GRM® Global Regulation

CER – The Wall Must Go

Separating what belongs together

Paul Friedrich
Dr Waldemar Grudzien

May 2026
Synopsis

Authors' note

- The horizontal division of resilience into cybersecurity (NIS2) and physical security (CER) across two pieces of legislation is contradicted by vertical regulation
- The CER Directive itself overturns this separation through recitals 20 and 21
- Content from the CER Directive can be transferred to the NIS2 Directive with little effort, analogous to the national approach of transferring content from the KRITIS Framework Act (KRITISDachG) into the BSI Act
- Different impact classifiers from the two laws present the business sector with unnecessarily high complexity
- The KRITIS Framework Act will only be legally defined upon the publication of up to nine implementing regulations, expected in summer 2026
- Resilience obligations under the KRITIS Framework Act are best implemented within the framework of the recognised BSI 200-4 standard
- The CER at European level and the KRITISDachG at national level should be incorporated into NIS2 and the BSI Act respectively and subsequently repealed – this saves resources for those affected and increases their overall security

Introduction

The German regulatory framework for the technical and organisational resilience of critical facilities, services and infrastructure is complete with the entry into force of the KRITISDachG on 17 March 2026. It supplements the cybersecurity regulations set out in the BSI Act by adding the area of physical security. At the European level, the framework includes the NIS2 and CER Directives, whilst on the German side it comprises the BSIG, KRITIS-V and KRITISDachG; depending on the sector, specific laws are also included – see Figure 1.

Regulation of cyber security and physical security in critical sectors in Europe and Germany

Not present / Present

Scope of the laws — Horizontal / Vertical

Sectors	Cyber security	NIS2 BSIG	CER KRITISDachG	Physical security
Energy	NCCS (VO 2024/1336 for electricity)	✓	✓	-
	-	✓	✓	EnWG, AtG
Transport & Traffic	EASA (Part IS for Aviation), Implementing acts for rail/sea	✓	✓	-
	-	✓	✓	AEG, LuftSiG, StVG / FStrG
Finance	DORA	✗	✗	-
	-	✓	✓	KWG, VAG
Benefits for jobseekers	eIDAS 2.0	✓	✗	-
	-	✓	✓	-
Health	MDR (VO 2017/745), IVDR (VO 2017/746), EHDS (VO 2025/327)	✓	✗	-
	-	✓	✓	SGB V, KHZG, MPDG, AMG
Water	Drinking water (RL 2020/2184)	✓	✓	-
	-	✓	✓	WHG, TrinkwV
Nutrition	-	✓	✓	-
	-	✓	✓	LFGB, ESVG
IT & Telecommunications	CRA (VO 2024/2847)	✓	✗	-
	-	✓	✓	TKG
Space	EU Space Strategy (2023), EU Space Act (Draft 2025)	✓	✗	-
	-	✓	✓	SatDSiG / SatDSiV, RAGG, TKG
Waste Disposal	-	✓	✓	-
	-	✓	✓	KrWG

Figure 1: Cybersecurity and physical security are mostly treated together in the EU and Germany

The question must be asked as to why, at both the European and national levels, resilience is divided into cyber security and physical security, particularly since it is, as Figure 1 clearly demonstrates, consistently treated as a single concept in sector-specific legislation. The all-purpose excuse of 'historical development' is likely to be invoked; nevertheless, both the European and German legislators had the opportunity to address resilience comprehensively, in all its facets, within a single piece of legislation. The hope remains that both facets will be unified in the next revision. Until then, it is worth studying this synopsis and taking on board the insight that what is currently treated separately belongs together.

In our synopsis "NIS2 – Groundhog Day", we have already dealt with the NIS2 Directive and its German implementation through the BSIG and KRITIS-V, i.e. with cybersecurity. Here now follows the second part, covering physical security under the CER Directive and the KRITISDachG.

Structure of the CER Directive

Figure 2 shows the CER Directive with its 29 articles. The following figure illustrates the KRITISDachG. The exclusion principle is applied to the applicability of cybersecurity and physical security, as, according to Article 1(2) of CER, the "CER Directive does not apply to matters falling under the NIS2 Directive". And further: "In view of the relationship

between the physical security and cybersecurity of critical infrastructure, Member States shall ensure the coordinated implementation of this Directive and Directive (EU) 2022/2555." This is the missed opportunity for the German legislature to merge the two – the BSIG and the KRITISDachG – into one.

