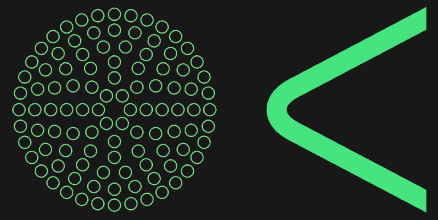
OPENKRITIS



EU NIS2 and RCE

Security and Resilience for Critical Infrastructures

February 2023 · OpenKRITIS

Critical Infrastructures in 2023

EU NIS2

EU 2022/2555

Cyber Security for EU operators

- Security and risk management
- Essential + Important Entities
- Operators by EU size-cap rule
- EU + national oversight

EU RCE

EU 2022/2557

Resilience for EU operators

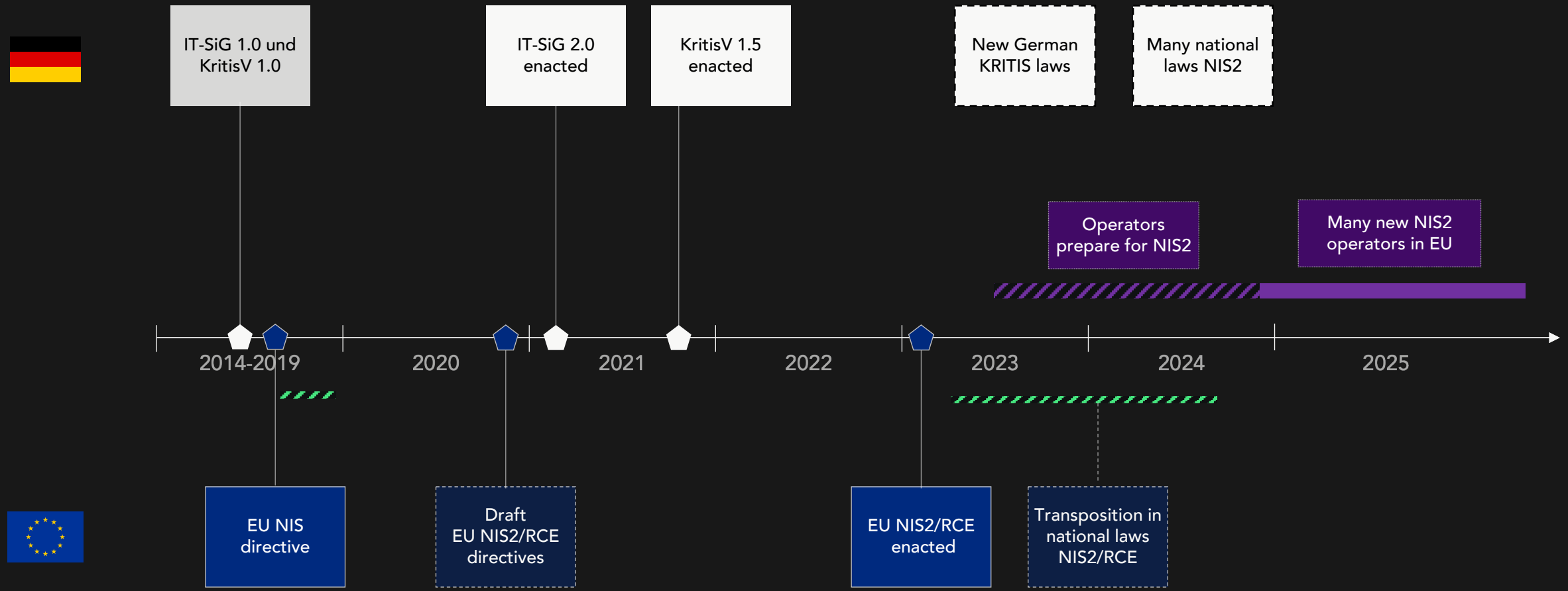
- Resilience, physical and risk
- Critical Entities
- Operators by criticality
- EU + national oversight

Transposition into national EU laws

until 10/2024

Large parts of EU economy affected

Roadmap of EU and German KRITIS



EU NIS 2: Cyber Security for the EU

NIS2 – EU 2022/2555

Scope

- Cyber Security
- Baseline for EU
- Many operators affected

Who is affected by NIS2?

