EU NIS 2

Implementations in EU Member States

February 27, 2024

NIS and CIP roadmap since 2014 (Germany)

EU NIS directive

Draft EU NIS2/RCE directives

EU NIS2/RCE in Force

Transposition in national law NIS2/RCE

Many new NIS2 entities in EU

2014-2019 — 2020 — 2021 — 2022 — 2023 — 2024 — 2025

German IT security act 1.0

German IT security act 2.0

Drafts KRITIS-Dachgesetz NIS2-UmsuCG

In force NIS2 Umsetzung Dachgesetz
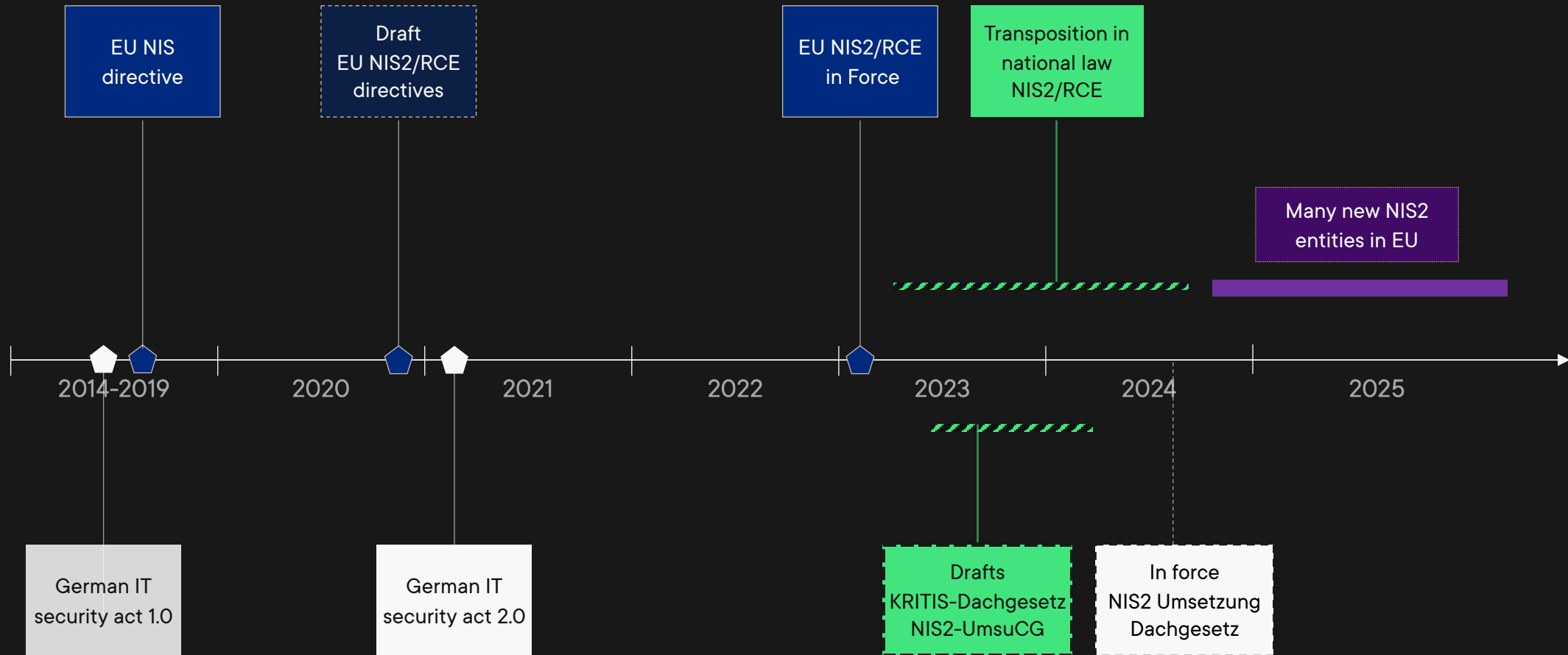
National implementation (example Germany)

until 10/2024	ETA 10/2024		until 10/2024	ETA 10/2024

EU RCE → *implemented by* → **KRITIS-DachG**

EU NIS2 → *implemented by* → **NIS2UmsuCG**

- Focus: Physical security and resilience
- Scope: Critical operators (Germany: KRITIS)
- Protects: Infrastructures/critical services
- National oversight (Germany: BBK)

