Cyber Security
Supply Chain Risk Management

Presentation by **William Sharp,** PwC – Technology & Security

Supply Chain security 13. maj 2025

Short intro

William Sharp
PwC | Partner
Technology & Security
D: +45 8932 0076 | M: +45 4040 1074
Email: william.sharp@pwc.com | www.pwc.dk
Nobelparken, Jens Chr. Skous Vej 1, DK-8000 Aarhus C

Agenda

1 Intro
2 What regulators say
3 Terminologi
4 Supply chain cyber risk management
5 Contractual considerations
6 Operational considerations
7 Wrap-up and questions

“

Den stadig **stigende digitalisering** af samfundets kritiske infrastruktur bærer en lang række fordele med sig, men øger også **behovet for at styrke cybersikkerheden** i organisationer og forsyningskæder.

NIS2 **styrker det generelle niveau af cybersikkerhed** i EU ved at **skærpe kravene til cybersikkerhed**.

Hurtigt overblik

- Godkendt i Folketinget – **træder i kraft 1. juli 2025.**
- **Flere sektorer omfattet**, inkl.: offentlige myndigheder, fødevare- og fremstillingssektoren, samt digital infrastruktur og udbydere mfl.
- NIS2 vil **påvirke hele forsyningskæden** (up- and downstream).
- NIS2 stiller betydeligt **skærpede krav til cybersikkerheden** i virksomheder og offentlige myndigheder, der er tilknyttet disse sektorer.
- **Ledelsesansvar:** Den **øverste ledelse** har fået en fremtrædende og central rolle, hvorfor medlemmer med ledelsesansvar kan ifalde **individuelt og personligt ansvar**.

Væsentligste krav i NIS2

1 Ledelsesansvar (Artikel 20)

Ledelsesorganerne skal

1) **godkende** organisationens risikostyring af cybersikkerhed,

2) **føre tilsyn** med implementeringen heraf,

3) modtage **regelmæssig træning** indenfor cybersikkerhed.

4) **Ledelsen kan holdes ansvarlig** for overtrædelser og pligtforsømmelser, jf. straffelovens § 155, 156 og 157 samt tjenestemandsloven, i henhold til overenskomst.

Medlemmer af Folketinget, regionsråd og kommunalbestyrelser er undtaget, idet ministeransvarsloven, kommunestyrelsesloven og regionsloven i stedet gør sig gældende på dette område.

2 Sikkerhedsforanstaltninger (Artikel 21)

Organisationen skal træffe **passende og forholdsmæssige** tekniske, operationelle og organisatoriske **sikkerhedsforanstaltninger til håndtering af cybersikkerhedsrisici**.

Disse skal baseres på en konkret risikovurdering under inddragelse af risikoeksponering og størrelse samt sandsynligheden for og konsekvenserne ved et angreb.

De skal som **minimum** omfatte de foranstaltninger, der er nævnt i direktivets Artikel 21, stk. 2, litra a-j, herunder fx **forsyningskæders sikkerhed**.

3 Rapporterings- og indberetningsforpligtelser (Artikel 23)

Krav om at

1. **informere kunder** om faktiske og potentielle cyberhændelser samt

2. **rapportere** sådanne hændelser til myndighederne.

Trinvis rapportering:

- Initiel "early warning" uden unødig ophold og **inden for 24 timer**.
- Supplereres med en udførlig hændelsesunderretning uden unødig ophold og **inden for 72 timer**.
- Løbende status ved anmodning.
- Endelig rapport bør indgives senest **en måned** efter hændelsesunderretningen.

4 Tilsyn og sanktioner (Artikel 32 og 34)

Tilsyn

- 'Vigtige enheder' enheder vil blive underlagt et reaktivt efterfølgende tilsyn (ex post).
- 'Væsentlige' enheder vil blive underlagt *ex ante* tilsyn, herunder tilfældige inspektioner, regelmæssige og ad hoc revisioner, sikkerhedsscanninger for at kontrollere sårbarheder samt anmodninger om visse oplysninger og dokumentation for overholdelse.

Sanktioner (ingen administrative bøder)

- I dansk ret gælder det generelle princip, at staten, regioner og kommuner kun kan straffes for overtrædelser begået ved udøvelse af virksomhed, der svarer til eller kan sidestilles med privat virksomhed (jf. straffelovens § 27, stk. 2).

NIS2 minimumskrav

2

Sikkerhedsforanstaltninger
(Artikel 21)

a) Politikker for risikoanalyse og informationssystem-sikkerhed

b) Håndtering af hændelser

c) Driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

d) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

e) Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

f) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

h) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

i) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

j) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Status i Danmark

Selvvurdering og registrering
Enheder er ansvarlige for at vurdere, om de er omfattet af NIS2, og skal selv registrere sig hos den kompetente myndighed.
Deadline: 17. april 2025 (bliver udskudt)

17. oktober 2024

NIS2-direktivet

1. juli 2025

NIS2 hovedloven
Rammelovgivning på tværs af sektorer.

2025

Bekendtgørelser
De specifikke krav til fx foranstaltninger vil blive fastsat i de sektorspecifikke bekendtgørelser.

Sektorspecifik lovgivning
Ikke omfattet af NIS2 hovedloven – særskilt reguleret.

Telesektor	Finanssektor	Energisektor
1. juli 2025	1. juli 2024	2025

Gennemførelsesretsakter
Direkte virkning, hvor der er behov for ensartet gennemførelse, fx organisationer med grænseoverskridende karakter.

September 2024

Udkast for digitale udbydere, fx cloud computing service providers, data centre service providers, managed service providers, managed security service providers mfl.

