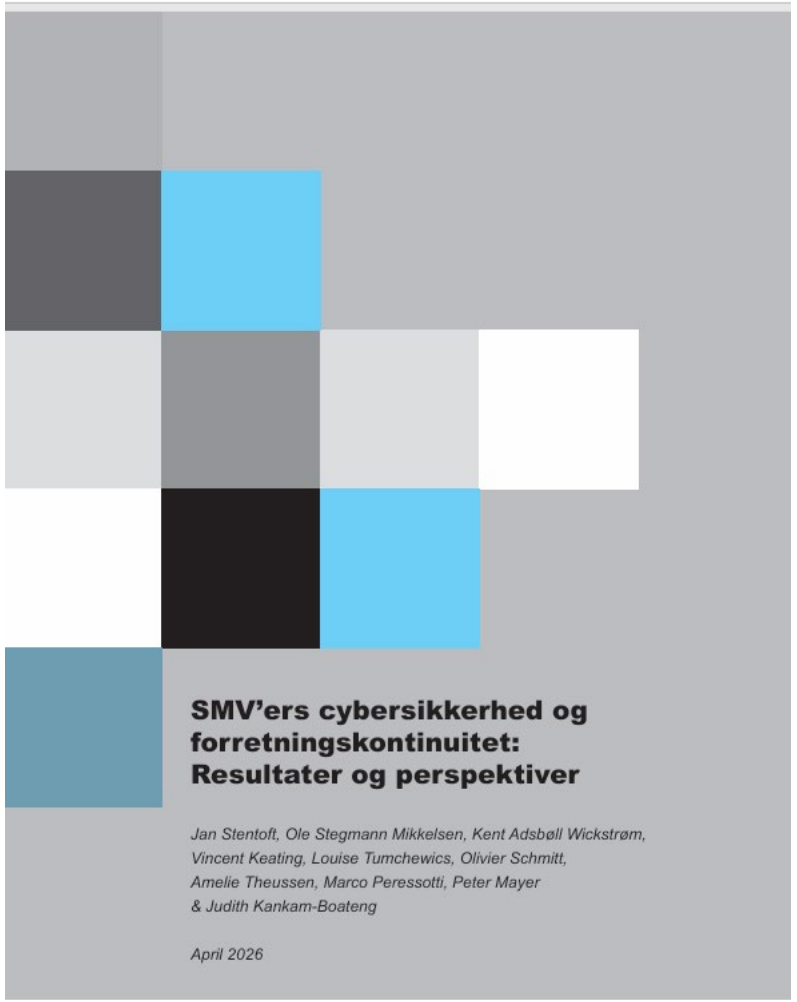
CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Den afsluttende rapport fra projektet er tilgængelig på: https://cyber-smv.dk/formidling/



Gør dine risici håndgribelige og målbare

Funktioner og udbytte:

- Din værktøjskasse til risikovurderinger og dokumentation
- Identifikation og vurdering af trusler, risici og konsekvenser
- Indbygget trusselscenarier og spørgsmål
- Beregning af omkostninger på sikkerhedsforbedringer
- Referencer til NIS-2, ISO27000, D-mærket og IEC62443
- Output: Rapporter med økonomiske vurderinger til beslutning

