

# Navigating regulatory cyber security

Regulations and ‘So what’  
for CISOs and the Board

# Frans Skovholm

## DAHL LAW FIRM

### Attorney (L)/ Partner

2008: Assistant attorney

2011: Lawyer

2020: Associate Partner DAHL Lawfirm


2022: Partner/owner DAHL Lawfirm

Specialized in

- Information Security Law (NIS 2)
- Data Protection Law (GDPR)
- Commercial compliance

 fsk@dahlaw.dk

 +45 27 87 85 03

ISO 27001 Lead implementer  
Certified by PECB 



Frans Skovholm heads DAHL's compliance team, which consists of a number of specialists within GDPR, ISMS, Legal compliance and ESG

Frans specializes in working systematically with risk management and advising on ISMS management systems, including ISO 27001.

In addition, Frans works with privacy law, where he has helped many companies implement internal rules that ensure that the requirements of the General Data Protection Regulation are complied with.

Frans regularly conducts courses, after-work meetings and legal presentations on current issues in his fields. Frans is hereby updated on new legislation and new case law.

# Bo Drejer

## Orange Cyberdefense

### GRC Manager

1992: M.Sc. Civil Engineering(ISO 9001)  
1999: Oracle Denmark - Product Manager Database  
2004: Microsoft Denmark - .NET & Cloud responsible  
2010: Cybercom - Head of Digital Solutions Nordic  
2014: Self Employed - EA and Security  
2020: PwC - Senior Manager - EA & Security  
2023: Orange Cyberdefense - GRC Manager

Specialized in

- Operational GRC
- Security Architecture
- Enterprise Architecture

 bo.drejer@orangecyberdefense.com

 +45 21 48 03 81

ISO 27001 Provisional Auditor (PECB)

CISM - ISACA certified 

CGEIT - ISACA certified

SABSA certified

CIPM - IAPP Certified



Bo Drejer is Orange Cyberdefense Denmark's GRC Manager and responsible for Orange Cyberdefense's GRC services and senior expert within the area.

Bo has +12 Years of GRC experience and has a technical as well as management background from IBM, Oracle, Microsoft and major consulting firms as well as self employment within GRC, Enterprise Architecture and Security Architecture.

# Overview of NIS2



NIS2 is the new European cybersecurity directive that will replace the existing NIS Directive starting **October 2024**.



It is the **most comprehensive EU cybersecurity legislation** to date, covering 18 sectors.

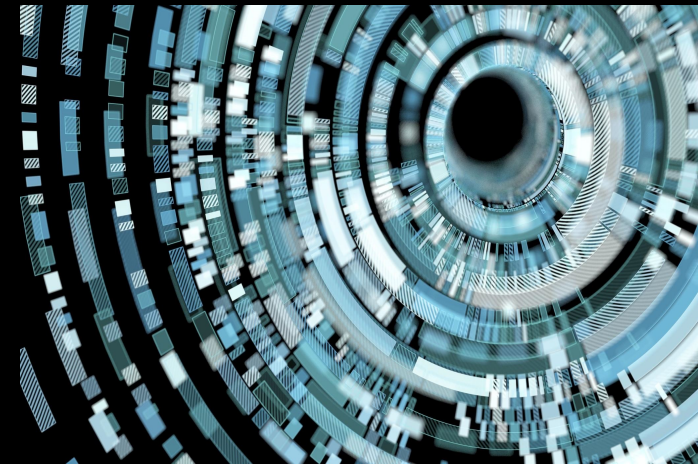
Member States have until October 17, 2024 to transpose the Directive into national law. This means that each organization encompassed by the Directive will be legally obligated to live up to its requirements by Q4 2024.



Its purpose is to **establish a baseline of security measures** for Essential and Important Entities, to **mitigate the risk of cyber attacks** and to **improve the overall level of cybersecurity in the EU**.

