

DORA und NIS2 für Provider

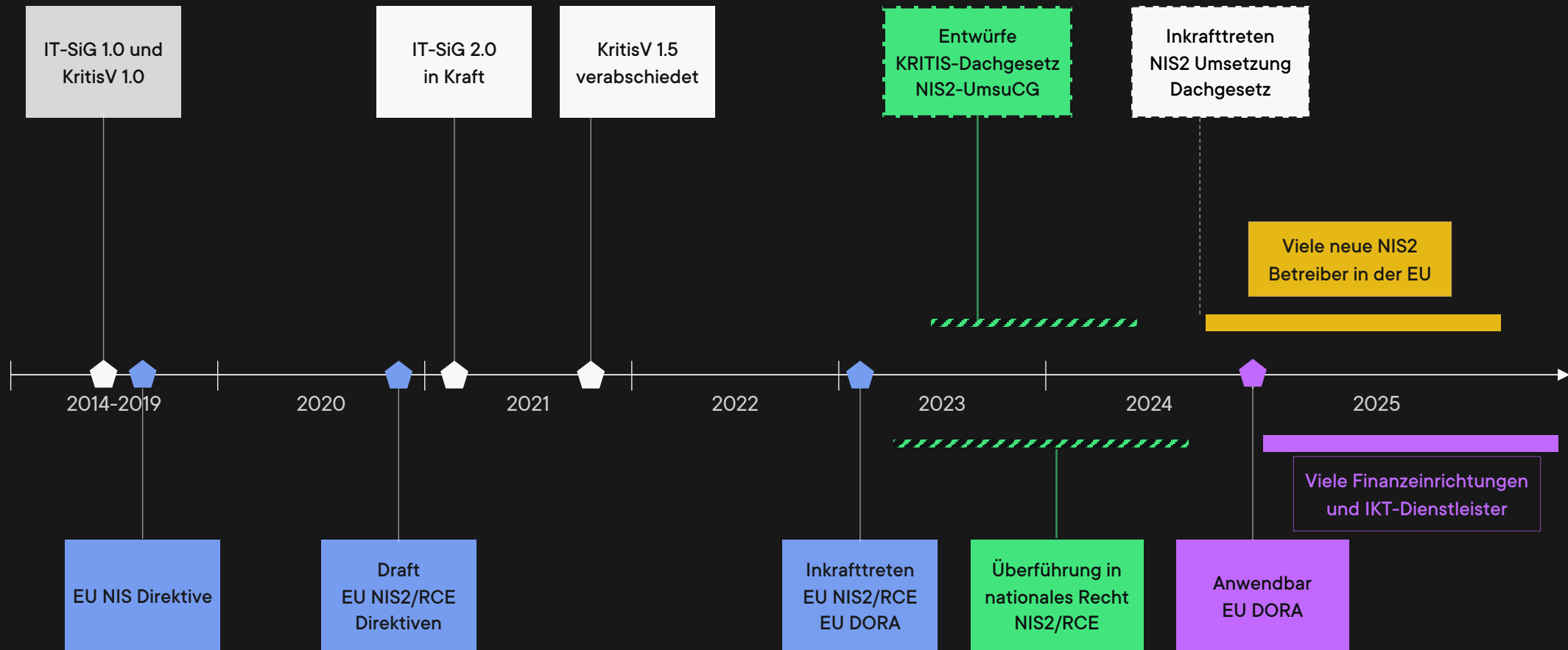
Was kommt auf IT-Dienstleister zu? (viel)

