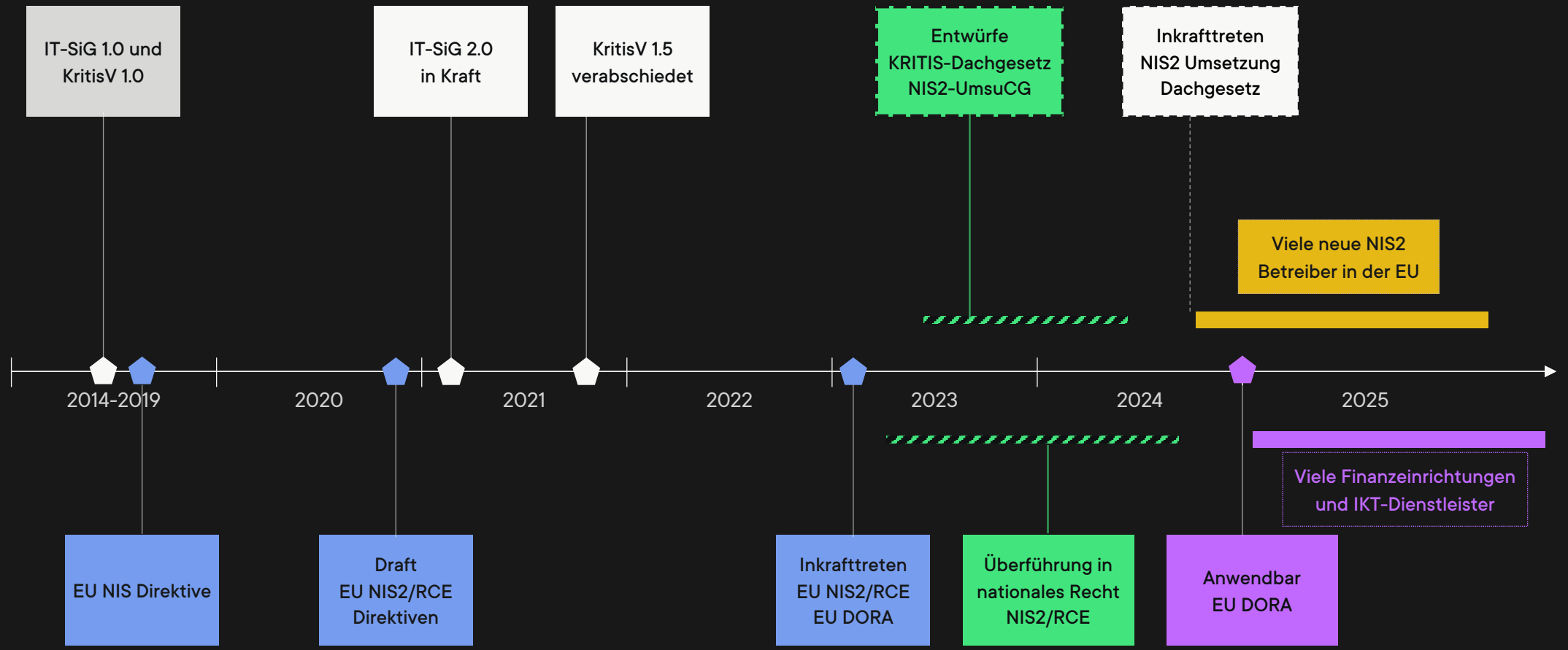
DORA und NIS2 für Provider

Was kommt auf IT-Dienstleister zu? (viel)

Juli 2024

EU NIS2 und DORA
Einleitung

KRITIS in Deutschland seit 2014



Neue Vorgaben durch die EU

EU NIS2
High common level of cybersecurity across the Union

EU DORA
Digital Operational Resilience Act

NIS2 als Mindestniveau für Cybersecurity in der EU. Unternehmen, die kritische Dienste und Infrastruktur in der EU betreiben, werden durch Mitgliedsstaaten reguliert.

DORA als Europäischer Rahmen für die digitale Resilienz im EU-Finanzsektor. Ziel: Harmonisierung von Cybersecurity und resiliente Infrastrukturen im Finanzmarkt.