EU size-cap

- Medium operators: >50 FTE, >10m revenue/assets
- Large operators: >250 FTE, >50m revenue/43m assets

Operators

- Essential and Important Entities (thousands + in EU)
- Eighteen sectors in the EU, complex size-cap rule

Special cases

- Some operators regulated independent of size NIS2
- Monopolies, cross-borders or critical dependencies

NIS2 and RCE sectors in the EU

Annex I

- Energy — RCE
- Health — RCE
- Transport — RCE
- Banks + Financial — RCE
- Water — RCE
- Digital Infrastructure — RCE
- ICT Service Mgmt.
- Public Admin — RCE
- Space — RCE

Annex II

- Postal and Courier
- Waste
- Chemicals
- Food — RCE
- Industry
- Digital Services
- Research

NIS2 RCE

Examples

- Large Energy Utility
  50k FTE, 10M revenue — RCE
- Regional IT integrator
  300 FTE, 60m revenue — maybe RCE
- Communal Utility
  50 FTE, 11m revenue — RCE
- Producer of car seats
  65 FTE, 15m revenue

Essential

Annex I

- Large operators Annex I
  - >250 FTE
  - >50m € revenue or >43m € assets
- Size-independent
  - TLD, qualified TSP
  - Central/regional gov.
  - Medium e-communic.

- Energy
- Health
- Transport
- Banks + Finance
- Water
- Digital Infrastructure
- ICT Service Provider
- Public Admin
- Space

Annex I | Annex II

- Special rule: sole provider, significant effect, systemic risk

RCE | national

- Additional: RCE Critical Entities, existing operators

Important

Annex II

- Postal and Courier
- Waste
- Chemicals
- Food
- Industry
- Digital Services
- Research

- Large operators Annex II
  - >250 FTE
  - >50m € revenue or >43m € assets
- Medium operators Annex II
  - >50 FTE
  - >10m € revenue or >10m € assets

Annex I

- Annex I sectors

- Medium operators Annex I
  - >50 FTE
  - >10m € revenue or >10m € assets

Security Requirements in NIS2

Governance, ISMS

Incident Reporting

IT resilience

Supply chain

Audit and tests

IT, crypto, access ...

Operator responsibilities

- Operators to implement cyber security: ISMS, policies, frame
- Measures need to be based on risk and threats to services
- Additional security incident notification to states and EU
- Normative cyber security will be prescribed in national laws
- EU defines a baseline – states and operaters can do more

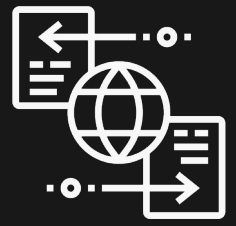
EU and national cooperation for NIS2

National governance

Member states

- National cyber security strategies
- Competent authorities for cyber security, incidents and CSIRTs
- Strong required governance and enforcement by states
- Incident reporting and threats

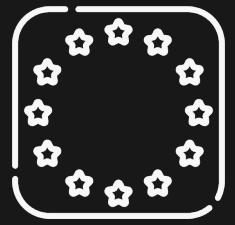
Cooperation



Collaboration in the EU

- National CSIRTs to collaborate
- Information sharing in case of cross-border incidents, pan-EU operators
- Joint assessments between states
- Joint incident response through EU-CyCLONe instrument

Oversight



EU and ENISA

- EU Cooperation Group as central
- European jurisdiction for specific operators, pan-EU businesses
- EU databases for operators, incidents, vulnerabilities
- State of cyber security by ENISA

Sanctions and fines in NIS2

Enforcement

- Strict enforcement and supervision regime by national authorities mandated
- Oversight on implementation and compliance of operators by authorities
- State intervention and monitoring

Sanctions

- Fines (baseline) with maximum principle
- In case of non-compliance to NIS2 regulations
- 10m EUR or 2% global revenue Essential
- 7m EUR or 1.4% global revenue Important

EU RCE: Resilience in the EU (CER directive)

RCE – EU 2022/2557

Scope

- Resilience
- Physical Security
- Specific operators

Who is affected by RCE?