# Regulation of information security law in Denmark

- 2016: NIS1
- Improve resilience and response capabilities in cybersecurity and critical infrastructure protection.
- 2018: NIS 1 implemented in Danish law
- 2018: Implementation of GDPR regulation
- May 2022: Digital Operational Resilience Regulation (Financial Sector - DORA)
- May 2022: CER Directive (Resilience of critical entities)
- December 2022: NIS2 Directive
- (At the latest) 17 October 2024: The Commission shall adopt implementing acts laying down the technical and methodological requirements for measures (Art. 21(5))
- Expected 1 January 2025: NIS 2 implemented in Danish law
- Sector-specific legislation
- January 2025: DORA Regulation enters into force
- (At the latest) 17 January 2025: Peer review of NIS 2 (Art. 19)



# Which companies will be subject to NIS2?

## Two factors\*

- Sector
- Size (can be group level)

## SME enterprise within the meaning of "Recommendation 2003/361/EC28"

- The SME category refers to enterprises employing more than 50 persons and having an annual turnover or balance sheet total exceeding EUR 10 million.

Essential entities (Annex 1 to the Directive)

Important entities (Annex 2 to the Directive)



# NIS2 affects various sectors, including...

On September 14, the European Commission published new guidelines explaining which sectors will be considered critical and what they should report to national authorities in the EU under the NIS2 directive.

## Essential Entities

|                                 |                        |                       |              |
|---------------------------------|------------------------|-----------------------|--------------|
| Energy                          | Transport              | Banking               | Space        |
| Financial market infrastructure | Health sector          | Drinking water        | Public admin |
| Wastewater                      | Digital infrastructure | IT service management |              |

## Important Entities

|                             |                                  |                   |
|-----------------------------|----------------------------------|-------------------|
| Food                        | Waste management                 | Chemicals         |
| Postal And courier services | Manufacturing of medical devices | Digital providers |
| Research organizations      |                                  |                   |

# What does **NIS2** mean for you?

## Cybersecurity risk management measures

- Risk management
- Security policies
- Incident handling (prevention, detection & response to incidents)
- Business continuity plans
- Supply chain security consider supplier vulnerabilities
- Vulnerability handling and disclosures
- Regular assessments to determine the effectiveness of cybersecurity risk management measures (e.g., reflection of state of art – security posture)
- The use of cryptography and encryption where warranted
- Basic cybersecurity hygiene & training
- The use of MFA or continuous authentication
- Crisis Management

## Incident reporting obligations

Report incidents with significant impact\* on the provision of services

Within 24 hours

An extensive  
report within 72  
hours

Within 1 month  
A final report  
progress report

Computer Security  
Incident Response  
Team (CSIRT)

Competent  
authority

Recipients of  
services

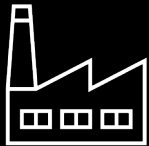
\*An incident is significant if it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned or if it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage



# Direct or indirect subject to NIS2

NIS 2

DORA



**Enterprise/  
Customer**



**Vender**

## **NIS2 Direct subject**

- **The critical infrastructure is divided into selected sectors**
- **Decisive whether the unit has activities in a selected sector**
- **Decisive whether the device has a real impact on the critical infrastructure (de minimis limit)**
- **The entity must be registered with the authorities**
- **Management can be made personally responsible**
- **Responsible for using the suppliers**

## **NIS2 Indirect subject**

- **The supplier is not directly covered by NIS2**
- **The customer can only contract with suppliers who can offer appropriate cybersecurity and preparedness**
- **Information security requirements must be contracted**
- **The customer will opt out of suppliers who cannot meet the requirements of NIS2**