Ledelsesansvaret i henhold til NIS2-direktivet

Artikel 20

1

Godkende de foranstaltninger til styring af cybersikkerhedsrisici, som organisationen har truffet med henblik på at overholde Artikel 21 om sikkerhedsforanstaltninger

- **Etablering af governance**
- **Godkende en strategi for risikostyring af cybersikkerhed** fx godkende anvendelsen af anerkendte sikkerhedsstandarder
- **Godkende risikovurderinger.** Samfundsperspektivet: hvilke risici og trusler kan kompromittere de samfundskritiske leverancer og samfundet?
- **Fastlægge risikoappetit på baggrund af cybersikkerhedsstrategien og risikovurderingerne.** Hvad er vi villige til at acceptere?
- **Godkende tekniske, operationelle og organisatoriske sikkerhedsforanstaltninger**, fx informationssikkerhedspolitik, politik vedrørende risikovurderinger, håndtering af hændelser, forretningskontinuitet, krisestyring, forsyningskædesikkerhed mv.
- **Sikre, at minimumskravene i NIS2 er opfyldt**

2

Føre tilsyn med implementeringen og efterlevelsen af foranstaltningerne

- **Modtage tilstrækkelig rapportering**, fx sikkerhedstest, hændelser mv.
- **Vurdere effektiviteten og efterlevelsen af de implementerede foranstaltninger** til styring af cybersikkerhedsrisici på baggrund af fx løbende rapporter og audits.

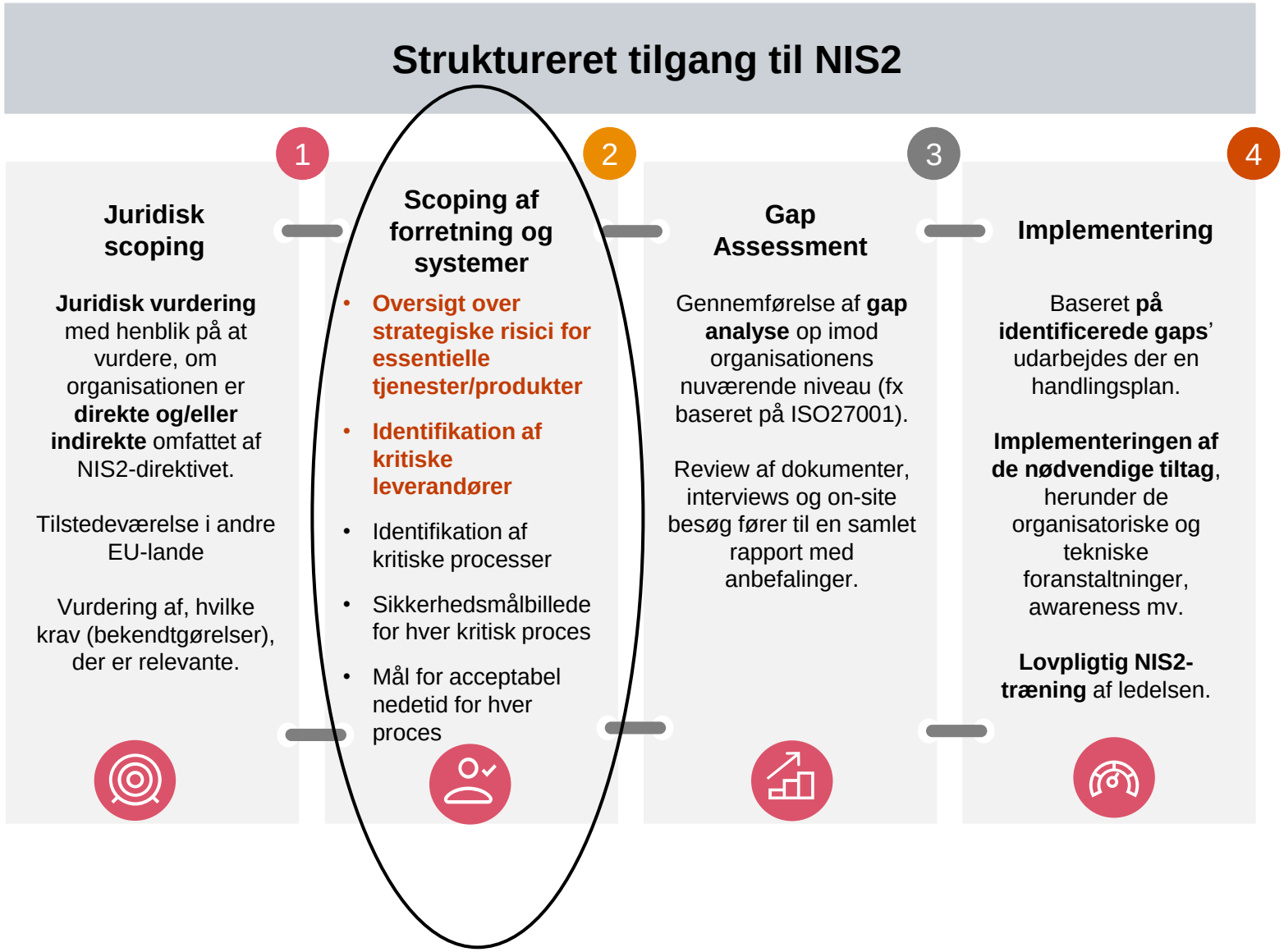
3

Modtage **regelmæssig træning** indenfor cybersikkerhed

- **Løbende at modtage træning** i form af fx kurser, så de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af organisationen.
- Ledelsesmedlemmerne skal også **tilskynde**, at ansatte i organisationen modtager tilsvarende løbende træning.

Ledelsesmedlemmer kan gøres **personligt ansvarlige** for manglende overholdelse af NIS2-direktivet