NIS2-Regulierung

- 10 Essentielle + 6 Wichtige EU-Sektoren
- Cybersecurity bei Betreibern
- Nationale Governance, EU-Aufsicht
- In Kraft seit 01/23, nationale Umsetzung

DORA-Regulierung

- Reguliert primär Finanzunternehmen
- Reguliert auch kritische IKT-Dienstleister
- Nationale (Banken) und EU-Aufsicht (IKT)
- In Kraft seit 01/23, gilt ab 01/25 EU-weit

Nationale Umsetzung von NIS2 und DORA

bis 10/2024

ab 10/2024

Bundesamt für Sicherheit in der Informationstechnik

EU NIS2 → Umsetzung durch → NIS2UmsuCG

- Fokus: Cybersecurity und Informationstechnik
- Betroffen: KRITIS-Betreiber + besonders wichtige Einrichtungen + wichtige Einrichtungen
- Schutzobjekt: Große Teile der Wirtschaft
- Deutsche Aufsicht (BSI) + EU

seit 01/2023

ab 01/2025

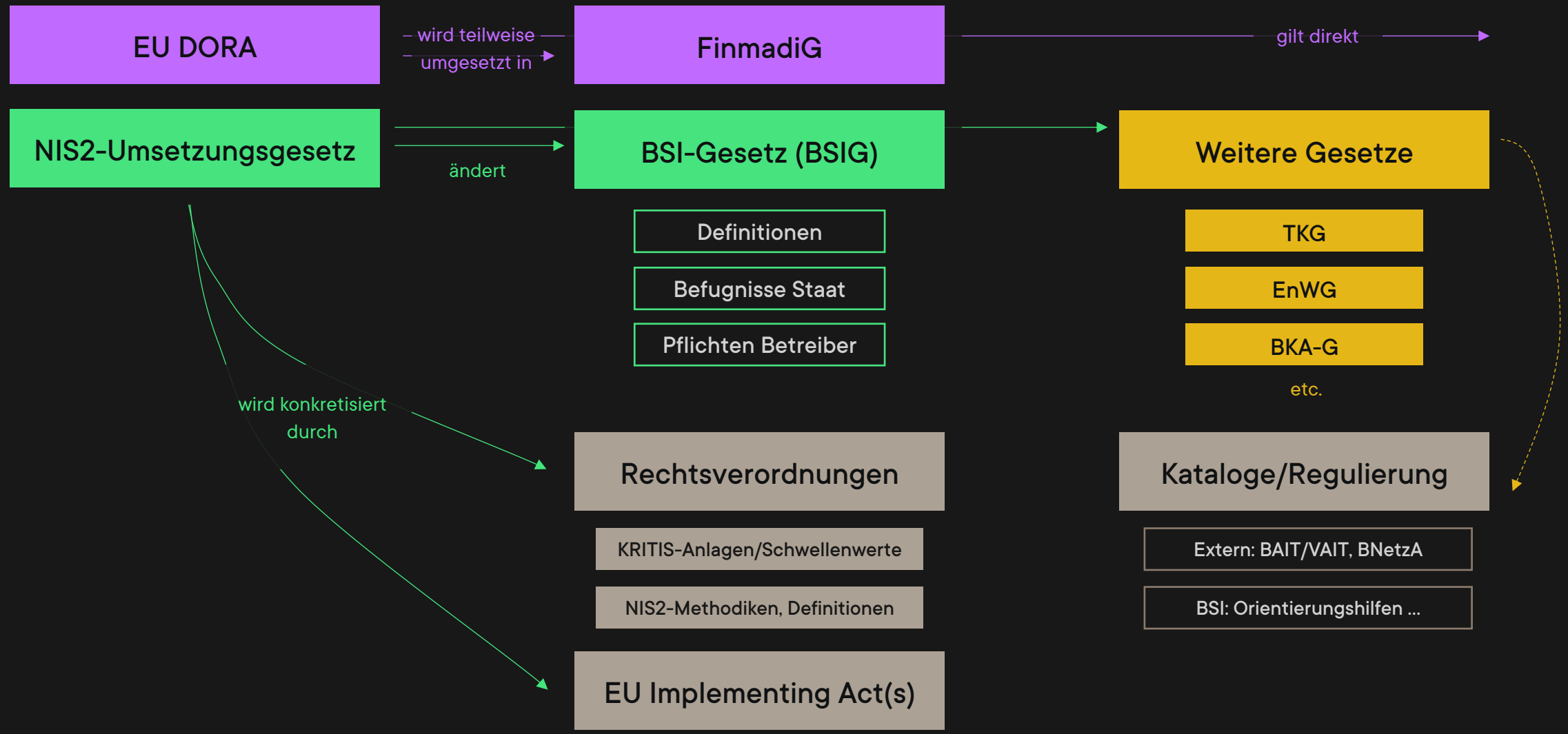
BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

EU DORA → Keine Umsetzung nötig* →

- Fokus: Cybersicherheit und digitale Resilienz
- Betroffen: Finanzunternehmen und kritische IKT-Dienstleister
- Schutzobjekt: EU Finanzmarkt
- Deutsche Aufsicht (BaFin), EU Aufsicht (ESA)

* Finanzmarktdigitalisierungsgesetz (FinmadiG)

Nationale Gesetze und Regulierung



Kritische Infrastrukturen in Deutschland

KRITIS
IT-SiG 1.0
IT-SiG 2.0

2014-23

NIS2

ab 2024

DORA

ab 2025

NEU

Wichtige Einrichtungen

NIS2-Pflichten (wichtig)

