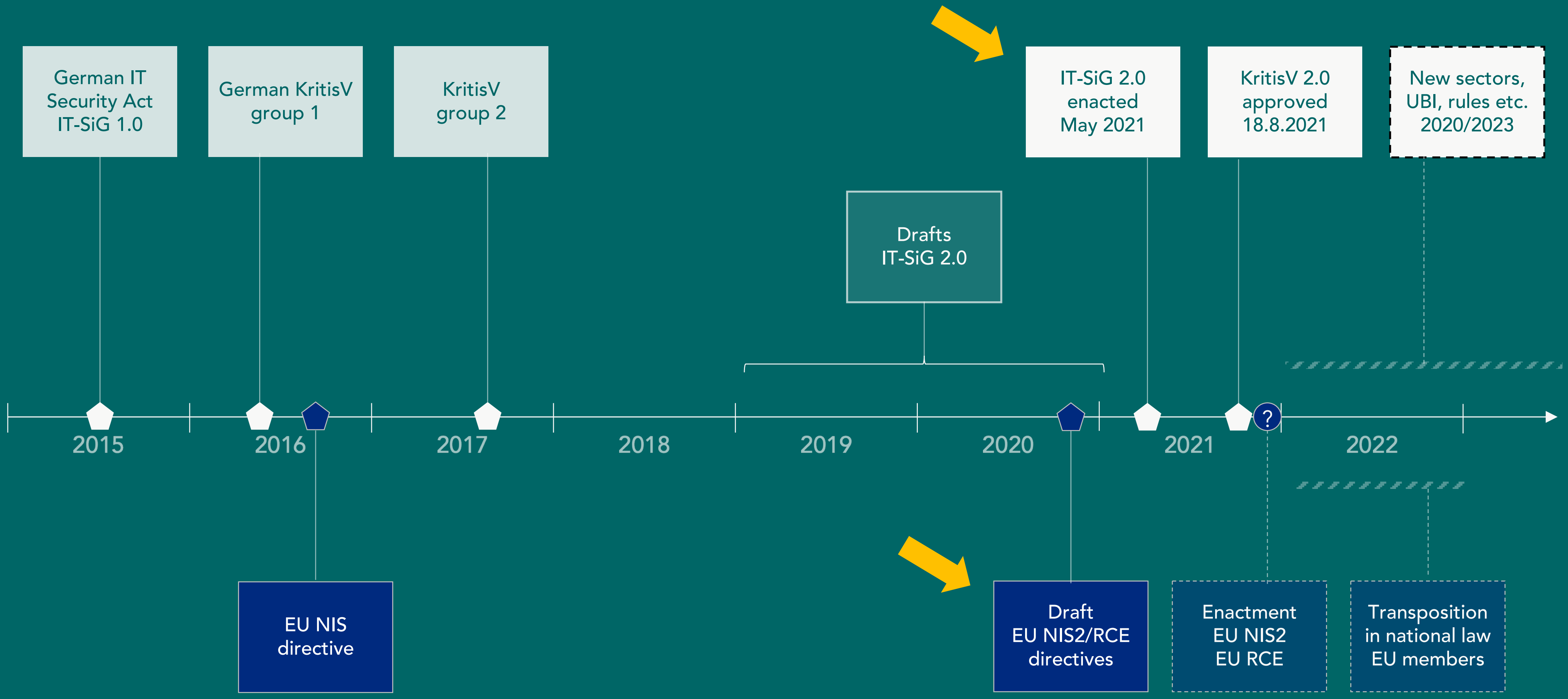
OPENKRITIS

German and EU Critical Infrastructures

IT-Sicherheitsgesetz 2.0 and EU NIS2/RCE

November 17, 2021 · OpenKRITIS

German and EU KRITIS law


German IT Security Act IT-SiG 1.0
German KritisV group 1
KritisV group 2
Drafts IT-SiG 2.0
IT-SiG 2.0 enacted May 2021
KritisV 2.0 approved 18.8.2021
New sectors, UBI, rules etc. 2020/2023
2015
2016
2017
2018
2019
2020
2021
2022
?
EU NIS directive
Draft EU NIS2/RCE directives
Enactment EU NIS2 EU RCE
Transposition in national law EU members

OPENKRITIS

Extended KRITIS scope in IT-SiG 2.0

New rules for operators

Detection of cyber attacks
More incident reporting
Critical components
Immediate registration

More operators in scope

CI sector waste management
Special public interest entities (UBI)
Lower thresholds (↓ 6)
More CI asset types (+17)

More government rights

Central reporting agency
Deep inspections
Protection of federal networks
More staff

