22nd Innovation Forum for Automation

CYBER RESILIENCE IN AUTOMATION:

UPCOMING EU REGULATIONS AND WHAT MANUFACTURERS AND OPERATORS SHOULD DO NOW!

Dr. Matthias Meyer – Division Manager Software Engineering & IT Security

https://lemontaps.com/tjpdfde9xo/

meyer-matthias

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

It is mandatory for companies to protect themselves and their products against cyber attacks

Increasing number of vulnerabilities and attacks

Companies from all domains

Automotive | Health | Finance | Production | ...

Upcoming laws regarding Cyber Resilience

- Network and Information Systems Directive (NIS 2)
- Digital Operational Resilience Act (DORA)
- EU Cyber Resilience Act (CRA)

New stars are born: The EU has issued new regulations!

Cyber Resilience Act (CRA)

Regulation

Security of **„products with digital elements“**

To be fulfilled by September 2026/ December 2027

Network and Information Systems Directive (NIS-2)

IT/OT Security for „KRITIS“, essential, and important entities

To be fulfilled by ~~Oct 18th, 2024~~ Sometime in 2025?

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

EU Cyber Resilience Act

Horizontal Cybersecurity Requirements for Products with Digital Elements

Applicable to:

Products (software and/or hardware) that may have a data connection to a device or network and are made available on the European market in the course of a commercial activity

Consequences of non-conformance:

- No CE marking / prohibited to be sold inside EU
- Product warning by federal agency (e.g., BSI, ENISA)
- Penalty payments up to millions of €

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

EU Cyber Resilience Act

Who is affected and how?

→ Make products compliant with all CRA requirements
→ Main focus of the regulation

Manufacturers

→ Only compliant products
→ Own name/trademark or substantial modifications
→ partly treated as Manufacturer!

Importers & Distributors

Operators (Users)

→ No obligations

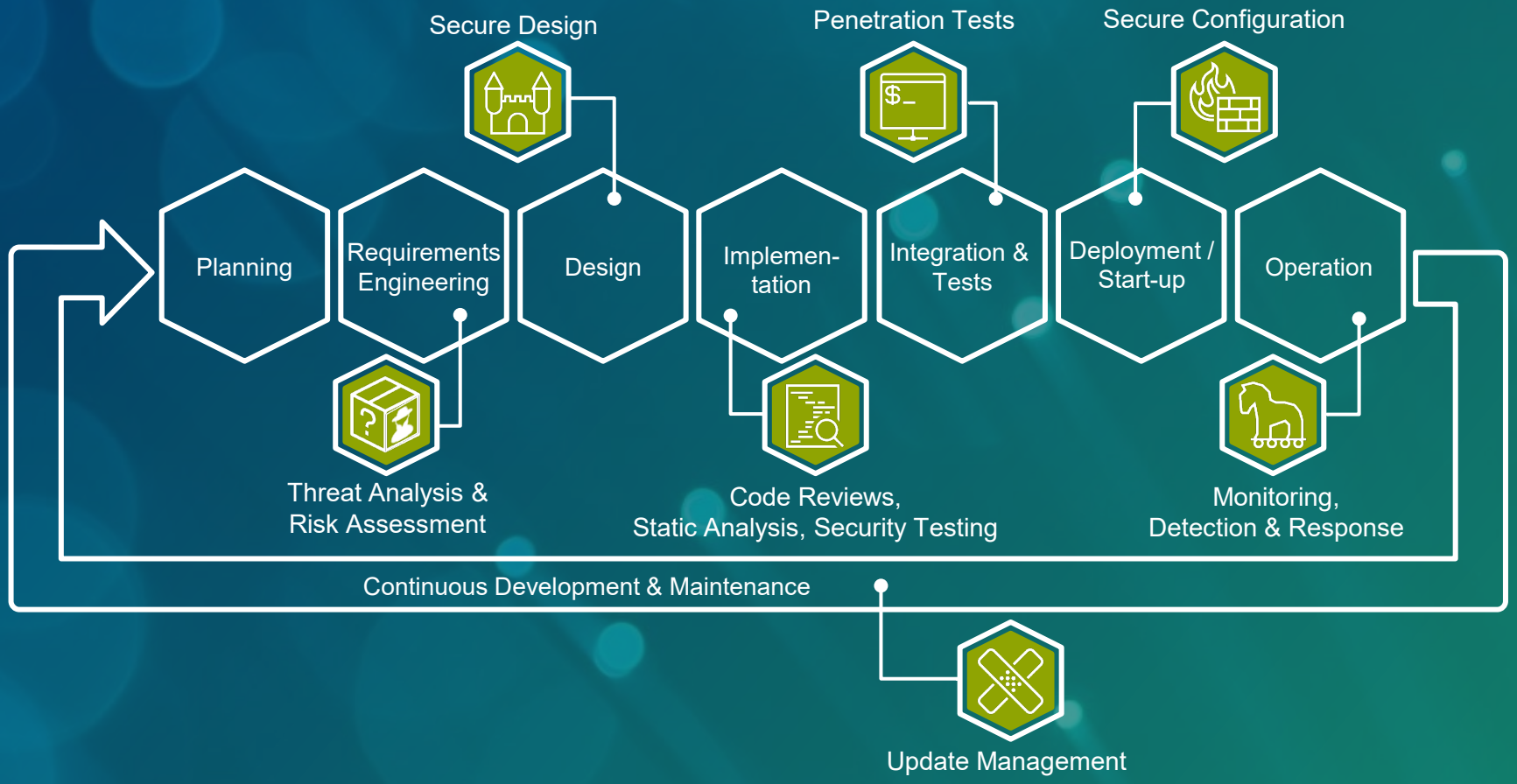
Wait for the NIS-2 part of the presentation! ☺