Orange Restricted

## Measures

Risk Assessment

Policy

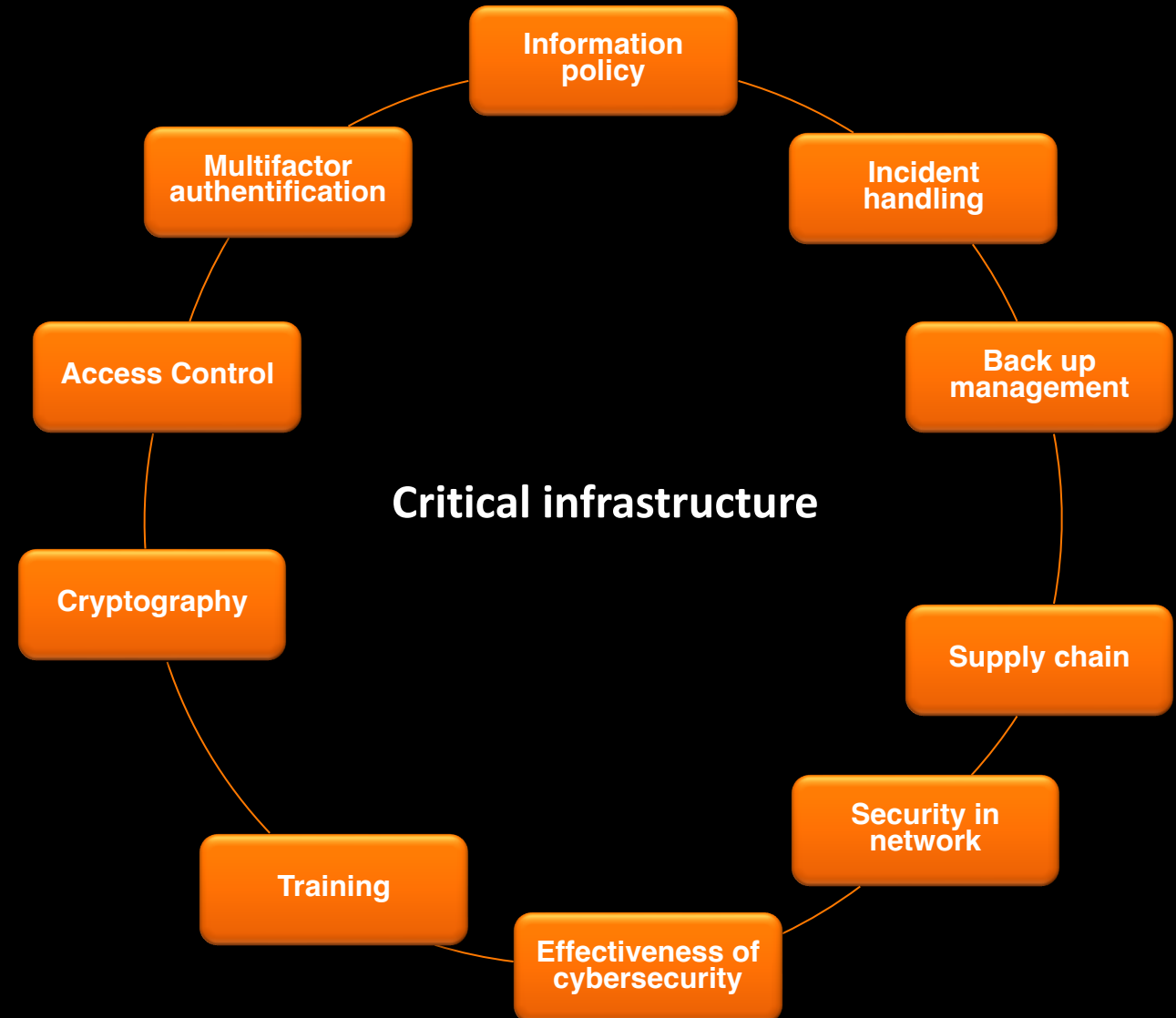
Technology Controls

Documentation

Contract clauses

Awareness

## Minimum requirements art. 21.2



# The managements responsibility (Art. 20)

There is a high level of responsibility for ensuring measures, which means that the management is responsible for:

- Approves cyber risk management measures that comply with the requirements of Article 21
- Is responsible for the entity's compliance with Art. 21
- Monitor the implementation of measures
- Follow courses
- Encourage employees to follow training
- Management and employees must acquire the knowledge to identify risks
- Management and employees must have insight into methods to manage cyber risk



