Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Title Page

DORA & NIS2: Connection and Relevance from the German Perspective

Study Program & Faculty
Cybersecurity & Business, Fachberiech 4

Author
Sindirinschi Timur

Subject
Scientific Writing

Location & Date
Berlin, 27.01.2026

Table of Contents

Title Page.....1

Table of Figures.....3

Index of Tables.....4

Index of Abbreviations.....5

1. Introduction.....6

1.1 Research gap.....6

1.2 Methodology.....6

1.3 Overview of chapters.....7

2. Foundational Understanding of the Legal Framework.....7

2.1 The shift from ex-post to ex-ante supervision.....8

2.2 The Lex Specialis Principle.....8

3. Addressing RQ1: NIS2 in Germany (NIS2UmsuCG).....9

3.1 Scope and "Betroffenheit".....9

3.2 The new duties of care.....10

3.3 Management Liability ("Chefsache").....10

4. Addressing RQ2: DORA and the Financial Sector.....11

4.1 BaFin's expanded role.....11

4.2 The Five Pillars of DORA.....11

4.3 Third-Party Risk Management (TPRM).....12

5. Discussion.....12

6. Conclusion.....12

7. Bibliography.....13

Appendix.....14

Table of Figures

Figure 1: The Five Pillars of Dora (SURECLOUD, 2025)..... 10

Index of Tables

Table 1: Essential and important entities (OpenKRITIS, 2025).....7
Table 2: NIS2 Sectors (OpenKRITIS, 2025).....9

Index of Abbreviations

- **BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)**
- **BSI – Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)**
- **BSIG – BSI-Gesetz (Act on the Federal Office for Information Security)**
- **DORA – Digital Operational Resilience Act**
- **ICT – Information and Communication Technology**
- **KRITIS – Kritische Infrastrukturen (Critical Infrastructures)**
- **NIS2 – Network and Information Security Directive 2**
- **NIS2UmsuCG – NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz**
- **CISO – Chief Information Security Officer**
- **CTPP – Critical ICT Third-Party Provider**
- **GDPR – General Data Protection Regulation**
- **TLPT – Threat-Led Penetration Testing**
- **TOMs – Technical and Organizational Measures**

1. Introduction

Throughout the last period, often termed “Digital Decade”, the European Union has pursued with resolute confidence a strategy of “Digital Sovereignty” that culminates in a tightly interlocked regulatory mesh that by design engineered a protective layer against Cyber threats, thereby safeguarding its internal market. At the time that General Data Protection Regulation (GDPR) was aimed at data privacy, the current push for digital regulations, the NIS2 Directive and the Digital Operational Resilience Act (DORA) specifically, the scope has shifted in the direction of resilience and operational up time.

In the context of the German state, this decision allows for a fundamental shift of the legal landscape. Standards are not being applied selectively and lose their voluntary nature, even for critical infrastructure. As of December 2025, the German Implementation of NIS2 (NIS2UmsuCG) brought into scope 14,500 newly affected enterprises according to government estimates in their specific cost-benefit calculations (Deutscher Bundestag, 2024, p.4). According to independent sources the total impact calculated represents an expansion of regulated entities from 4,500 prior up to 30,000 (Freshfields Bruckhaus Deringer, 2025, BSI, 2025). Moreover, DORA has created a unified, direct and rule book aimed at applicability for the financial sector, thus removing variances at the national level in how insurers and banks manage and mitigate ICT risk.

1.1 Research gap

Professional and academic discourse treat the NIS2 and DORA pair often with a separated classification. For German conglomerates and service providers the linkage of these regulations is convincingly noticeable. The lack of guidance integration is showing, especially in the explanation of German implementation nuances, such as personal liability of management boards (“Geschäftsleitung”) alongside the EU mandates of DORA. Furthermore, the practical coordination between the *Bundesamt für Sicherheit in der Informationstechnik* (BSI, Federal Office for Information Security) and the *Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin, Federal Financial Supervisory Authority) is a source of disarray for compliance officers.

In order to address this gap, this research examines two critical questions:

- **RQ1 -** How does the German NIS2UmsuCG alter the liability landscape for corporate management?