NEU

Besonders wichtige Einrichtungen

NIS2-Pflichten (besonders wichtig)

KRITIS-Betreiber nach IT-Sicherheitsgesetz 1.0/2.0, KritisV, Anlagen, Schwellenwerte

→

Betreiber kritischer Anlagen

NIS2-Pflichten (besonders wichtig)

KRITIS-Pflichten, §8a BSIG

NIS2-“KRITIS“-Pflichten + DachG

NEU

Finanzinstitute

DORA-Pflichten

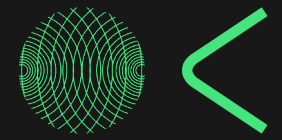
NEU

Kritische IKT-Dienstleister

DORA-Pflichten

2014-2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026

NIS2 Einrichtungen und Sektoren



Betreiber kritischer Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen	
2.000	6.250	21.600	
Betreiber (KRITIS)	Großunternehmen + Sonderfälle	Mittlere Unternehmen	Großunternehmen Mittlere Unternehmen

- Energie
- Transport und Verkehr
- Finanzunternehmen → In großen Teilen von NIS2 ausgenommen → EU DORA
- Gesundheit
- Wasser und Abwasser
- Digitale Infrastruktur → Teils auch als kritische IKT-DL
- Siedlungsabfallentsorgung
- Weltraum
- Ernährung
- Bundeseinrichtungen

- Post und Kurier
- Chemische Stoffe
- Verarbeitendes Gewerbe
- Forschung
- Anbieter Digitaler Dienste
- Siedlungsabfallentsorgung
- Ernährung

DORA Einrichtungen

In großen Teilen von NIS2 ausgenommen

NIS2

DORA

In DORA reguliert

In DORA wenn kritisch

Finanzunternehmen

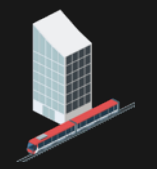
- Kredit- und Zahlungsinstitute
- Wertpapierfirmen
- Versicherungen, Rückversicherungen
- Handelsplätze
- Ratingagenturen
- Crowdfunding-Dienstleister
- ...

Digitale Infrastruktur

Digitale Dienste	Cloud Computing
Datendienste	Data Analytics
Hardware as a Service	Software
Technische Unterstützung	Data center services
Softwareaktualisierung	...
Firmwareaktualisierungen	...
DORA Art. 3 (21)	DORA Recital 63

Einrichtungen in DORA und NIS2

Unternehmen	Sektoren	Mitarbeiter	Umsatz	Bilanz
Besonders wichtige Einrichtungen	NIS2 Anlage 1	a) ≥ 250 b)	> 50 Mio. EUR und	> 43 Mio. EUR
Wichtige Einrichtungen	NIS2 Anlage 1 NIS2 Anlage 2	a) ≥ 50 b)	> 10 Mio. EUR und	> 10 Mio. EUR
Kritische Anlagen	KRITIS-Sektoren	Schwellenwerte werden pro Anlage definiert		
Finanzunternehmen	DORA	Festlegung nationaler Markteintritt und EU		
Kritische IKT-Dienstleister	DORA	Einstufung als kritisch durch EU-Behörden		



Einstufung als kritischer IKT-Drittdienstleister

- Erbringung von Dienstleistung mit hohen Risiken
- Einstufung als kritisch nach Bewertung durch ESA
- Überwachung durch EU-Behörde
- Einstufung anhand von Kriterien

Art. 31 (1) Nr. 8: Ausschlüsse: Gruppeninterne, Bank-zu-Bank, nur 1 EU MS

Systemische Auswirkungen

Können Betriebsstörung beim IKT-Dienstleister haben Auswirkungen auf Stabilität, Kontinuität oder Qualität der Finanzdienstleistung haben?

Systemischer Charakter

Sind der IKT-Dienstleister bzw. die auf ihn zurückgreifenden Finanzunternehmen systemrelevant?

Abhängigkeit von Dienstleistungen

Sind kritische oder wichtige Funktionen von dem selben IKT-Dienstleister abhängig?

Grad der Substituierbarkeit

Gibt es ein Mangel an alternativen IKT-Dienstleistern oder ist die Migration zu einem anderen Dienstleister schwierig?

Kritische Kriterien Art. 31

Pflichten und Cybersecurity

NIS2-Pflichten für Einrichtungen

Risikomanagement

Meldepflichten

Registrierung

Nachweise

Informationspflichten

Governance

KRITIS-Anforderungen

! Diverse Ausschlüsse und Sonderregeln vor allem für Risikomanagement (§§30-31) existieren. Teils durch BNetzA, teils durch EU-Vorgaben reguliert: Telekommunikation, Cloud/Online/Provider, Energieversorgung, nationale Sicherheit.

