NIS2 Compliance:

Krav til asset management, risikostyring og incident rapportering

René Matthiassen

KISS 2024, 2 oktober

Agenda

- Introduktion til NIS2-direktivet
- Asset Management under NIS2
- Risikostyring
- Incident rapportering
- Er der behov for servicedesk til NIS 2?
- Spørgsmål og svar

- René Matthiassen
  Partner
  Frontdoorsecurity Aps – *we do compliance*

  - CCNP, CISM, CISSP, ISO27001 Senior Lead Implementer, ISO27001 Senior Lead Auditor, NIS2 Senior Lead Implementer, Certified Trainer

  - 30 års erfaring med sikkerhed, heraf OT siden 2007

  - President for ISA.org i Danmark som udgiver ISA/IEC62443 serien.
  - Medlem at ISA99 som udvikler ISA/IEC62443

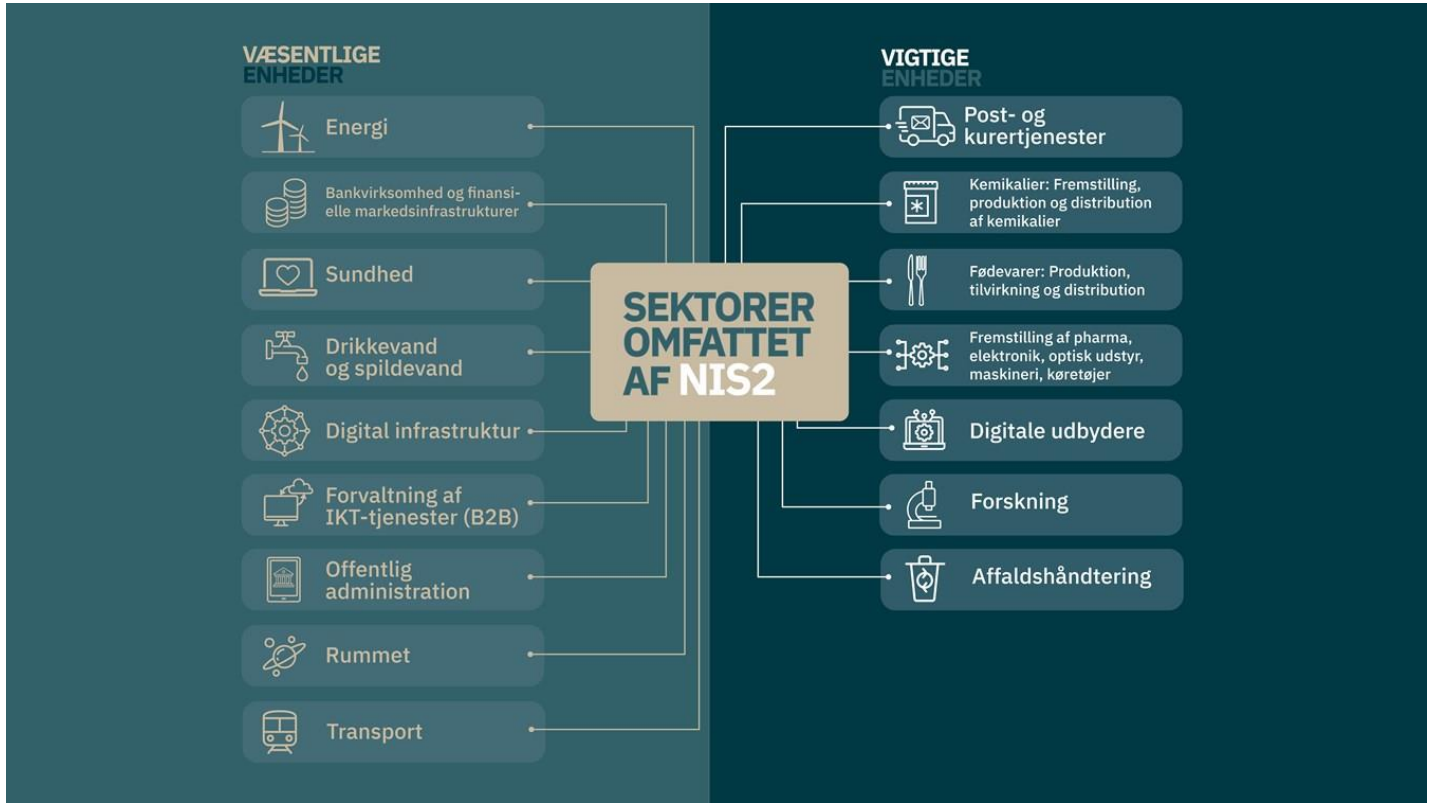
  - Medlem af Dansk Standard S-441 udvalg som udvikler standarder indenfor cyber og informationssikkerhed - medforfatter til ISO/IEC 27001 serien

  - Medlem af CEN/CLS JTC13 CRA expert group, som udvikler sikkerhedskrav til Cyber Resilience Act, samt adhoc group.

  - Tidligere rådgiver for Datatilsynet og kammeradvokaten.

