Gaia-X
FEDERATION SERVICES
GXFS

WHITEPAPER

Information security of critical infrastructures

Law and regulation for Gaia-X and the Gaia-X Federation Services

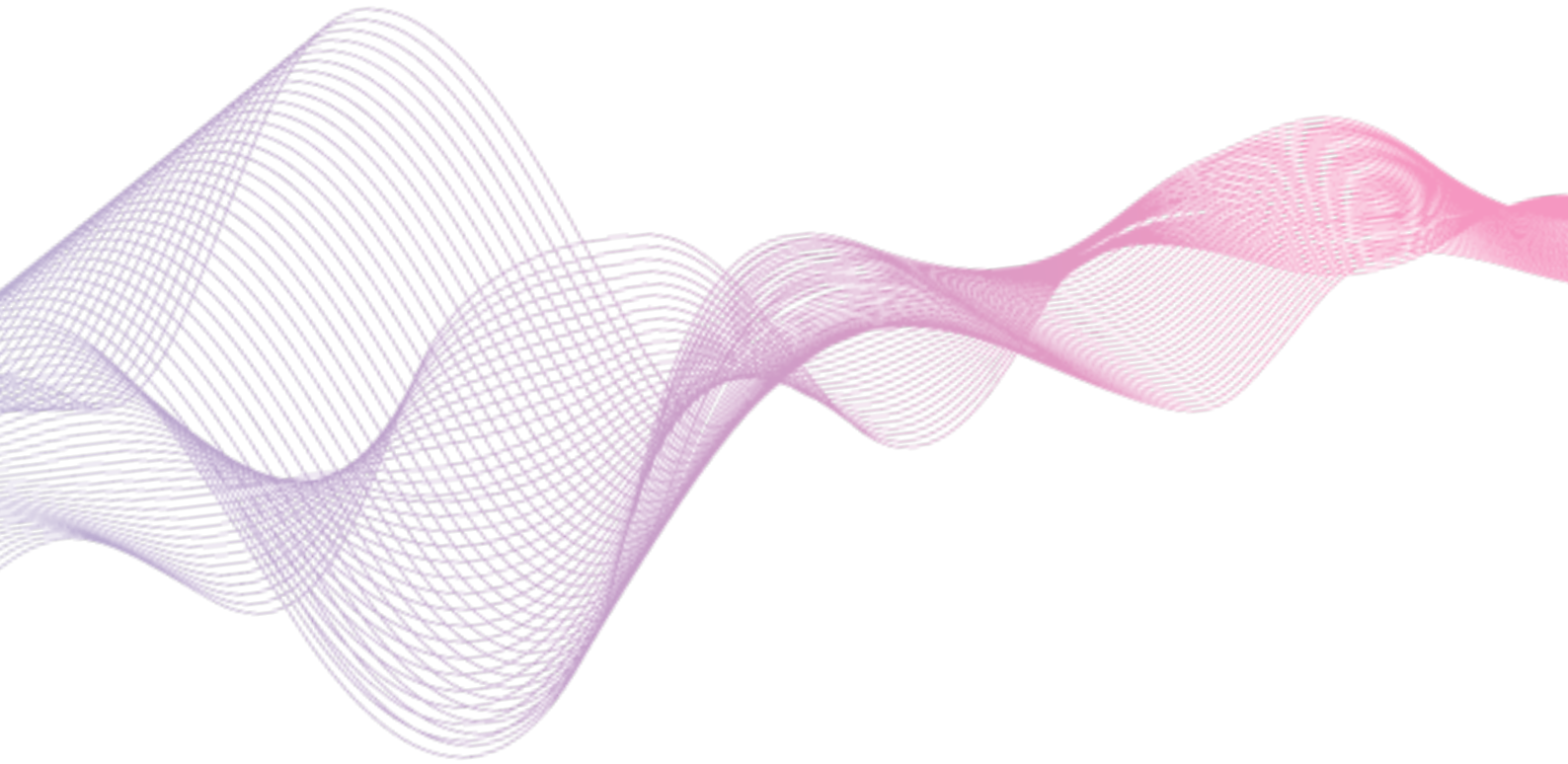
Supported by:

Federal Ministry
for Economic Affairs
and Climate Action

on the basis of a decision
by the German Bundestag

www.gxfs.eu

Table of contents



Information security of critical infrastructures: Law and regulation for Gaia-X and the Gaia-X Federation Services

Introduction

It is a matter of course for all stakeholders in the provision of public or private services to operate within the boundaries of law. In the Constitutional State, administrative action is always based on constitutional principles and legality, while the private sector is bound by the relevant management and due diligence obligations of stock corporation or GmbH law, to which board members and management must adhere. However, the legal framework that they all follow is subject to constant change. For digital offers under keywords such as cloud computing, data centre services and digital communication in the very broadest sense, the legal situation has fundamentally changed, not only in terms of content: Above all, the scope of regulation has been considerably expanded, so that already today, and in the future many more, companies and other institutions are subject to specific obligations that in the past still functioned without such formal rules.

Legal obligation of Digital Service Provider

The changed legal framework leads to more regulation in an extended scope of application

This whitepaper attempts to shed light on a blind spot that exists in much of the digital economy and which has also been easy to overlook in the Gaia-X environment and its Federation Services: Are the operating bases of the company's own platform and its services to be classified as so-called "critical infrastructure" and therefore subject to State regulation? Which criteria and standards are used to arrive at such a classification? Which legal obligations and regulatory measures result if the operation of a service is considered "critical"? Which technical and organisational standards with regard to information security must then be observed?

Are we a "critical infrastructure" and if so, what are the consequences?

In order to answer these core questions of critical infrastructures adequately, both their operation and the regulation to which they are subject, a broad understanding and in-depth knowledge are required. One must first become familiar with the fact that the framework is constantly being updated and changed. With the current developments of the legal basis and the resulting regulations for its implementation, both the circle of addressees is drawn wider than before and the number of companies operating within the affected sectors is increased many times over. This whitepaper reflects the status of the legislation from the beginning of March 2023; it therefore offers a reliable overview of the German and European legal frameworks in force at this point in time.

Constant changes in legislation

Current version March 2023

When analysing the rules and evaluating their applicability to the stakeholders in the Gaia-X context, two perspectives must be kept in mind: First, anyone who acts as a provider, or "Federator", within the Gaia-X environment may well be classified as a critical infrastructure operator (in Germany also often abbreviated to "KRITIS") themselves. Second, the issue of a service provider whose customers are themselves operators of critical infrastructure must be appreciated separately. Even though in individual cases the service provider may not be classified as a KRITIS company, evidence may have to be provided that is required as part of the proof, reporting and notification obligations and compliance with specific requirements of these customers. As an outsourcing partner of a KRITIS operator, you may have to subject yourself to rules that would not necessarily result from your own business activities without such a customer.

Case 1: Gaia-X is a critical infrastructure

Case 2: Gaia-X customers are a critical infrastructure

Side note: Financial market supervision

An example: Sector-specifically regulated companies such as credit institutions and insurance companies are subject to control by different supervisory bodies, provided they are classified as critical infrastructures. The Federal Financial Supervisory Authority (BaFin) points out that the additional burden on institutions due to the dual supervisory function should be "reduced as much as possible". Nevertheless, the approximately 90 companies in the financial sector that are currently registered with the German Federal Office for Information Security (BSI) as operators of critical infrastructure are still subject to the statutory requirements of financial market regulation under the German Banking Act (KWG), the Payment Services Supervision Act (ZAG) or the Insurance Supervision Act (VAG) and the associated supervision by BaFin (and the largest of them also by the Single European Banking Supervision Mechanism), but must also comply with the statutory requirements for operators of critical infrastructures under the KRITIS regulation (KritisV) of the BSI. The service providers who operate parts of their critical infrastructure for financial companies may therefore be required to allow BaFin to carry out checks directly on them and to issue orders, provided that key activities for the banks are outsourced to them.

Double regulation

Third-party service providers are also subject to supervision

There are similar intertwinings of requirements and official supervision in the energy sector and for telecommunications operators - for them the two relevant supervisory authorities would be the Federal Network Agency (BNetzA) and the BSI. We will outline the mechanisms of multilateral control later, but what is most important is that in case of doubt, every institution that is authorised to supervise operators of critical infrastructures will also take action against those who merely work as third-party service providers for the regulated sectors.

Is Gaia-X a critical infrastructure?

It is also necessary to examine how the regulatory or legal framework affects Gaia-X itself as the operator of a critical infrastructure. Whether Gaia-X or the stakeholders of the platform can actually be KRITIS companies is still up for debate. At the latest under the stipulations of the European legislation that will come into force at the beginning of 2023, it can be assumed that large parts of the Gaia-X environment and the Federation Services can at least potentially be classified as a critical infrastructure.

Obligations for KRITIS operators using external services

Finally, the requirements for operators of critical infrastructures are also dealt with, for example if they use Gaia-X services. In all Member States of the European Union, there are uniform obligations on how external service providers are to be integrated into the risk management of the KRITIS operators in order to meet the information security requirements of their critical infrastructure. Such obligations must be backed up by contractual principles and control powers that go far beyond the usual service level agreements between service providers and customers.