- **RQ2 -** In what ways does DORA function as *lex specialis*, and where do the two frameworks overlap?

1.2 Methodology

This research utilizes a legal dogmatics analysis of the primary texts: the EU Regulation 2022/2554 (DORA) and the German *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2UmsuCG), passed in November 2025. This is supplemented by a review of supervisory statements ("Aufsichtsmitteilungen") issued by BaFin and the BSI between 2024 and 2026.

1.3 Overview of chapters

- **Chapter 2** establishes the foundational legal principles, more specifically focusing on the *lex specialis* rule.
- **Chapter 3** provides a immersive perspective into NIS2 in Germany, focusing on the categories of crucial importance.
- **Chapter 4** analyzes the impact DORA manifests on the financial sector and its supply chain.
- **Chapter 5** discusses the practical conflict points for German industry.
- **Chapter 6** concludes with a summary of the new German Cybersecurity architecture.

---

2. Foundational Understanding of the Legal Framework

In order to comprehend the current German regulatory environment, one must distinguish between the these two EU legal frameworks utilized: the Directive (NIS2) and the Regulation (DORA). The legislation distinguishes between important entities (*wichtige Einrichtungen*) and essential entities (*besonders wichtige Einrichtungen*), assigning different supervision protocols to each (Deutscher Bundestag, 2024, p.3).

"Essential entities **§28 (1)** are large enterprises operating in certain sectors, some companies independent of their size and operators of critical infrastructures. Important entities **§28 (2)** are large and medium enterprises in a broad spectrum of sectors." (OpenKRITIS, 2025)

Table 1: Essential and important entities (OpenKRITIS, 2025)

Category	Size Criteria	Sectors & Conditions
Essential Entities *(Besonders wichtige Einrichtungen)* **§ 28 (1)**	**Large Enterprises** (250+ employees or >€50M turnover)	**Annex 1 Sectors:** Energy, Transport, Finance, Health, Water, Digital Infrastructure, Space
	Size-Independent	**Specific Digital Services:** • Qualified Trust Services • TLD Name Registries • DNS Service Providers
	Medium Enterprises	**Telecommunications:**

Category	Size Criteria	Sectors & Conditions
		Providers of public telecommunication networks or publicly available telecommunication services
	Size-Independent	**Critical Infrastructure:** Designated operators of critical infrastructure (KRITIS)
Important Entities *(Wichtige Einrichtungen)* **§ 28 (2)**	**Medium Enterprises** (50-249 employees or €10M-€50M turnover)	**Annex 1 Sectors:** Energy, Transport, Finance, Health, Water, Digital Infrastructure, Space
	Large & Medium Enterprises	**Annex 2 Sectors:** Postal/Courier, Municipal Waste, Chemicals, Food, Manufacturing, Digital Services, Research
	Size-Independent	**Trust Services:** General providers of trust services (non-qualified)

2.1 The shift from ex-post to ex-ante supervision

Historically, German IT security law (IT-Sicherheitsgesetz 2.0) has managed operations on a reactive basis for various sectors. The new framework employs a bifurcated supervisory model:

1. Before the event supervision (ex-ante): Applied to essential entities, formerly KRITIS and currently including new high-risk sectors. The BSI has the power of auditing these entities before an incident would occur.

2. After the event supervision (ex-post): Applied to important entities, referring to the broader economy. The BSI acts only when proof of non-compliance is present, e.g., a major incident report.

2.2 The *Lex Specialis* Principle

A central concept in German law is *lex specialis derogat legi generali* (the specific law overrides the general). DORA is explicitly designed as a *lex specialis* to NIS2.

- NIS2 is the general law for Cybersecurity across 18 sectors.
- DORA is the specific law for the financial sector.

Consequently, a bank based in Germany shall not report incidents to the BSI under NIS2, rather it reports to BaFin under DORA. “So ist jetzt die BaFin in Deutschland der nationale Melde-Hub für IKT-Vorfälle im Finanzsektor." (BaFin, 2025) (“For example, BaFin in Germany is now the national reporting hub for ICT incidents in the financial sector.”, author’s translation). However, this is not an absolute separation. Financial entities must actively maintain situational awareness of cases of a particularity regarding broader national threat that is being monitored by the BSI.