- besonders wichtig
- wichtig
- kritische Anlagen

DORA-Pflichten für Finanzinstitute

Risikomanagement

Schutz der IT

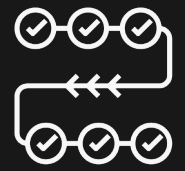
Detektion Reaktion

Resilienz

Stresstests

Drittparteien

Vorfallsmeldungen



Informationen

IKT-Dienstleister
- Verträge
- Einbezug

DORA-Pflichten für kritische IKT-Dienstleister

Risikomanagement

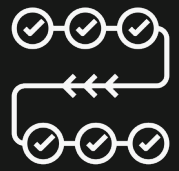
Detektion, Reaktion

Schutz der IT

Test und IKT-Audits

Physische Sicherheit

Governance



Interoperabilität

Standards

! Kritische IKT-Dienstleister können zusätzliche Pflichten über Verträge oder durch Einbezug in Resilienztests von Finanzunternehmen erhalten. Durch die Verpflichtung von Finanzunternehmen, Dienstleister zu steuern und Risiken von Drittparteien zu managen entstehen auch Auswirkungen auf nicht kritische IKT-Dienstleister.

Mapping DORA auf ISO 27001 und NIS2

Eindeutige IDs

Referenz auf Artikel

ID	DORA	Anforderung	NIS2	C5:2020	ISO 27001
D.5.1	Art. 5 (1)	Governance- und Kontrollrahmen	*oberhalb ISMS und IT-RM*		
D.5.2	Art. 5 (2)	Verantwortung der Geschäftsleitung	38.1	BCM-01	5.1 A.5.31
D.5.3	Art. 5 (3)	Funktion zur Überwachung von Vereinbarungen mit IKT-Drittdienstleistern	-	SSO-01	A.5.2 A.5.19
D.5.4	Art. 5 (4)	Kenntnisse und Fähigkeiten der Geschäftsleitung	38.3	HR-03	7.2 7.3 A.5.2 A.5.4 A.5.31 A.6.3
D.6.1	Art. 6 (1) Art. 6 (2) Art. 6 (3)	IKT-Risikomanagementrahmen, Geltungsbereich, geeignete Strategien, Policies und Verfahren	30.1.1 30.2.1a 30.2.1b	OIS-01 OIS-02 OIS-03 OIS-06 OIS-07	4.1-10.2 A.5.1 A.5.2 A.5.4
D.6.4	Art. 6 (4)	Unabhängige Kontrollfunktion	-	OIS-04	A.5.2 A.5.3

Zuordnung NIS2
Anforderungen aus BSI Konkretisierung Maßnahmen

Zuordnung ISO 27001
Management und Kontrollen aus ISO/IEC 27001:2024

Zuordnung C5:2020
Informationssicherheit im Cloudcomputing (BSI)