- Focus: Cybersecurity and information technology
- Scope: Entities providing NIS2 services in EU
- Protects: Large parts of EU economy
- National oversicht (BSI) + some EU

EU NIS2 requirements

Risk management

Reporting
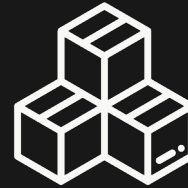
Registration

Evidence

Information

Governance

Sectors, definitions

● National differences
● Uncertainties likely

! Several exclusions and special definitions in NIS2 for risk management (Art. 20 and 21). Some of these will be regulated by sector-specific legislation, some through EU acts: Telecommunications, cloud and online, energy, national security

Sector definitions in the EU

Critical Entities	Essential Entities	Important Entities	
Entities (RCE)	Large enterprises + special cases	Medium enterprises	Large enterprises Medium enterprises

Energy		
Transports		Postal and Courier
Financial markets		Chemicals
Health		Manufacturing
Drinking water and waste water		Research
Digital Infrastructure		Digital Services
ICT Service Management		Waste management
Space		
Food	Public Administration	Food

NIS 2 Implementations in EU Member States

Information on EU NIS2 in countries is partially incomplete, non-public and still in-flux. Draft content.
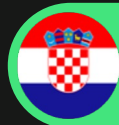
EU NIS2 member states covered today

Five EU member states selected for and discussed in this webinar.

Belgium

Croatia

Czech Republic

Finland

Germany

● final draft available

● consultation completed

NIS 2 Implementation in Belgium

Belgium

Centre for Cybersecurity of Belgium (CCB)

"NIS2 Law"

Timeframe unknown

Transition periods for evidence obligations

Last Draft: November 11, 2023

Vulnerability Management

- Mandatory policy for disclosure of vulnerabilities

### Several Options for Compliance Evaluation

- Audit-like inspection conducted by CCB without additional fees
- External ISO27001-Audits combined with national reference framework
- Optional self-assessment for important entities

Security Policy for IT Systems

- Documentation of risk analysis outcomes for networks and IT systems mandatory
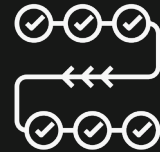
NIS 2 Implementation in Croatia
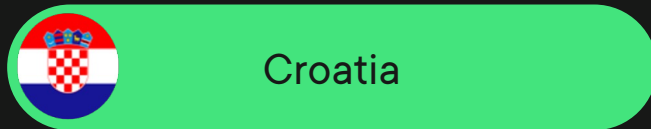
Croatia

Security and Intelligence Agency (SOA)

"Zokona o Kiberenetičkoj Sigurnosti"

Timeframe unknown

Transition period < 9 months

Last Draft: December 13, 2023

Transition Period

- Additional guidelines published until July 2025
- Criteria for classification of important / essential entities
- Criteria for compliance assessments

More Sectors

- Education system "Sustav Obrazovanja" as additional sector

Evidence Obligations

- Audits are the only option
- Audit cycle: 2 years, mandatory (essential entities)
- Self-assessment optional (important entities)

NIS 2 Implementation in Croatia

Croatia

Security and Intelligence Agency (SOA)

"Zokona o Kiberenetičkoj Sigurnosti"

Timeframe unknown

Transition period < 9 months

Last Draft: December 13, 2023

Reporting Obligations

- Apply to important and essential entities
- 24- / 72-hour requirement missing
- CARNET will provide national reporting platform

Comprehensive Cyber Defense

- SOA provides national cyber attack detection system
- Available to important / essential entities

Multiple CSIRTs

- SOA is competent CSIRT in principle
- National CSIRT responsible for certain sectors (banking, financial market infrastructures, digital infrastructure, research, education)

NIS 2 Implementation in the Czech Republic

Czech Republic

National Cyber and Information Security Agency

"Zákon o kybernetické bezpečnosti"

Next phase: Legislative Council must approve

Transition period for reporting obligations

Last Draft: December 22, 2023

Relevant NIS 2 Implementation Acts

- Act on cyber security: obligations applicable to parties (entities, governmental institutions)
- Additional acts: separate documents for operators of regulated services, important + essential entities