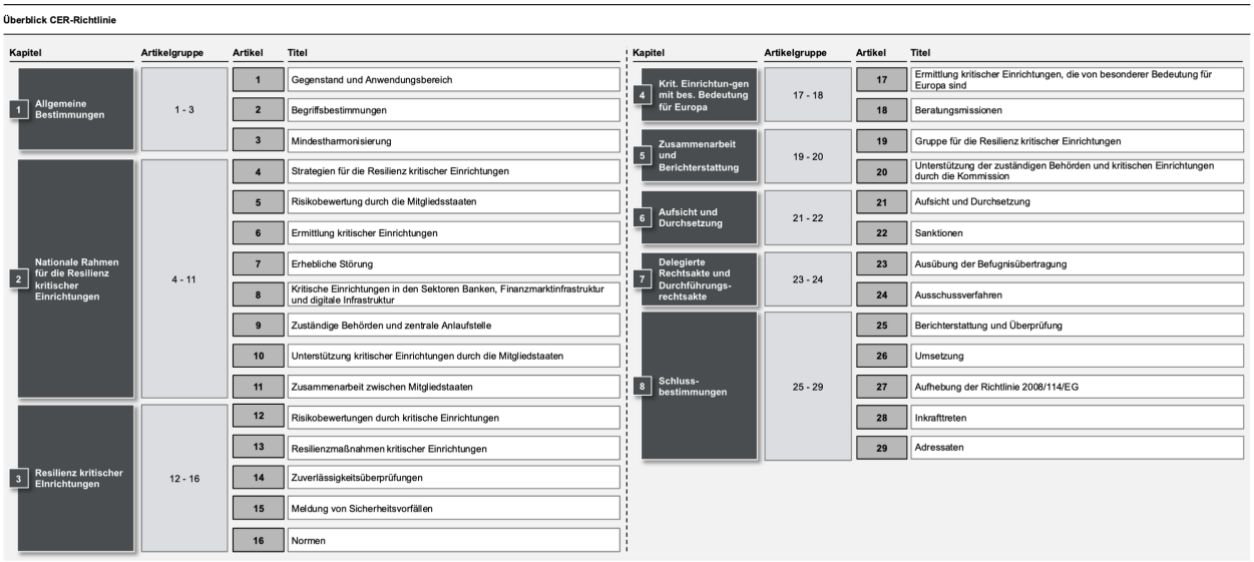

Figure 2: Overview of the CER Directive

Article 8 of CER excludes the application of the Directive to critical facilities in the banking, financial market infrastructure and digital infrastructure sectors, as do Recitals 20 and 21. However, both recitals serve as a 'gateway' for national regulations that require a higher level of resilience: Recital 20 excludes the obligations set out in Article 11 and in Chapters III, IV and VI of the CER Directive where the NIS2 Directive applies to entities in the digital infrastructure sector, and Recital 21 excludes them where the DORA Regulation applies to financial entities, "in order to avoid duplication and unnecessary administrative burdens". However, both recitals require the identification of entities in the digital infrastructure sector and the financial sector, respectively, as critical infrastructure entities based on the criteria and procedures set out in the CER Directive.

Structure of the KRITIS Framework Act

The KRITIS Framework Act (KRITISDachG) consists of 26 sections (Figure 3). Nine sections are not applicable to the financial sector in whole (Sections 9, 10, 12 to 16, 18, 20) or in part (Sections 3(8), 19(2), 21(6)); operators of critical infrastructure are the addressees in only eleven sections, of which nine are directly applicable (§§ 4, 8, 12, 13, 14, 18, 20, 24, 26) and two indirectly applicable (§§ 5, 9). What follows is a brief assessment of the sections in the form of a tour de force:

- Section 1 sets out the Federal Government's strategy for improving the resilience of critical infrastructure. This can only be welcomed.
- It is important to note from Section 3 that the Federal Office for Civil Protection and Disaster Assistance (BBK) is the so-called central point of contact for all those affected, and that the competent authority varies depending on the sector.