Requirements, legal bases and industry standards

This white paper cannot compile a complete matrix of sector-specific security standards, reporting and notification requirements that govern companies in each sector. It does, however, unfold a broad overview of the essential requirements for operating a critical infrastructure in compliance with regulations. We limit ourselves to a description of the legal basis and relevant industry standards that are used in the respective context. We provide an outlook on specific suggestions that arise in an individual case assessment and which could be recommended for implementation. Without a detailed consideration of the context, it is almost impossible to formulate clearly the right demands on the services and the implementation of the requirements for their information security. This also applies to both sides, both the Federators and the Gaia-X infrastructure as well as the users, who, as operators of a critical infrastructure, ensure compliance with their own specifications. All that is necessary here is the insight that specific measures are also indispensable in the Gaia-X environment for conformity with laws and regulations for critical infrastructures.

Contextualisation for the Gaia-X environment

Critical infrastructures in German legislation and regulation

Critical infrastructures are facilities of general interest that are of particular importance for public life and the disruption or failure of which could significantly affect the basic needs of people or even have catastrophic consequences. The abstract term describes the entirety of all technical and organisational systems, without the functioning of which the continued existence of society would be endangered. The focus is on energy supply, transport and traffic, state and administration, nutrition, water, health, media and culture, and last but not least the digital infrastructure: Information technology and telecommunications.

Definition of "critical infrastructre": Facilities of general interest

Until the 1990s, such infrastructures were predominantly run by the State. However, their privatisation has not relieved the State of its responsibility for infrastructure, which in Germany results from the Basic Law (Article 20 para. 1 Basic Law (GG). The welfare state principle, which is anchored there, is the basis of regulatory responsibility wherever the public sector has withdrawn from the actual service of general interest. For the critical infrastructures, this responsibility results in the regulatory task of imposing minimum requirements on the operators of mostly privately organised services in order to guarantee security of supply even where the State does not act directly itself.

Responsibility of the State for the regulation of critical infrastructure

Self-regulation of the operators of critical infrastructures

Ever since there has been talk of critical infrastructure, the question of whether utility companies or public sector institutions belong to this group of particular importance for public life has repeatedly been answered anew and often differently. Whether a company or government agency provides critical infrastructure is just as difficult to determine as assessing what level of importance to the maintenance of public life the institution has. The first approach after introducing the concept of critical infrastructure into the debate on threats and risks to the public in Germany was initially to have both questions answered by the operators of a presumed critical infrastructure themselves: Both the importance of a service for the security of supply and the extent of its criticality were assessed by the institutions themselves.

Self-assessment by the operator is the basis for the "classification as a "critical infrastructure

This freely agreed evaluation of criticality was replaced by the introduction of an umbrella strategy for information security by the Federal government, under the leadership of the Ministry of the Interior and with technical support from the BSI. The so-called "Implementation Plan for Critical Infrastructures" (UP KRITIS) resulted from this national information security strategy published in 2005 under the title "National Plan for the Protection of Information Infrastructures" (NPSI). Although the NPSI was replaced in 2011 by the Federal government's more networked cyber security strategy, the UP KRITIS continues to exist as a public-private partnership for self-regulation with over 800 organisations participating today. The "Implementation Plan for the Federal Administration" (UP Bund), which was launched at the same time, is still in use and is constantly being updated. The UP Bund regulates, for example, the requirements for the use of information technology, the connections to the federal networks and other technical framework conditions for data traffic from administrations, but primarily requires formal and organisational basics such as the introduction of information security management systems (ISMS) in all Federal institutions, reporting requirements and much more.

KRITIS imple-mentation plan

PPP for self-regulation

Federal implementtion plan

The committee work of the member institutions in UP KRITIS and UP Bund will continue regardless of the legal basis for classification as an operator of critical infrastructures that has now been established and the mandatory regulations. UP KRITIS maintains a number of industry and topic working groups whose members jointly develop and agree on concepts and recommendations for information security for KRITIS operators. Working groups for the KRITIS sectors from energy to telecommunications and the Internet stand alongside those for topics such as the statutory audits and standards or joint exercises for crisis situations. A separate

Joint development of recommendations for action and concepts

industry working group for data centres and hosting was also established. For example, model contracts - service level agreements - for suppliers of hardware and software for use in critical infrastructures are created for the member companies in UP KRITIS in order to anchor a high level of security in the components used. Since there is no legal requirement for the minimum standard for such components, a contractual agreement is the only way to hold suppliers to the catalogue of requirements and information security best practices. UP KRITIS also represents companies on the German government's National Cyber Security Council and is therefore an active participant in setting the strategic course for protecting information security for the State and society.

The contractual basis creates binding security level

Legislation with relevance for critical infrastructures

The legal framework for operators of critical infrastructures is laid down in a series of individual laws and regulations that have been developed, constantly expanded, specified and updated over the past twenty years. The main focus is on the aspect of protecting the networks and information systems needed to maintain the operation of critical infrastructures. Very close in time to each other, Germany and the European Union have established binding measures to ensure a high level of security in information technology and networks used to operate critical infrastructures.

Legislative determinations in Germany and the European Union in the same period of time

The legal framework currently valid in Germany for operators of critical infrastructure is made up of the following individual laws:

German legal framework

- BSI Act (BSIG)
- Telecommunications Act (TKG) and Telemedia Act (TMG)
- Energy Industry Act (EnWG) and Atomic Energy Act (AtG)
- Book V of the Social Code (SGB V)

The most important regulation derived from the BSIG is the KRITIS regulation (BSI-KritisV from 2016, amended in 2017 and 2021). It is decisive for the classification of critical infrastructure operators above defined thresholds, and sets the framework for implementing the requirements of the law.

KRITIS regulation

The term "IT Security Act" (IT-SiG), which is often used as a brand name in public discussion ("IT-SiG", "IT-SiG 2.0"), refers to article laws that are a collection of new or amended paragraphs of several laws - there is no independent specialist law for information security under this title.

IT-SiG

German legislation is closely intertwined with the European legal framework, which mainly consists of two guideline documents:

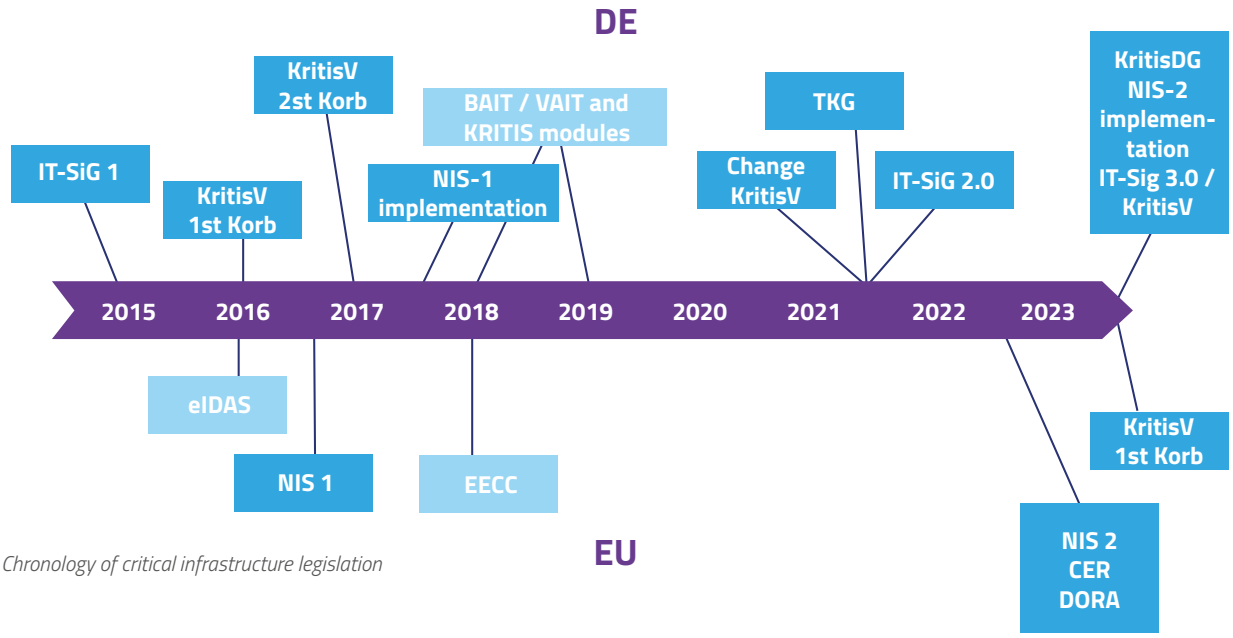
European legal framework

- NIS - Network and Information Security (NIS 1 2016, NIS 2 2022)
- CER - Critical Entities Resilience (2022; replaces the previous directive ECI - European Critical Infrastructures from 2008)

Other legally binding requirements of the European Union include directives and regulations that affect sector-specific or other information security concerns.