FRONTDOOR SECURITY

Introduktion til NIS2



- Formål med NIS2
  - Styrke EU's cybersikkerhed
  - Harmonisering.
  - Opdatering af NIS
- Nøgleændringer fra NIS
  - Udvidet anvendelsesområde
  - Strengere sikkerhedskrav
  - Skærpede sanktioner

Asset Management under NIS2

- **Risikoanalyse og sikkerhedspolitikker (**Artikel 21, stk. 2, litra f**):**
  - *Enheder skal udføre risikoanalyser og implementere passende sikkerhedspolitikker for at håndtere de identificerede risici.*
  - *Effektiv risikoanalyse kræver et fuldstændigt overblik over alle netværks- og informationssystemer (aktiver). Uden en opdateret aktivliste er det umuligt at vurdere risici korrekt*.
- **Sikkerhed i net- og informationssystemers erhvervelse, udvikling og vedligeholdelse** (Artikel 21, stk. 2, litra e):
  - *Enheder skal sikre, at sikkerhed integreres i alle faser af netværks- og informationssystemers livscyklus.*
  - Dette kræver en løbende registrering og overvågning af alle hardware- og softwareaktiver for at sikre, at de er opdaterede og sikre mod kendte sårbarheder.
- **Leverandørkædens sikkerhed** (Artikel 21, stk. 2, litra d)
  - *Enheder skal tage hensyn til sikkerhedsaspekter i relation til deres leverandører og tjenesteudbydere.*
  - *For at styre risici i leverandørkæden skal organisationer have et klart billede af alle aktiver, der leveres eller vedligeholdes af tredjepart.*

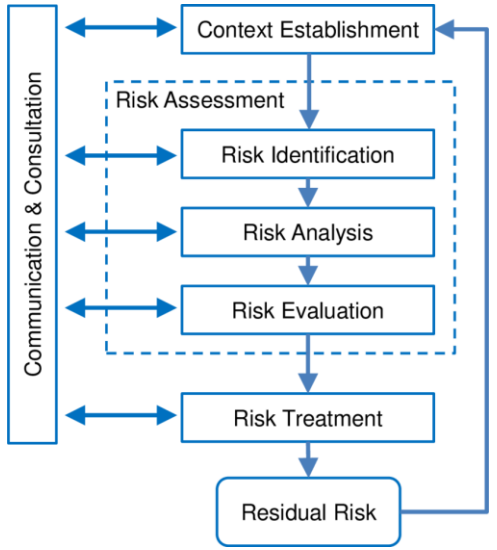
Asset Management under NIS2

- **Politikker og procedurer til vurdering af cybersikkerhedsforanstaltningers effektivitet (Artikel 21, stk. 2, litra h)**
  - *Enheder skal etablere politikker for at evaluere effektiviteten af deres sikkerhedsforanstaltninger.*
  - *Evaluering af sikkerhedsforanstaltninger kræver detaljeret viden om de aktiver, der skal beskyttes, og hvordan de er sikret.*

Risikostyring

- Holistisk tilgang (Artikel 21, stk. 1)
- Proaktiv risikostyring
- Forudse og mitigere risici før de materialiserer sig.
- Løbende overvågning af trusselslandskabet.

  - *Du kan ikke risikovurdere det du ikke kender. Først når du kender dine aktiver kan du se på trusler og sårbarheder.*

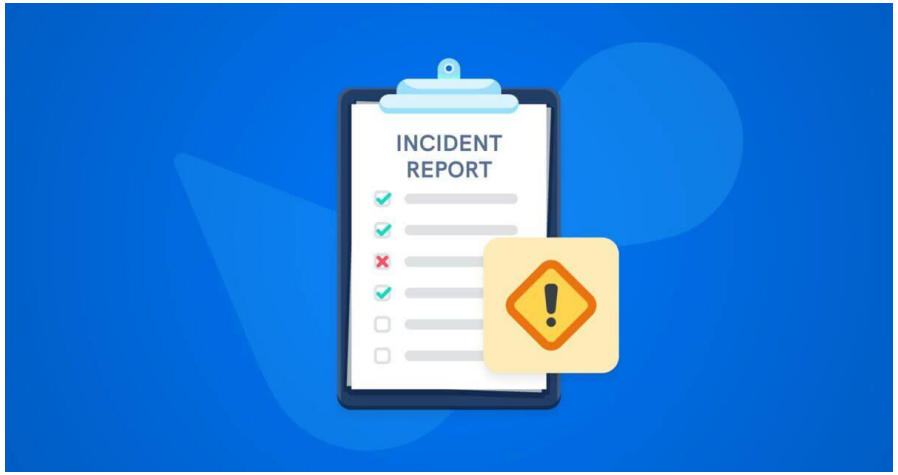


Risikopoint for specifik risiko					
Sandsynlighed	Risikopoint: Sandsynlighed x Konsekvens				
Næsten sikkert (5)	5	10	15	20	25
Sandsynligt (4)	4	8	12	16	20
Muligt (3)	3	6	9	12	15
Sjældent (2)	2	4	6	8	10
Usandsynligt (1)	1	2	3	4	5
	Ubetydeligt (1)	Mindre (2)	Moderat (3)	Større (4)	Katastrfalt (5)
	Konsekvenser for et mål (f.eks. omkostninger, tid eller omfang og indhold)				