---

3. Addressing RQ1: NIS2 in Germany (NIS2UmsuCG)

The *NIS-2-Umsetzungsgesetz* entered into force on December 6, 2025, marking the most significant expansion of German IT security law in history.

3.1 Scope and "Betroffenheit"

The law abandons the old threshold that was based on an entity serving 500,000 people in favor of clear size-cap rules. Following the adoption of NIS2, any entity in a regulated sector with 50+ employees or €10M+ annual turnover is now affected. (OpenKRITIS, 2025)

Table 2: NIS2 Sectors (OpenKRITIS, 2025)

Sector Category	Sectors of High Criticality (Annex 1)	Other Critical Sectors (Annex 2)
Energy	**Energy:** Power supply, district heating/cooling, fuel/heating oil, gas	—
Transport	**Transport:** Air, rail, shipping, road	**Postal and Courier Services**
Finance & Insurance	**Finance:** Banks, financial market infrastructure	—
Health	**Health:** Services, reference laboratories, R&D, pharma (NACE C 21), Medical devices	—
Water & Waste	**Water:** Drinking water, waste water	**Municipal Waste:** Waste management
IT & Telecommunications	**Digital Infrastructure:** IXPs, DNS, TLD, cloud providers, data center services, CDNs, TSP, electronic communication/services, managed services and security services	**Digital Services:** Marketplaces, search engines, social networks
Space	**Space:** Ground infrastructures	—
Industry & Manufacturing	—	**Manufacturing:** Medical/diagnostics; IT, electronics, electrics, optical (NACE C 26 and 27); Mechanical engineering (NACE C 28), vehicles/parts (NACE C 29), other vehicles (NACE C 30)

Sector Category	Sectors of High Criticality (Annex 1)	Other Critical Sectors (Annex 2)
Chemicals	—	**Chemicals:** Trade, import (NACE 20)
Food	—	**Food:** Wholesale, production, processing
Research	—	**Research:** Research institutions

The BSI estimates this encompasses roughly 29,500 companies in Germany. More importantly, companies must determine their status themselves ("Selbsteinschätzung"). There is no notification from the government telling a company it is regulated, yet the company must register with the BSI by March 6, 2026 (BSI, 2025).

3.2 The new duties of care

Affected entities must implement appropriate, proportionate, and effective technical and organizational measures (TOMs).

1. **Risk Management:** This includes mandatory concepts for risk analysis, incident handling, business continuity, supply chain security, and cryptography.
2. **Reporting (Meldewesen):** Germany has implemented a strict three-stage reporting regime for significant incidents:
    - Early Warning (24 hours): A red flag to the BSI indicating a potential crisis.
    - Incident Notification (72 hours): A fuller assessment of the severity and compromise.
    - Final Report (1 month): A detailed forensic analysis and root cause statement.

3.3 Management Liability ("Chefsache")

Perhaps one the most debated aspect of the German state's implementation is the strictness in matter of liability for management bodies (*Geschäftsleitung*). Section §38 of the new BSIG mandates that management must approve and oversee cybersecurity measures. (Bundestag, 2024, p.43)

- **Non-Delegable:** Management cannot delegate this responsibility to a CISO to avoid liability.
- **Personal Liability:** If a company suffers damages due to a lack of NIS2 compliance, e.g., failure to patch a known vulnerability, the company has a mandatory claim for damages against its own managers (*Regresspflicht*). The managers are liable with their private assets.
- **Training:** Managers must regularly participate in Cybersecurity training to gain the competence required to assess these risks.

4. Addressing RQ2: DORA and the Financial Sector

NIS2 covers the broad economy, yet it is DORA that regulates the financial sector with much higher particularity. Applicable since January 17, 2025, DORA is enforced in Germany primarily by BaFin.