- Section 4 defines the scope of application as covering 10 sectors (see Figure 4) whilst simultaneously restricting it for certain sectors. In addition, a statutory instrument (see Figure 5) is being introduced to define critical services within the sectors. According to reliable sources, the drafts for designating critical services are at a very advanced stage and are expected by summer 2026.
- Section 5 introduces the technical term ‘significance of a facility’. According to this, ‘significance’ defines a ‘critical facility’ as a facility that is significant for the provision of a critical service. The classifiers used to identify significance are the facility category, the threshold value for the standard figure of 500,000 residents to be supplied, and the reference date. Only a ‘critical facility’ must meet the requirements set out in subsequent sections.
- Section 8 governs the registration of critical facilities with the BBK. As Section 8 corresponds to Section 33 of the BSIG, companies that were required to register with the BSI under the BSIG by 6 March 2026 under the BSIG, do not now need to register a second time with the BBK. All other affected companies must carry out this registration.
- The next two sections, 9 and 10, address critical facilities of particular importance to Europe and should not place any further burden on them, as these are only of particular importance if they possess a corresponding scale and market power and are therefore already well regulated.
- The next pair of sections, 11 and 12, deal with risk analyses and risk assessments. Section 11 governs their preparation by the competent state authorities, whilst Section 12 governs their preparation by operators of critical infrastructure. In doing so, operators must take into account the national risk analyses and risk assessments set out in Section 11. Two comments on this:
    - Of the CIAA canon of protection objectives, only availability is cited as a risk factor. This is noteworthy insofar as a breach of physical security can also have consequences for the other three protection objectives.
    - Both parties responsible for drawing up the plans must carry out the risk assessments ‘as required, but at least every four years’. In light of other regulations and their mostly annual cycles, this is to be regarded as generous.
- Section 13 is where the focus of this Act lies, concerning resilience obligations. It deals with measures throughout the incident lifecycle and the physical protection of properties and critical infrastructure. Operators must “set out and apply” these measures in a resilience plan. For details, see Figure 6.

- Section 14 introduces cross-sectoral and sector-specific minimum requirements as well as industry-specific resilience standards. Under the first approach, the BMI may determine cross-sectoral minimum requirements to specify the obligations under Section 13(1). The second approach builds a bridge to the "industry-specific security standards" (B3S) of the NIS1/IT-SiGv1.0 era. Whilst the second approach is therefore familiar and tried-and-tested, the community can look forward with anticipation to the corresponding statutory instrument.