- DORA - Digital Operational Resilience Act (Directive and regulation came into force in 2022; regulates digital operational resilience in the financial sector)

- CRA - Cyber Resilience Act (still in process, adoption expected in 2023; regulates information security requirements for IT products, excluding digital services)



Chronology of critical infrastructure legislation

Chronology of the legal framework in Germany and Europe

BSI Act and KRITIS Regulation (KritisV)

Within the German legal framework, the BSI Act is primarily decisive for the information security of critical infrastructures. The key points on a future "KRITIS umbrella law" (KritisDG), which were approved by the cabinet in December 2022, point out that there is not yet a "cross-sector and cross-hazard" law that addresses the inconsistent or missing regulation of the physical protection of critical infrastructure. So while the announced KritisDG targets the entire system for the first time, the cyber security of critical infrastructures is already comprehensively regulated in the BSIG.

§§ 8a and 8b BSIG

According to the BSIG, anyone who is identified as an operator of critical infrastructure must firstly have appropriate state-of-the-art security precautions ready (§ 8a para. 1 BSIG) and secondly fulfil regular obligations to provide evidence (according to § 8a para. 3 BSIG). As with data protection in Article 32 of the GDPR or the Federal Data Protection Act (BDSG, § 71), the BSIG also refrains from specifying what exactly is to be understood by the respective state of the art to be taken into account. Leaving open the benchmark for compliance with technical requirements in this way allows ongoing adjustments to the development of risks and their treatment, which would rather be restricted by specifying specific measures. "State of the art" has been established as an indeterminate legal term for decades and has also been accepted by the Federal Constitutional Court since 1978. What is meant is that complete security is not possible, but therefore the application of technologies as a whole cannot be dispensed with: Provided that measures appropriate to the "state of the art" are taken to secure information technology, the consequences of incidents occurring despite appropriate measures are "inescapable and insofar to be borne as socially adequate burdens".

Statutory requirements: State of the art and obligation to provide evidence

Risk handling is continuously adjusted

Even though the dynamic orientation towards the state of the art has therefore proven its worth and serves as a guideline for proving adequate security precautions as a rule, the BSIG allows for specific measures to be formulated in the form of industry standards. Compliance with these catalogues of measures is automatically considered state of the art for industries that have such standards.

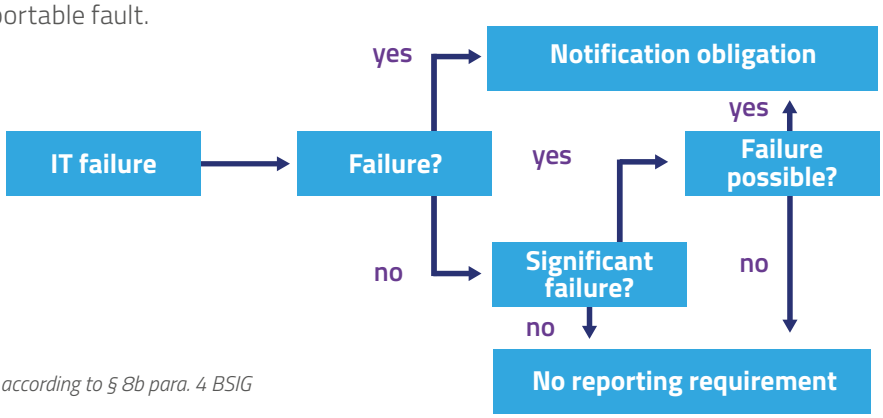
Additional specific measures in industry standards

The obligation to use an attack detection system was subsequently included in the BSIG and the Energy Industry Act (EnWG) in the course of the IT Security Act 2.0 (§ 8a para. 1a BSIG, § 11 para. 1f EnWG). It will apply to all operators of critical infrastructures from 1 May 2023, and its implementation must be verified as part of the biennial audits pursuant to § 8a.

Attack detection as a new obligation

All operators of critical infrastructures are obliged to designate a contact point through which they must be reachable at all times. The reporting of security incidents to the BSI is mandatory according to § 8b para. 4 BSIG. A distinction is made between "usual" and "significant" disruptions, which in the former case are reportable if they have caused a failure or a significant impairment of the critical infrastructure. On the other hand, a disturbance that is considered "significant" does not have to have any effects at all: The obligation to report already applies if there is even the possibility that the functioning of a critical service provided is threatened. This is where the BSIG differs from the NIS Directive, which only considers failures that have already occurred as a reportable fault.

Registration and reporting obligation



Reporting according to § 8b para. 4 BSIG

Procedure for reporting security incidents

A deadline is not set for the report according to § 8b para. 4, but it should be done "immediately", i.e. as soon as the operator of the critical infrastructure who is obliged to report has a sufficiently clear picture of the situation to make a meaningful report.

§ 8c: Specific requirements for Digital Service Providers

For "telemedia offered on a business basis", the first IT Security Act in the Telemedia Act (TMG old until 2021, § 13 para. 7) had already anchored the obligation in 2015 to ensure through technical and organisational precautions that no unauthorised access to systems is possible and that they are secured against data protection violations and disruptions through external attacks.

Digital Service Providers are obliged

With the implementation of the NIS Directive of 2016 in national law, an amendment to the BSIG became necessary, which stipulates special requirements for "Digital Service Providers", i.e. the providers of digital services (ADD), with the insertion of a new § 8c. According to § 2 para. 11 BSIG, this extension only includes companies that operate

Special forms of regulation for search engines, clouds and trading platforms

- Online search engines
- Cloud computing services
- Online market places

However, the Digital Service Providers (ADD) are not subject to ex-ante regulation like the KRITIS institutions, so they do not have to provide the BSI with regular reports on the status of their security measures. Registration is also not necessary. However, Digital Service Providers (ADD) are obliged to report security incidents with

significant effects to the BSI - the criteria for when this case occurs are defined in the NIS according to the duration of the failures, the number of people affected and the individual damage they incur.

Undertakings of special public interest (UBI)

"UBI": additional sectors and special companies in the regulation

The "undertakings in special public interest" (UBI) defined in § 2 para. 14 BSIG are not included in KRITIS in the narrower sense, which correspond to the "important facilities" of the NIS-2 Directive. They are divided into three categories:

UBI category	Affected companies
UBI 1 (AWV-UBI)	(Armaments) companies according to § 60 Foreign Trade Ordinance (AWV), i.e. manufacturers of weapons, ammunition and other armaments, but also IT security products "for processing State classified information".
UBI 2 (value-added UBI)	The companies that are among the largest in Germany and their key suppliers.
UBI 3 (Incident UBI)	Operators covered by the Major Incidents Ordinance (Störfallverordnung, StöV) under the Federal Immission Control Act, where hazardous substances are present in quantities above a threshold specified therein.

Different scope and depth of regulation with regard to KRITIS

Different deadlines apply to the registration as a UBI, the reporting obligations and the procedure for self-declarations on IT security according to § 8f BSIG para. 1, depending on the category: Companies in the UBI 1 category must register with the BSI from 1 May 2023 and then submit a "self-declaration" every two years, in which not only contact details and contact persons are requested: All certifications acquired and audits carried out in the period of the last two years must be stated and they must explain how they ensure adequate protection of their IT systems and components and the processes to be particularly protected. There is no obligation to register for incident UBI of category UBI 3, but they are allowed to register voluntarily with the BSI. The obligation to report security incidents results from the Major Incidents Ordinance and has been in force since 1 November 2021. For companies in category UBI 2, the obligations to register and self-declare do not apply until two years after the entry into force of the legal ordinance establishing their membership of the largest companies in Germany. It will be drawn up in a manner comparable to the so-called Top 100 Panel of the Monopolies Commission. In addition, it must define the criteria for assigning materiality to the suppliers of the largest companies and is currently not yet available.

Minimum standards for the Federal administration and other public bodies

Minimum standards to be met by public bodies

Minimum standards are used to determine which information security measures are to be applied by Federal agencies, public bodies and foundations or public companies as operators of critical infrastructures. Their compliance will be verified within the framework of the tests according to § 8a. Minimum standards are guidelines published by the BSI for those institutions to which the BSI itself can issue specifications pursuant to § 8 para. 1 BSIG, but to which affected companies or other authorities can also orient themselves.