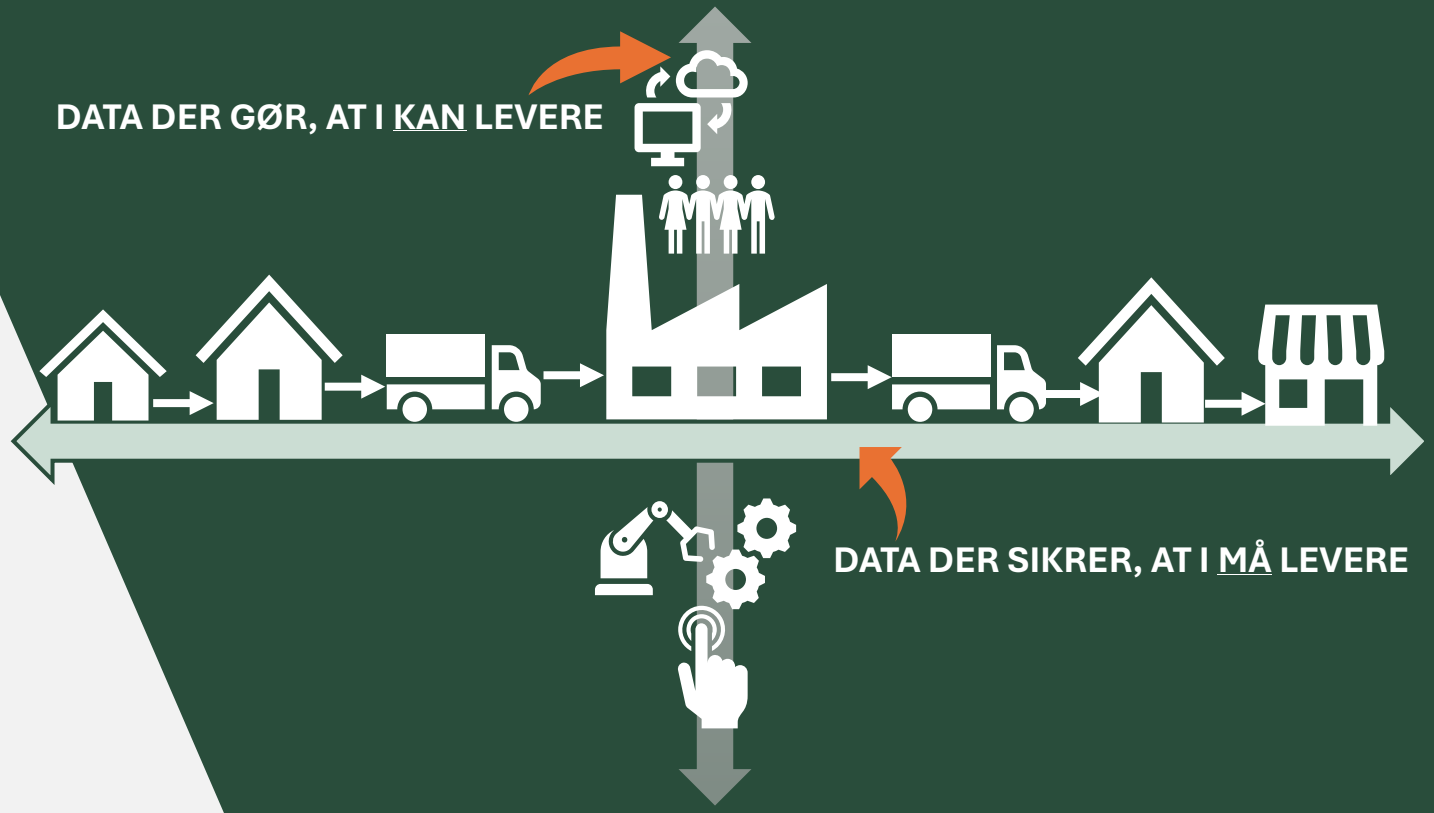
INDUSTRIENS FOND

Food & Bio Cluster Denmark

SecuriOT Risk Assessment Tool

CYBERSIKRE FØDEVAREVÆRDIKÆDER

SIKKERHED STYRKER FORRETNINGEN



Finansieret af
INDUSTRIENS FOND

Food & Bio Cluster Denmark

SecuriOT

SDU

Cybersikre Fødevareværdikæder

At styrke cybersikkerhed og konkurrenceevne i fødevareproduktion ...

...for at blive mere leveringssikre i en tid med flere og mange trusler, og...

... få mere indsigt i forsynings- og værdikædens betydning for forretningen!

Virksomhedsworkshops

1. Kortlægger af jeres forsyningskæde
2. Identificerer kritiske afhængigheder og sårbarheder
3. Risikovurdering, anbefalinger til konkrete sikkerhedstiltag
4. Adgang til værktøjet RAT (Risk Assessment Tool)
5. Forskellige værktøjer – guides og skabeloner

Relevante deltager fra virksomheden – salg, indkøb, logistik/supply chain, produktion, m.f.

Værdikædeworkshop – datadeling i værdikæden

1. Overblik over dataflow i værdikæden
2. Fælles fokus på sårbarheder og risici i digitale processer
3. Styrket beredskab mod cyberangreb, der kan ramme flere led samtidigt
4. En vurdering af værdikædens resiliens
5. Forskellige værktøjer – guides og skabeloner

→ Det er gratis at deltage – tid og engagement!

Virksomheds – og værdikædeworkshops

Virksomheds workshop

Introduktion til værktøjer

Virksomhedsworkshop

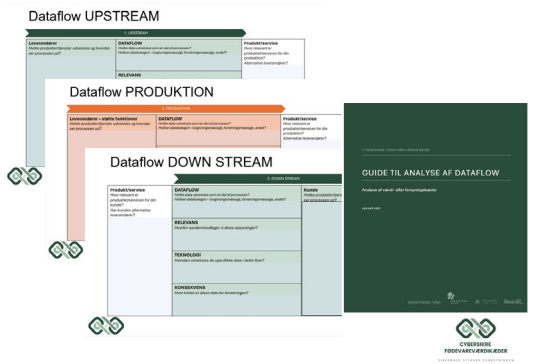
Værdikæde kortlægning
Risikohåndtering

Output

Anbefalinger til handlinger

Værdikæde workshop

Introduktion til værktøjer

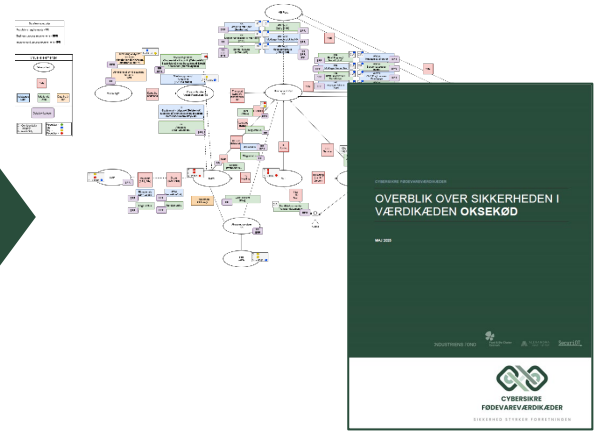


Værdikædeworkshop

Dataflow i værdikæden

Output

Overblik over dataflow
Rapport over værdikædens resiliens



Links til de øvrige projekter i cyberporteføljen

Cyber Safe Robotics, **Odense Robotics** – link til projektet

Cybersikre Fødevareværdikæder, **Food & Bio Cluster Denmark** – link til projektet

Styrket cybersikkerhed for SMV'er, **Erhvervshus Midtjylland** – link til projektet

Cybersikre forsyningskæder, **CBS** - link til tool

Tak til:

Industriens Fond,
styregruppen,
referencegruppen,
deltagerne i udvikling af scenarier,
deltagerne fra case-virksomhederne,
de fire øvrige projekter i cyberporteføljen
+ studerende fra SDU