# Contractual NIS2 requirements

## Examples of relevant requirements:

- Service descriptions, including security and backup requirements
- Change access
- Service goals and penalties
- Right of termination and termination
- Audit access, auditing, reporting requirements and access to information
- Security incident briefing
- Collaborative organization and reporting
- Subcontractor approval, notification by amendment
- Approval by geography, notification by change
- Certification requirements/standards



# NIS 2 – Who is responsible for the tasks?

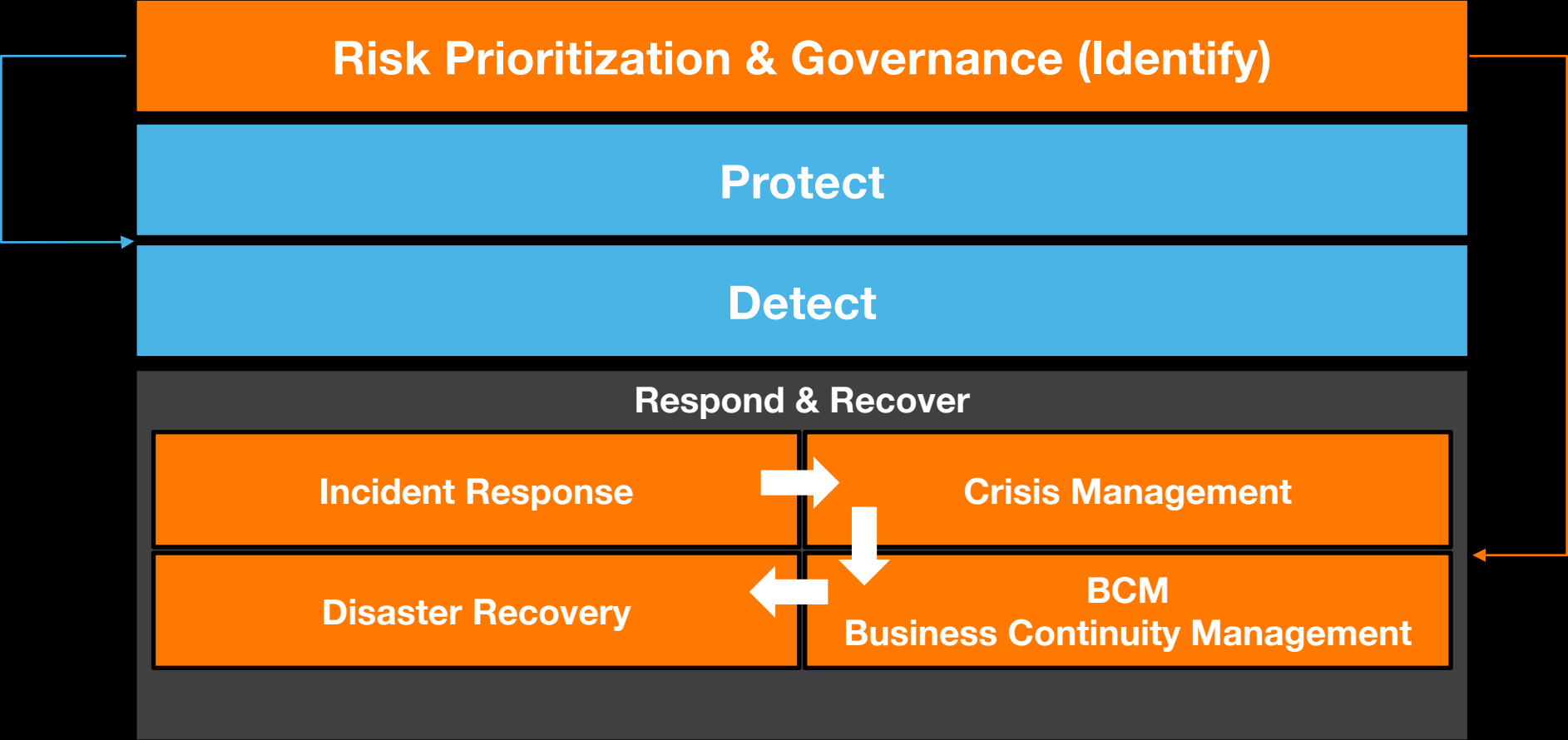
|                     |                     |            |
|---------------------|---------------------|------------|
| Contract management | IT                  | Management |
| GDPR                | Risk Assessment     | Policy     |
| Contract customer   | Technology controls | Awareness  |
| Contract Supplier   | Documentation       |            |