https://www.openkritis.de/massnahmen/dora-nis2-kritis-mapping.html

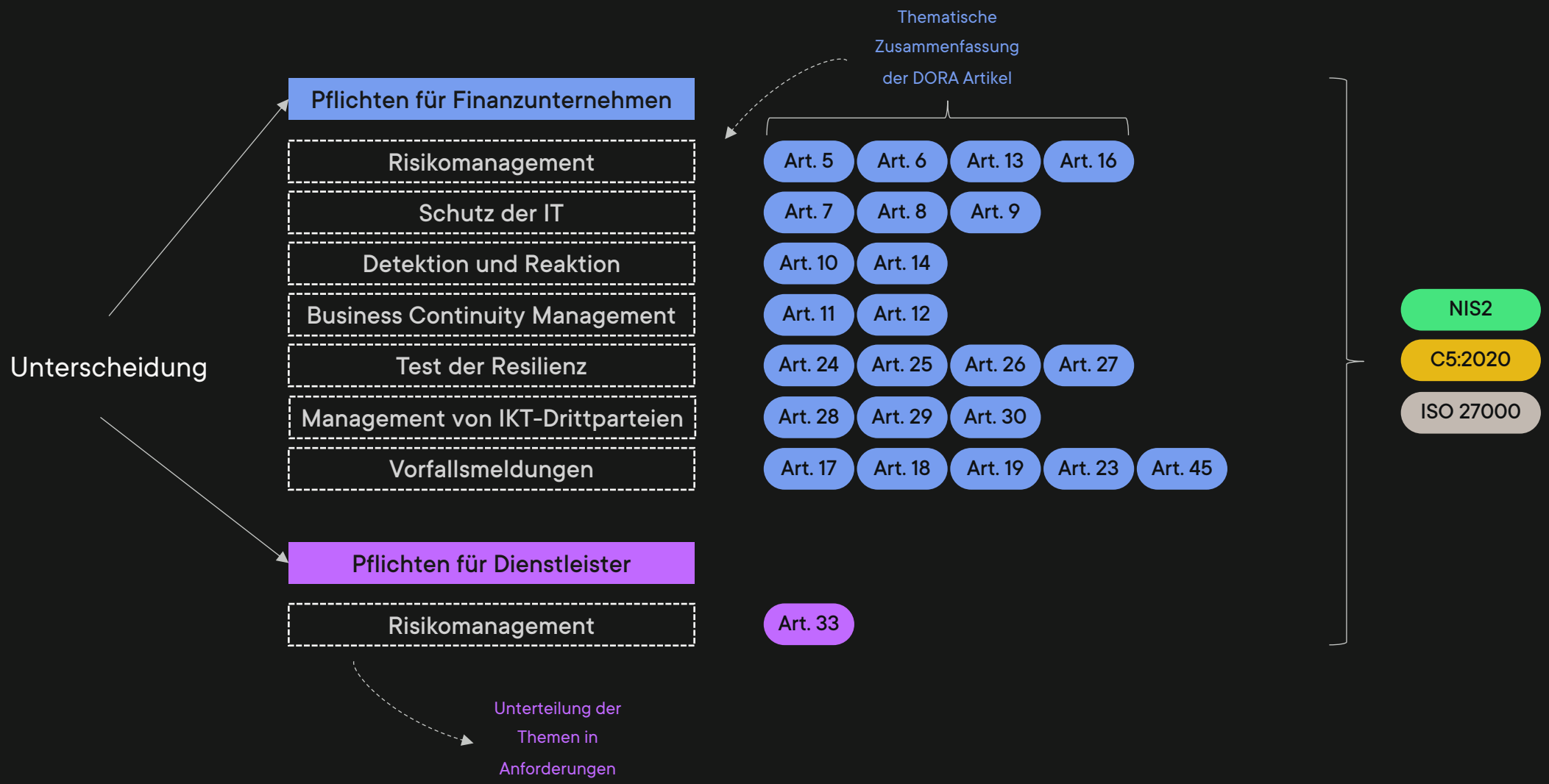
Mapping DORA auf ISO 27001 und NIS2

Methodik

- Aufschlüsselung der DORA-Absätze und Nummern in einzelne Anforderungen
- Thematische Zusammenfassung der Inhaltlichen Anforderungen
- Mapping zu Vorgaben aus dem NIS2UmsuCG, ISO/IEC 27001:2022 und BSI C5:2020
- Pflichten für Finanzunternehmen und Pflichten für Dienstleister

ID	DORA	Anforderung	NIS2	C5:2020	ISO 27001
D.11.1	Art. 11 (1) Art. 11 (2) Art. 11 (4) Art. 11 (8)	Business Continuity Management	30.2.3a 30.2.3d	BCM-01 BCM-03	A.5.29 A.5.30 A.5.31 A.8.14
D.11.3	Art. 11 (3) Art. 11 (8)	IKT-Reaktions- und Wiederherstellungspläne	30.2.3c	BCM-03	A.5.29 A.5.30
D.11.5	Art. 11 (5)	Business Impact Analyse (BIA)	-	BCM-02	-
D.11.6	Art. 11 (6)	Regelmäßige Business Continuity Tests	-	BCM-04	A.5.30
D.11.7	Art. 11 (7)	Krisenmanagementfunktion	-	-	-
D.11.9	Art. 11 (9)	Jährliche Kosten- und Verlustmeldung durch IKT-bezogene Vorfälle	-	-	-
D.12.1	Art. 12 (1) Art. 12 (2) Art. 12 (3) Art. 12 (6) Art. 12 (7)	Backup und Wiedergewinnung/Wiederherstellung	30.2.3b	OPS-06 OPS-07 OPS-08 OPS-09	A.8.13
D.12.2	Art. 12 (4) Art. 12 (5)	Logische und physische Redundanzen	-	PS-02 PS-06	A.8.14

Mapping DORA auf ISO 27001 und NIS2



Mapping DORA auf ISO 27001 und NIS2

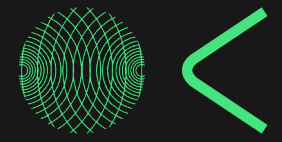
Abdeckung von DORA durch ISO/NIS2

ISO 27001 vorhanden	Schutz der IT, Detektion & Reaktion, Entwicklung, Personal, Dienstleister, Schulungen, Incident Mgmt, Verbesserung
Teilweise	Governance, Notfallkommunikation, BCM, Risikomanagement
Fast nicht/unklar	Übergreifende Governance/RM, Krisen-management, Digitale operationale Resilienz, Stresstest, TLPT, Meldewesen
Kritische IKT-Dienstleister	Große Teile in ISO 27001 vorhanden, Lücken bei physischer Sicherheit, Übertragbarkeit und Interoperabilität

Mit bestehendem ISO/NIS2-ISMS: was nun?