Strategically Important Services

- High availability requirements for certain services
- Defined in Cyber Security Act Art. 27, 28 + additional act for entities in higher obligations annex 9

More Obligations

- Highly detailed obligations in additional acts
- Mandatory ISMS for essential entities
- Strong focus on supply chain security

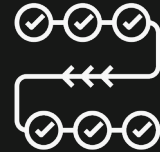# NIS 2 Implementation in the Czech Republic II

Czech Republic

National Cyber and Information Security Agency

"Zákon o kybernetické bezpečnosti"

Next phase: Legislative Council must approve

Transition period for reporting obligations

Last Draft: December 22, 2023

Registration Deadlines

- 90 days from affectedness
- 30 days from (self-)identification
- Shorter period applies

Reporting obligations

- Not limited to significant incidents
- Possibly also for minor incidents

More sectors

- Military industry as additional sector
- Waste water + drinking water merged water management
- Banking + financial market infrastructures merged into financial mrk.
- Digital infrastructure + ICT = digital infrastructure and services
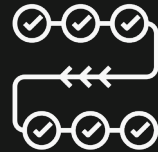
NIS 2 Implementation in Finland

Finland

Ministry of Transport and Communications (LVM)

"Laki kyberturvallisuuden riskienhallinnasta"

Spring 2024 into parliament

Transition periods for registration obligations

Last Draft: November 01, 2023

Transition Period

- Registration obligations come into force January 1st, 2025

Missing Evidence Obligations

- Evidence obligations not mentioned

- LVM authorized to impose an audit on entities

Sectors

- Many sectors without explicit label

- Banking and financial market infrastructures not defined in draft

NIS 2 Implementation in Germany

Germany

Federal Office for Information Security (BSI)

"NIS2-Umsetzungsgesetz"

Publication planned 4/24

No transition periods

Last Draft: September 2023

Entities and operators

- Two groups: Entities (NIS2) and operators (KRITIS)
- KRITIS: Operators of critical infrastructures as additional group with more obligations and different method

Lower Thresholds

- NIS2 "and" became "or" in German
- Small: 50 employees or 10 Mio. EUR turnover + 43 Mio. EUR balance

Different Sectors

- Gas and Hydrogen consolidated into „Gasversorgung"
- Public administration not yet listed in annex
- ICT service management and digital infrastructure = "IT and Telco"

NIS 2 Implementation in Germany II

Germany

Federal Office for Information Security (BSI)

"NIS2-Umsetzungsgesetz"

Publication planned 4/24

No transition periods

Last Draft: September 2023

Evidence and audits

- Operators need to be audited every three years
- Authorities might audit on a by-case basis

Risk management

- Sector-specific requirements and authorities (NRG, Telco)
- State guidance will be needed/updates for Art. 21

Legislation

- Needs "KRITIS ordinances" for implementation
- Common processes and definitions with RCE (DachG)
- Two laws for entities/operators: NIS2 and RCE

And now?

Status in countries

Found something (OpenKRITIS)

Belgium	Germany	Finland	France	Italy
Croatia	Netherlands	Austria	Sweden	Czech Republic
Hungary				

Found nothing (or almost)

Bulgaria	Denmark	Estonia	Greece	Ireland
Latvia	Lithuania	Luxembourg	Malta	Poland
Portugal	Romania	Slovakia	Slovenia	Spain
Cyprus				

February 2024

Observations February 2024

Implementation and measures

Registration
- Many different authorities
- Complex EU entities

Risk management
- NIS2 is baseline, *however*
- Country/sector-specific

Reporting
- Many authorities involved
- Large reporting effort!