# GRC - optimizing and operationalizing risk mitigation & investments

Significant part of organizational resilience

Why - **What** - When

What  
& how



What  
& how

# NIS 2 – Who is responsible for the tasks?

|                     |                     |            |
|---------------------|---------------------|------------|
| Contract management | IT                  | Management |
| GDPR                | Risk Assessment     | Policy     |
| Contract customer   | Technology controls | Awareness  |
| Contract Supplier   | Documentation       |            |

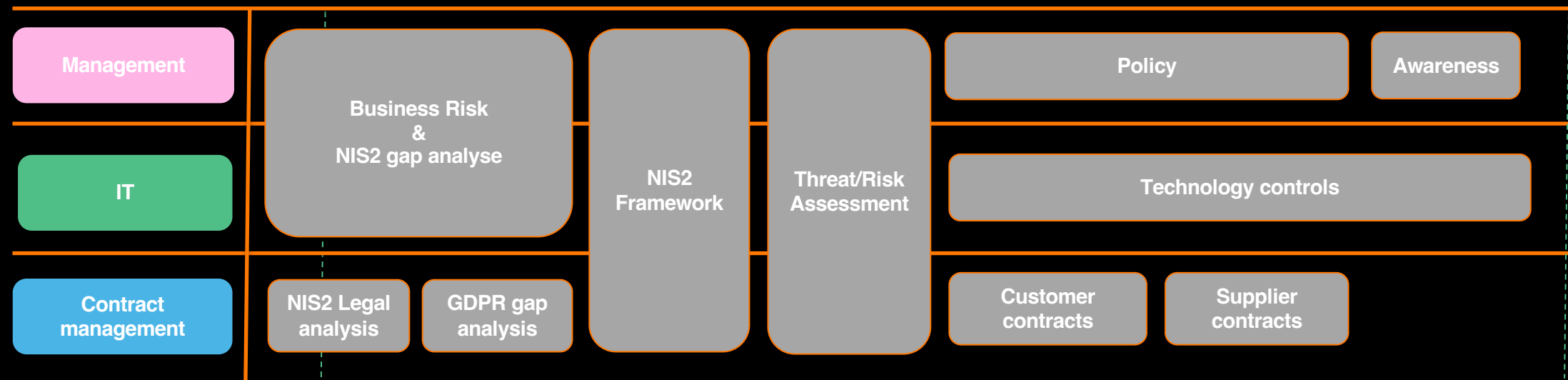
# It's time to prepare...



\*Deadline for EU Member States to transpose directive into local law. Essential and Important entities will have 30 and 18 months to comply.



# NIS2 Timeline with tasks



# Overview of DORA



**DORA** is the **Digital Operational Resilience Act**



DORA is a sector-specific directive for **financial institutions**, targeting their approach to operational risk. It introduces rules for managing all aspects of operational resilience, particularly emphasizing protection, detection, containment, recovery, and repair capabilities against ICT-related incidents.



What are the main differences between **NIS2** and **DORA**?

NIS2 is a directive that allows countries to develop rules based on their specific national needs. In contrast, **DORA is a regulation**, leaving no room for discretion at the Member State level.

# Overview of DORA

## Enhance cybersecurity and resilience of the financial sector

- 1. Governance and organisation (Article 4)
- 2. ICT risk management (Articles 5 to 14)
- 3. ICT incident reporting (Articles 15 to 20)
- 4. Cyber resilience testing (Articles 21 to 24)
- 5. Risk assessment of 3rd party ICT suppliers (Articles 25 to 39)
- 6. Sharing knowledge and information on cyber incidents (Article 40)