Struktureret tilgang til NIS2

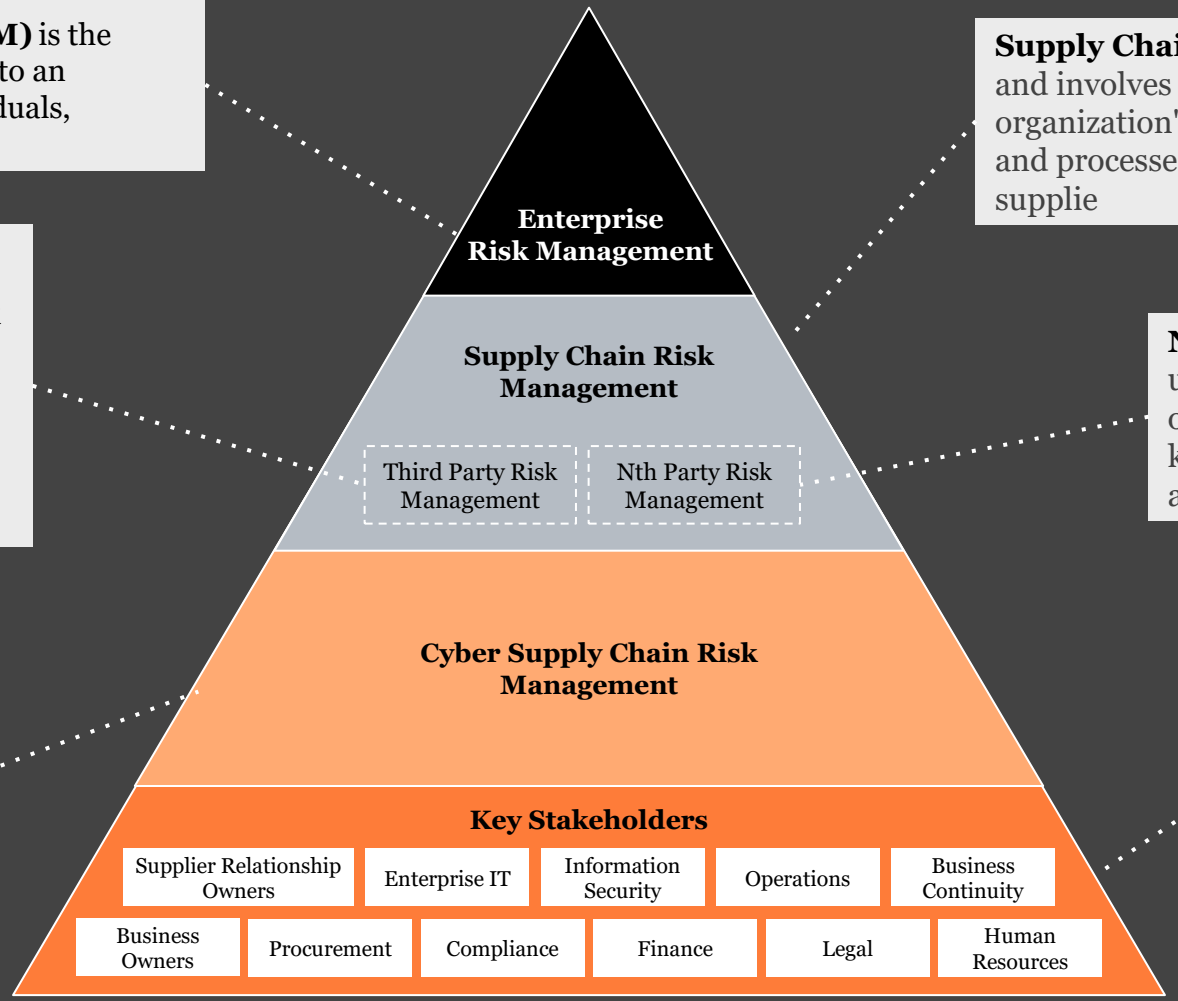


Terminology Baseline

Enterprise Risk Management (ERM) is the program and processes to manage risks to an organization's operations, assets, individuals, environment, and supply chain.

Third Party Risk Management (TPRM) is a subset of supply chain risk management that systematically manages risks from an organization's direct suppliers and their products and services, without extending to their supply chain.

Cyber Supply Chain Risk Management (C-SCRM) systematically manages cyber risk exposures, threats, and vulnerabilities throughout the supply chain, and develops response strategies for risks from suppliers, products, services, and the supply chain itself.



Supply Chain Risk Management is part of ERM and involves systematically managing risks in an organization's supply chain, including resources and processes between the organization and its supplie

Nth Parties include the upstream/downstream suppliers of an organization's third parties, also known as fourth, fifth, sixth parties, and so on.

Key stakeholders include various business units and roles responsible for executing or supporting C-SCRM activities. Executive Leadership, such as the CEO, CFO, CIO, CTO, and COO, sets the tone and direction for these activities across the organization.

Common Supply Chain Challenges Across Industries

The inability of organizations to effectively manage cyber risks in their supply chains can lead to significant incidents or business disruptions and ultimately result in operational, financial, regulatory, and reputational damage. Some of the common challenges faced by organizations regarding managing cyber supply chain risks are depicted below.

Lack of visibility

- Incomplete inventory of third-party suppliers, vendors, and partners
- No inventory and limited understanding of fourth- and subsequent party suppliers, vendors and partners
- Limited or no visibility into the security posture of known third-, fourth- and subsequent parties

Non-existent programs and insufficient organizational structure

- Non-existent processes and technology for managing upstream and downstream supply chain risk posed by third-, fourth- and subsequent party suppliers, vendors and partners
- Lack of resources dedicated to supply chain risk management

Process gaps, inconsistencies and inefficiencies

- Existing processes to perform due diligence, continuous monitoring, onboarding and offboarding of third-parties are manually intensive and ripe with inconsistencies
- No processes are in place for managing fourth- and subsequent parties
- Supply chain decisions are delayed or made with incomplete or inaccurate information particularly about inherent cyber risks

Limited understanding of cyber resilience of suppliers

- The technology and operational resilience of third-, fourth-, and subsequent parties to withstand adverse cyber events is not understood
- Organization's own plans for business continuity, incident response and disaster recovery are ill-conceived, incomplete, or not viable altogether due to this lack of understanding

Common Supply Chain Challenges Across Manufacturing

The heavy reliance on outsourced services and functions has created a condition where manufacturing organizations no longer fully control or have visibility into the supply chain ecosystem of their products and services. This lack of control and visibility significantly impedes their ability to understand and manage the associated cyber risk inherent in their supply chain. Moreover, the lack of supply chain cyber risk management can lead to significant incidents (breaches) which can lead to material operational, financial, regulatory, and reputational damage.