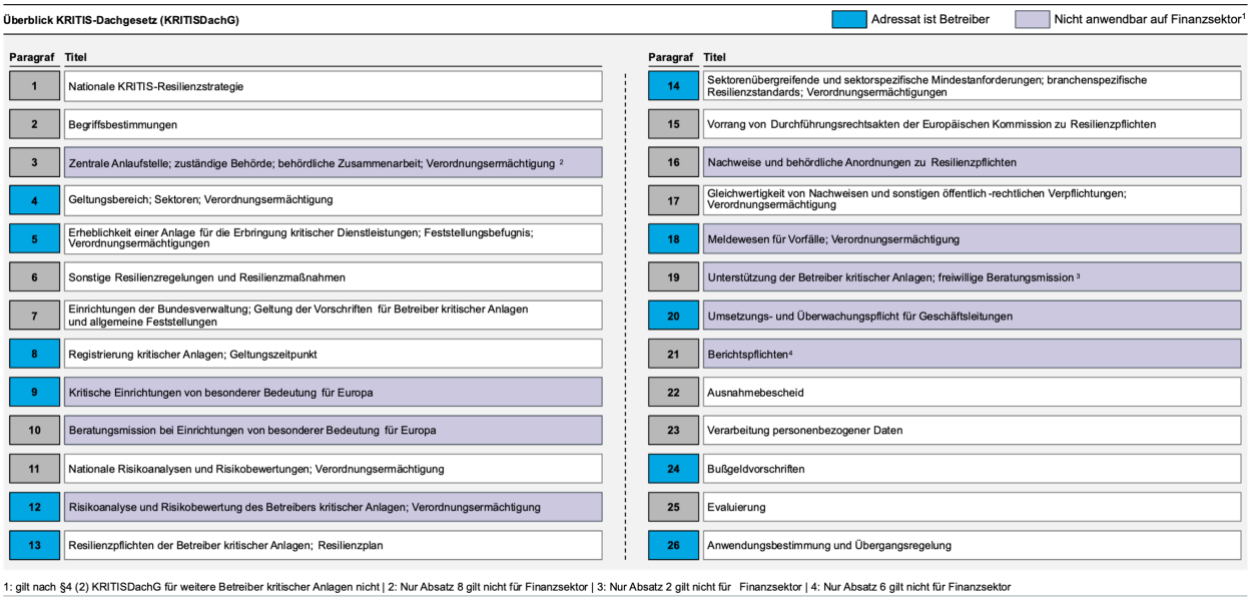

Figure 3: Overview of the KRITIS umbrella law

- Sections 16 and 17 set out the types of evidence required to demonstrate compliance with resilience obligations: evidence under Section 39 of the Federal Information Security Act (BSIG) (duty of operators of critical infrastructure to provide evidence), audit reports, inspections by the competent authority, or certifications. In addition, where deficiencies are identified, the competent authority may require a rectification plan, including evidence that the deficiencies have been rectified.
- Section 18 governs the reporting system. There is an obligation to submit an initial report within 24 hours of becoming aware of the incident and a 'detailed' report after one month. Interim reports are only indirectly required through the obligation to update the initial report in the event of an 'ongoing incident'.
- Section 19 governs the support services provided to operators of critical facilities by the BBK (templates, guidelines, advice, training, exercises) and the BMI (advisory mission). An advisory mission is intended to clarify whether the operator has fulfilled the obligations set out in Sections 12, 13 and 18. Section 19 should clarify that advisory missions relate exclusively to 'critical facilities of particular importance to Europe' (as restricted by Article 18 of the CER) and by no means to every critical facility.
- Section 20 emphasises the implementation and monitoring obligations for management. In doing so, the KRITISDachG continues the tradition of reiterating things that are already clear – namely, that management is generally responsible for the success or failure of an enterprise. Here, this responsibility is extended to include resilience measures (Section 13).

- Of the remaining sections, only Section 24 is of interest to operators, which brings us to the fines, which are graded according to the nature of the infringement into four categories: 100k, 200k, 500k and 1 million euros.

Sectors affected

Figure 4 lists all the sectors covered by KRITIS-V, the BSIG and the KRITISDachG. Critical facilities under KRITIS-V are automatically classified as particularly important facilities under the BSIG. KRITIS-V is incorporated into the BSIG to establish a link to the 'critical infrastructures' from the NIS1/IT-SiGv1.0 era and to transfer these infrastructures into the nomenclature and classification under NIS2 / BSIG. The KRITISDachG combines the critical facilities from the KRITIS Regulation with the particularly important facilities from the BSI Act.