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Secure Product Lifecycle (Security by Design)

Requires Security Activities along the entire product life cycle – until end of operation!

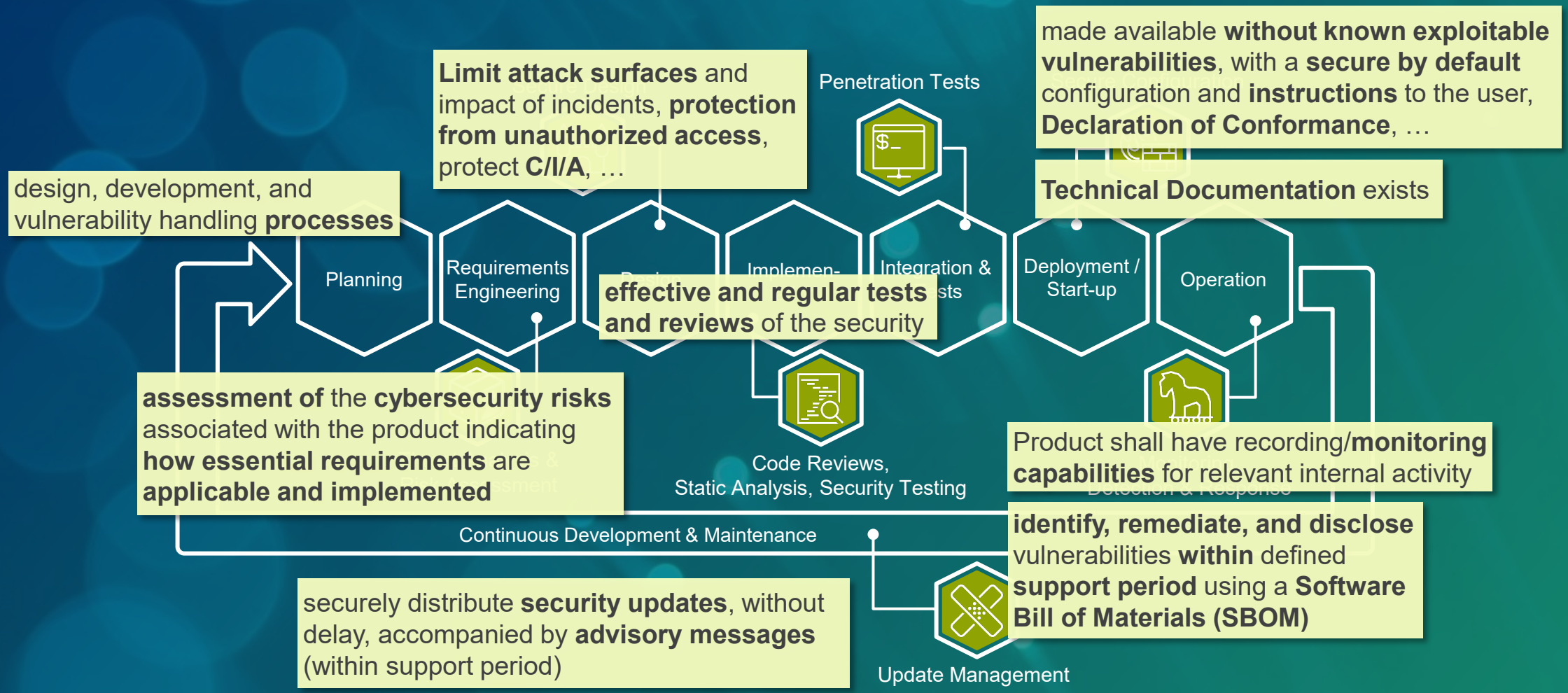


HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Secure Product Lifecycle (Security by Design)

Mapping with EU Cyber Resilience Act requirements (excerpt)



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

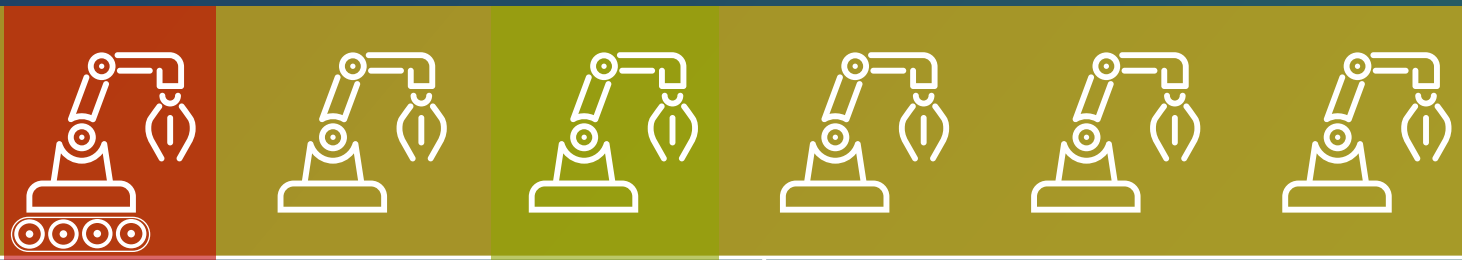
Deadlines & Conditions for compliance

Every single product counts!

Supplier Part

Compatible support period of CRA-compliant supplier parts

Product Type A



Support period
Min. 5 years, BUT corresp. to expected time of use

Substantial modification

Full compliance required!

Spare part

No compl. required

Sept. 11th, 2026

Comply with reporting obligations:
Actively exploited vulnerability → Early warning to ENISA within 24h

For all products on the market!