Providing evidence and reporting obligation

This overview serves to complete the providing evidence and reporting obligations, which deviate from the system according to § 8a (evidence) and § 8b (reporting):

Additional or different obligations for evidence and reports

Sector	Obligation to provide evidence	Notification obligation
Energy	Certification according to the IT security catalogue according to § 11 para. 1b Energy Industry Act (EnWG) and regular reviews by the BNetzA (facilities according to § 7 Atomic Energy Act (AtG) are regulated differently)	Reporting of security incidents to the BSI, which must report "without delay" to the BNetzA (or, in the case of nuclear facilities, to a reporting chain for reactor safety).
Telecommunications	Security concept according to § 166 TKG and regular reviews by the BNetzA	In the past, security incidents only had to be reported to the BNetzA, but since NIS implementation they have had to be reported to both the BSI and the BNetzA.
Health	Security reports on components and services are submitted by the telematic infrastructure operators to the BSI for review.	Operators report security incidents to gematik, which in turn reports them to the BSI.
Financial	Annual audit also serves as evidence according to § 8a para. 3	Report to the BaFin (reporting chain for European supervision) and to the BSI
Digital Service Providers (ADD)	None, but ex-post supervision by the BSI	Reporting of security incidents to the BSI

KritisV for the implementation of the methodology and specifications for identification

Three-stage methodology for the identification of critical infrastructure in the KRITIS Regulation

In order to determine the criticality of an infrastructure, § 10 para. 1 BSIG prescribes a methodology based on three procedural steps. The application of this methodology is the subject of the KritisV, which came into force for the first time in 2015 and in a greatly expanded version in 2021. In preparing the specifications, the BSI practised "extensive participation" of Federal departments and representatives of the affected industries beyond the normal framework of public and association hearings in order to pursue a "cooperative approach" appropriate to the complexity of the provisions. The KritisV specifies the requirements of the BSIG by defining the threshold values and the facilities for the individual KRITIS sectors, on the basis of which facility operators can be identified as critical infrastructure within the meaning of the legal definition. With the 2021 amendment to the KritisV, thresholds have been lowered and facility categories have been added, which has expanded the group of identified critical infrastructure operators.

IT Security Act (IT-SiG 2.0)

IT Security Act and NIS Directive as first specific legal foundations

The first IT-SiG, which came into force in 2015, was an article law that put the core objectives of information security and the protection of IT systems and services on a specific legal basis for the first time in the German

legal area. The timing of the legislation is remarkable in that the Federal Government did not wait until the European Union's first NIS Directive was adopted, but implemented the binding measures contained in the NIS draft in anticipation. Gaps for the final enactment of the NIS were closed in 2017. In particular, the new category of Digital Service Providers (ADD) was one of the changes that were taken into account in the NIS Implementation Act.

IT-SiG 2.0: More obligations for more companies, stricter requirements, more supervisory powers

The "Second Law to Increase the Security of Information Technology Systems" (IT-SiG 2.0), which has been in force since May 2021, put the previous regulation of KRITIS operators on a much broader basis. The Article Law contains amendments to the BSIG, EnWG, TKG, AWV and SGB X that, in summary, impose more obligations on a larger circle of affected companies, while at the same time significantly increasing the requirements for their information security and granting more powers to the supervisory authorities. In anticipation of changes in the European directives NIS 2 and CER, measures are now mandatory and can be demanded from May 2023: Systems for attack detection and their evaluation, organisation and control for security incidents, regular penetration tests and vulnerability management.

Sector expansion and new UBI categories

In addition to the newly introduced category in § 2 para. 14 sentence 1 no. 2 BSIG, the UBI, already explained in the section on the BSIG, the main addition in the IT-SiG 2.0 is the expansion of the KRITIS sectors to include municipal waste management. While the legal changes have been completed, the affected sectors are still waiting for the definitive specifications that are to be made as part of a planned KritisV amendment and other statutory regulations.

Further laws

Telecommunications Act (TKG)

Telecommunications networks and services are subject to their own legal definition outside the BSIG

For the operators of public telecommunications networks or services, the special security requirements and the obligation to provide evidence pursuant to § 8a para. 1 BSIG do not exceptionally apply, even if they are classified as critical infrastructure. Telecommunications network and service operators are subject to the TKG insofar as facilities serve the operation of telecommunications networks or the provision of telecommunications services. However, not every KRITIS facility they operate falls under this exemption: Hosting services that a telecommunications company also offers would continue to be treated according to § 8a para. 1 BSIG.

Stricter and clearly defined specifications

The provisions of the TKG on compliance with information security requirements are often more stringent and, above all, more clearly defined. We describe the security requirements in detail below, so they are only mentioned briefly here: The TKG contains explicit regulations for information security management and technical specifications up to the certification of critical components.

Energy Industry Act (EnWG)

Energy suppliers with a specific safety catalogue

§ 11 para. 1a EnWG requires "appropriate protection against threats to telecommunications and electronic data processing systems that are necessary for secure network operation." To this end, a catalogue of security requirements will be drawn up by the Federal Network Agency in consultation with the BSI. The difference to the requirements for other KRITIS sectors, which are obliged to comply with the "state of the art" according to § 8a para. 1 sentence 2 BSIG, are the specific measures that the catalogue prescribes: If they are implemented and proven, the protection is considered adequate.

Social Security Code Book V (SGB V)

The fifth book of the Social Security Code (SGB V) is decisive for the health sector. Since 1 January 2022, according to § 75c SGB V, all hospitals - not just those that are part of the critical infrastructure - have been obliged to "take reasonable precautions, in accordance with the state of the art, to prevent disruptions to their information technology systems that are relevant to the functioning of the respective hospital and the security of the patient information processed". As the state of the art is constantly changing, the law also stipulates that the systems used must be adapted "at the latest every two years". The hospitals are to orientate themselves on the industry-specific security standards (B3S), which are released by the BSI. There are two such B3S for the healthcare sector, in addition to the one for information technology security for healthcare in hospitals, another one for pharmaceutical manufacturers.

Sector-specific safety standards for hospitals

For the area of the critical infrastructure for network services in the health sector, § 291b of SGB V regulates the reporting and providing evidence obligations of the so-called telematics infrastructure, which is operated by the Gesellschaft für Telematik (gematik).

Deviating legal basis for health telematics

European legal framework

Network and Information Security (NIS) 2

With the Network and Information Security (NIS) Directive, the European Union had defined the security obligations for operators of critical infrastructures across Europe for the first time in 2016. Above all, the procedure for identifying critical infrastructure in Germany, which was established within the framework of the KritisV and its specific threshold values for the criticality of the services, was shaped by the system of the NIS.

Systematically similar to the legal basis in Germany

Roughly simplified, there is a correlation between the NIS 2 "essential entities" and the German KRITIS classifications, while the "important entities" correlate with the German UBI. In the future, like UBI, Digital Service Providers (ADD) will at least be absorbed by the operators of important services, they will no longer be considered separately.

New standard: essential and important entities

In the preparation of the implementation into German law, which must take place by 17 October 2024 at the latest, a significant difference to the KritisV is immediately apparent: According to the newly introduced "size-cap rule", all operators will be classified from the size of a medium-sized company, measured solely by the number of employees (more than 50) and turnover (annual turnover/total assets greater than 10 million euros) and therefore no longer on the basis of threshold values as laid out in the KRITIS Regulation. The Federal Statistical Office estimates that the number of "essential entities" will increase approximately sixfold compared to the institutions recorded under the previous NIS guideline.

Company size is a decisive criterion

Although the letter of NIS 2 no longer stipulates that an identification process be carried out as under NIS 1 and BSIG or KritisV, as things stand, Germany intends to retain the previous risk-based classification of critical infrastructure operators for companies requiring special protection. If it stays that way, the categories of institutions will change according to the BSIG:

Previous KRITIS classifications are to be continued

Category	Charakterisierung
KRITIS	Operators of critical infrastructures, identified according to the previous KritisV methodology.
Federal administration	Federal agencies and public institutions
Essential entities	Coverage of the KRITIS sectors according to the German reading, some of which are divided into different sub-sectors, plus some additional ones such as ground infrastructure for space-based services. They are identified exclusively by company size.
Important entities	Postal and courier services, production of various goods, some of which are already included in the KritisV. UBI and Digital Service Providers (ADD) are merged into this category.

In line with the General Data Protection Regulation (GDPR), the fine framework for information security is no longer set only in absolute amounts, but depends on the turnover of the company that violates the rules. Unlike in data protection, however, a distinction is made between essential and important facilities for fines for violations of the NIS 2 requirements: The former will be sanctioned with a maximum of ten million or two per cent of global annual turnover, the latter with seven million or 1.4 per cent. Although this is comparable to the maximum amounts under IT-SiG 2.0 (up to now, fines of up to 20 million euros can already be imposed if companies refuse to implement a security defect remedy ordered by the BSI), for large companies, the turnover-based determination of fines can reach considerably higher sums than before. The managerial responsibility stipulated for the first time in the directive also means that they can be held personally liable for failures to comply with statutory security measures. The sanctions regime for violations of the information security rules is therefore taking a direction that promises a similarly dynamic implementation of the regulatory requirements in European companies as was the case in 2018 with the application of the GDPR.

Significantly stricter catalogue of fines

Personal liability of directors

Supervision and enforcement

What is new compared to NIS 1 is a three-stage reporting procedure: An early warning of an incident should be reported to the responsible supervisory authorities within 24 hours, the comprehensive security report should be submitted before the end of 72 hours - within a period chosen analogous to data protection incidents under the GDPR - and the report on the incident and resolution should be submitted no later than one month after this message.

New reporting procedure

Even after the restructuring of the scope, the requirements for "important entities" will be less stringent than for actual KRITIS operators or the "essential entities". Essential entities are continuously checked by the competent authority (usually the BSI in Germany) according to NIS 2 (by requesting information, on-site inspections, regular or ad hoc inspections); in the case of important entities, this only occurs on the basis of a reasonable suspicion.