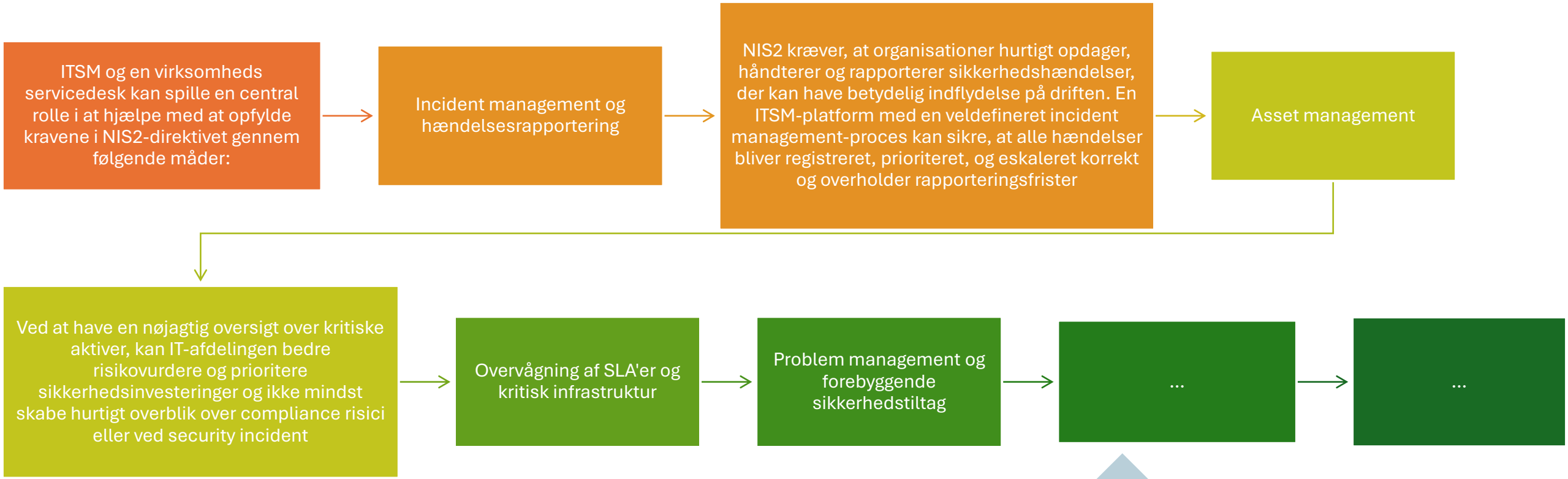
Risikograd Mindre Moderat Høj Kritisk

Incident rapportering

- Anmeldelse af signifikante hændelser (Artikel 21, stk. 1)
  - **Essentielle** og **vigtige** enheder skal uden **unødig forsinkelse** rapportere **signifikante hændelser** til den relevante **CSIRT**(Computer Security Incident Response Team) eller **kompetente myndighed**.
  - **Inden for 24 timer** efter at have opdaget hændelsen skal enheden indsende en indledende anmeldelse (jf. Artikel 23, stk. 4).
  - **Inden for 72 timer** efter den indledende varsling skal enheden indsende en opdateret rapport med yderligere oplysninger (jf. Artikel 23, stk. 5)
  - Om muligt, en kort beskrivelse af hændelsen, herunder dens art og de berørte systemer.



Er der behov for servicedesk til NIS 2?



rem@frontdoorsecurity.dk

Mobil: +45 2245 0045

FRONTDOOR SECURITY

Østersø 12
3670 Veksø

Pakhustorvet 12, st.
6000 Kolding

intertek
Total Quality. Assured.

CERTIFICATE OF REGISTRATION

This is to certify that the management system of:

NetCloud A/S

CVR.nr: 37395722

Main Site: World Trade Center, Borupvang 3, DK-2750 Ballerup, Denmark

has been registered by Intertek as conforming to the requirements of:

ISO/IEC 27001:2022

The management system is applicable to:

Development, service, operation, and sales of NetCloud based solutions.

This is in accordance with the statement of applicability Version 1.
Date 19th September 2024.

Certificate Number:
0192822

Initial Certification Date:
24 September 2024

Date of Certification Decision:
24 September 2024

Issuing Date:
01 October 2024

Valid Until:
23 September 2027

ISO 27001:2022 CERTIFICATION ™ intertek

UKAS MANAGEMENT SYSTEMS 014

Calin Moldovean
President, Business Assurance

Intertek Certification Limited, 10A Victory Park, Victory Road, Derby DE24 8ZF, United Kingdom

Intertek Certification Limited is a UKAS accredited body under schedule of accreditation no. 14.

Spørgsmål?

Jesper Andersen

jesper@netcloud.dk

61 68 49 07

Rene Matthiassen

rem@frontdoorsecurity.dk

22 45 00 45

echo®
powered by NetCloud

FRONTDOOR SECURITY