Dec. 11th, 2027

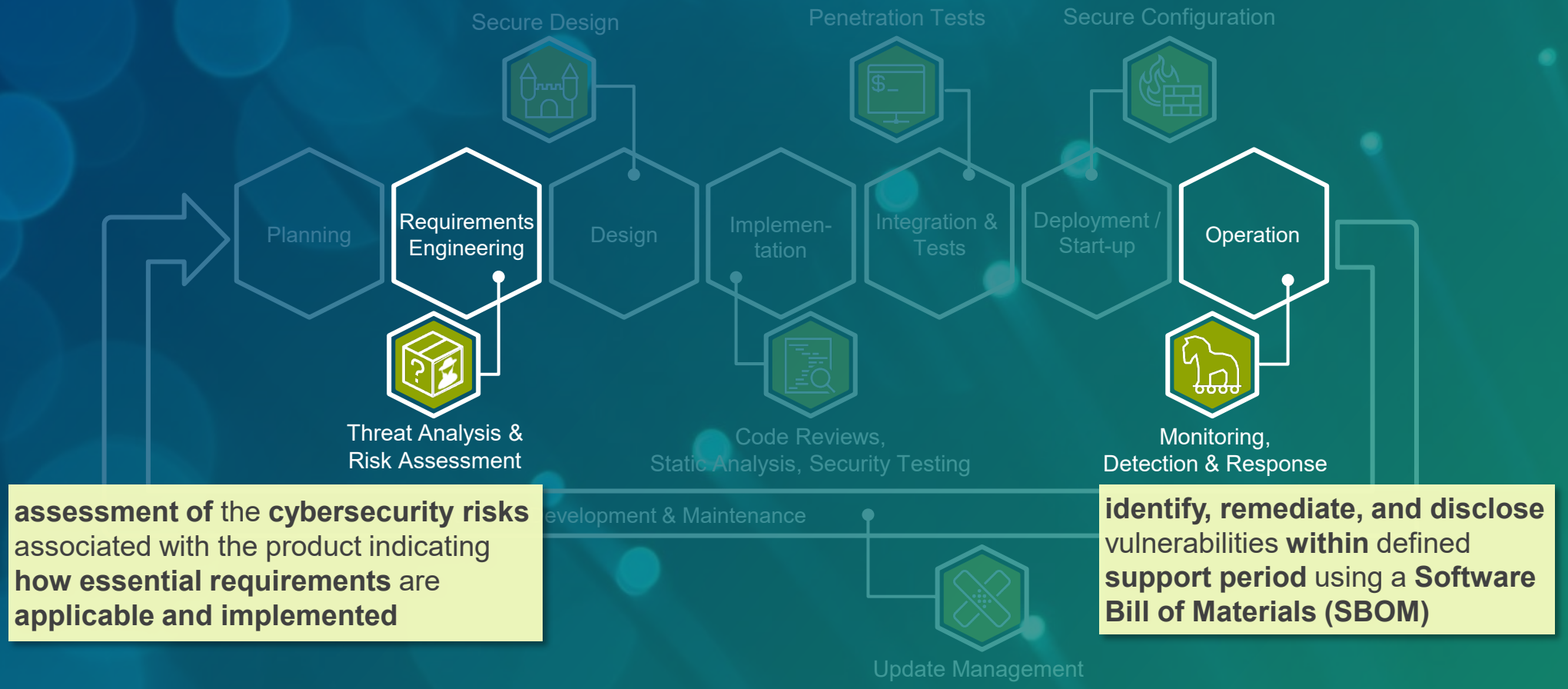
Full compliance with CRA requirements

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

How to Prepare for the Cyber Resilience Act?

Where to start?



assessment of the **cybersecurity risks** associated with the product indicating **how essential requirements** are **applicable and implemented**

identify, remediate, and disclose vulnerabilities **within** defined **support period** using a **Software Bill of Materials (SBOM)**

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

How to Prepare for the Cyber Resilience Act?

Where to start:

1. Security is not a one-time thing:
   Establish a **Product Security Incident Response Team (PSIRT)!**
   → **React and report timely.**

2. **Know your risks!**
   Conduct **Threat Analysis & Risk Assessment** for your products!
   → **Make informed decisions & plans.**

3. Conduct **Cyber Resilience Assessments:**
   Identify **status quo &** define **roadmaps** for improving products & engineering processes!
   → **Know what to do when.**

New stars are born: The EU has issued new regulations!