Tiered requirements and test methods

The catalogue of minimum security requirements according to Article 21 para. 1 of the NIS 2 will be included in the BSIG in the future, but differentiated according to categories. Among other things, NIS 2 has adopted the security requirements of the European Code for Electronic Communications (EECC Directive), whose own implementation in national law should have taken place as early as 2020, but is delayed. The eIDAS (electronic IDentification, Authentication and trust Services) regulation was also transferred to NIS 2. EECC and eIDAS are therefore not referenced separately in this paper, but are mentioned where they remain important as influencing factors.

Harmonisation with previous EU directives

Directive on Critical Infrastructure Resilience: Critical Entities Resilience (CER) Directive

When it came into force in 2008, the predecessor directive "European Critical Infrastructures" (ECI) was the very first binding European regulation in the field of critical infrastructures, which until then had been subject exclusively to national rules or not regulated at all. Two interesting changes compared to the ECI can be observed in the CER: There is no longer talk of "critical infrastructure", but "critical entities", and it is no longer about their protection ("protection"), rather their fail-safety characteristics ("resilience"). There is more to this than just a changed choice of words: Maintaining operations (in the sense of "Business continuity management", BCM standardised according to ISO 22301) pursues a different objective than the traditional approach of avoiding incidents. The focus is therefore moving away from a Major Incidents Ordinance, which has to deal with the consequences of failures, to a systematic consideration of regular business processes and how they can be continuously operated even under threat scenarios.

Resilience as a criterion for critical infrastructures

Continuation of business processes instead of incident analysis

All critical infrastructure operators identified according to the criteria of the CER automatically also fall under the "essential facilities" of NIS 2. In Germany, this identification for both the physical and digital protection of critical infrastructures is to coincide in the KRITIS umbrella law, which is currently being prepared.

CER-classified facilities are automatically the highest KRITIS level

The implementation of the directive into national law will take place in Germany within the framework of the planned KritisDG.

Digital Operational Resilience Act (DORA)

In addition to NIS 2, a regulation to strengthen information security in financial services was adopted in parallel, the "Regulation on Digital Operational Resilience in the Financial Sector": Digital Operational Resilience Act (DORA). It came into force on 16 January 2023 and will be applied from 17 January 2025 after a two-year transition period. Until then, the European supervisory authorities will draw up guidelines and Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS). The requirements specified in DORA apply to the entire financial industry, from insurance companies to credit and payment institutions to rating agencies, cryptocurrency platforms or specialised services such as trade repositories. When it comes to the question of which of these obligations will be relevant depending on the size of the company, DORA takes a deeper approach than NIS 2, because the same rules apply to small companies (annual turnover/total assets of 2 to 10 million euros, 10-50 employees) as to medium-sized ones, only not to micro-enterprises below these limits.

Special regulation for the financial sector

Scope also includes smaller companies

DORA requirements also apply to all third-party digital infrastructure service providers acting on behalf of these financial entities: Data centres, IT and telecommunications infrastructure, cloud operators and other providers of information and communication technology for the industry. Financial companies are required by the regulation to integrate these third parties into their risk management and to ensure that contractual arrangements with them based on an "ICT Third Party Risk Strategy" meet the relevant information security requirements. In any case, however, this also includes access, inspection and audit rights with the third parties.

Third-party service providers explicitly regulated

"Third-party ICT service providers" are defined as "digital and data services that are made available to one or more internal or external users on a permanent basis via ICT systems" (Article 3 sentence 1 no. 21): The providers of the Federation Services within GXFS therefore belong to the group of obligated parties under this regulation if they provide services for financial companies. The far-reaching monitoring and integration obligations of third-party providers according to DORA are to be specified even further by the time of application in 2025.

GXFS is therefore in the scope of application when used by financial industry

Cyber Resilience Act (CRA)

The Cyber Resilience Act introduces rules for "products with digital components" - IT products - that must be observed in order to ensure the security of hardware and software. It is aimed at manufacturers of devices and applications that are only allowed to produce and market products whose implementation of the CRA requirements can be proven. To confirm this conformity, they are CE marked by the European Committee for Electrotechnical Standardisation (CENELEC).

Approval rules for IT products

Three security categories are introduced for the evaluation of IT products (standard, critical class I and II), which are assigned according to criteria such as functionality, intended use and possible effects of security problems:

Security categories depending on the intended use

Security category	Examples of products
Standard	Text and image processing software, smart speakers, hard drives, games
Critical class I	Browsers, identity and password managers, virus protection programs, network interfaces, firewalls and intrusion detection, microcontrollers such as CNC controllers, SCADA etc.
Critical class II	Operating systems for servers, desktops and mobile devices; virtualisation; CPUs; public key infrastructure, plus some products from Critical class I but for industrial use (routers/switches, firewall/intrusion detection, microcontrollers.

Assessment of conformity usually by the manufacturers

How they prove the security of their products is, with exceptions, left to the manufacturers. Conformity assessment procedures required in the CRA, depending on the safety categories, range from self-assessment by manufacturers to third-party testing. Mandatory conformity assessment by independent third parties exists in the CRA only for the top Critical class II.

The formal agreement in the trilogue between the European Commission, the Council and the Parliament and the finalisation of the legislative process for the CRA is expected in the course of 2023.

In preparation: KRITIS umbrella law (KritisDG)

For the physical protection of critical infrastructures, there are a large number of individual provisions in specialised laws in which requirements for operators or powers of the authorities are already regulated. These previous individual regulations, supplemented by indirectly effective regulations on the use of and compliance with norms and standards (e.g. in construction technology), explicitly refer to critical infrastructure. However, since the interdependencies and mutual dependencies of different sectors are not sufficiently taken into account in the individual regulations, the area of physical protection is now to be consolidated and expanded in a cross-departmental and cross-sectoral law. Specifically, analogous to the European initiative of the Critical Entities Resilience Directive, a bracket is to be drawn for all requirements that are not directly related to cyber security but are essential for the security of supply of critical infrastructures overall.

Physical protection is so far hardly established or only in individual regulations

New law aims to close the gap between cyber and physical security

With the KritisDG, which should already integrate the requirements of the CER, there will be mandatory protection standards for physical security for the first time. Another new feature will be a reporting system to be introduced for this purpose, which does not yet exist in this form with regard to physical security incidents. However, many of the measures envisaged are not new requirements for operators because, for example, from an information security perspective, they have long been practised in conducting their own risk management and carrying out risk analyses and assessments. What the requirements for technical and organisational measures for facilities will look like in terms of their physical protection is not yet foreseeable, but here, too, it is more likely to be refined rather than to set completely new standards. The key points paper on the draft KRITIS umbrella law mentions, for example, "the erection of fences and barriers, the use of detection devices, access controls, security checks, but also the provision of redundancies and the diversification of supply chains" as suitable measures. In future, the Federal Office of Civil Protection and Disaster Assistance (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK) will monitor the depth of regulation and minimum standards to be complied with here, which will be considerably expanded for this purpose and - this is also new - will function as a central reporting office for incidents related to the physical security of critical infrastructures.

Protection standards and reporting system

The BBK will be the supervisory authority

The draft bill for the KritisDG and its introduction into the legislative process is expected in the course of 2023.

Criteria and requirements for critical infrastructure

Definition of terms

The KritisV specifies the definition of critical infrastructure with regard to the components to be considered: "Facilities" are understood in the Ordinance to mean anything that is an operating site, machinery, equipment or software and services that are "necessary for the provision of a critical service". "Critical services" are all services that are necessary to supply the general public, "whose failure or impairment would lead to significant supply bottlenecks or endanger public safety". The term facility is important because not every operator is subject to regulation, but only those who operate a facility for the provision of their critical services, all of which are explicitly named in the KritisV and provided with threshold values.

KRITIS are facilities for the provision of critical services

To distinguish this from the concept of system relevance, it should be noted that every component of the overall system for ensuring the supply of vital goods and services to the population is a systemically relevant contribution. It may or may not be classified as critical infrastructure. The BBK puts it in a nutshell: "According to this, while all critical infrastructure is also systemically important at the same time, not all systemically important facilities are also critical."

Critical or system relevant?

Methodology for identification (according to § 10 para. 1 sentence 1 BSIG)

Identification as a critical infrastructure operator is still based to a certain extent on a self-assessment by the operators. With its specification of the framework conditions and the specific standards for classification, the KritisV transfers this self-regulating element into a systematic assessment and designation of critical infrastructures.

Systematic identification

In accordance with § 10 para. 1 sentence 1 BSIG, the KritisV uses a three-stage method to identify the operators of critical infrastructures. Whether a company has to subject itself to the KRITIS regulation is first determined according to a catalogue of criteria that determines for each of the eight sectors which of their services are to be classified as critical services due to their importance. This determination is the prerequisite for the second step in which the facilities operated to provide these services can be assigned to sector-specific facility categories - if the facilities are not included in the categories in the Annex to KritisV, the services are not to be

1st step: Sector-specific criteria

2nd step: Facility categories

classified as critical infrastructure. In the last step, if the operation of a critical infrastructure facility is involved, the supply level is considered: At the end of the process of identification according to this methodology, only those companies whose facility operations exceed the threshold values defined in the annexes of the KritisV are subject to regulation.