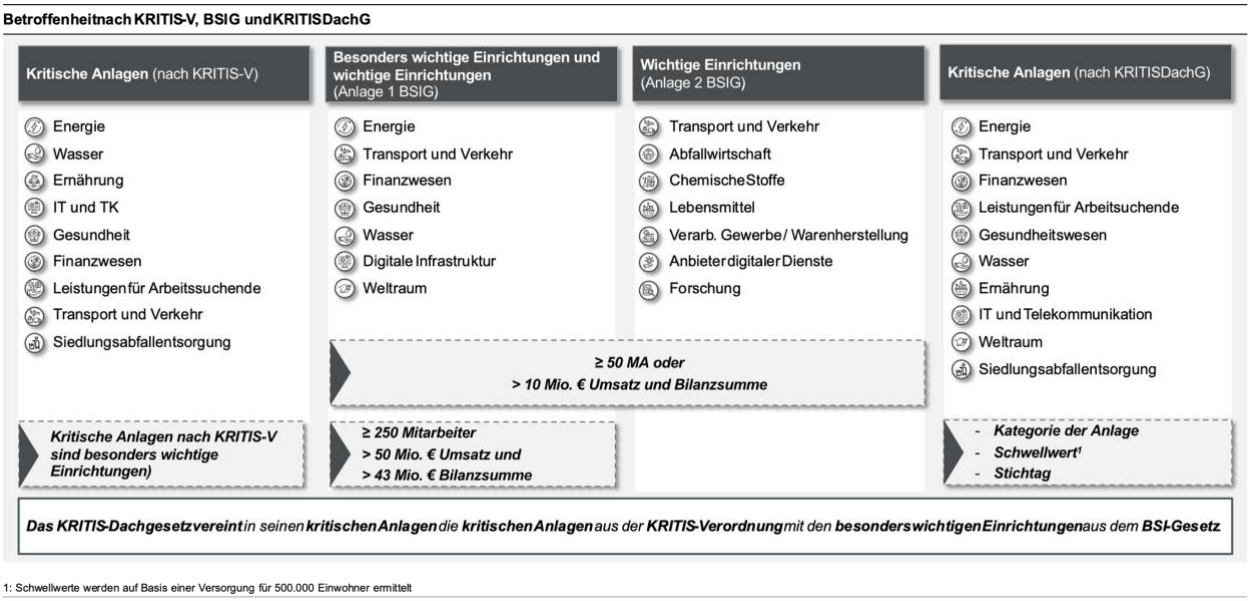

Figure 4: Affected sectors and critical facilities under the BSIG and KRITIS-V

This linguistically harmonises the sectors of the cyber world under the NIS2 Directive with the sectors of the physical world under the CER Directive. This consolidation is extremely important for the acceptance and practicability of both legislative packages. The term 'legislative package' is indeed the case, as the KRITISDachG establishes nine further statutory regulations, as shown in Figure 5.

What does all this mean for a company that must comply with both the BSIG and the KRITISDachG, and for which no exemption applies, as is the case, for example, for DORA-regulated financial entities? This company must first determine the scope of application under both laws, i.e. thresholds for staff numbers, turnover and balance sheet total under the BSIG, and under the KRITISDachG for materiality, the provision of essential services to 500,000 inhabitants, and categories of facilities. This is followed by compliance with the requirements of both laws and the derivation of measures for these dual requirements. This framework must then be integrated into the existing risk management framework.

Regulations under the KRITISDachG

Of the nine regulations under the KRITISDachG, the following are considered particularly important from a business perspective: the statutory regulation under Section 4 (3) of the KRITISDachG (No. 2 in Figure 5) on the determination of critical services in the ten critical sectors, as well as the statutory order pursuant to Section 5(1) of the KRITISDachG (No. 3 in Figure 5) on the determination of the categories of facilities, thresholds and reference dates. These three classifiers are used to determine the significance of a facility and, consequently, whether that facility is classified as critical.

Other relevant statutory instruments concern the methodological and substantive requirements for risk analyses and risk assessments for competent authorities under Section 11(8) and for operators of critical facilities under Section 12(3). The statutory instrument under Section 14(1) of the KRITISDachG (No. 7 in Figure 5) is also of particular importance for specifying the obligations under Section 13(1) regarding cross-sectoral minimum requirements. It remains to be seen which statutory instruments the BBK will actually issue and when these will be published.