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



EU NIS2

Umsetzung
durch

ab 10/2024



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



EU DORA

Keine
Umsetzung
nötig*

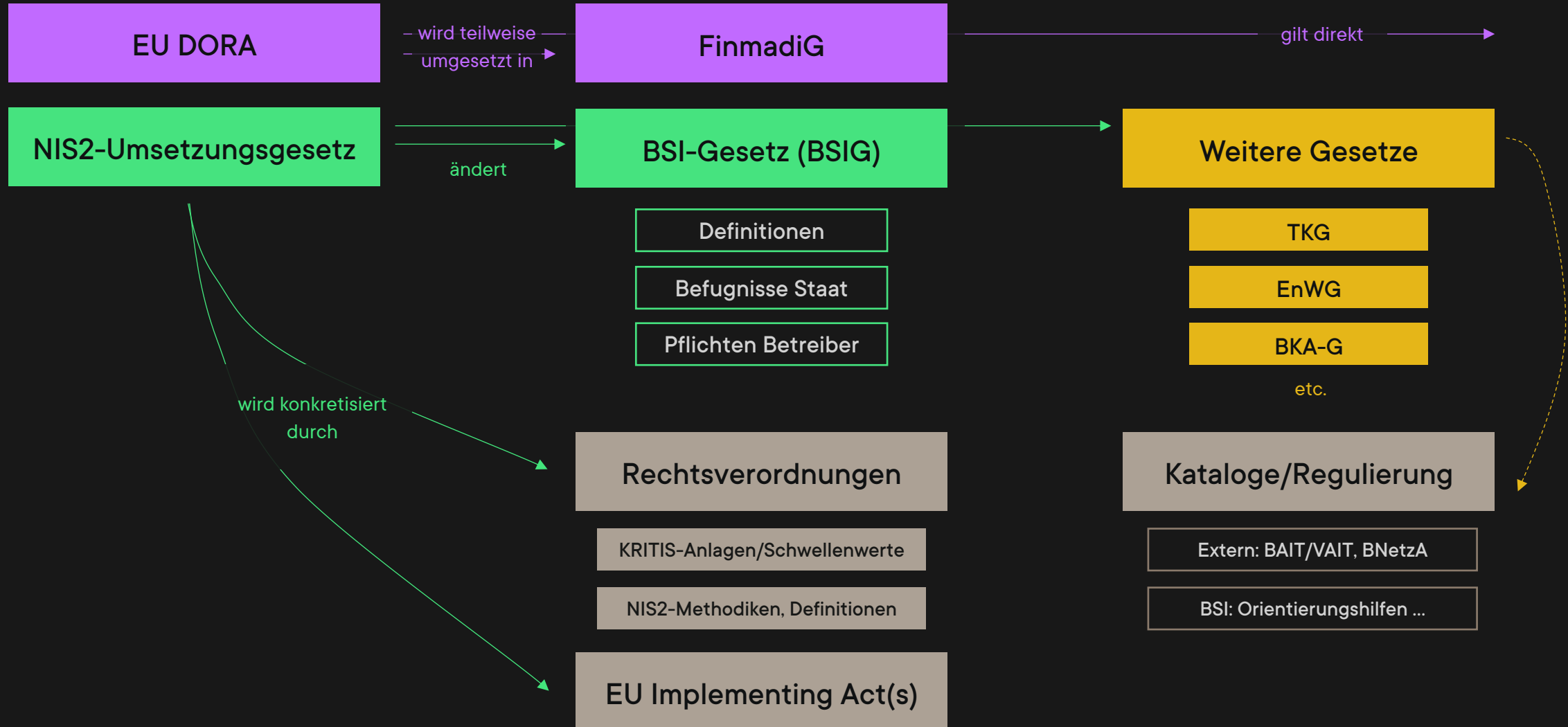
ab 01/2025



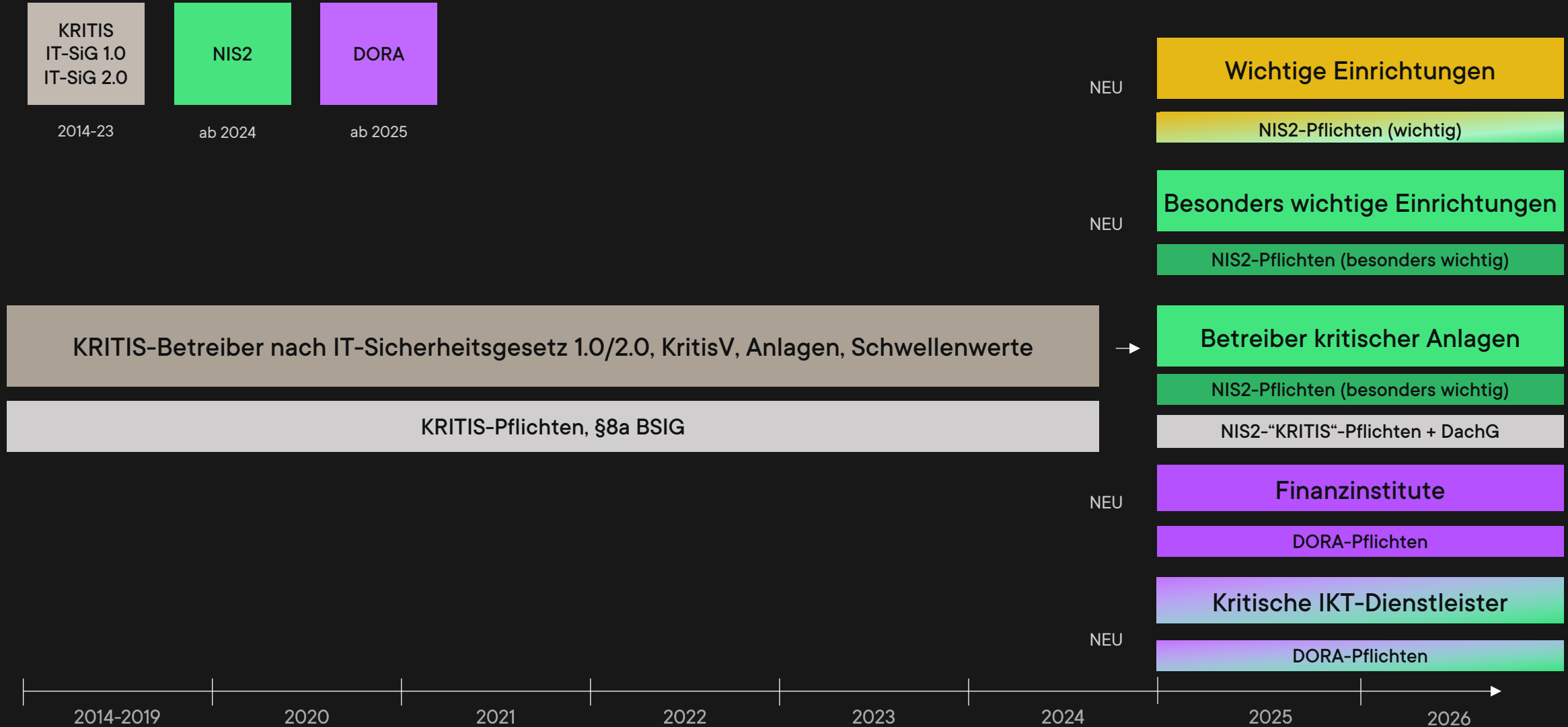
- Fokus: Cybersicherheit und digitale Resilienz
- Betroffen: Finanzunternehmen und kritische IKT-Dienstleister
- Schutzobjekt: EU Finanzmarkt
- Deutsche Aufsicht (BaFin), EU Aufsicht (ESA)

* Finanzmarktdigitalisierungsgesetz (FinmadiG)