3rd step: Supply level

Identification of critical services by importance

In paragraphs 2 to 8 of the KritisV, a list is drawn up for each sector of the services to be considered critical because of their importance for services of general interest.

Critical services

Sector	Critical services
Energy	Electricity and gas, fuel and heating oil and district heating supply
Water	Trinkwasserversorgung und Abwasserbeseitigung
Nutrition	Food supply including production, processing and trade
Information technology and telecommunications	Voice and data transmission as well as data storage and processing including housing, hosting and trust services
Health	Inpatient medical care, supply of "directly life-sustaining medical devices" and prescription drugs, blood and plasma concentrates, and laboratory diagnostics
Finance and insurance	Cash supply, payment transactions (card-based and conventional), clearing of transactions with securities and derivatives, insurance services (only primary insurers, no reinsurers)
Transport and traffic	Passenger and freight transport with all modes of transport (air, rail, road, inland and maritime), but excluding motorised private transport

Determining categories of facilities to provide these services

For each of the sectors mentioned, the KritisV adds a separate annex defining the categories of facilities operated to provide the critical services. Certain categories already contain a pick-up threshold that must at least be reached in order to be considered an "facility" within the meaning of the regulation. For data centres, for example, this means having at least one enclosed room with at least ten racks. If there is a close spatial or operational connection, several facilities can be evaluated as one and the entire facility can be classified as critical infrastructure if the individual facilities achieve a critical level of supply in the sum of their services.

Facility categories with minimum sizes

Sector-specific criteria, facility categories and thresholds

According to the KritisV methodology, individual facilities to be assessed as critical are derived from the categories according to the degree of supply and importance for the general public. In order to determine from the facility categories of all sectors which of these are to be assessed as critical, parameters are used with which threshold values are determined using specific calculation formulas for each sector. The basis for the calculation is mainly the assumption that a critical level of supply of significance for the general public is reached when the security of supply for 500,000 people depends on it. For the individual facility categories,

Parameters for critical supply level as basis for calculation

this must be converted into performance indicators that are precisely defined for each sector. One example is the information technology and telecommunications sector:

Example sector IT and telecom-munications

Facility category	Threshold value (output)
Access network	100,000 subscriber connections
Transmission grid	100,000 contractual partners of the respective service
Internet Exchange Nodes	100 connected Autonomous Systems (AS) on annual average
DNS resolver	100,000 contractual partners in the access network in which it is operated
Authoritative DNS servers	250,000 domains for which it is authoritative or which are delegated from the zone
Top-Level-Domain-Registry	250,000 managed/operated domains
Housing (data centre)	3.5 MW
Hosting (server farm)	10,000 physical or 15,000 virtual instances
Content delivery network	75 PB of delivered data volume per year
Trust services	500,000 qualified or 10,000 server certificates

Applicable safety standards and regulation

UP Bund 2017 and minimum standards of the BSI

minimum standards of the federal government

With the "Guidelines for Information Security in the Federal Administration", the Federal Implementation Plan 2017, minimum requirements have been defined for all departments and federal authorities, compliance with which has already been made mandatory. The legal basis followed in the IT-SiG (IT Security Act 2.0), in which the new version of § 8 para. 1 sentence 1 BSIG (Law on the Federal Office for Security in Information Technology) now obliges all

- federal agencies,
- the corporations, institutions and foundations under public law as well as their associations irrespective of their legal form at Federal level, as far as ordered by the respective competent supreme Federal authority, as well as
- public enterprises which are majority-owned by the Federal Government and which provide IT services for the Federal Administration

Example: Cloud computing use by the federal administration

to implement so-called „minimum standards", which the BSI as the competent authority drafts and publishes. One of these minimum standards regulates the security requirements for the use of cloud services by federal institutions. Among the requirements that the cloud provider must fulfil is the submission of a test report according to the „Cloud Computing Compliance Criteria Catalogue" (C5) - not an obligatory certification as according to the IT-Grundschutz Compendium of the BSI, but at least a test certificate by an independent

auditor, which must be available. Without a C5 attestation, the authority may not consider the provider when procuring cloud services.

Parameters for critical supply level as basis for calculation

According to Article 3 sentence 1 (d) of NIS 2, facilities of the „public administration of the central government" or - measured on the basis of the risk of a disruption for the security of supply - also regional administrative facilities are declared to be critical infrastructure (or essential facilities). Thus, the information security requirements specified in the directive also apply to them.

Security requirements according to the Telecommunications Act (TKG)

Own security catalogue for the operators of telecommunication networks

While legislation is still pending in other sectors, the TKG already has clearly formulated provisions for the operators of telecommunications networks, specifically geared, for example, to the certification of critical components. The „Catalogue of Security Requirements for the Operation of Telecommunications and Data Processing Systems and for the Processing of Personal Data pursuant to § 109 of the German Telecommunications Act (TKG)" is prepared by the BNetzA in consultation with the BSI and the BfDI, and is the basis for the security concept that must be prepared by every telecommunications operator. NB: The title of the catalogue is misleading because since the amendment of the TKG in IT-SiG 2.0 2021 the references are no longer correct: The paragraphs of the TKG referenced in the security catalogue still refer to the old version since the currently valid version was adopted a year before the TKG amendment.

The security concept according to the TKG

Proof of compliance with the requirements shall be provided at least every two years by means of a review of the security concept carried out by the BNetzA (Federal Network Agency) itself. According to § 166 TKG, the security concept must document „which technical precautions or other protective measures have been taken or are planned to fulfil the (...) specified obligations (...)". Where the catalogue of security requirements only defines goals, the security concept must prove that its measures actually achieve these goals.

Critical components must be certified

The required certification of critical components before they are used for the first time in critical telecommunications infrastructures is anchored in § 165 para. 4 TKG. So far, it has only been explicitly applied to public 5G mobile networks, but there it covers the entire range of functions identified as critical and is particularly clearly defined with its own technical guideline (BSI TR-03163): Certifications of core network functions, management and orchestration of virtualised networks as well as management system security functions are carried out according to the „Common Criteria for Information Technology Security Assessment" (CC), functions of actual radio operation and network management in the Radio Access Network (RAN) according to a certification scheme called NESAS CCS-GI, and voice and data transport functions as well as IP network transitions and services outside the own facilities are tested in the Accelerated Security Certification (BSZ) procedure.

Other sectors not yet committed

Other sectors are not yet regulated to this level of detail. So far, they have had to register their critical components and present a guarantee from the manufacturer, but they have not yet been forced to certify the components. However, it can be assumed that similar catalogues of criteria and legal bases will also be developed and adopted for the other KRITIS sectors: § 2 para. 13 No. 3 BSIG provides that the critical components for all sectors are defined in law.

Security officer according to § 166 TKG

The TKG also requires, in the same paragraph as for the security concept, that every network operator in the telecommunications sector must appoint a security officer who is the point of contact for the supervisory authority, and - for providers outside the European Union who operate networks here - the designation of a responsible contact person.

IT security catalogue according to § 11 paragraph 1a EnWG (BNetzA)

Security catalogue for energy suppliers

The IT security catalogue obliges energy plant operators to implement minimum IT security standards. The core requirement is the establishment of an information security management system (ISMS) in accordance with DIN EN ISO/IEC 27001 and its certification. This regulation was tightened again in 2021 in such a way that energy suppliers and network operators can no longer refer to their certificates if they are managed by third parties, but must themselves be certified. A transition period allows to prove this certification until 31 March 2024.

Standardised according to ISO 270XX

Unlike the catalogue for the security requirements for telecommunications operators, the IT security catalogue for energy producers and network operators pursuant to § 11a para. 1a EnWG is based on the standards of the ISO 270XX family: EN ISO/IEC 27001 for the information security management system (ISMS), the implementation instructions for the ISMS of EN ISO/IEC 27002 and the supplementary information security measures for energy supply from EN ISO/IEC 27019.

MaRisk, BAIT and VAIT

Requirement catalogues for banks and insurers

For the financial sector, which is under the supervision of BaFin, there has been a separate catalogue on the „Banking Supervisory Requirements for IT" (BAIT) since 2017, and „Insurance Supervisory Requirements for IT" (VAIT) since 2019, both of which are based on the „Minimum Requirements for Risk Management" (MaRisk), but specify the legal obligations under the KWG in even greater detail. For example, in a separate chapter on IT emergency management, the BAIT set detailed requirements for the emergency and business continuation concepts and recovery plans that are abstractly required in the MaRisk.

Different legal basis

Since § 25a para. 1 sentence 3 nos. 4-5 KWG requires „an adequate staffing and technical-organisational equipment of the institution" and „the definition of an appropriate emergency management, in particular for IT systems", the supervisory authority specifies the requirements for information security itself , instead of relying on industry-specific security standards approved by the BSI, as they are used in other sectors.