4.1 BaFin's expanded role

BaFin managed to integrate DORA supervision principles into its existing audit infrastructure. Previously, German circulars such as BAIT (Banks), VAIT (Insurance), and KAIT (Capital markets) operated independently and are currently being phased out or face reinterpretation to align with DORA, e.g., BAIT will be fully repealed by December 2026, as DORA takes precedence. (Bruder et al., 2025)

4.2 The Five Pillars of DORA

DORA is built on five pillars that financial entities must document:

1. **ICT Risk Management:** A comprehensive internal governance framework.
2. **Incident Reporting:** A streamlined process to report major ICT incidents to BaFin.
3. **Digital Operational Resilience Testing:** This ranges from basic vulnerability scans to advanced TLPT (Threat-Led Penetration Testing) for significant entities.
4. **Third-Party Risk Management (TPRM):** Management of ICT third-party risk, including registers of information and notification duties.
5. Information Sharing: Voluntary exchange of threat intelligence.

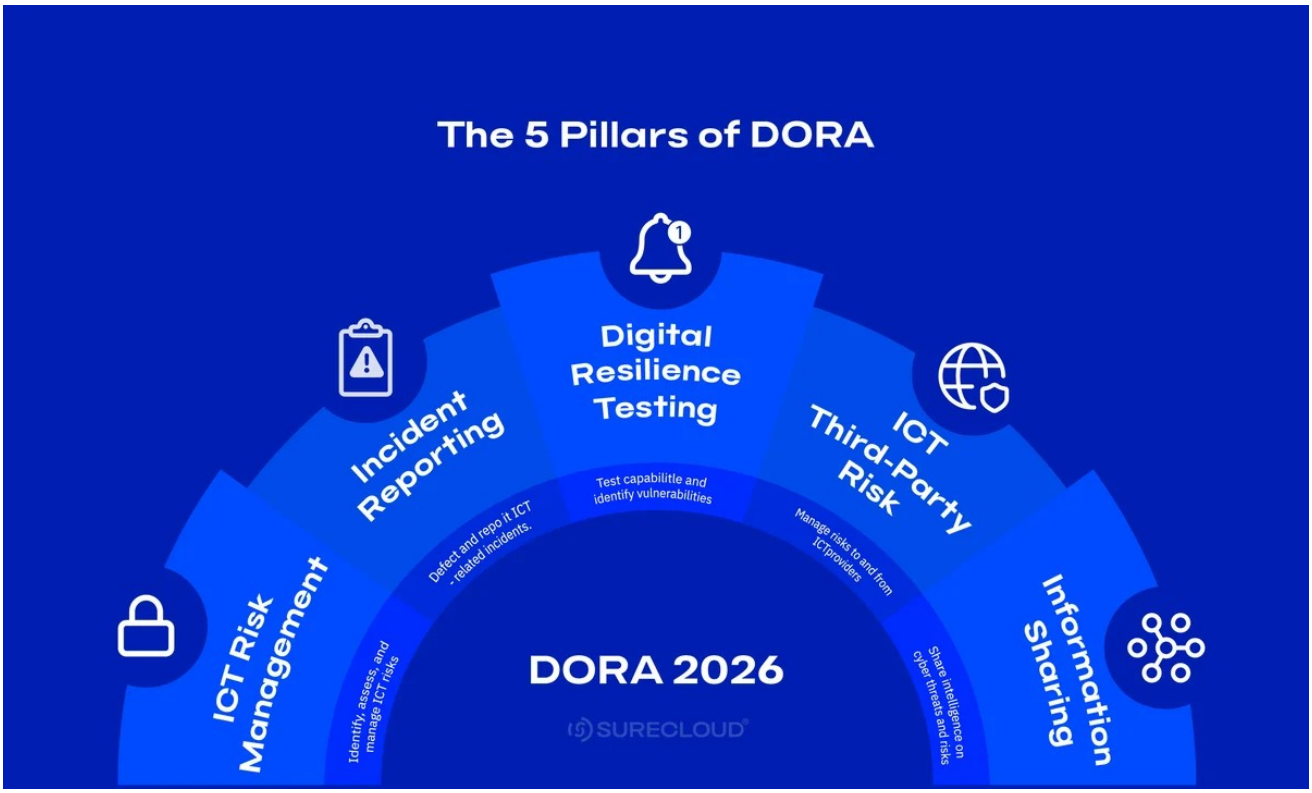

Figure 1: The Five Pillars of Dora (SURECLOUD, 2025)