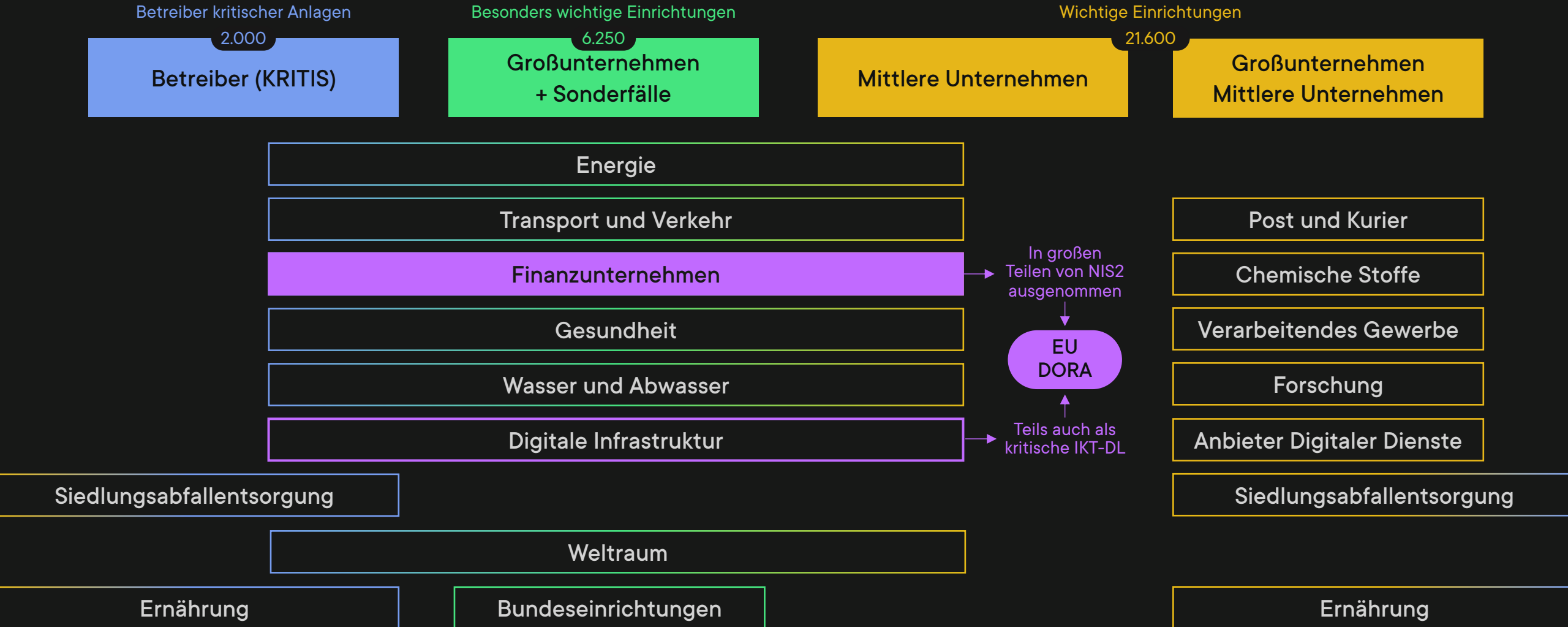
Nationale Gesetze und Regulierung



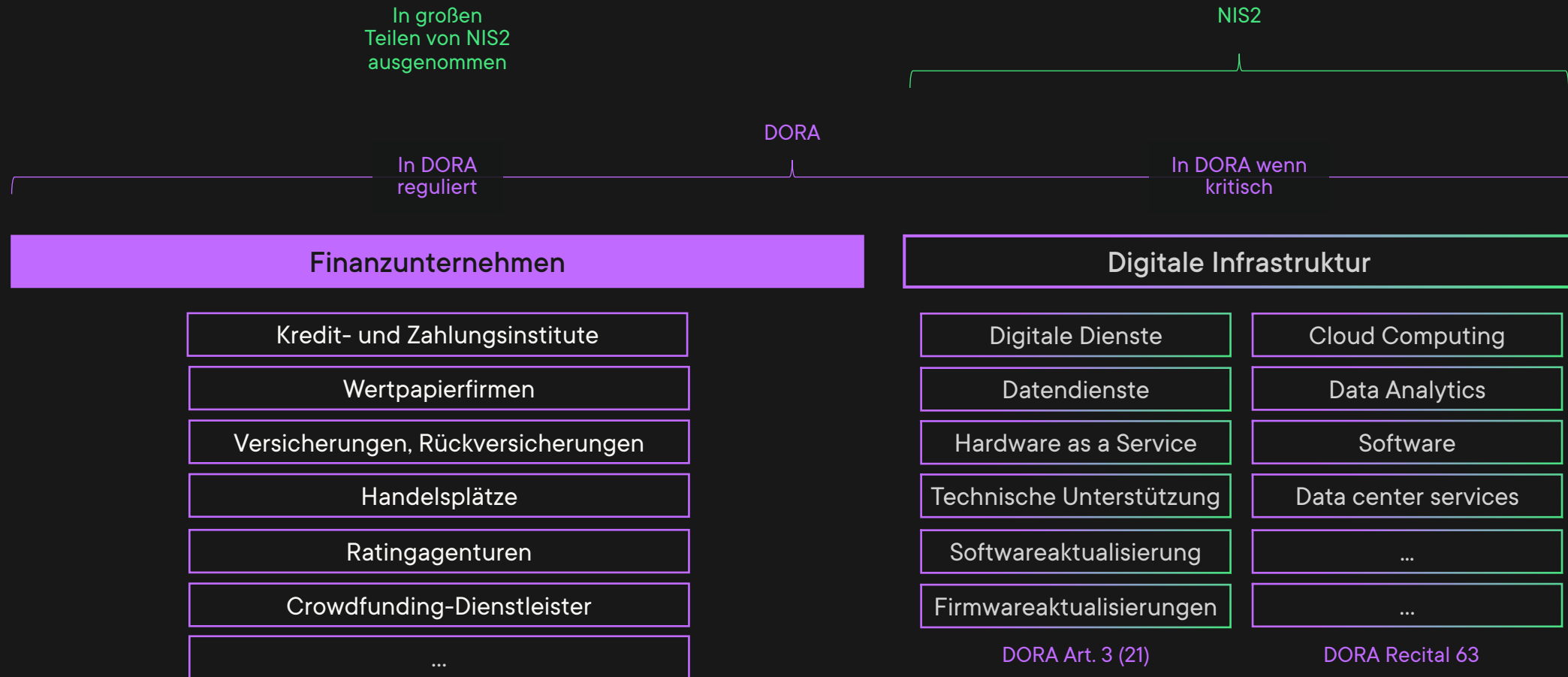
Kritische Infrastrukturen in Deutschland



NIS2 Einrichtungen und Sektoren



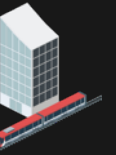
DORA Einrichtungen



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	Systemischer Charakter
Können Betriebsstörung beim IKT-Dienstleister haben Auswirkungen auf Stabilität, Kontinuität oder Qualität der Finanzdienstleistung haben?	Sind der IKT-Dienstleister bzw. die auf ihn zurückgreifenden Finanzunternehmen systemrelevant?
Abhängigkeit von Dienstleistungen	Grad der Substituierbarkeit
Sind kritische oder wichtige Funktionen von dem selben IKT-Dienstleister abhängig?	Gibt es ein Mangel an alternativen IKT-Dienstleistern oder ist die Migration zu einem anderen Dienstleister schwierig?
Kritische Kriterien Art. 31	