Lack of visibility

- Incomplete inventory of third-party suppliers, vendors and partners
- No inventory and limited understanding of fourth- and subsequent party suppliers, vendors and partners
- Limited or no visibility into the security posture of known third-, fourth- and subsequent parties

No program and insufficient organisational structure

- Non-existent processes and technology for managing upstream and downstream supply chain risk posed by third-, fourth- and subsequent party suppliers, vendors and partners
- Lack of resources dedicated to supply chain risk management

Process gaps, inconsistencies, and inefficiencies

- Existing processes to perform due diligence, continuous monitoring, onboarding/offboarding of third-parties are manually intensive and ripe with inconsistencies
- No processes are in place for managing fourth and subsequent parties
- Supply chain decisions are delayed or made with incomplete or inaccurate information particularly about inherent cyber risks

Limited understanding of cyber resilience of suppliers

- The technology and operational resilience of third-, fourth-, and subsequent parties to withstand adverse cyber events is not understood
- Organization's own plans for business continuity, incident response and disaster recovery are ill-conceived, incincomplete, or not viable altogether due to this lack of understanding

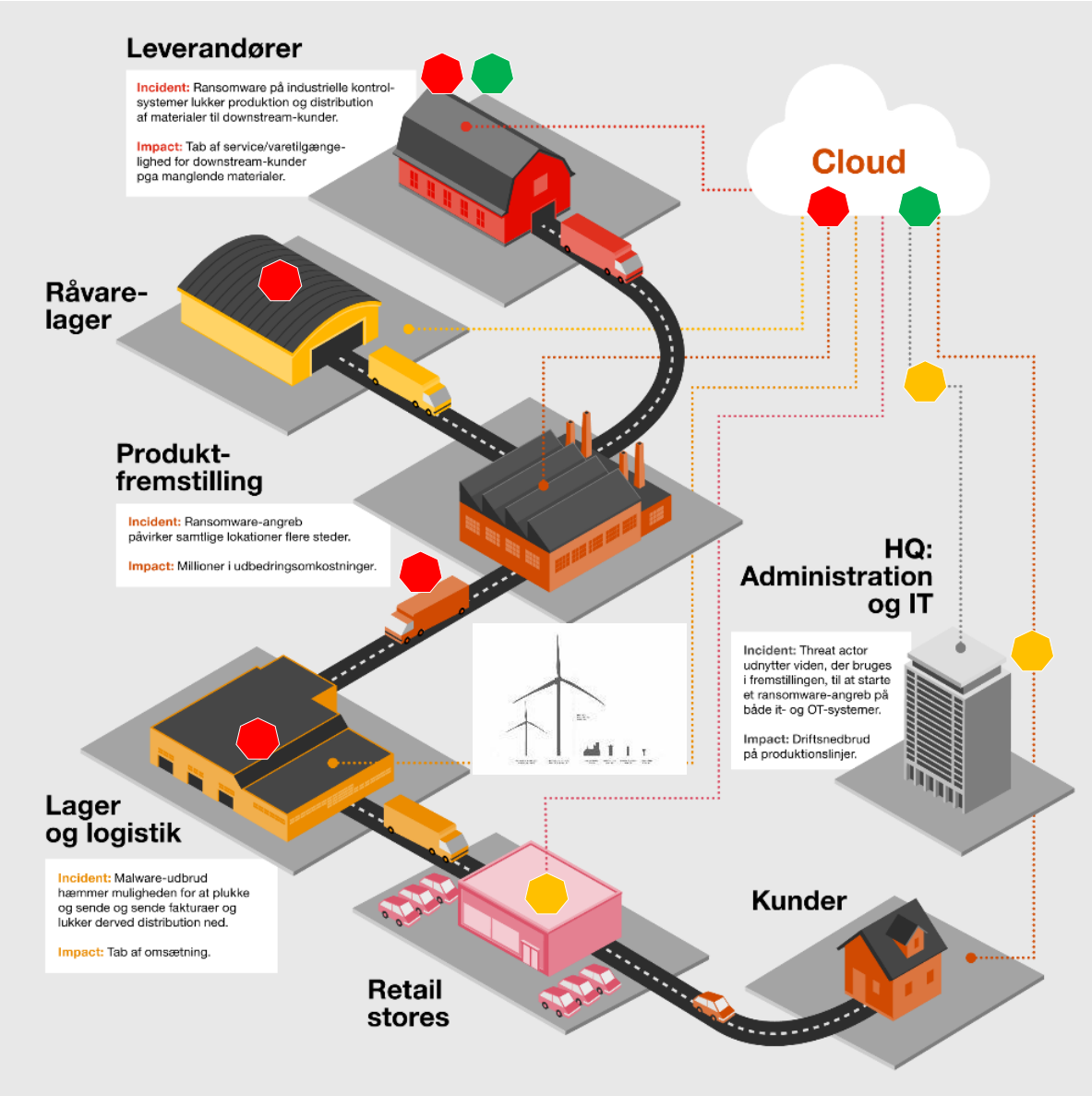
Lack of secure OT development

- Limited or no visibility into security processes implemented by third party suppliers to ensure secure development of Operational Technology (OT) used in manufacturing operations
- Lack of availability of security updates from third party vendors to address vulnerabilities in OT products

Lack of mature Physical Security Program

- Manufacturing facilities are often located in developing countries where physical security environments are more conducive to IP theft, hardware tampering, and other types of threats

What is Supply Chain cyber risk?



Common Challenges:

Lack of **risk transparency** in value and supply chain.
Increasing threats of technology convergence.
Unclear security posture due to **low visibility**.
Legacy security challenges.
Lack of **asset visibility**.
Regulatory and **compliance** issues.