Specific KRITIS rules for IT in the financial sector

In order to support the institutions of the banking and insurance industry, which are counted as critical infrastructures and are thus subject to reporting obligations to the BSI in addition to BaFin supervision, KRITIS modules were added to BAIT 2018 and VAIT 2019 respectively, which explain exactly which additional requirements are to be fulfilled in accordance with § 8a BSIG that are not congruent with those of their own supervision. The advantage of this approach is that all security requirements can be proven within the framework of the annual audit, which is obligatory for credit institutions - and this proof then also satisfies the BSI.

Binding pentests

BAIT and VAIT also go further than comparable sets of rules: The BAIT amendment of 2021 already anticipates aspects of the DORA directive because they are fed from the same source: Both BAIT and DORA incorporate the guidelines of the European Banking Association (EBA), which were published in 2019 and have fundamentally defined the entire area of financial IT. There are even requirements for conducting penetration tests, which are not even mentioned in other sectors

Industry-specific security standards (B3S) for various KRITIS sectors.

Testing principles are developed by industry associations themselves

Industry-specific security standards (B3S) are approved as a basis for testing in order to carry out the mandatory verification tests for operators of critical infrastructures every two years in accordance with § 8a BSIG. They are usually created by the industry associations themselves and are released by the BSI upon application if the authority determines that they are suitable - suitability is always certified for a period of two years. B3S also serve as a guideline for companies that remain below the thresholds for classification as critical

infrastructure and are not obliged to comply with them. The implementation of the specific requirements for one's own industry meets with broad acceptance and improves the level of information security. However, the application varies depending on the industry: While the healthcare industry is very closely oriented towards the B3S concept, there are also B3S in the financial and telecommunications sectors, but rather for niches that are not already comprehensively covered by the more powerful instruments BAIT/VAIT or the requirements under the TKG. In the financial sector, for example, a B3S was launched that specifically targets the payment systems of statutory health insurance funds and long-term care insurers. In the IT and telecommunications sector, B3S were created for the system categories „Data centre", „Server farm" and „Content delivery network", which were not taken into account in the TKG.

Closing the gap in specifications for special categories of installations

Sectors and industries in the extended KRITIS regulation

Current status and foreseeable development

The Federal Ministry of the Interior and Community (BMI) assumes that around 29,000 operators are to be classified as essential or critical facilities if all systems falling under KritisV, NIS 2 and CER are added together. The approximately 1,250 KRITIS operators currently registered with the BSI therefore make up less than five per cent of the facilities to be taken into account in the future. In the case of the UBI, which are only gradually coming under regulation, the absolute numbers are still unclear, but a similar order of magnitude will tend to be reached. If you take the UBI 3 category as an example, around 3,000-4,000 facility operators are already subject to reporting under the StöV. It is not quite certain what number will be agreed on for the largest German companies, category UBI 2 (even if it will probably stay with the hundred top-selling companies included in the top 100 panel of the Monopolies Commission) - and how many of their key suppliers belong in the same circle, as well. On the other hand, the question of how many important facilities under NIS 2 will ultimately be subject to regulation is unresolved. The 5,000 UBIs, which can be roughly regarded as the upper limit, are certainly no longer a yardstick when it comes to counting the „important entities".

Number of critical infrastructure operators multiplied

Development at UBI similar

Important facilities according to NIS 2 unknown factor

Expansion of the sectors

With the IT-SiG 2.0, the municipal waste disposal sector was added to the scope of the BSIG in 2021. However, concrete details on the critical services, the categories of installations and threshold values have not yet been included in the KritisV. They will be included there as an additional sector in the upcoming amendment of the KritisV (draft bill expected in the first half of 2023). With the CER and NIS 2 guidelines, the number of sectors in which critical infrastructure is operated has now increased to eleven. New additions to KritisV and BSIG are above all public administration, ICT service management, space and research, as well as some sectors that are currently only partially or differently recorded in Germany.

Different coverage regarding sectors between EU Directives and KritisV

Example essential facilities

	KRITIS	NIS 2	NIS 2	Notes
Sector	x	x	x	
Energy	x	x	x	
Transport / Traffic	x	x	x	Sectors separated in NIS 2 and CER
Banking / Finance	x	x	x	Sectors separated in NIS 2 and CER
Health	x	x	x	
Drinking water / waste water	x	x	x	Sectors separated in NIS 2 and CER
Digital infrastructure		x		In KRITIS as IT and telecommunications
ICT Service Management		x	x	
Public administration	x	x	x	
Space	x	x	x	In KRITIS only partially considered in Transport
Nutrition				In NIS 2 only as an "important entity" in Food

For the complete picture, these critical sectors are supplemented by the newly added „important entities" of NIS 2, which only have a partial equivalent in KRITIS and UBI, but do not appear at all in CER.

Example of important facilities

Sector	KRITIS / UBI	NIS 2	Notes
Postal and courier services	x	x	Partially included in KRITIS sector Transport
Waste management	x	x	As municipal waste disposal KRITIS sector
Chemicals	x	x	Category UBI 3
Industry	x	x	Category UBI 2 only partially covers the sector
Digital services	x	x	Not UBI, but regulated according to TMG
Research		x	

Company size as a determining factor

Exceptions according to criticality

With the expansion of the sectors, additional industries have come into focus. The question of determining enterprise sizes was actually conclusively clarified with NIS 2: Basically, only medium and large enterprises are affected, i.e. those with more than 50 employees and an annual turnover or balance sheet total of more than 10 million euros per year. However, depending on the importance and criticality for security of supply, there are exceptions in almost all sectors and industries that can also raise small companies to the level of an essential facility. It is difficult to estimate how many companies will be affected by these mechanisms, especially if government declarations are made outside of the systematics for the special treatment of particularly critical cases.

Development of the reference framework - rigid parameters or risk-based?

When the thresholds in the KRITIS reference framework were lowered, which was reflected in the KritisV in 2021, a number of companies from different sectors had already been covered by the new criteria - the explanatory memorandum to the amendment of the IT-SiG already contained an estimate of the additional KRITIS facilities, which included, for example, around 130 power generators, seven data centres, three IXPs and so on. The significance of these thresholds, even if they were to be lowered even further, may lose momentum in the context of the NIS-2 typical assessment by company size, because the larger part of companies will no longer be subject to risk-based individual assessments, but will be identified on a blanket basis due to their importance or materiality.

Critical digital services

Digital infrastructure and related services (according to KritisV and NIS 2)

Four categories of digital services are always essential facilities

The first NIS from 2016 already considered DNS, TLD, cloud computing, trust services and IXPs. At the same time, German legislation already knew data centres and server farms. Complete consistency of definitions and scopes has not yet been achieved even after NIS 2 and CER. However, the core areas of regulation are clearly identified in terms of the nature of the services that are covered. There is a gradation of importance or criticality assigned to individual services of the digital infrastructure, starting with the four most important ones, which always belong to the essential facilities - regardless of the size of the company. This special regulation applies to:

1. Domain Name Service (DNS)
2. Registry of Top-Level Domains (TLD)
3. Internet Nodes (IXP)
4. Trust services

All four categories are therefore to be included in the critical infrastructure in the sense of essential facilities of NIS 2 even if they are operated by micro-enterprise

DNS

DNS without root server

The approximately 1,600 instances of the root zone, which represent the global backbone of the DNS, have explicitly not been included in the scope of NIS 2 following controversial negotiations with the European Commission. Of the 12 root name server operators that exist worldwide, ten are located outside of Europe, the vast majority in the USA, including government institutions: Before the directive was adopted, it was realised that it could not claim to be able to audit the US Department of Defence or NASA, for example.

TLD registry

National and European registries of top-level domains

The tasks of managing TLDs (country codes: ccTLD, generic: gTLD or new: nTLD) delegated by the Internet Corporation for Assigned Names and Numbers (ICANN) are performed by independent organisations, the TLD registries, often also called Network Information Centers (NIC). Of the generic TLDs, only .info is delegated to a European register; in the other TLDs, there are dozens of independent NICs.

Internet nodes

Exchange node for data traffic between provider networks

The network nodes of the Internet, Internet Exchange Points (IXP), are also found within the scope of NIS 2, regardless of the company size of their operators. In addition to the 20 largest, typically nationally significant facilities in the EU member states, there is a number of regional node operators (two dozen in Germany, for example), all of which are considered critical infrastructure operators. In total, over 150 IXPs are currently active in Europe, almost half of all nodes worldwide. In their data centres, they create connections between the autonomous systems (AS) of the Internet infrastructure service providers connected to the respective IXP, as an exchange platform for data traffic between the network operators. This includes not only access networks (in NIS 2 terminology: public electronic communications networks and publicly available electronic communications services), but also content delivery networks (CDNs).

Trust services

Certificate-based electronic identification and authentication

The suppliers of products and services for the creation, verification and validation of (qualified or unqualified) electronic signatures as well as certificates for the authentication of websites are of particular interest for the provision of secure tools for data communication. Since 2016, a separate regulation, the „European

Identification, Authentication and Trust Services Regulation" (eIDAS), has regulated the area of these trust services. Originally intended only for genuine third-party trust identity models, the eIDAS has opened up in the direction of so-called „self-sovereign identities" (SSI), which are anchored in the „European Self-Sovereign Identity Framework" (ESSIF). Since then, trust service providers can be integrated in an SSI network via an SSI eIDAS bridge. Whether and how the SSI broker must also be considered critical infrastructure is currently unclear.