Fines and consumer protection

Higher fines for operators
More possible violations
More certifications

More IT-SiG 2.0 Cyber Security

Detection of attacks

❑ Cyber attack detection

❑ Mandatory systems and processes for attack detection

❑ = SOC, SIEM, correlation

Incident reporting

❑ More reporting to BSI needed

❑ Notifications in emergencies on reaction and response

❑ To include personal data (PID)

Components

❑ Critical components in critical infrastructures

❑ Approval required from the German interior ministry

❑ Defined for the telco sector

Registration

❑ Immediate registration required at BSI as operator

❑ Includes central SPOC

❑ BSI might register operators

New in IT-SiG 2.0: Waste and UBI

Waste management

❑ New critical sector *Municipal waste*

❑ Essential service *Disposal of municipal waste:*

a. Collection

b. Disposal

c. Recycling

❑ Asset classes and thresholds still to be defined

UBI (UNBÖFI)

❑ Special public interest entities (German "UBI")

❑ Important but ≠ critical infrastructure, 3 groups:

1. UBI defense, arms, VS-IT (export controlled)
2. UBI economic relevant entities + suppliers
3. UBI hazardous materials (chemicals)

❑ Special cyber security requirements for UBIs

More operators in IT-SiG 2.0 scope

Lower thresholds

□ Lower thresholds = more affected critical infrastructures

□ 5 thresholds lowered ↓

↓ Electricity supply lower

↓ IT hosting/housing/exchanges lower

□ 3 other changes to thresholds

More critical infrastructures

□ More critical infrastructures defined in existing sectors = more operators

→ Energy: 6 new, 4 removed
→ Health: 1 new, 2 removed
→ Transport: 6 new, 1 removed
→ IT/telco: 1 new
→ Finance: 3 new

More operators

□ More critical operators expected with new IT-Sicherheitsgesetz 2.0

□ +270 more operators to 1600 current

□ Most impact in energy and finance

□ New UBI & waste not yet covered, to be handled in more regulation

EU with additional KRITIS regulation

EU RCE

Directive on the resilience of critical entities

RCE is the resilience baseline for EU operators. Companies that provide critical services in the EU will be regulated for resilience and risk and supervised.

RCE regulation

- 10 Critical EU sectors and entities
- Resilience requirements for operators
- National governance, EU oversight

EU NIS2

Directive for a high common level of cybersecurity across the Union

NIS2 is the cyber security rulebook for EU operators. Companies that provide essential services and infrastructure in the EU will be regulated for cyber security and supervised.

NIS2 regulation

- 10 Essential and 6 important EU sectors
- Cyber security requirements for operators
- National governance, EU oversight

EU and German KRITIS regulation

	EU RCE	EU NIS2	IT-SiG 2.0
Sectors	10 Critical	10 Essential 6 Important	8 Critical KRITIS 3 Important UBI
Operators	Identified by national gov's Entities reported to EU	Medium and large enterprises DSP register with ENISA	National thresholds with operators self-identification
Measures	*For critical services*: a. Prevention b. Physical security c. Crisis management d. BCM and suppliers e. Personnel security f. Awareness	*For networks and IT systems*: a. Policies b. Incident Management c. BCM and crisis management d. Supply chain security e. Test and audit f. Cryptography	*For IT of critical services*: a. Security organization b. Secure technologies c. Cyber attack detection d. Critical components
Reporting	Incident reporting Risk analysis and planning	Incident reporting Audit and evidence	Self-identification/registration Incident reporting Scope definition Audit and evidence
National	Resilience authority - Inspections and audits	Cyber authorities, CSIRT - Enforcement, audits, sanctions	BSI - Evidences, audits, sanctions

KRITIS in Germany: What now?

Existing KRITIS

- Detection of cyber attacks - SIEM/SOC
  from 2023
- Identify new critical infrastructure
- Check for lower critical thresholds
- Implement new reporting reqs

New KRITIS

- Identify critical infrastructures
- Register as operator at BSI
- Implement cyber security measures
- Implement reporting reqs

Telecom operators

- Identify "critical components"
- Report and clear critical components

UBI/UNBÖFI

- Register as SPIE with government
  from 2021/23/24
- Implement cyber security measures
  from 2023/24
- Implement reporting reqs
  from 2021/23/24

All: Prepare for EU regulation

from ~2022

Don't miss out on Critical Infrastructures:

OpenKRITIS.de

(40+ articles, podcast, webinars)

OpenKRITIS

Open information resource on critical infrastructures.

German and EU KRITIS

Date: November 17, 2021

Version: 1.0

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

OPENKRITIS