Pflichten und Cybersecurity

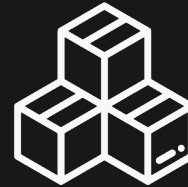
NIS2-Pflichten für Einrichtungen



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



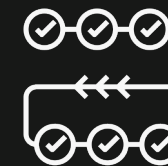
Stresstests



Drittparteien



Vorfallsmeldungen



Informationen

IKT-Dienstleister

 Verträge

 Einbezug

DORA-Pflichten für kritische IKT-Dienstleister



Risikomanagement



Detektion, Reaktion



Schutz der IT



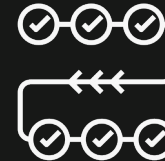
Test und IKT-Audits



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	<i>oberhalb ISMS und IT-RM</i>		
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

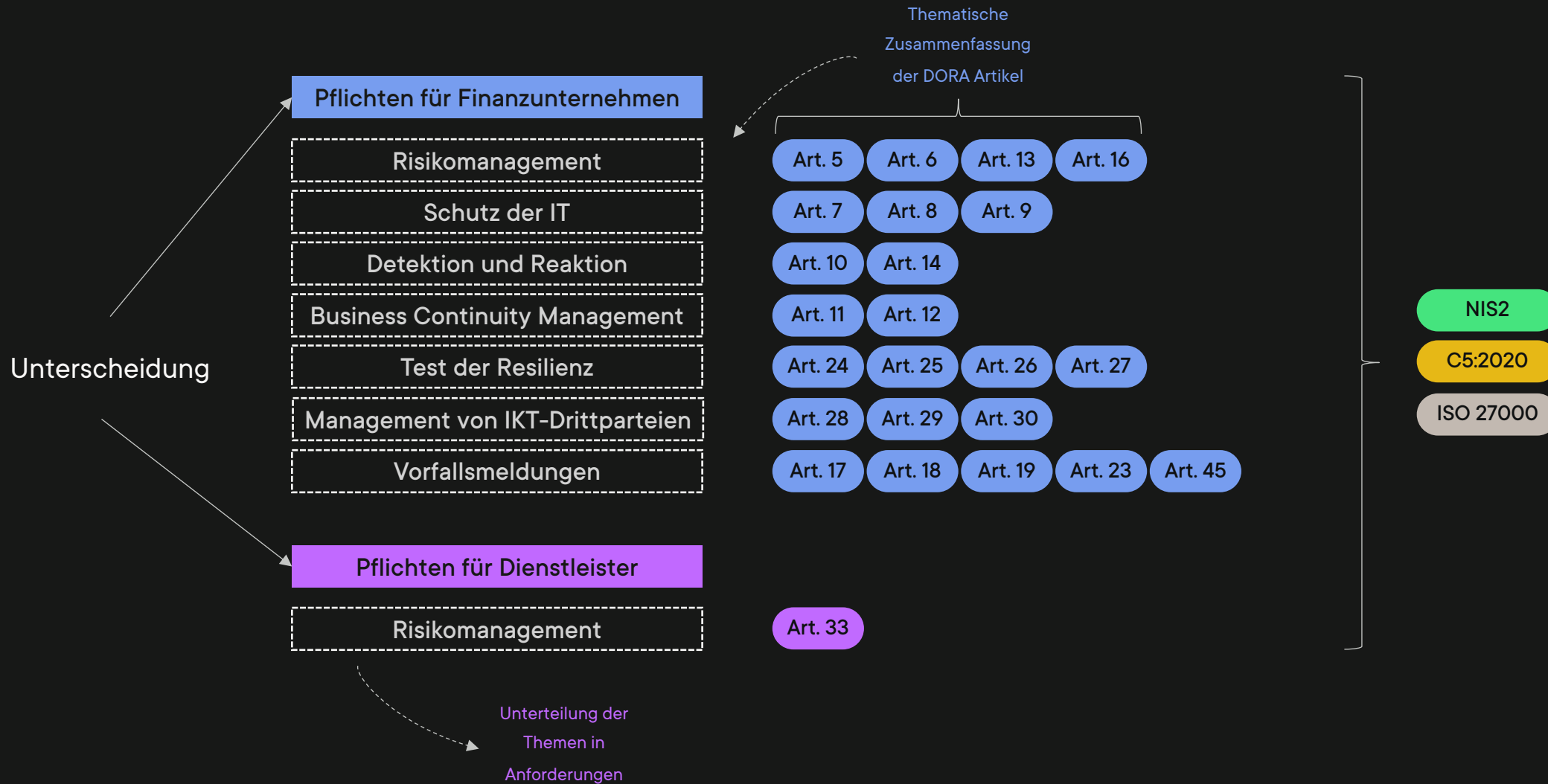


Methodik

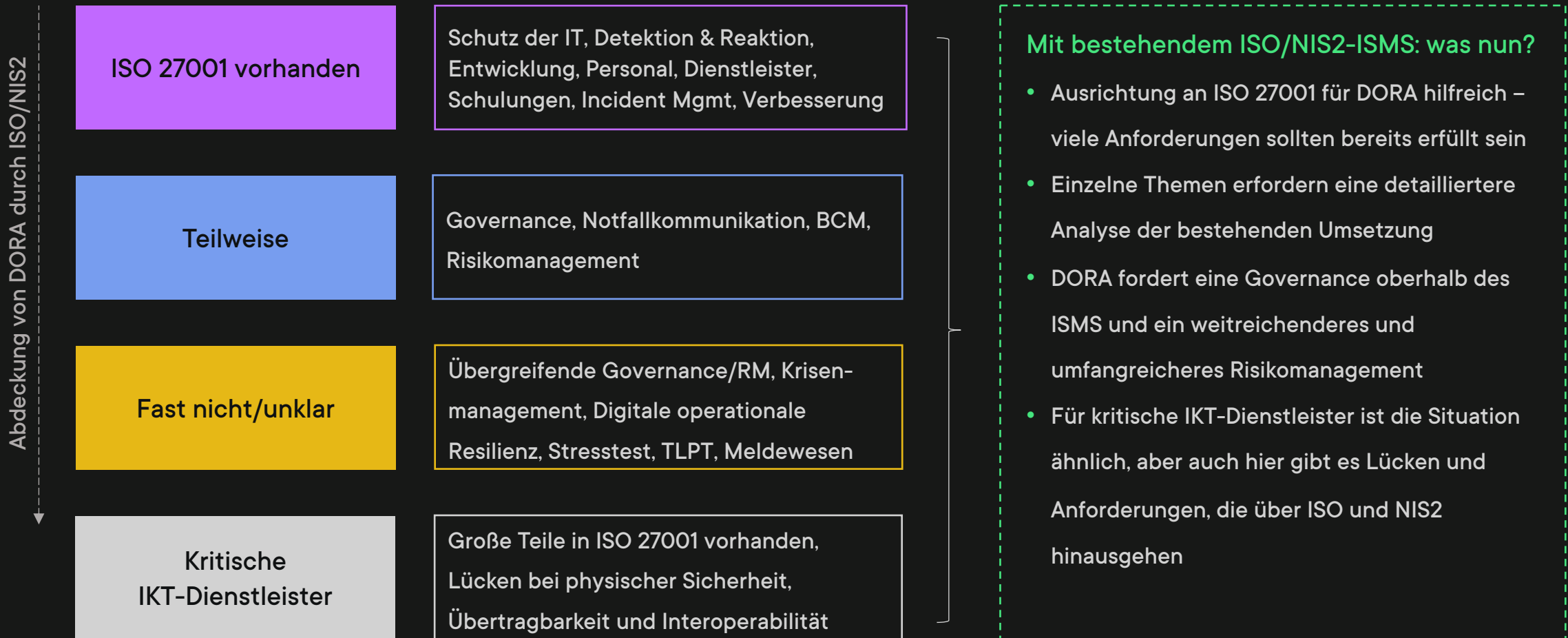
- Aufschlüsselung der DORA-Absätze und Nummern in einzelne Anforderungen
- Thematische Zusammenfassung der Inhaltlichen Anforderungen
- Mapping zu Vorgaben aus dem NIS2UmsuCG, ISO/IEC 27001:2022 und BSI C5:2020
- Pflichten für Finanzunternehmen und Pflichten für Dienstleister