Suppliers criticality

- Critical
- Severe
- Non critical

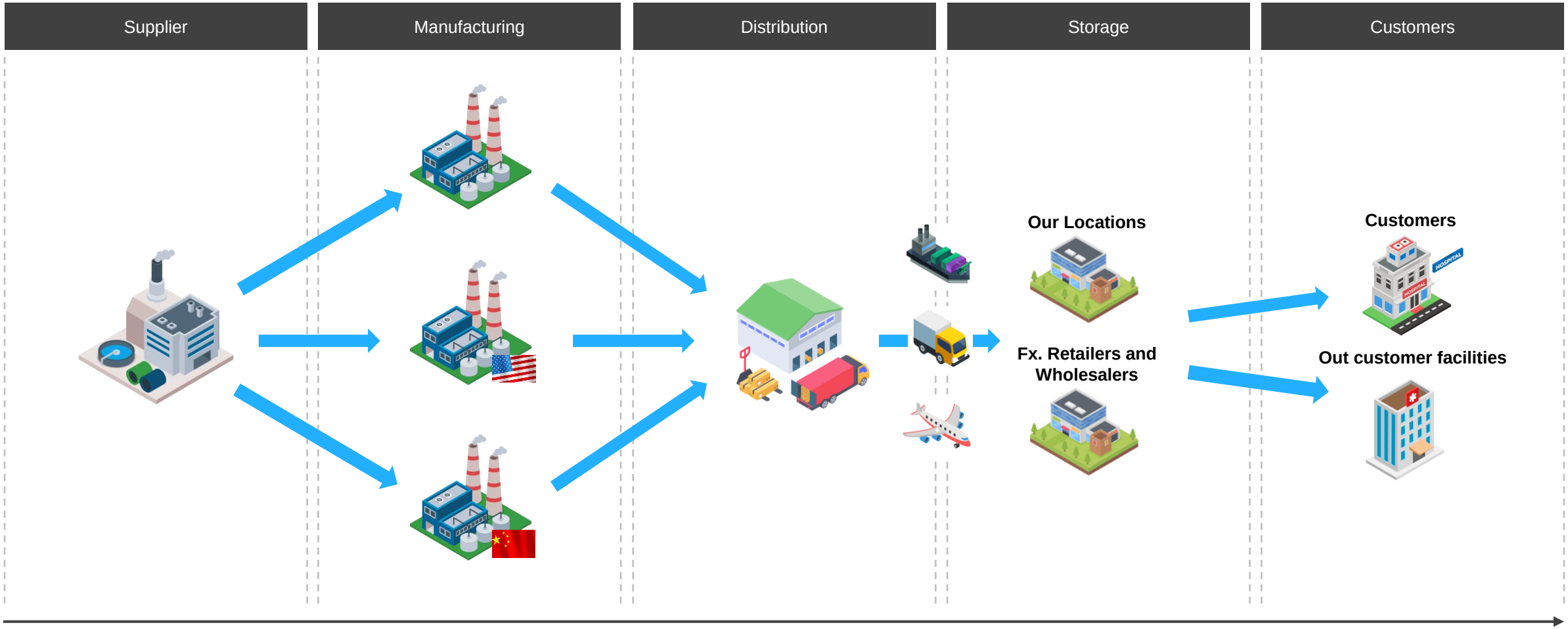
Includes OT/IoT etc.

Assembly lines, Robots, Conveyance, Relays, packaging, power controllers, AGV, Boilers, CT/MR Scanners, X-ray, Pumps, etc. etc etc **OT for many companies IS the business**

Illustrative value chain

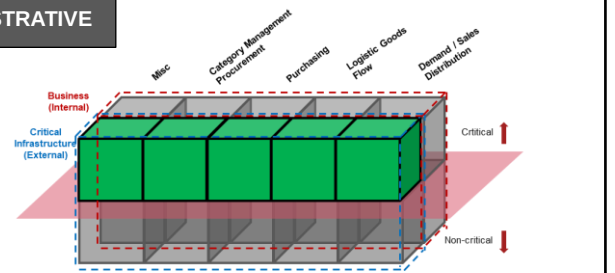
Understanding the value chain

Illustrative!



Illustrative process and system mapping

*ILLUSTRATIVE



Understanding the value chain

Process

Supplier	Manufacturing	Distribution	Storage	Customers

System

XXX				
XXX		XXX		XXX
XXX	XXX			XXX
XXX			XXX	
				XXX

Infrastructure

Assessed in collaboration with IT as a part of the actual NIS2 project

Enhancing Cybersecurity through Effective Third-Party Management

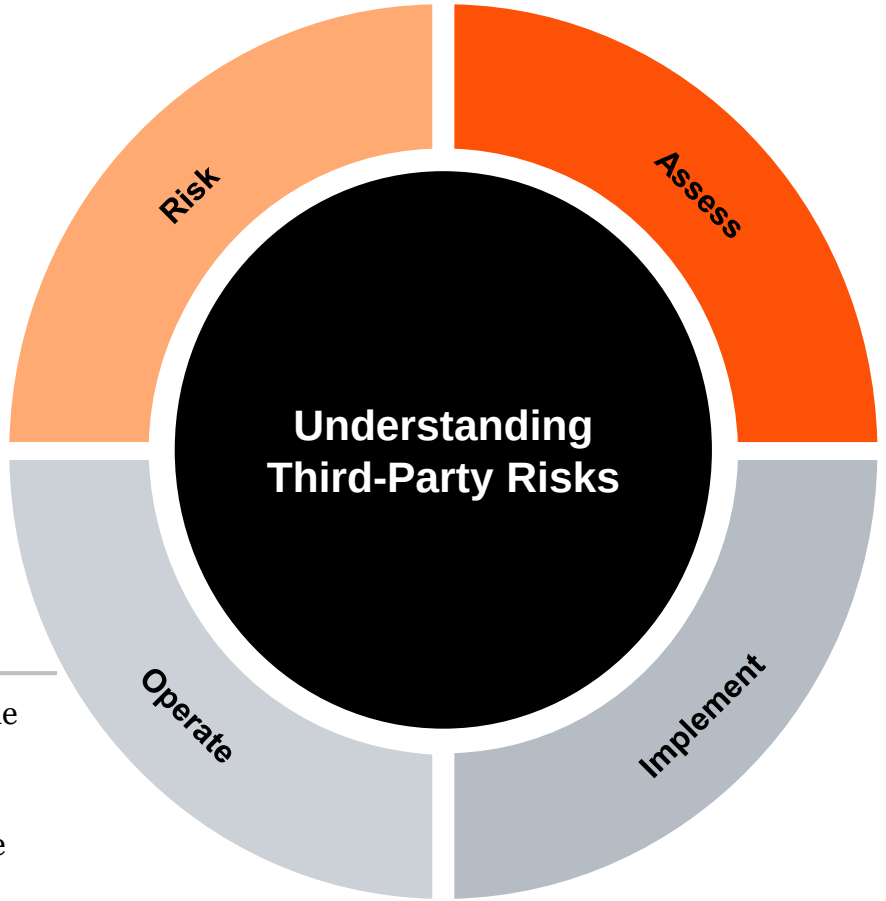
Effective third-party cyber management is essential for mitigating risks and protecting an organisation's assets.

Risk Assessment and Due Diligence

- Third-party vendors can have access to critical systems and data ☐ potential targets for cyberattacks.
- Common risks include data breaches, unauthorised access, and supply chain vulnerabilities.
- Conduct thorough risk assessments to identify and evaluate potential vulnerabilities associated with third-party vendors.
- Implement a robust due diligence process to ensure vendors meet security standards and comply with regulations.

Contractual Agreements and SLAs

- Establish clear contractual agreements that outline security requirements and responsibilities.
- Include Service Level Agreements (SLAs) – concrete deliveries and obligations where possible to ensure vendors adhere to agreed-upon security measures and response times.