Formalities

Sector definitions
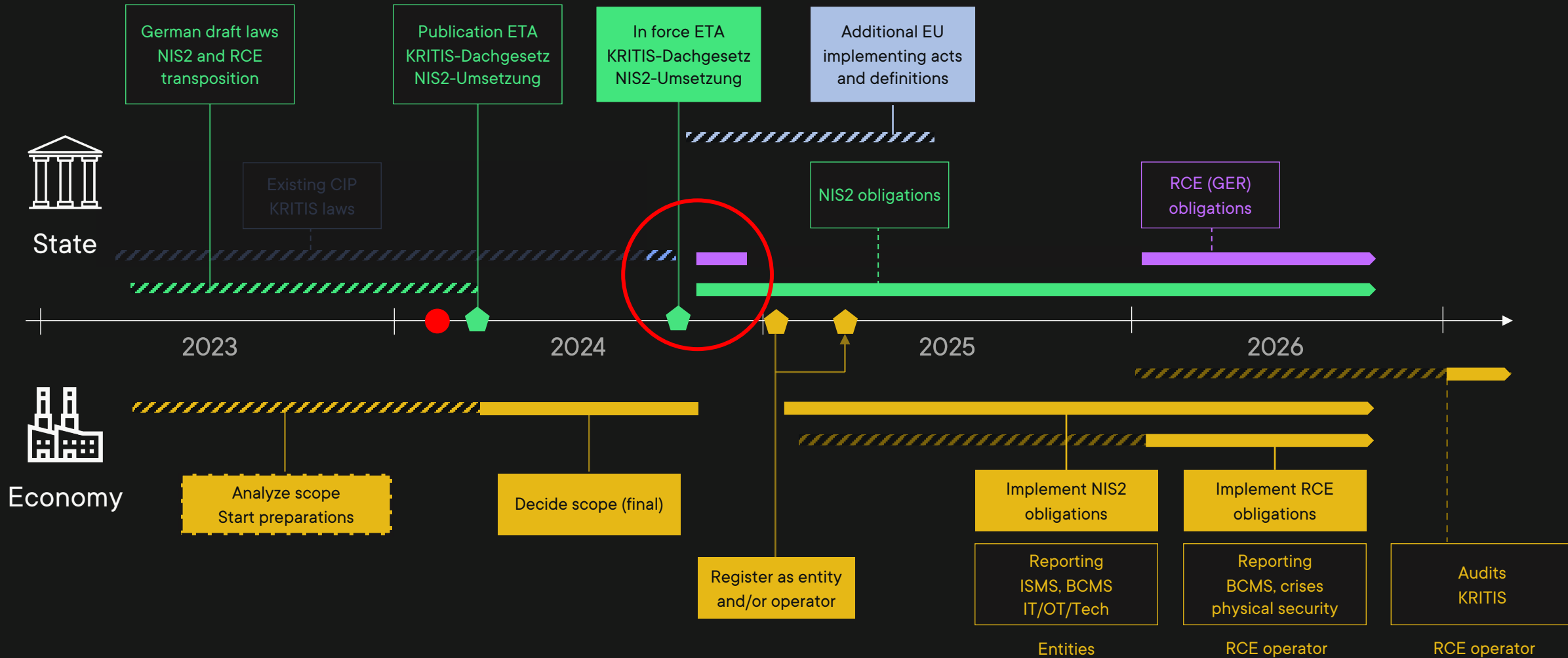- Many differences, gaps
- Some exclusions

Entity definitions
- Entities defined differently
- Legal entities, sales …

Deadlines
- Will countries make it?
- What if not?

NIS2 Roadmap 2023-2026 (Germany)

German draft laws NIS2 and RCE transposition

Publication ETA KRITIS-Dachgesetz NIS2-Umsetzung

In force ETA KRITIS-Dachgesetz NIS2-Umsetzung

Additional EU implementing acts and definitions

State

Existing CIP KRITIS laws

NIS2 obligations

RCE (GER) obligations

2023   2024   2025   2026

Economy

Analyze scope
Start preparations

Decide scope (final)

Register as entity and/or operator

Implement NIS2 obligations

Implement RCE obligations

Reporting
ISMS, BCMS
IT/OT/Tech

Reporting
BCMS, crises
physical security

Audits
KRITIS

Entities   RCE operator   RCE operator

Q & A
Your questions

All the latest on critical infrastructures:

OpenKRITIS.de

OpenKRITIS Conference 2024: openkritis.de/konferenz

EU NIS2 countries: NIS2 in EU-Ländern

NIS2 implementation in GER: NIS2 in Deutschland

Kontakt: info@openkritis.de und OpenKRITIS auf LinkedIn

NIS 2 and EU

OpenKRITIS

Information and analyses for Critical Infrastructures and NIS2

NIS 2 and EU

Date: February 27, 2024

Version: 1.0