Rechtsverordnungen im KRITISDachG

	KRITISDachG	Inhalt der Rechtsverordnung
1	§3 (3)	**Das BMI kann für weitere kritische Dienstleistungen**, die in der Rechtsverordnung nach § 4 Absatz 3 festgelegt werden, **zuständige Bundesbehörden festlegen**. Für die kritische Dienstleistung des Betriebs von Bodeninfrastrukturen für die Erbringung weltraumgestützter Dienste im Sektor Weltraum kann das Bundesministerium für Forschung, Technologie und Raumfahrt eine oder mehrere zuständige Bundesbehörden festlegen.
2	§4 (3)	**Das BMI bestimmt die kritischen Dienstleistungen**, die jeweils zu den Sektoren nach Absatz 1 gehören.
3	§5 (1)	Das BMI bestimmt 1. **Kategorien von Anlagen**, 2. allgemeine […] **Schwellenwerte zum Versorgungsgrad**, bei deren Erreichen eine Anlage einer bestimmten Kategorie nach Nummer 1 nach einem bestimmten Stichtag als erheblich für die Erbringung einer kritischen Dienstleistung gilt und bei deren Unterschreiten eine Anlage nach einem bestimmten Stichtag nicht mehr als solches gilt, 3. **Stichtage** nach Nummer 2 sowie 4. Kategorien von Anlagen, die unabhängig von Nummer 2 als erheblich für die Erbringung einer kritischen Dienstleistung gelten.
4	§5 (7)	Das BMI kann Kriterien und Verfahren festlegen, mit denen die Länder feststellen können, ob eine Anlage für die Erbringung einer kritischen Dienstleistung erheblich ist, ohne die Voraussetzungen der Rechtsverordnung des Absatzes 1 Satz 1 zu erfüllen. Die Länder können dies für Anlagen feststellen, bei denen für die betroffene Dienstleistung eine Landesbehörde die zuständige Behörde ist. Bei der Festlegung der Kriterien werden die Kriterien nach Absatz 2 berücksichtigt.
5	§11 (8)	Das **BMI kann methodische und inhaltliche Vorgaben für die Risikoanalysen und Risikobewertungen** der nach Absatz 1 Satz 1 und 2 **zuständigen Stellen** bestimmen.
6	§12 (3)	Das **BMI kann inhaltliche und methodische Vorgaben einschließlich Vorlagen und Muster für die Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen bestimmen**. Das BMI kann die Ermächtigung nach Satz 1 durch Rechtsverordnung auf das BBK übertragen.
7	§14 (1)	Das **BMI kann zur Konkretisierung der Verpflichtungen nach § 13 Absatz 1 sektorenübergreifende Mindestanforderungen bestimmen**. Das BMI kann die Ermächtigung nach Satz 1 durch Rechtsverordnung auf das BBK übertragen.
8	§17 (3)	Das BMI kann feststellen, dass bestimmte **Verpflichtungen** auf Grund sonstiger öffentlich-rechtlicher Vorschriften, die auch für Betreiber kritischer Anlagen gelten, **gleichwertig** mit bestimmten Verpflichtungen sind, die für Betreiber kritischer Anlagen nach diesem Gesetz gelten. (4) Die Verpflichtungen nach diesem Gesetz gelten als eingehalten, soweit die in der Rechtsverordnung nach Absatz 3 Satz 1 als diesen gleichwertig festgestellten sonstigen Verpflichtungen eingehalten werden. Feststellungen anderer Behörden zur Einhaltung der sonstigen Verpflichtungen sind bindend.
9	§18 (7)	Das **BBK übermittelt den zuständigen Behörden**, den nach § 3 (5) benannten Landesbehörden sowie den nach § 11 (1) zuständigen Stellen **Auswertungen zu Vorfallsmeldungen** vorab zw. BBK und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der Vertraulichkeit. Das BMI kann die Prozesse zur Weitergabe der Meldungen an die Länder regeln. Die Rechtsverordnung beschreibt die Rahmenbedingungen, insb. die technischen und personellen Voraussetzungen, Kriterien für eine Weiterleitung von Meldungen und die Prozessbeschreibung für den Informationsaustausch.

Figure 5: Statutory regulations in the KRITISDachG

Figure 6 summarises the resilience obligations of operators of critical infrastructure under Section 13 and provides an outlook on a more stringent solution. Paragraph 1 sets out the requirements of the section with four core tasks. These are specified in more detail by measures in accordance with paragraphs 2 and 3. When selecting the measures, national and operator-specific risk analyses and risk assessments must be taken into account. Last but not least, the BBK provides templates for the resilience plan in accordance with paragraph 4.

A note on the measure ‘access controls’: it can be assumed that the legislator intended to address ‘physical access controls’ rather than ‘logical access controls’. The KRITISDachG sets out requirements for physical protection and thus for physical access (German “Zutritt”). ‘Logical access’ (German “Zugang”) refers to access to systems, applications and infrastructure in the sense of logical authorisation, whereas ‘physical access’ describes physical authorisation to buildings and rooms.

On the right-hand side of Figure 6, Article 13 is translated into the terminology of BSI Standard 200-4 “Business Continuity Management”. Instead of Article 13, the German legislator could have referenced this BSI standard and, by doing so, provided companies with an approach they were already familiar with.