- Ausrichtung an ISO 27001 für DORA hilfreich – viele Anforderungen sollten bereits erfüllt sein
- Einzelne Themen erfordern eine detailliertere Analyse der bestehenden Umsetzung
- DORA fordert eine Governance oberhalb des ISMS und ein weitreichenderes und umfangreicheres Risikomanagement
- Für kritische IKT-Dienstleister ist die Situation ähnlich, aber auch hier gibt es Lücken und Anforderungen, die über ISO und NIS2 hinausgehen

Mapping für IKT-Dienstleister auf ISO 27001



DORA Art. 33 → ISO 27001

Risikomanagement	Detektion, Reaktion, Vorfallsmeldung	Schutz der IT	Test und IKT-Audits
6.1, 8.2, 8.3, A.5.29, A.5.30, A.5.31, A.8.14	A.5.24, A.5.25, A.5.26, A.5.28, A.6.8, A.8.15, A.8.16	viele	9.2, A.5.35, A.5.36, A.8.29, A.8.31, A.8.33, A.8.34

Physische Sicherheit	Governance	Übertragbarkeit und Interoperabilität	Einschlägige Standards
A.7.*	5, A.5.2, A.5.4	A.5.23	

DORA-Pflichten per Vertrag

Finanzunternehmen
in DORA

Verträge

alle Verträge

bei kritischen Funktionen

- Beschreibung der Dienstleistung
- Standortinformationen
- Datenschutzbestimmungen
- Zugang zu Daten bei Exit
- Unterstützung bei IKT-Vorfällen
- Zusammenarbeit mit Behörden
- Teilnahme an Resilienzschulungen

DORA Mindestinhalte für Verträge zwischen Finanzunternehmen und IKT-Drittdienstleistern

- Leistungsziele
- Berichtspflichten
- Notfallpläne
- Beteiligung an TLPT
- Recht auf Überwachung
- Ausstiegsstrategien

Zusätzliche Inhalte wenn kritische oder wichtige Funktionen unterstützt werden

DORA-Pflichten per Erwartungen

Finanzunternehmen
in DORA

Erwartungen

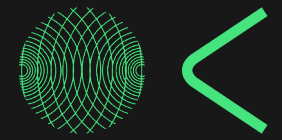
IKT-Dienstleister

Mitarbeit/Beteiligung

- Meldepflichten
- Tests
- Auditrechte
- Nachweise
- Sichere IT
- Standards

Erwartungen häufig in bestehenden Verträgen und SLAs

Aufsichtsbefugnisse Lead Overseer



Befugnisse gegenüber kritischen IKT-Dienstleistern

Powers Lead Overseer
Art 35

- Request informations
- Recommendations ICT
- Recommendations Security
- Recommendations Terms
- Coordinate etc.
- Good faith
- Penalty payments

Informations
Art 36

- All information necessary
- Formal requests
- Providers shall supply

Investigations
Art 38

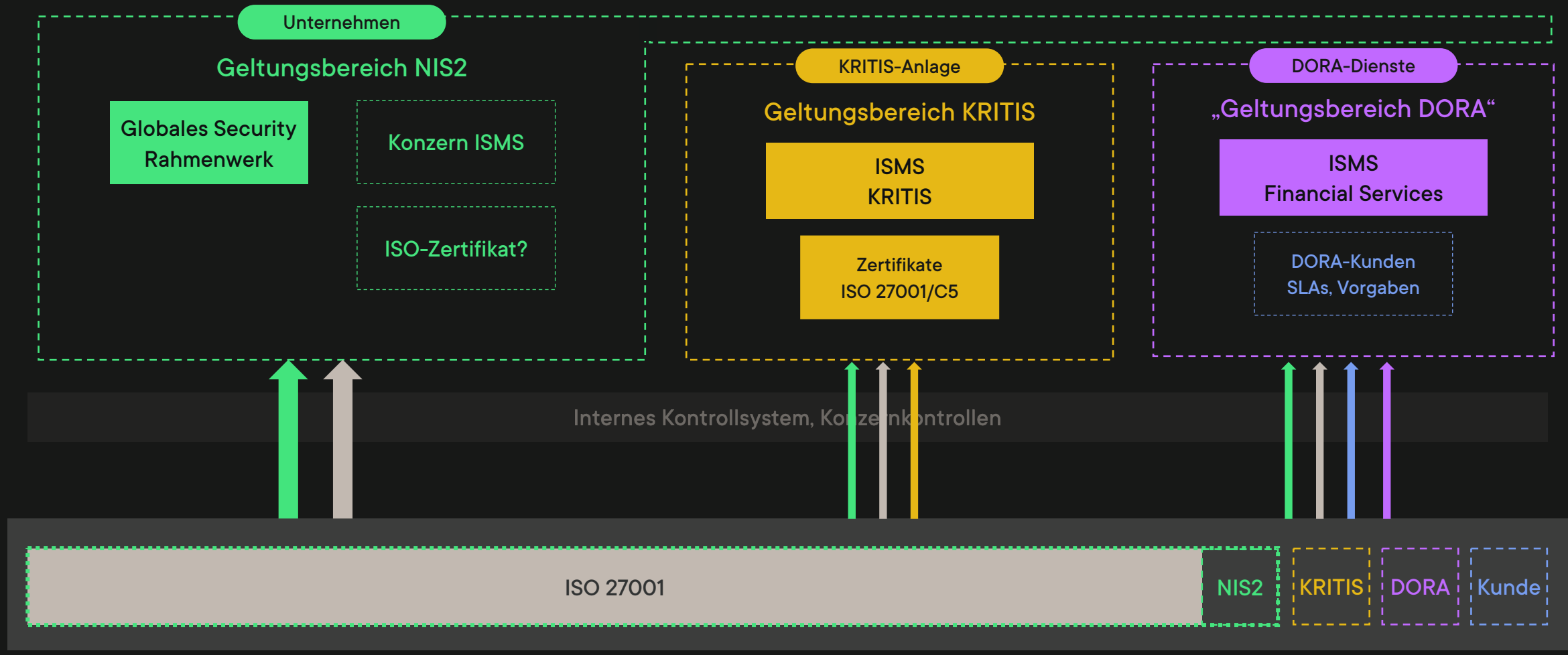
- Joint Examination Team
- Examine records, data
- Take copies, extract data
- Summon representatives
- Interview any person
- Telephone and data traffic
- Providers to submit