Cyber Resilience Act (CRA)

Regulation

Security of **„products with digital elements“**

To be fulfilled by September 2026/ December 2027

Network and Information Systems Directive (NIS-2)

IT/OT Security for „KRITIS“, essential, and important entities

To be fulfilled by ~~Oct 18th, 2024~~ Sometime in 2025?

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

Network and Information Systems Directive (NIS-2)

Who is affected?

Essential Entities (examples)

- Digital Infrastructure: DNS providers
- Energy: Electricity Producers
- Banking: Credit institutions
- ICT service management (B2B): Managed service providers

Primarily large organizations

Operators of Critical Infrastructure

Important Entities (examples)

- Postal service providers
- Manufacturing: Manufacture of
  - computer, electronic and optical products
  - machinery and equipment

Medium-sized & large organizations

! Obligation to register:
Check affectedness and register in time!

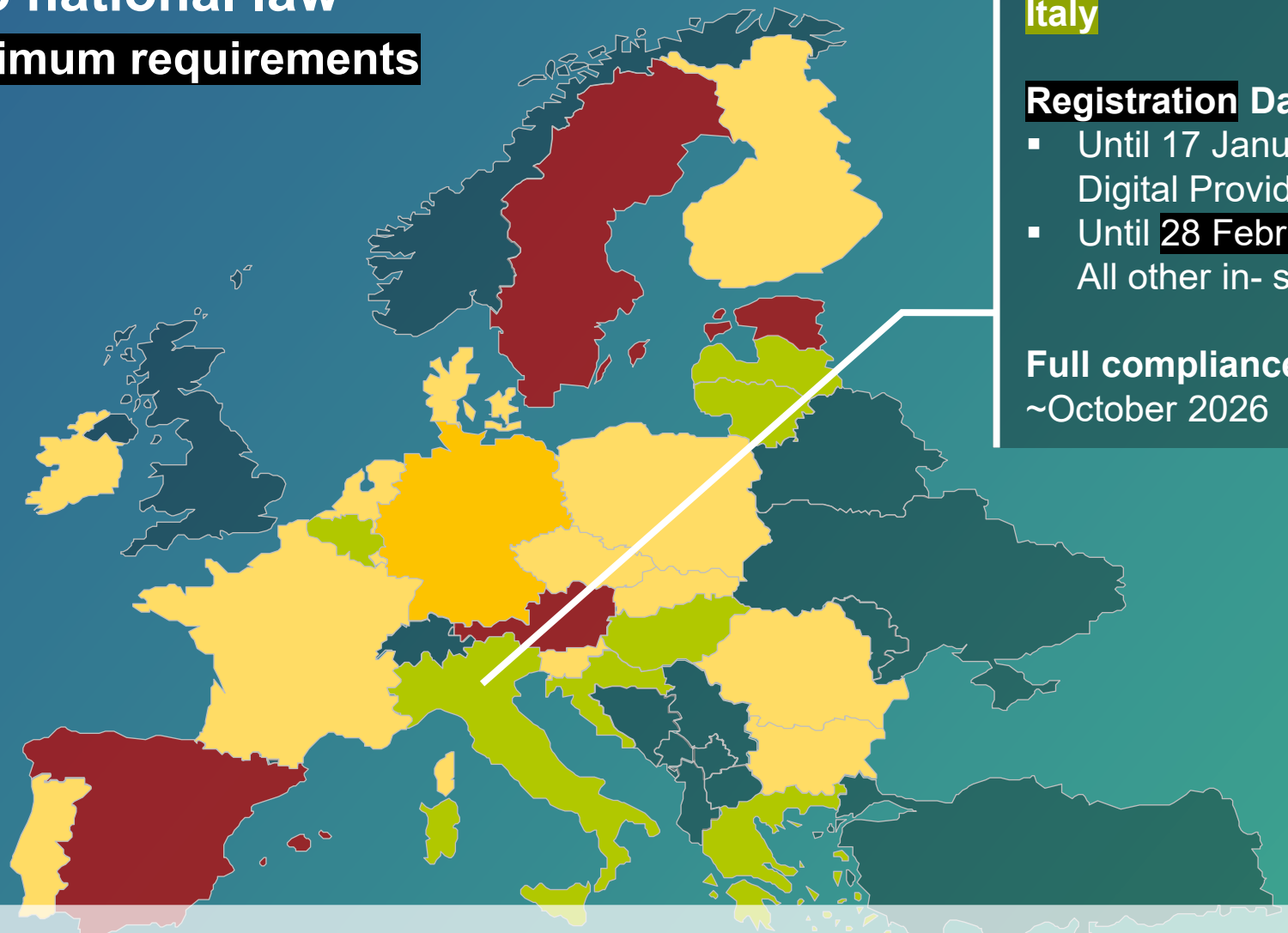
BSI online check: https://betroffenheitspruefung-nis-2.bsi.de/