Continuous Monitoring and Auditing

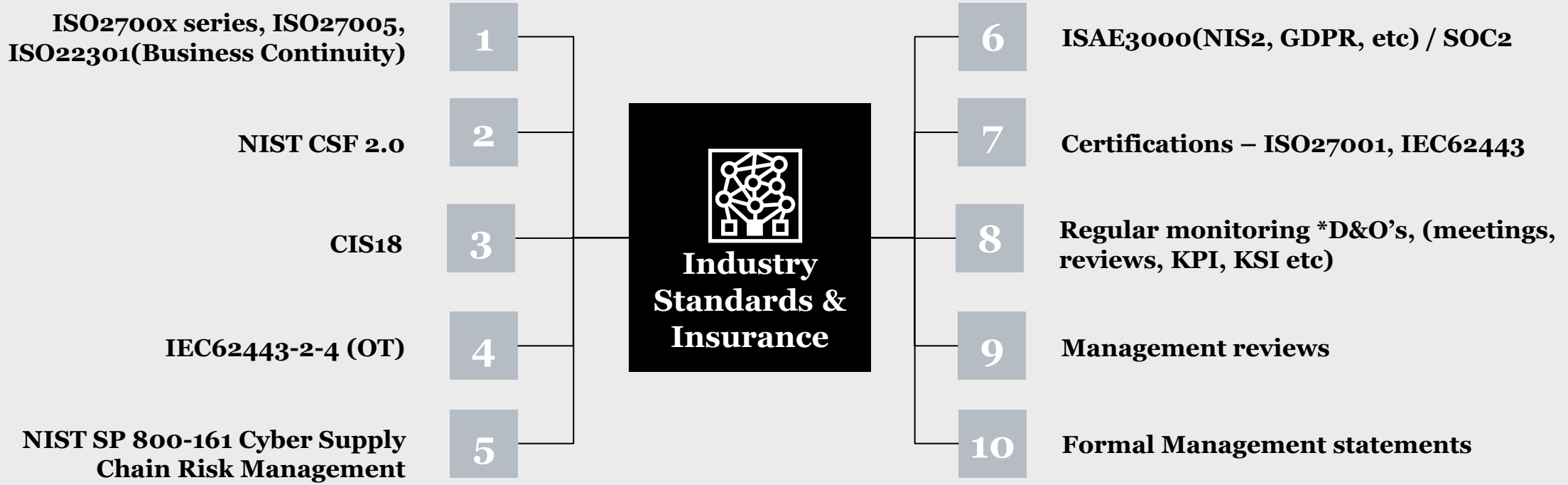
- Regularly monitor and audit third-party vendors to ensure compliance with security policies and procedures.
- Utilise automated tools and technologies to detect and respond to potential threats in real-time.

Incident Response and Recovery

- Develop and implement an incident response plan that includes third-party vendors.
- Ensure vendors are prepared to collaborate during a cybersecurity incident and assist in recovery efforts.
- Involve critical third parties in continuity testing

Relevant Frameworks

Examples of various frameworks can be used for controlling and addressing third party supplier risk along with industry frameworks, and regulatory guidance, to ensure a comprehensive **approach** to measure and assess their deliveries and obligations or the maturity in i.e. acquisitions(M&A), RFP etc.



* D&O: Measurable contractual agreed deliveries and obligations.

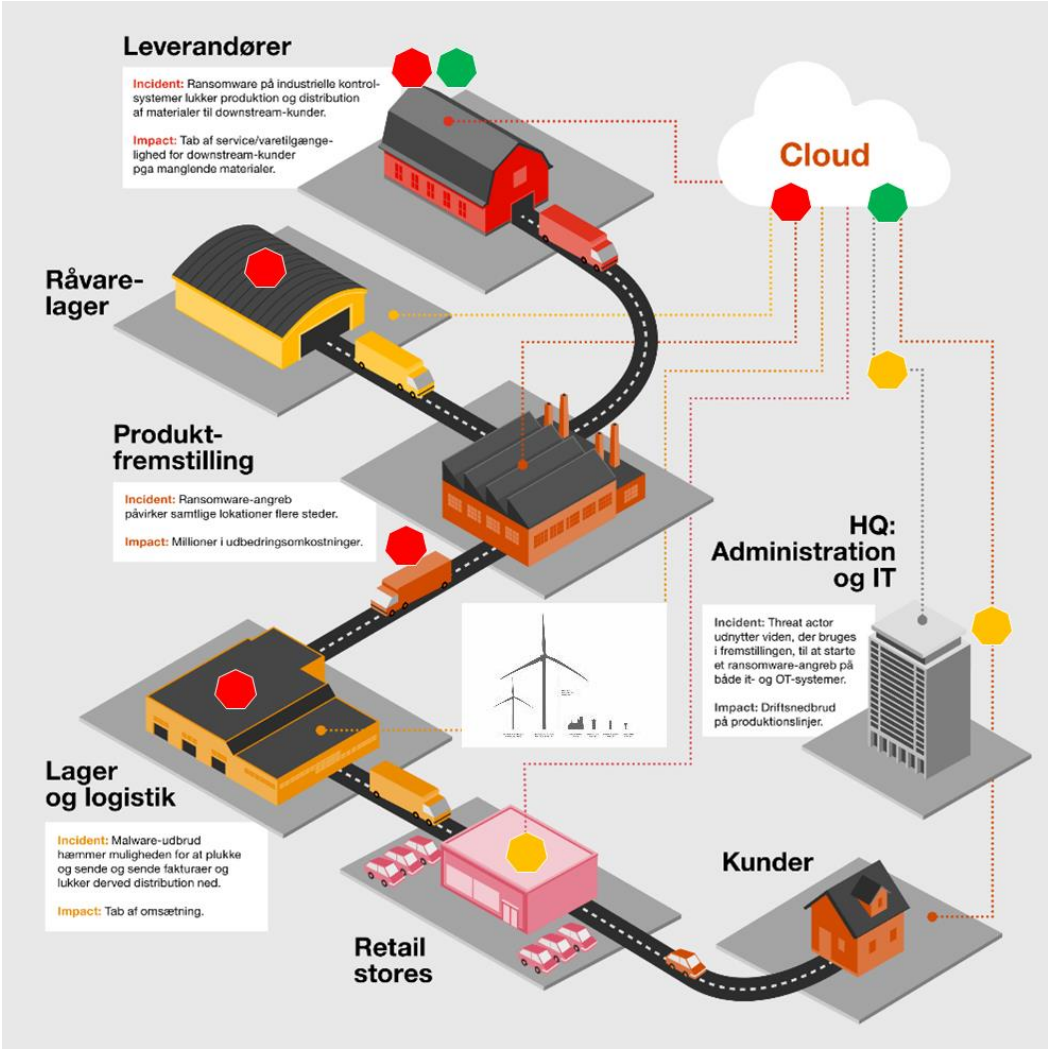
Risk

Examples of a simple and pragmatic risk assessment.