ID	DORA	Anforderung	NIS2	C5:2020	ISO 27001
D.11.1	Art. 11 (1)	Business Continuity Management	30.2.3a	BCM-01	A.5.29
	Art. 11 (2)		30.2.3d	BCM-03	A.5.30
	Art. 11 (4)				A.5.31
	Art. 11 (8)				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)	Backup und Wiedergewinnung/Wiederherstellung	30.2.3b	OPS-06	A.8.13
	Art. 12 (2)			OPS-07	
	Art. 12 (3)			OPS-08	
	Art. 12 (6)			OPS-09	
	Art. 12 (7)				
D.12.2	Art. 12 (4)	Logische und physische Redundanzen	-	PS-02	A.8.14
	Art. 12 (5)			PS-06	

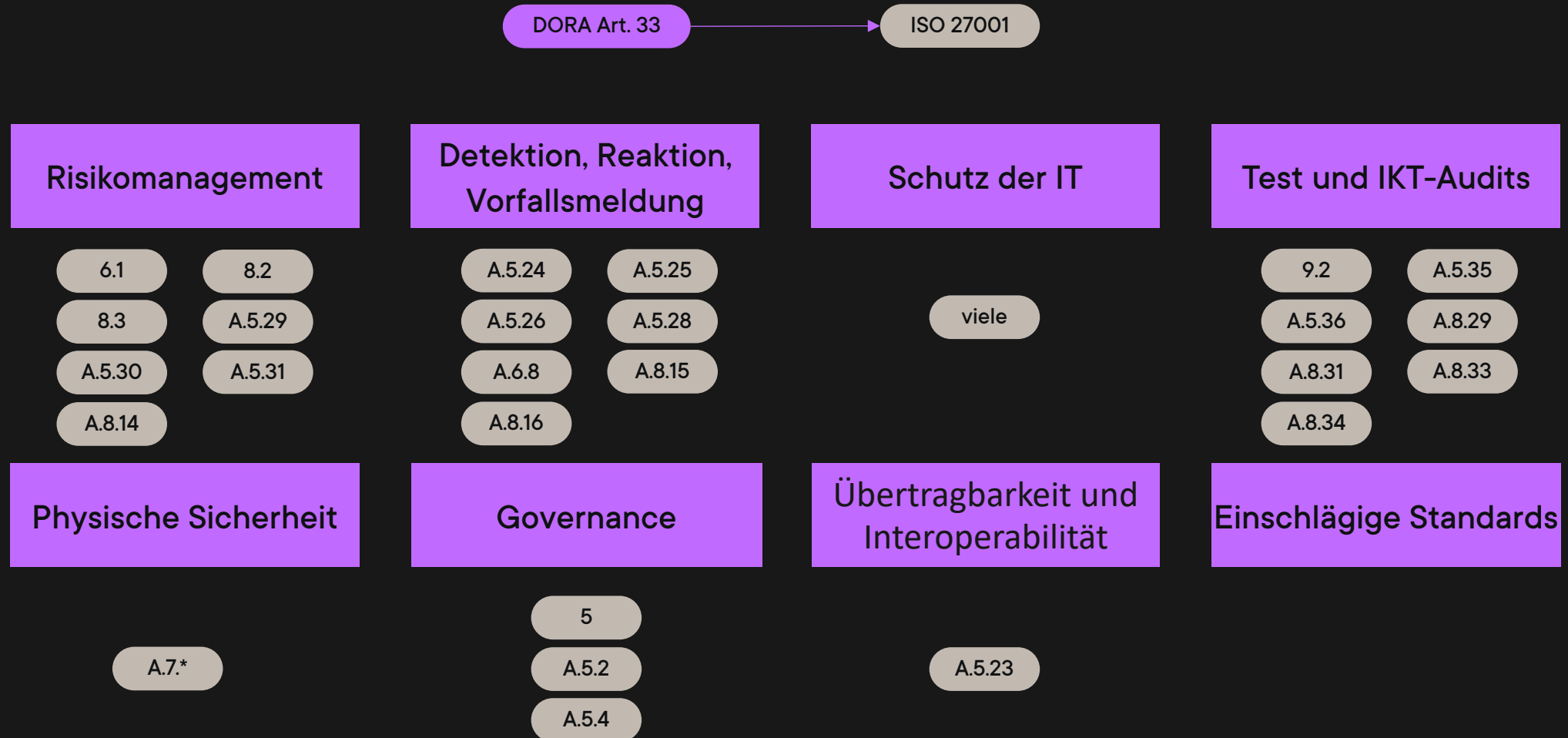
Mapping DORA auf ISO 27001 und NIS2



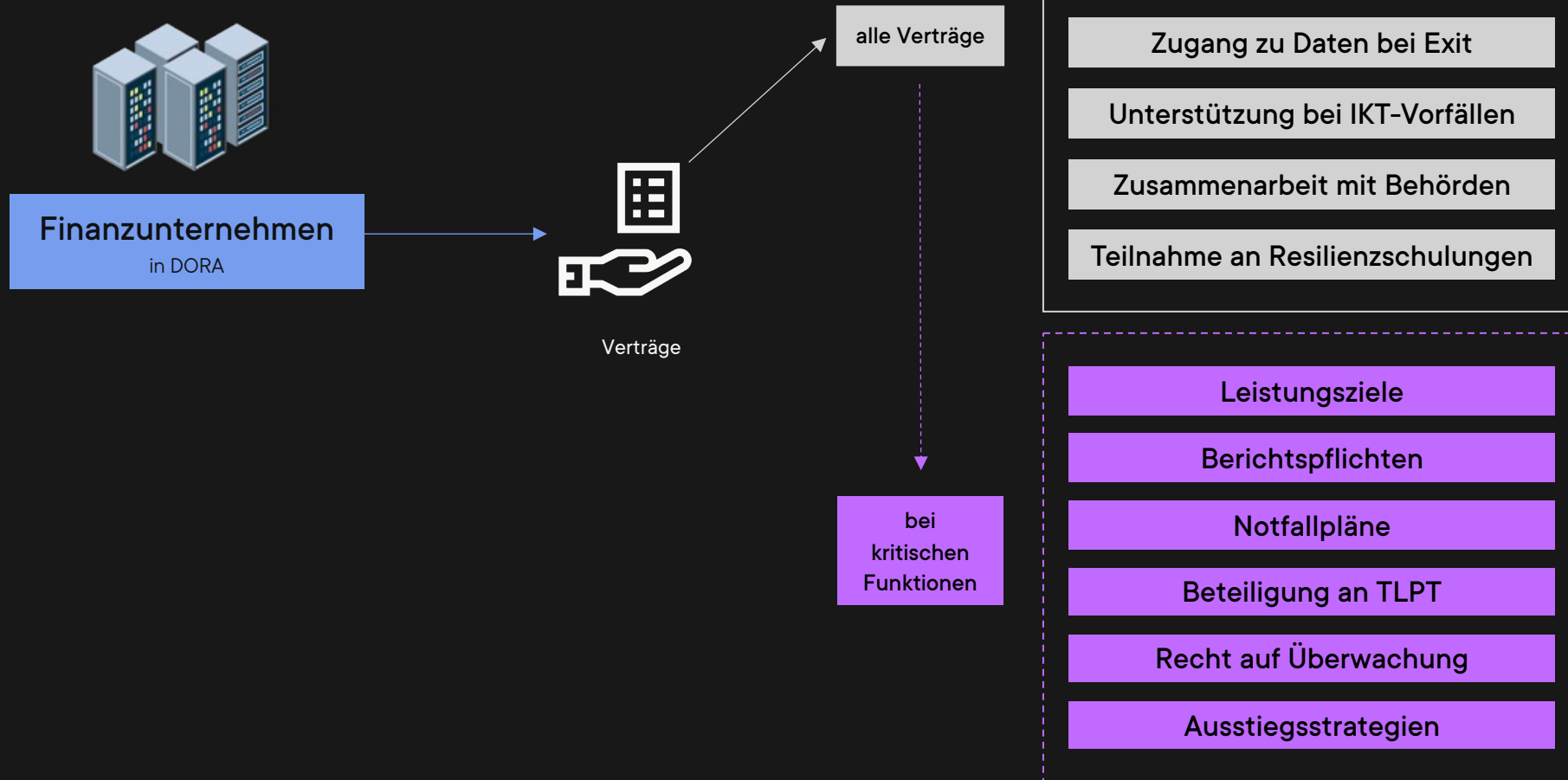
Mapping DORA auf ISO 27001 und NIS2



Mapping für IKT-Dienstleister auf ISO 27001



DORA-Pflichten per Vertrag



DORA Mindestinhalte für
Verträge zwischen
Finanzunternehmen und
IKT-Drittdienstleistern