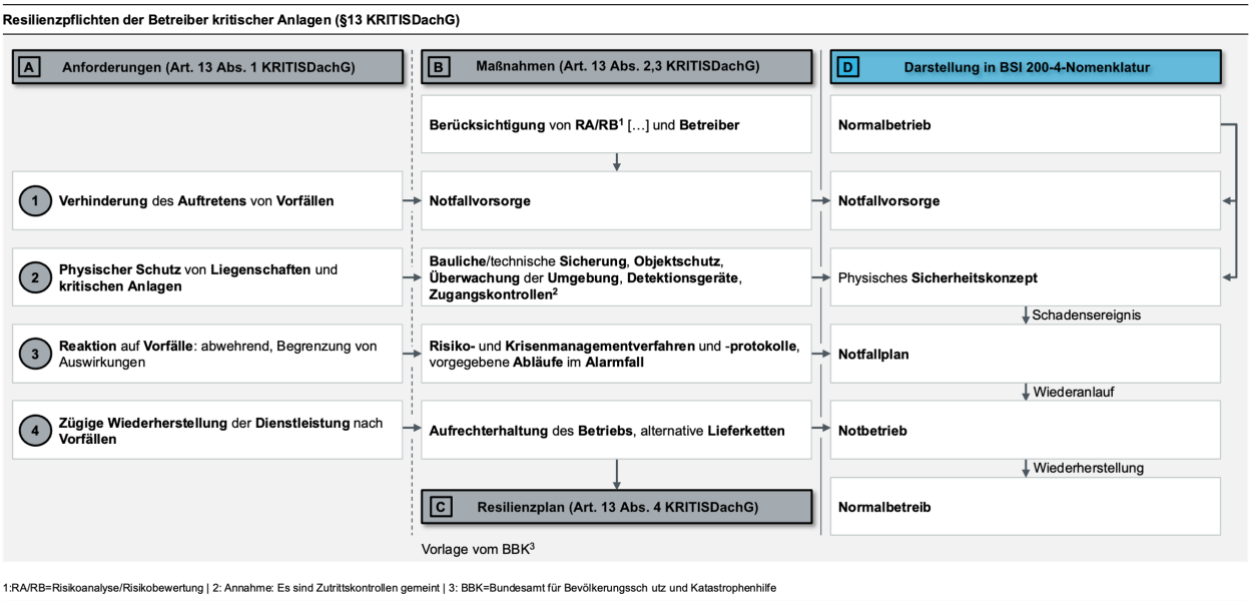

Figure 6: Resilience obligations of operators of critical infrastructure, notation according to BSI 200-4

Proposed solution

As noted in the introduction, the authors consider the division of resilience into cybersecurity and physical security, and the EU’s separate treatment of these in the two directives NIS2 and CER, to be the second-best solution. It would be better to address both issues together within a single piece of legislation. There are compelling reasons for this:

- In recognised standards such as ISO/IEC 27001 for information security or key regulations such as DORA, physical security is naturally treated as an inherent part of overall security.
- It makes no logical sense to extract one area – however important – from the set of requirements in a security catalogue and treat it in isolation. As a result of this separation, interdependencies between the individual security domains are either not recognised or are only vaguely understood and addressed.
- Two sets of regulations require two management systems, which necessitate duplicate structures in terms of personnel, technology and organisation, and ultimately cost time and money.
- If this separation is to be maintained, physical security should be completely removed from the NIS2 Directive, as otherwise double regulation will be exacerbated.
- Finally, an argument against this separation based on the legislation itself: Recital 20 CER argues that, for entities in the digital infrastructure sector, the requirements of the NIS2 Directive are ‘at least equivalent’ to those of the CER Directive and, for this reason, the obligations set out in Article 11 and in Chapters III, IV and VI of the CER Directive should not apply to these entities, ‘in order to

avoid duplication of work and unnecessary administrative burden'. In other words, the exclusion of the CER Directive's applicability to entities in the digital infrastructure sector is justified on the grounds that the NIS2 Directive also adequately regulates physical security. But not for other sectors. This logical contradiction – the exclusion applies to only one sector – and this circular reasoning – a law (NIS2) regulates something (physical security) for a sector that it does not regulate – cannot be justified by anything.

All in all, this dual regulation under NIS2 and CER, or the German implementation via BSIG / KRITIS-V and KRITISDachG, does not increase the resilience of operators of critical infrastructure, but rather weakens it due to the double burden. The aim of the next revision, both at EU level and nationally, should be to merge the two security spheres into a single regulatory framework. In doing so, the CER Directive should be integrated into the NIS Directive, and the KRITISDachG into the BSIG.