4.3 Third-Party Risk Management (TPRM)

DORA acts as a backdoor regulation for big tech, creating a direct oversight framework for Critical ICT Third-Party Providers (CTPPs), such as major cloud platforms (AWS, Azure, Google Cloud). German financial entities were required to submit their initial Register of Information, providing a detailed map of all outsourcing contracts to BaFin by early 2025. This register allows BaFin to identify concentration risks, e.g., if all German banks are reliant on a single cloud provider for their core operations. (BaFin, 2025)

---

5. Discussion

The manner in which NIS2 and DORA are implemented in Germany at this date has formed a complex matrix in regard to compliance. For the 30,000 entities under NIS2, the immediate challenge is the registration deadline (BSI, 2025). Many important entities e.g., food processors or waste management firms are facing cyber regulation for the first time and lack the maturity of the essential entities such as energy or water sectors (OpenKRITIS, 2025).

The financial sector faces a contractual challenge, as DORA requires banks to renegotiate contracts with thousands of ICT suppliers to clarify if they meet the strict audit and security rights required by Article 30 of DORA. This has led to a significant administrative burden in 2025 and 2026 (BaFin, 2025).

A unique German nuance is the severity of the sanctions. Under the NIS2UmsuCG, essential entities face fines of up to €10 million or 2% of global turnover, while important entities face €7 million or 1.4%, as aforementioned in § 65 of the new BSIG (Deutscher Bundestag, 2024; OpenKRITIS, 2025).These are GDPR-level penalties, indicating that operational uptime is viewed as as critical as data privacy by German state legistators.

---

6. Conclusion

The years 2025 and 2026 mark a pivotal moment for digital law in Germany. With the NIS2UmsuCG entry into force and the application of DORA, Cybersecurity moves past being a voluntary measure, proving to be rather a strict legal requirement. Germany has deputized the private sector in order to ensure national digital security.

The message is loud for corporate management as well, redefining Cybersecurity as no longer an IT problem, but a liability issue at the board and C-suite level. Shifting to personal liability for directors under the German NIS2 implementation ensures that Cyber resilience will remain a primordial item on the agenda for the foreseeable future.

---

7. Bibliography

BaFin (2025). *DORA - Digital Operational Resilience Act*. Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht. [online] Available at: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html [Accessed 16 Jan. 2026]

Bruder, A.H., Yaros, O., Hörauf, M., Kapotwe, M. and Beck, B. (2025). *Cybersecurity in the Financial Sector: EU's Digital Operational Resilience Act Takes Effect*. [online] Mayer Brown. Available at: https://www.mayerbrown.com/en/perspectives-events/publications/2025/01/cybersecurity-in-the-financial-sector-eus-digital-operational-resilience-act-takes-effect [Accessed 21 Jan. 2026].

BSI (2025) NIS-2-regulierte Unternehmen [online] Available at: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Starterpaket/nis-2-start_node.html [Accessed 17 Jan. 2026].

Deutscher Bundestag (2024). *Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*. Drucksache 20/13184. Berlin: Deutscher Bundestag. [online] Available at: https://dserver.bundestag.de/btd/20/131/2013184.pdf [Accessed 19 Jan. 2026].

Freshfields Bruckhaus Deringer (2025). *Germany implements NIS2: What you need to know now*. [online] Freshfields Tech Quotient. Available at: https://technologyquotient.freshfields.com/post/102lwz4/germany-implements-nis2-what-you-need-to-know-now [Accessed 15 Jan. 2026].

OpenKRITIS (2025). *NIS-2 Betroffenheit: Wer fällt unter das Gesetz?*. [online] Available at: https://www.openkritis.de/eu/eu-nis-2-germany.html [Accessed 27 Jan. 2026].

SureCloud (2025). *The 5 Pillars of DORA Explained*. [online] Available at: https://www.surecloud.com/blog-hub/five-pillars-of-dora-explained [Accessed 27 Jan. 2026].

Appendix