Critical Entities

- Identification through national authorities
- Disruptive effect on essential services

Operators

- Critical Entities, equivalent to Essential in NIS 2
- 11 sectors in the EU, fewer than NIS 2 (see slide 5)

Special cases

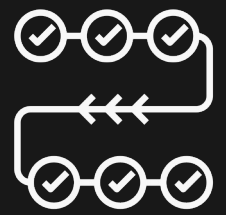
- Operators with special EU significance
- Several exclusions (IT, financials, digital)

Resilience Requirements in RCE

Prevention

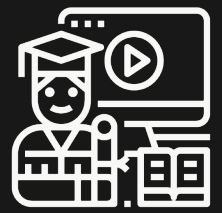
Physical Security

Crises



BCM

Personnel



Awareness

Operator responsibilities

- Operators to improve BCM, risk management and physical
- Measures based on availability and disruptions of services
- More notifications on crises and incidents to states and EU
- Normative resilience will be prescribed in national laws
- EU defines a baseline

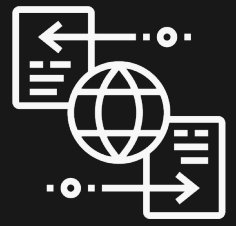
EU and national cooperation for RCE

National governance

Member states

- National resilience strategies
- Competent authorities for resilience (another agency!)
- State identification of operators
- Incident reporting and threats

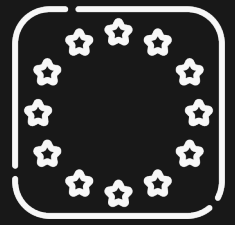
Cooperation



Collaboration in the EU

- Information sharing for cross-border incidents and pan-EU operators
- Assessment of EU-wide risks and operators

Oversight



EU and ENISA

- EU CERG as cooperation body
- EU register of operators and risks
- Special operators of particular European relevance
- Oversight by the commission

What comes next?

States

- EU NIS2 in national law until 9/2024
- EU RCE in national law until 9/2024
- Harmonize national CI identification
- Rules for "legacy" CI operators and laws
- Notification rules national vs. EU
- National standards for NIS2 and RCE
- Rules for multinationals and EU players

Operators

- Identify own NIS2/RCE scope
- Check how clients are affected (many will)
- Risk management and supply chains
- Strenghthen cyber security measures
- Notifications and incident reporting
- Increase physical security (often deficient)
- Really implement BCM, IT-SCM, crisis

Who is who? KRITIS, UBI and NIS2

KRITIS --- more important ---> **UBI** --- might be part of ---> **NIS2/RCE**

	KRITIS	UBI	NIS2/RCE
Scope	▪ Specific assets within operators ▪ Identified by KRITIS thresholds	▪ Whole companies in industries ▪ Identified by products/size	▪ Medium/large operators (NIS2 size-cap) ▪ Critical operators (RCE) by states
Measures	▪ IT security + some resilience * ▪ Audit evidence to BSI, penalties ▪ Incident notifications to BSI	▪ IT security foundations ▪ (some) Self declaration, penalties ▪ (some) Incident notifications to BSI	▪ Cyber security and resilience * ▪ Evidences, strong penalties ▪ Additional incident notifications