Zusätzliche Inhalte
wenn kritische oder
wichtige Funktionen
unterstützt werden

DORA-Pflichten per Erwartungen



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“

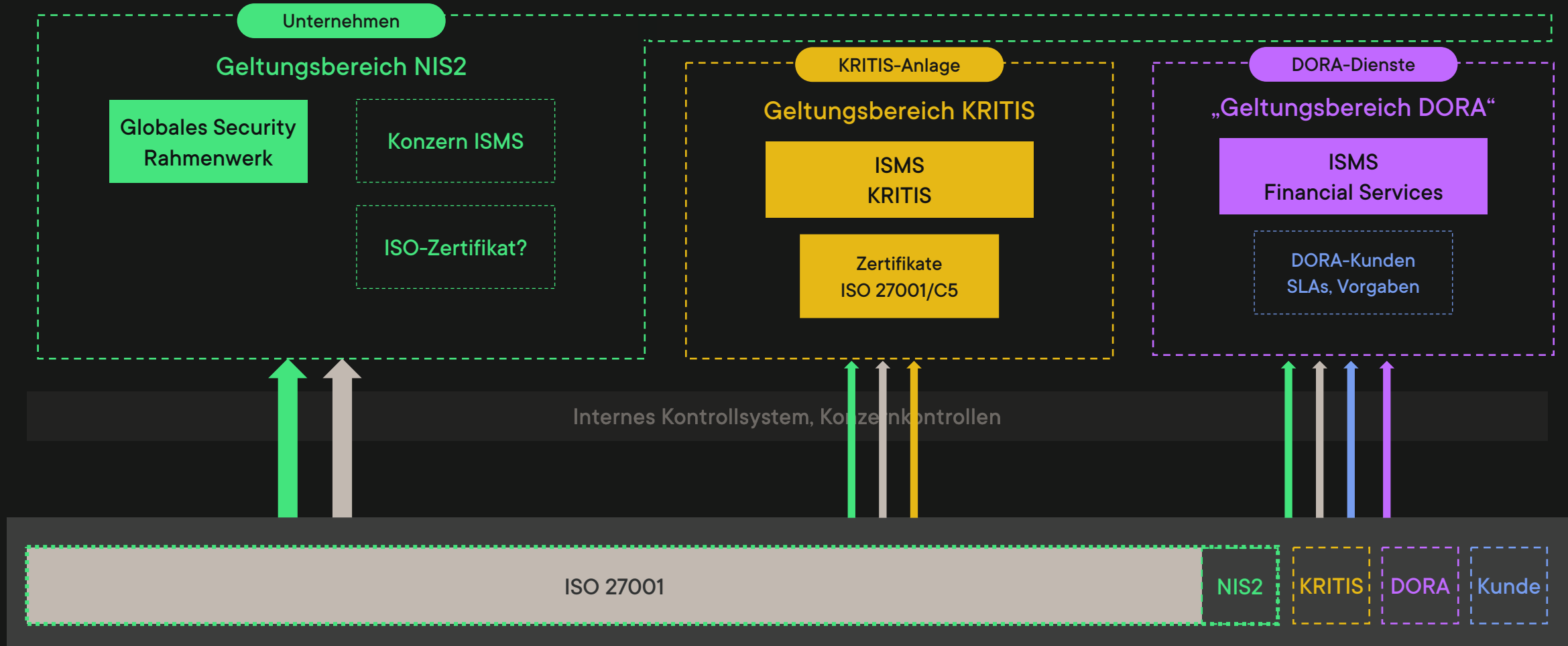
Providers to submit

Inform of consequences

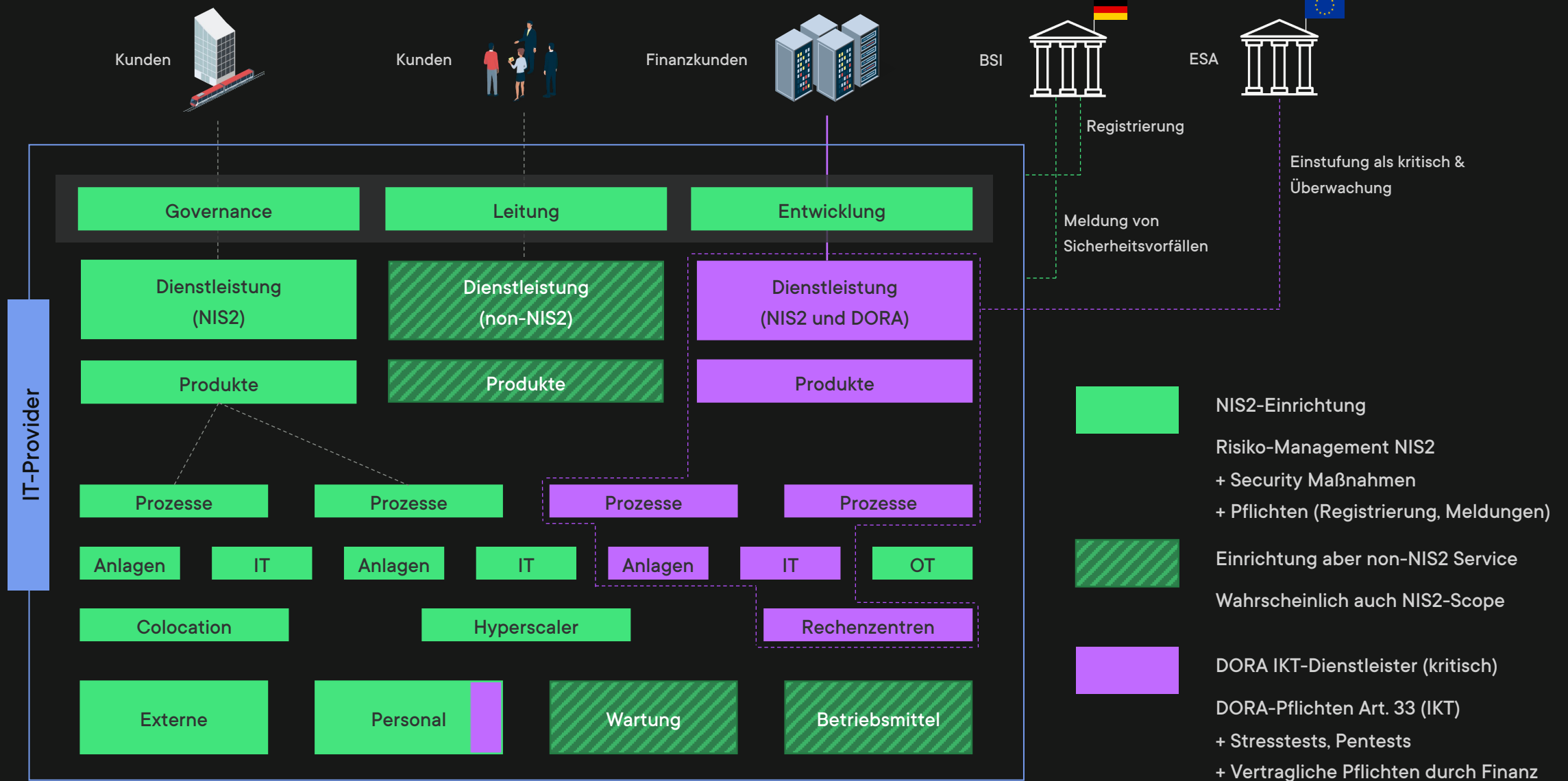
Scoping



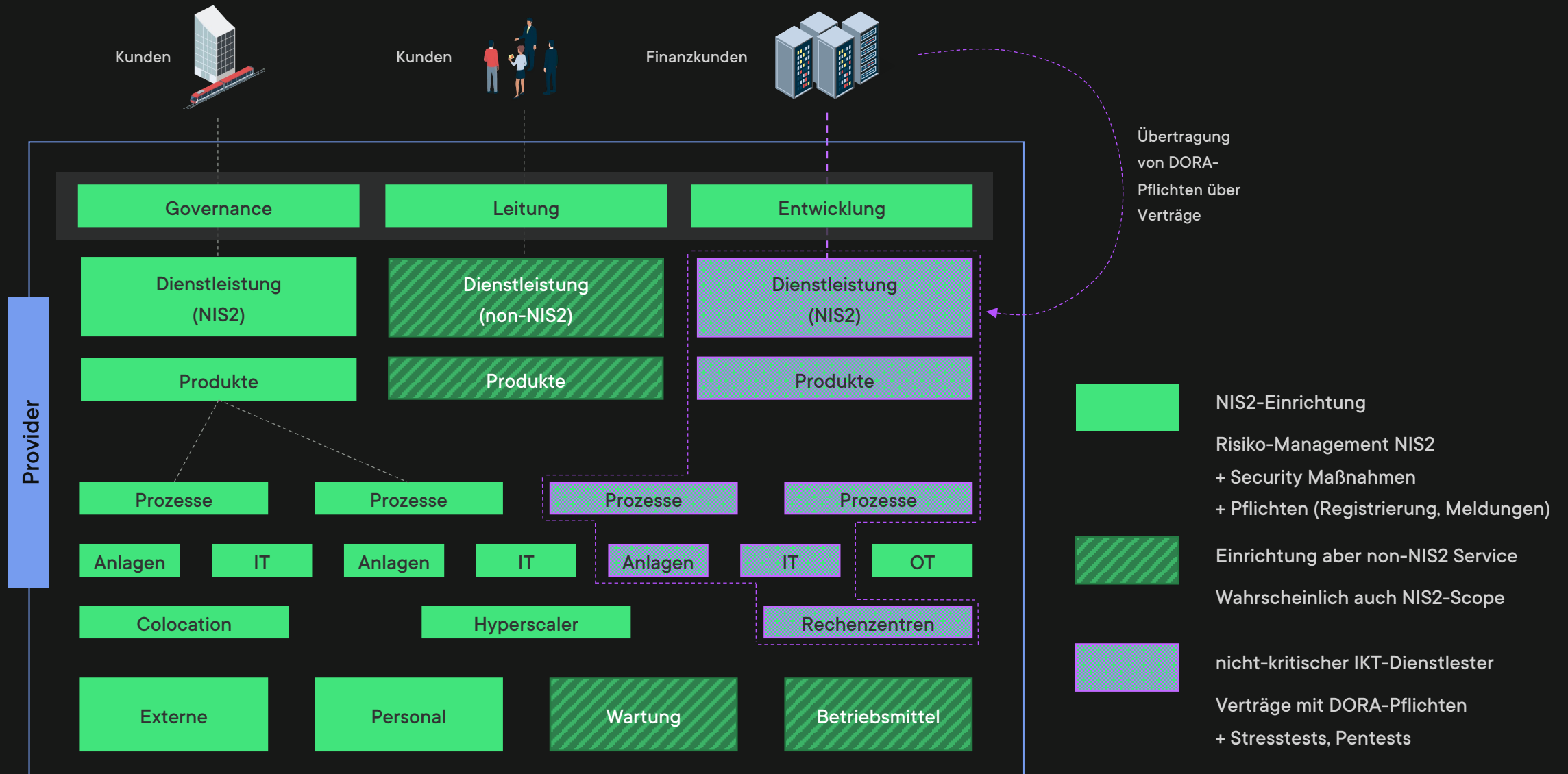