Inspections
Art 39

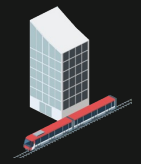
- Joint Examination Team
- Onsite inspections
- Seal premises or records
- Cover full range ICT
- „Reasonable notice“
- Providers to submit
- Inform of consequences

Scoping

Mapping auf ISMS-Scopes



NIS2 und DORA-Dienstleistungen



Registrierung

Meldung von Sicherheitsvorfällen

Einstufung als kritisch & Überwachung

IT-Provider

Governance | Leitung | Entwicklung

Dienstleistung (NIS2) | Dienstleistung (non-NIS2) | Dienstleistung (NIS2 und DORA)

Produkte | Produkte | Produkte

Prozesse | Prozesse | Prozesse | Prozesse

Anlagen | IT | Anlagen | IT | Anlagen | IT | OT

Colocation | Hyperscaler | Rechenzentren

Externe | Personal | Wartung | Betriebsmittel

NIS2-Einrichtung

Risiko-Management NIS2
+ Security Maßnahmen
+ Pflichten (Registrierung, Meldungen)

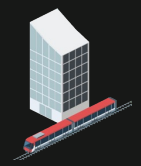
Einrichtung aber non-NIS2 Service

Wahrscheinlich auch NIS2-Scope

DORA IKT-Dienstleister (kritisch)

DORA-Pflichten Art. 33 (IKT)
+ Stresstests, Pentests
+ Vertragliche Pflichten durch Finanz

NIS2 und DORA als nicht-kritischer DL



Kunden

Kunden

Finanzkunden

Übertragung von DORA-Pflichten über Verträge

Provider

Governance

Leitung

Entwicklung

Dienstleistung (NIS2)

Dienstleistung (non-NIS2)

Dienstleistung (NIS2)

Produkte

Produkte

Produkte

Prozesse

Prozesse

Prozesse

Prozesse

Anlagen

IT

Anlagen

IT

Anlagen

IT

OT

Colocation

Hyperscaler

Rechenzentren

Externe

Personal

Wartung

Betriebsmittel

NIS2-Einrichtung

Risiko-Management NIS2
+ Security Maßnahmen
+ Pflichten (Registrierung, Meldungen)