Risk matrix (Leverandører)			
Sandsynlighed/ Konsekvens	Lille	Medium	Stor
Stor			
Medium			
Lille			

Risk matrix (Leverandører) - Frekvens for vurdering			
Sandsynlighed/ Konsekvens	Lille	Medium	Stor
Stor	**Årligt**	**Årligt**	**Løbende kontrol**
Medium	**Ved behov**	**Hvert andet år**	**Årligt**
Lille	**Ved behov**	**Ved behov**	**Hvert andet år**

Løbende kontrol, dog minimum hvert ½ år
Årligt, eller ved ændringer, rygter om brud på sikkerhed eller andet
Hvert andet år, eller ved ændringer, rygter om brud på sikkerhed eller andet



Risk

Examples of a simple and pragmatic risk assessment. How do we consider monitoring and assurance

Risk matrix score Riskokategori			
Tilsyn/frekvens (eksempel)	Ved behov, stikprøver, dog min. xx år	Typisk hvert eller hvert andet år eller ved væsentlige ændringer	Løbende kontrol/årligt/halvårligt og ved ændringer
ISAE3402 / SOC 1/SOC2	Er relevant - afhænger af leverandør/produkt. Eksempel på produkter/leverandører: Hyldevarer som Snagit, Adobe Reader,	Er relevant. Undersøg om erklæringen er dækkende helt eller delvist for GDPR/ITGC kontroller. Kan være tilstrækkelig i denne kategori.	Er relevant. Undersøg om erklæringen er dækkende helt eller delvist for GDPR/ITGC kontroller. Kan være tilstrækkelig i denne kategori.
Ret til Audit	Vi skal altid forbeholde os retten til audit hos leverandøren, udført af Selskabet eller 3 part godkendt af Selskabet	Vi skal altid forbeholde os retten til	Vi skal altid forbeholde os retten til audit hos
Investigative support	Sædvanligvis ikke relevant	K	
Authentication, Authorization, & Assurance	Sædvanligvis ikke relevant	E	
ISAE3000 - GDPR	Sædvanligvis ikke relevant - kan eventuelt indhentes i forbindelse med etablering af databehandler aftale og herefter periodisk		
ISRS 4400 - KUN hvis relevant	Sædvanligvis ikke relevant - kan eventuelt indhentes i forbindelse med etablering af databehandler aftale og herefter periodisk	K	
Intern revision(leverandørens)	Sædvanligvis ikke relevant.	S	
Ledelseserklæringer	Sædvanligvis ikke relevant.	S	
Certificering (ISO27001)	Sædvanligvis ikke relevant	Selskabet kan forholde sig til om det er tilstrækkeligt hvis leverandøren er ISO27001 certificeret på relevante områder irt ydelsen. SOA skal være inkluderet og en evt gennemgang med leverandøren kan være nødvendig. Ikke i sig selv tilstrækkelig	Selskabet kan forholde sig til om det er tilstrækkeligt hvis leverandøren er ISO27001 certificeret på relevante områder irt ydelsen. SOA skal være inkluderet og en evt gennemgang med leverandøren kan være nødvendig. Ikke i sig selv tilstrækkelig
Generel tjek af medier/internet mht omdømme, IT hændelser mm	Der følges op på eventuel omtale mht hændelser eller generel omtale mth informationssikkerhed	Der følges op på eventuel omtale mht hændelser eller generel omtale mth informationssikkerhed	Der følges op på eventuel omtale mht hændelser eller generel omtale mth informationssikkerhed
Penetration/red team testing	Kan være elevant. Se executive summary hvis tilgængelig	Se executive summary	Se rapport og mitigerende handlinger og foretag ud fra dette en vurdering
Underleverandører	Kan være relevant. Beskriv hvordan det sikres at underleverandører overholder leverandørens krav.	Kan være relevant. Beskriv hvordan det sikres at underleverandører overholder leverandørens krav og hvordan der følges op/dokumenteres på dette	Kan være relevant. Beskriv hvordan det sikres at underleverandører overholder leverandørens krav og hvordan der følges op/dokumenteres på dette
BCP- Business Continuity Plan	Sædvanligvis ikke relevant	Beskriv den overordnede process	Beskriv den overordnede process
IT sikkerhedspolitik	Del af den samlede vurdering	Del af den samlede vurdering	Del af den samlede vurdering