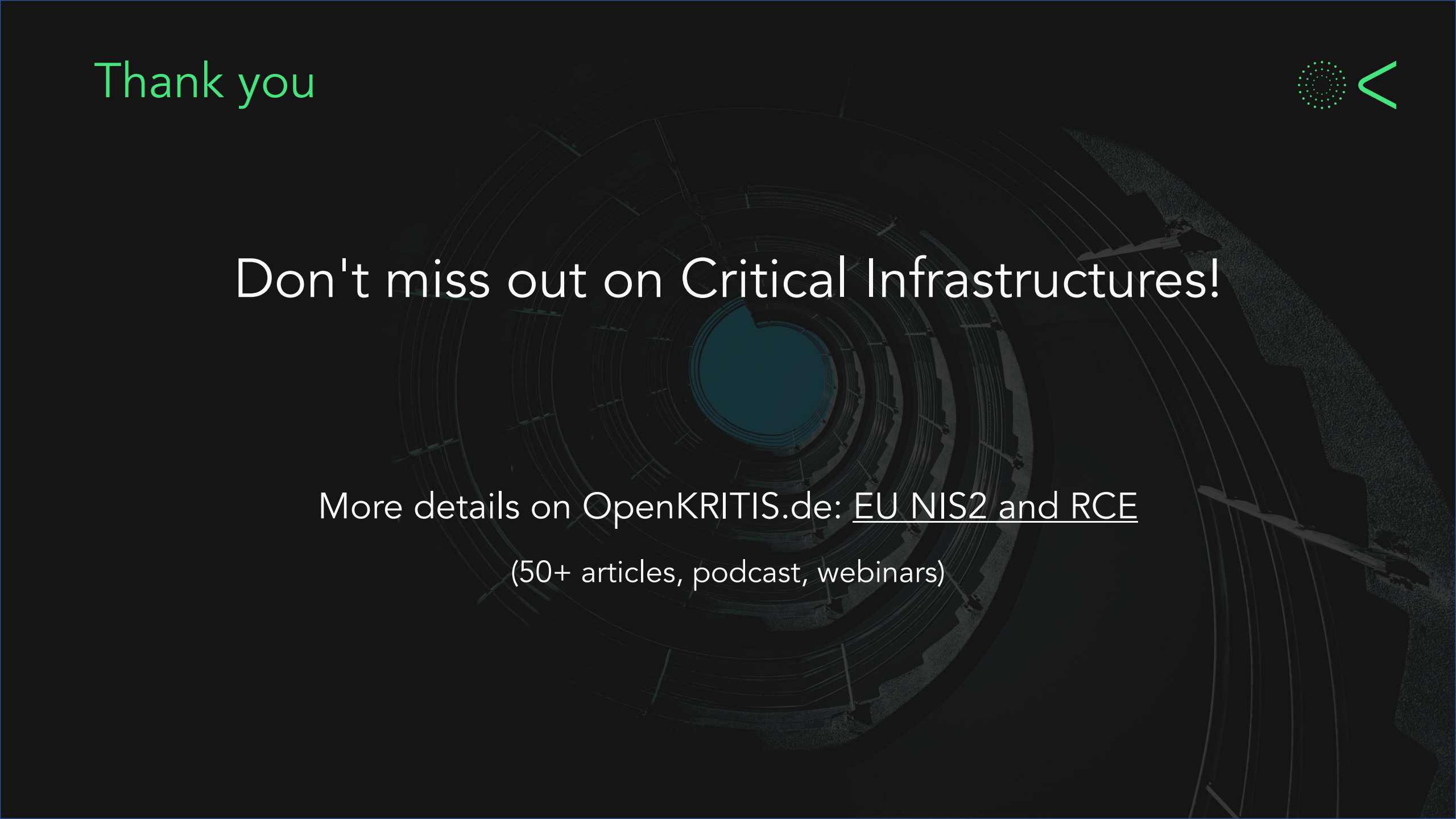
Sectors

KRITIS		Dachgesetz	unklar	UBI	NIS2/RCE		Essential	Important	RCE
Energie	Dach	Öff. Verwaltung		Rüstung	Energy	RCE	Postal and Courier		
Gesundheit	Dach	Raumfahrt		Volkswirtschaft	Health	RCE	Waste		
Transport/Verkehr	Dach	Medien + Kultur		Chemie	Transport	RCE	Chemicals		
Banken/Versicherung	Dach	Bildung + Betreuung			Banks + Financial	RCE	Food	RCE	
Wasser	Dach				Water	RCE	Industry		
IT und TK	Dach				Digital Infrastructure	RCE	Digital Services		
Ernährung	Dach				ICT Service Mgmt.		Research		
Entsorgung	Dach				Public Administr.	RCE			
					Space	RCE			

* specific rules still TBD

* severall exceptions

Thank you



Don't miss out on Critical Infrastructures!

More details on OpenKRITIS.de: EU NIS2 and RCE

(50+ articles, podcast, webinars)

About

OpenKRITIS

Independent platform on EU critical infrastructures.

EU NIS2 and RCE
Stand: 30 March 2023
Version: 1.3

Imprint

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn, Germany

https://www.openkritis.de · ISSN 2748-565X
info@openkritis.de · +49 176 58952135