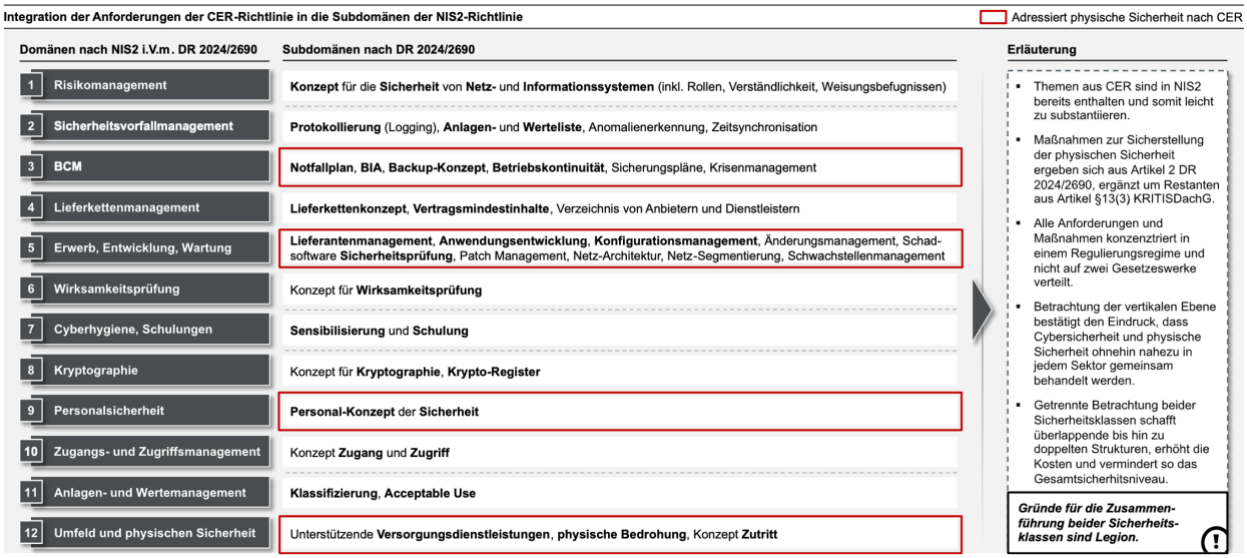

Figure 7: Integration of physical security under CER into the NIS2 domain structure

In other words: as described in our synopsis "NIS2 – Groundhog Day", the NIS2 Directive is met through measures set out in DR 2024/2690 across a total of 12 security domains. In doing so, the physical security objectives from CER are integrated into the relevant domains of NIS2 (Figure 7). In return, CER at EU level and the KRITISDachG at German level are withdrawn. This brings together what belongs together, avoids double regulation, reduces compliance costs and thus increases the resilience of critical infrastructure.

Sources

1. Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical infrastructure (CER)

2. Act on the Federal Office for Information Security and on Information Security in Institutions (BSI Act – BSIG), date of enactment: 2 December 2025

3. Ordinance on the Designation of Critical Infrastructure under the BSI Act (BSI-Kritis Ordinance – BSI-KritisV), date of enactment: 22 April 2016

4. Framework Act on Strengthening the Physical Resilience of Critical Infrastructure (KRITIS Framework Act – KRITISDachG), 11 March 2026

Authors

Paul Friedrich
Managing Director

As a forensic investigation specialist, Paul brings a unique perspective to risk management. As a trusted point of contact for confidential matters, he has handled high-profile cases in various financial centres. With his expertise in risk and financial management, he ensures that even complex project environments run smoothly in day-to-day operations.

Email: pfr@globalregulation.com

Dr Waldemar Grudzien
Managing Director

Waldemar is an expert in financial regulatory audits, information security and data protection. He supports clients throughout all phases of regulatory audits and in meeting information security and data protection requirements. A particular focus of his work is the assessment and management of compliance risks within the regulatory environment.

Email: wgr@globalregulation.com

About Global Regulation Management

GRM leverages regulation. Our mission is to establish compliant corporate structures for organisations operating globally. In doing so, we rely on a deep understanding of business processes, the legal requirements in target markets, and the targeted use of modern software solutions. The focus is on the close integration of business development, risk management and regulatory requirements in a globalised economy. The result of our work is secure, legally compliant and internationally operating corporate structures.

Copyright Notice

The information provided is for general information purposes only. It does not claim to be up to date or complete and is subject to individual interpretation. We strongly recommend that you verify the information yourself.

We accept no liability for any errors, omissions or inaccuracies, nor for any consequences arising from the use of the information. Likewise, we are not responsible for content on linked third-party websites.

The authors reserve the right to change, update or remove the content of this publication at any time. The logos or trademarks depicted in texts or graphics are the property of the respective companies. Global Regulation Management AG uses these exclusively for educational purposes and makes no claim to ownership rights.

Contact

Global Regulation Management AG
Baarerstrasse 52
6300 Zug
Switzerland

info@globalregulation.com
globalregulation.com