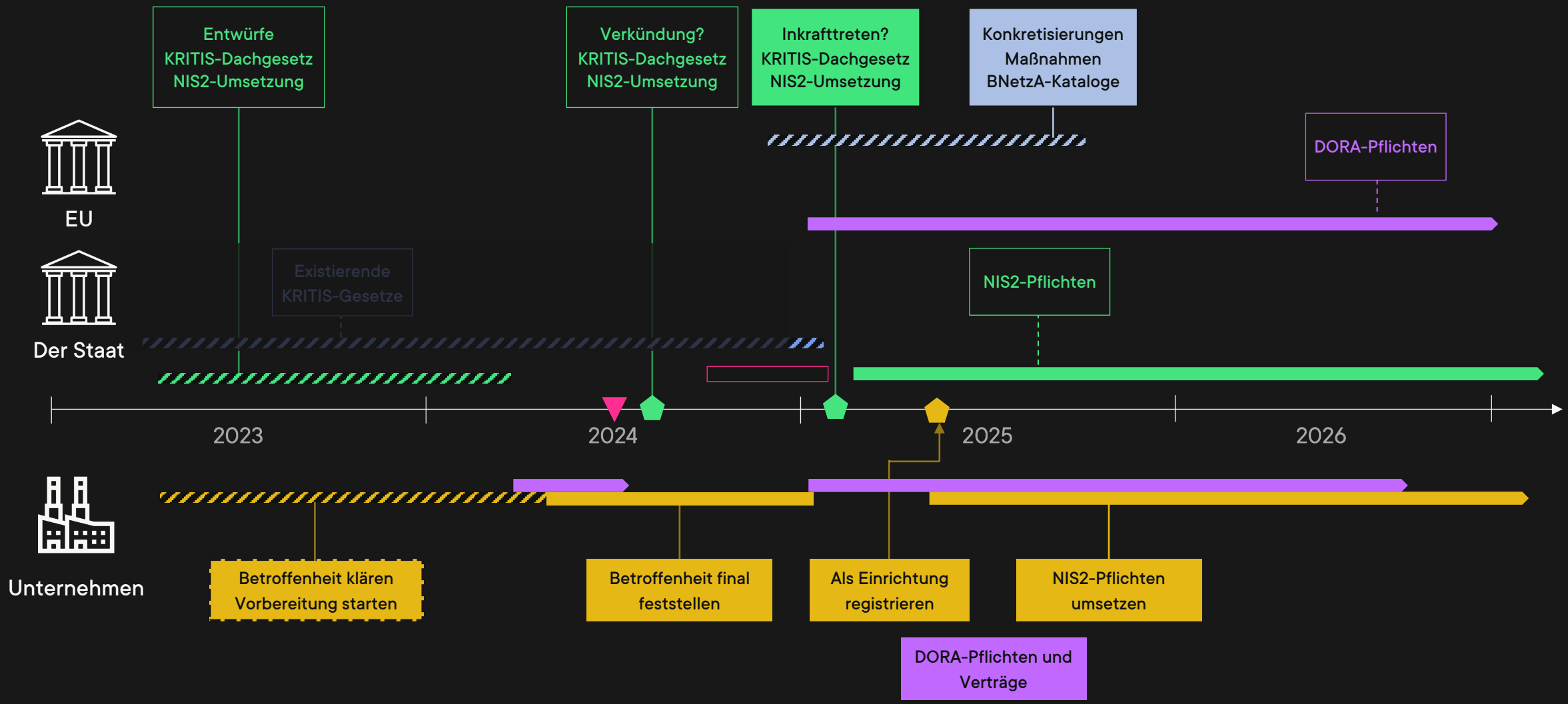
Einrichtung aber non-NIS2 Service

Wahrscheinlich auch NIS2-Scope

nicht-kritischer IKT-Dienstlester

Verträge mit DORA-Pflichten
+ Stresstests, Pentests

NIS2 und DORA ab 2024/25



Split Personalities – DORA und NIS2

IT-Provider

Verwaltung IT Cloud Produkte

Unternehmensgröße in einem der NIS2-Sektoren im NIS2-Umsetzungsgesetz, z.B. Sektor IT im Cloud Service mit >50 MA

NIS2

- ISMS im Unternehmen aufbauen
- Vorbereitung auf Krisen, Ausfälle
- §30 NIS2-Maßnahmen + EU Act
- Meldepflichten BSI
- Dokumentationspflicht

Personal
Beratung/RA
Verträge
!

Cloud-Services für Finanzkunden, Einstufung durch die ESA als kritisch wahrscheinlich (usw.)

DORA

- ISMS und RM für DORA-Services
- Krisen, Ausfälle, Tests
- DORA IKT-Maßnahmen
- Meldepflichten ESA
- Aufsicht, Tests, Verträge, SLAs

Nichts zu Kritischen Infrastrukturen verpassen:

OpenKRITIS.de

DORA auf OpenKRITIS: EU DORA

DORA und NIS2-Mapping auf OpenKRITIS: DORA Security Mapping

NIS2 Implementing Act Mapping auf OpenKRITIS: NIS2 IT Implementing Act

NIS2-Umsetzung auf OpenKRITIS: NIS2 in Deutschland

Kontakt: info@openkritis.de und OpenKRITIS auf LinkedIn

NIS 2 und DORA

OpenKRITIS

Das freie Informationsportal für Kritische Infrastrukturen.

EU NIS2 und DORA
Stand: 2. Juli 2024
Version: 1.0

Impressum

Insignals GmbH
Paul Weissmann
Rheinwerkallee 6
53227 Bonn

https://www.openkritis.de · ISSN 2748-565X

info@openkritis.de · +49 176 58952135