Risk

Examples of a simple and pragmatic risk assessment. How do we choose

Opfølgning og kontrol med databehandlere

Kontrolmuligheder (ikke begrænset til nedenstående)	Kontrolbeskrivelse	Supplerende oplysninger
ISAE3000 - GDPR/NIS2/XXX	Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Selskabet (den Dataansvarlige). Erklæringen er udviklet af Cybersikkerhedsudvalget under FSR – danske revisorer i tæt samarbejde med Datatilsynet, som er kommet med bemærkninger til erklæringens udformning og indhold. Erklæringen bygger ligeledes på Datatilsynets skabelon til databehandleraftaler. ISAE 3000 erklæringer kan udformes til at dække andre områder end GDPR.	**Type 1** dækker typisk et billede af hvordan designet af kontrolmiljøet ser ud, og/eller hvordan kontrolmiljøet ser ud på det tidspunkt revisionen udføres. Den dækker således sjældent en periode men er et øjebliksbillede pr. given dato. Kan være tilstrækkelig ifm kundespecifik erklæring ved kontraktindgåelse med henblik på senere type 2 erklæring, eller når der ikke foreligger en service der har været etableret i en periode over 6 måneder. **Type 2** anvendes for at afdække om kontrolmiljøet har været opretholdt til et givet og tilstrækkeligt niveau i en periode. Minimum 6 måneder. Type 2 erklæringer kan således afgives med sikkerhed for en given periode. **Bemærk** Der skelnes mellem kundespecifikke erklæringer og generelle erklæringer. Kundespecifikke erklæringer indebærer mulighed for stærkere kontrolbevis end en generel erklæring, da den typisk er tilpasset den specifikke kontrakt mellem parterne eller et specifikt aftalt scope mellem parterne. Den generelle erklæring kan ofte være tilstrækkelig eksempelvis for Cloud udbydere eller andre udbydere hvor der ikke er forskelle i den leverede service og services er omfattet af samme kontroller for alle, eller at det er tilstrækkeligt iht risikovurdering.
ISAE3402 / SOC1	Uafhængig revisors ISAE 3402-erklæring med sikkerhed vedrørende de generelle it-kontroller????, der er knyttet til de driftsaktiviteter, der som standard tilbydes leverandørens kunder. Revisorerklæringen anvendes af leverandørens kunder og disses revisorer. Erklæringerne afgives i overensstemmelse med retningslinjerne i revisionsstandard 3402 "Erklæring med sikkerhed om kontroller hos en serviceleverandør" Erklæringen kan i væsentlig grad omfatte kontroller relevante for GDPR. Fx adgangskontroller, netværk, operativsystemer, databaser, infrstruktur og fysisk sikkerhed. Ønsker man at anvende denne erklæring skal man som alle andre erklæringer forholde sig til omfang og afgrænsninger. Evt. kan man supplere med udvalgte egenkontroller.	
SOC2	Sammenlignelig med ISAE3000. Uafhængig revisors erklæring med sikkerhed om informationssikkerhed og kontrolmiljø, som er beskrevet i en systembeskrivelse, har været passende designet og effektive og giver rimelig grad af sikkerhed for, at serviceorganisationens forpligtelser og systemkrav har været effektive baseret på de gældende kriterier for de omfattede/aftalte ydelser. "Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy"	
ISRS 4400	Denne erklæringstype retter sig mod opgaver vedrørende regnskabsmæssige oplysninger. Den kan imidlertid være retningsgivende ved opgaver om ikke-regnskabsmæssige oplysninger, herunder fx. udvalgte GDPR kontroller, under forudsætning af, at revisor har tilstrækkeligt kendskab til det pågældende område, og at der er rimelige kriterier, som observationer og resultater kan baseres på.	Målet med en opgave om aftalte arbejdshandlinger er, at revisor udfører revisionslignende arbejdshandlinger, som revisor, Selskabet og enhver relevant tredjepart er blevet enige om, og erklærer sig om de faktiske resultater. Revisor afgiver alene erklæring om de faktiske resultater vedrørende de aftalte arbejdshandlinger, og der udtrykkes ingen grad af sikkerhed. I stedet vurderer Selskabet (og evt andre brugere af erklæringen) selv de arbejdshandlinger og forhold, som revisor erklærer sig om og drager deres egne konklusioner af revisors arbejde. Erklæringen er begrænset til de parter, som er blevet enige om, hvilke arbejdshandlinger der skal foretages, idet andre, som ikke kender begrundelserne for arbejdshandlingerne, kunne misfortolke resultaterne.
Intern revision, egenkontrol	Denne kontrol kan anvendes for at opå helt eller delvis overbevisning om tilstrækkeligt GDPR kontrolmiljø. Kan anvendes i kombination med andre kontrolformer, fx erklæringer for at afdække en restrisiko hvis kontrollerne oikke vurderes tilstrækkelige.	Eks. 1: Der foreligger en ISAE3000 GDPR type2 generel erklæring. Det vurderes at der er enkelte væsentlige afvigelser fra en standard leverance som der bør opnås kontroloverbevisning for. Det aftales mellem parterne at der foretages en række specifikke revisions handlinger. Fx. En kontrol af brugere hos databehandleren med adgang til databaser indeholdende persondata. Eks. 2: Det vurderes at der grundet omfang og risiko ifm bemærkninger i erklæringen skal udføres en række opfølgende revisionshandlinger på de omtalte afgrænsninger.

Ledelseerklæringer	Kan anvendes som et kontrolredskab hvis der er lille risiko, eller som supplerende til andre kontrolmuligheder. Kontrolbeviset anses ikke som stærkt og giver ikke udtalelser med sikkerhed om effektive kontroller.	
Certificering (Fx ISO27001)	Kan anvendes som et kontrolredskab hvis der er lille risiko, eller som supplerende til andre kontrolmuligheder. En certificering betyder at der er implementeret ledelsessystem herunder politikker, processer og procedurer for informationssikkerhed. Kontrolbeviset anses ikke som stærkt og giver ikke udtalelser med sikkerhed om effektive kontroller.	Det er væsentligt at forholde sig til databehandlererens SOA (Statement of Applicability). SOA'en beskriver certificeringens afgrænsning.
NDA eller lign.	Fortrolighedserklæring. Kan anvendes hvis man får tilfældig læseadgang til data eller skal færdes på kontorer mm. Fx i forbindelse med en anden ydelse som ikke er behandling af persondata. Der er ikke tale om decideret databehandling.	
Andre….		

Examples of monitoring controls for party cyber risk management

Roles and responsibilities in third party risk management

Clearly defined roles and responsibilities in third-party cybersecurity are crucial for maintaining a secure supply chain.

- All stakeholders must understand their specific duties,
- Effectively manage and mitigate risks.
- Facilitate compliance with regulatory requirements
- Reduce the likelihood of legal issues.
- Enhance coordination and communication among teams, leading to a more resilient and responsive cybersecurity posture.
- Build trust with partners and customers, safeguarding the organization's reputation.

Supervision/Assurance (example)

- "ISAE3402 / SOC 1/SOC2 "
- Right to Audit
- Investigative support
- Authentication, Authorisation, & Assurance
- ISAE3000 - GDPR
- ISRS 4400 – ONLY if applicable
- Internal audit (supplier's)
- Management Statements
- Certification (ISO27001)
- General check of media/internet regarding reputation, IT incidents etc.
- Penetration/red team testing
- Subcontractors
- BCP- Business Continuity Plan
- External monitoring services (UpGuard, Bitsight, SecurityScorecard etc)

Thank you