Mapping auf ISMS-Scopes



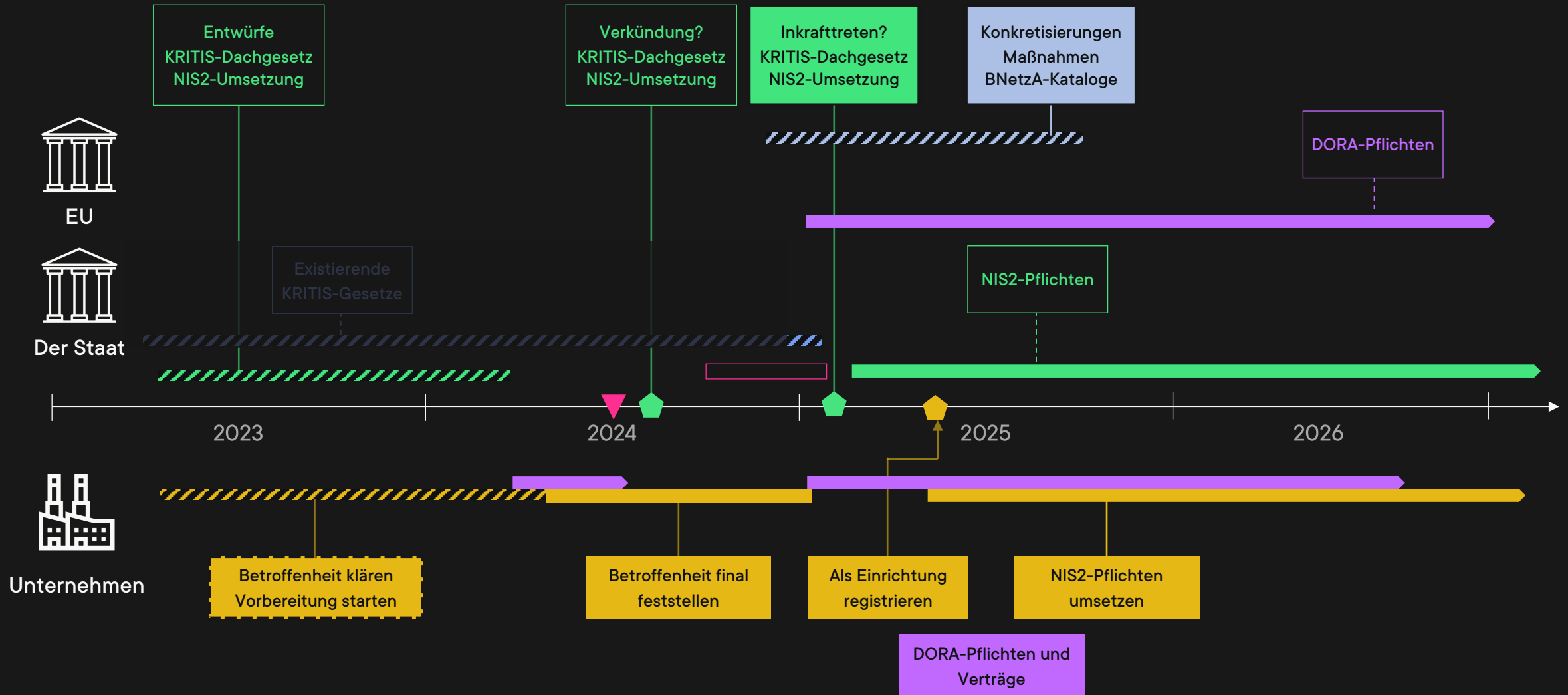
NIS2 und DORA-Dienstleistungen



NIS2 und DORA als nicht-kritischer DL



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

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



NIS2

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

Personal
Beratung/RA
Verträge !



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](https://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

© Copyright Paul Weissmann 2024

Impressum

Insignals GmbH

Paul Weissmann

Rheinwerkallee 6

53227 Bonn

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

info@openkritis.de · +49 176 58952135