Transposition into national law

Directive defines minimum requirements

- Unknown
- Draft exists
- Implemented

(As at 18.12.2024)



Italy

Registration Dates:

- Until 17 January 2025: Digital Providers
- Until 28 February 2025: All other in- scope entities

Full compliance due ~October 2026

! Locations in several countries? → The local implementation laws must be taken into account!

Core NIS-2 requirements (Article 21 & 23)

Cybersecurity risk-management measures (Article 21)

- Take technical, operational and organisational measures to manage the security risks of IT used for operations or the provision of services, including at least:
  - policies on risk analysis and information system security (ISMS)
  - incident handling
  - business continuity, such as backup management and disaster recovery, and crisis management;
  - supply chain security
  - […]

Reporting obligations (Article 23)

- Essential and important entities notify, without undue delay, its CSIRT and possibly users of their services of any incident that has a significant impact on the provision of their services
- Significant: (a) capable of causing severe operational disruption or financial loss, (b) capable of causing considerable material or non-material damage
- Within **24 hours**: Early warning
- Within **72 hours**: Initial assessment of severity and impact
- Within **1 month**: Final report

! BSI-Grundschutz, ISO27001, TISAX v6 Lv. 2 provide very good orientation

Duties and liability of the management

Members of the Management bodies of essential and important entities…

… approve the cybersecurity risk-management measures taken to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

… are required to follow training on a regular basis to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices

… can be temporarily prohibited from exercising managerial functions (at chief executive officer or legal representative level) [applies to essential entities only]

… can be held liable for breach of their duties to ensure compliance with this Directive

How to Prepare for NIS-2?

What to do now:

1

Do you have to comply with NIS-2, and in which countries?

Conduct a legal assessment! If affected, register in time!

Know if & how you are affected.

2

Be prepared for a cyber security incident anyway!

Train managers; do a GAP analysis; Setup an ISMS; setup and practice a business continuity & recovery plan (cf. Article 21)!

Know what to do in an incident & recover fast.

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer IEM

How to Prepare for CRA & NIS-2?

CRA

Cyber Resilience Act

Security of **„products with digital elements“**

1. **Establish PSIRT**
2. **Threat & Risk Analysis**
3. **Cyber Resilience Assessments**

NIS-2

Network and Information Systems Directive (NIS-2)

IT/OT Security for „KRITIS“, essential, and important entities

1. **Clarify affectedness & register**
2. **Business continuity & recovery plan** (+ other parts of Art. 21)

Contact

Dr. Matthias Meyer

Division Manager
Software Engineering & IT Security
Phone +49 5251 5465 -122
matthias.meyer@iem.fraunhofer.de

Fraunhofer IEM
Zukunftsmeile 1
33102 Paderborn
www.iem.fraunhofer.de

https://lemontaps.com/tjpdfde9xo/

meyer-matthias

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Fraunhofer
IEM