Cloud computing services

Transparent, dynamically scalable computing power and storage applications

Cloud computing generally means the provision of resources that are integrated via a shared, mostly external computer network that is often largely integrated into the internal IT systems. A characteristic of cloud services is their scalable capacity, which can grow or shrink elastically without further contract changes, be shared across several locations and is made available transparently. Cloud services can offer all forms of data processing, from storage space and computing power to the use of software including specialised applications. The area of responsibility between the user and the provider of the cloud services can outweigh one side or the other: Infrastructure as a service (IaaS) offers a virtualised hardware framework, so to speak, in which the data processing taking place within the cloud resources and thus the responsibility for the information security of the applications lies almost entirely with the customer, while software as a service (SaaS) sees an almost 100 per cent operational and security responsibility with the cloud provider. The many operating models of cloud offerings offer proposed solutions for almost all IT problems that companies or other institutions face - if one realises that this always takes place under the premise of delegating the processing of data outside one's own area of responsibility. The resulting data protection questions, including the transmission to possibly inadmissible third countries, are not a direct subject of the classification as critical infrastructure, but they have to be answered within the framework of the information security requirements.

Data centre services

Data centres as digital infrastructure

All data centre operators are providers of infrastructure services, which were given a comprehensive definition for the first time in 2014 with their own DIN standard (DIN EN 50600). The term data centre is broadly defined in the standard because it focuses on functionality - in principle, according to DIN EN 50600, any server room can be a data centre. Within the KRITIS sector, data centres represent a separate system category, which is provided with a threshold value in Annex 4 of the KritisV based on the power consumed (previously 5 MW, now 3.5 MW after the change in 2021).

Online platforms: Search engines, marketplaces, social media

Separate categories, common regulation for platform operators

Introduced in 2018, ADD includes search engine operators, among other services, defined as online platforms. The BSI justifies the inclusion in the ADD's catalogue of connected services using the example of online marketplaces, which offer their services in bundled form to third parties in order to broker goods to buyers: „The purpose of the standard is to protect the quasi-infrastructural importance of the marketplace." With NIS 2, they are not among the essential facilities, but they are the important ones.

Content delivery networks

Decentralised cache and edge services for large data volumes

Content delivery networks (CDN) are networks of decentralised servers to ensure high availability, network topologically or geographically direct access and fast retrieval of digital content or services of all kinds: The palette ranges from social media content and video streaming to the distributed provision of software, for example. They work on behalf of providers who place their offers in the CDN at bridgeheads within or at the edges of the networks where their customers are located.

Public electronic communications networks and publicly available electronic communications services

The definitions for public electronic communications networks and publicly available electronic communications services come from the EECC, which was transferred to NIS 2: The former is an electronic communications network dedicated wholly or mainly to the provision of publicly available electronic communications services that enable the transmission of information between network termination points. The latter includes "Internet access services", interpersonal communication services (such as email) and "services consisting wholly or primarily in the transmission of signals, such as transmission services used for machine-to-machine communications and for broadcasting". All internet providers and most of the services offered in their networks fall under this broad definition, but also the classic TV cable network operators, as far as they are not included as an internet access service.

Electronic communication (everything except TC)

Relevance and consequences for Gaia-X and the Gaia-X Federation Services

The application of the KRITIS regulation to the operation in and for the Gaia-X environment is possible in several respects, not always mandatory, but possibly also necessary if it does not seem to be indicated according to formal criteria. It is important to make the decision on an informed basis, because breaches of critical infrastructure regulation obligations can result in severe sanctions, even if they may be unintentional or result from ignorance of the obligation of one's own company and service.

Check affectedness - avoid breaches of regulation

Among the factors that need to be considered is, at infrastructure level, the operation of the data centres and their networks in the foreground. Against the background of the threshold values for an electrical output of 3.5 MW according to the current KritisV, the area of critical infrastructure is clearly affected here, even if the platform is operated across several data centres - most data centres in which GXFS offers are processed are likely to be above this threshold. In the portfolio of the Federation Services themselves, practically the entire range of services that belong to the digital services according to KritisV and NIS 2 is represented, without making any statement about compliance with or exceeding the threshold values. The extent to which this is achieved in detail needs to be examined.

Application of known thresholds

The inclusion and validation process for federated services already includes the confirmation of documented „policy rules" and other rules that are used as a „compliance framework" to ensure compliance with requirements from, for example, the areas of encryption, data protection standards and interoperability. This is a mandatory requirement for accreditation within the „Federated Catalogue" of the Gaia-X environment, but is not directly related to security requirements applied in the context of a critical infrastructure operator classification. The motivation is another: After validation in the process of accreditation as a federation service provider, verifiable credentials are issued documenting security levels and are automatically accepted within the GXFS context. Outside the GXFS environment, these credentials may provide an indication that compliance with security standards is an essential part of the federation service, but for the specific requirements of KRITIS regulation, they serve only as an indicator, not as a rule-compliant proof.

Gaia-X Policy Rules for environmental validation

Possible indicator for KRITIS compliance

Guide for evaluating the GXFS portfolio

The answer to the question of whether a particular offering within the Federation Services portfolio meets the criteria for classification as critical infrastructure can only be approached iteratively. Schematically, the decision follows a catalogue of criteria that is clearly classified, at least formally, according to service and company size.

Schematised classification

Services	Large companies	Medium-sized companies	Micro and small businesses
DNS			
TLD registry			
Qualified trust services			
Public communication networks/services			
IXP			
Cloud computing services			
Data processing centres			
Content delivery networks (CDN)			
Non-qualified trust services			

Test scheme for classification as an operator of critical infrastructure

Essential entities
Important entities
Neither essential nor important

Electronic communication (everything except TC)

The catch to this still manageable allocation: It is only true as long as a service is not promoted to the next higher level of importance or even materiality for other reasons. Reasons for a small company with fewer than 50 employees to be included among the essential critical infrastructure facilities would exist, for example, if no one else in the national environment under consideration provided this service to be classified as critical. Exceptions to the size of the company as a benchmark for the classification are not only for the application areas of public electronic communication networks and services, for trust service providers and the TLD register. In principle, any company, even a very small one, can be raised to the level of materiality if a failure of its services leads to substantial disruption of services of general interest.

Exceptions are the rule

Federation Services self-assessed as critical infrastructure

By 17 October 2024, the European Commission will adopt implementing acts laying down the technical and methodological requirements of all eligible services. These legal acts are announced for services with high criticality such as DNS, TLD registries, trust services, cloud computing, data centres and CDN, but in addition also for managed IT and security services, online marketplaces and search engines, and social networking platforms. Even with such a definition of the concrete specifications, however, the question still remains as to whether a specific service from one's own offering belongs to the critical services - and after assessment of the schematised test criteria and individual assessments of significance now actually falls under the regulation of critical infrastructure.

Concretisation of the requirements by autumn 2024

The decision whether to be classified in this way is initially made by the operators of the services themselves. No authority will systematically check tens of thousands of companies for their criticality and importance, but the self-assessment will usually not deviate from state expectations: The mechanisms of risk assessment are basically always the same. The approach for an assessment of the Federation Services with regard to the question of whether they are to be considered critical infrastructure themselves or are at least offered to critical infrastructure operators as a third-party service follows the principles of the probability of occurrence of failures or disruptions and the expected damage that would result. The only difference to a company's risk management is the assessment of the impact on the general public. This may not represent a classic risk factor for corporate goals, but with regard to the state's obligation to provide services of general interest, it forces private providers to regulate.

Trust services unquestionably affected

The question of criticality and significance for security of supply is easy to answer for the services that must also be assessed as essential according to NIS 2 and thus indispensable according to the standards of the

Evaluation criteria from risk management - apart from significance for the common good

KRITIS requirements. Within the Federation Services, these would be, for example, the trust services, insofar as they are offered as qualified services: The SSI framework does not cover all the requirements for this on its own because it does not represent a qualified trust service, but the "real", i.e. qualified identities are operated via the eIDAS SSI Bridge, this status is achieved, and the classification as an essential facility takes effect immediately.

Trust services unquestionably affected

It is even easier to determine the classification on the basis of whether Federation Services are used by Gaia-X users and to what degree of significance for the operation of critical infrastructures. Put into a simple formula: Even a service that is not critical in itself can be essential to the provision of critical services. Ultimately, the responsibility for acting in accordance with the regulations lies with the KRITIS operators themselves, not with the third-party service providers. However, it is to be expected from them that they themselves make their offers available in such a way that a regulatory-compliant use is possible, that it must be verifiable at any time and must also be verifiable on site. The most radical way in which the supervisory authorities take action on third-party service providers is certainly regulated in the financial sector. There it would actually be possible for BaFin to demand access to the facilities of third-party service providers if they work for credit institutions or insurance companies.

Non-critical services are also critical if they contribute significantly to the provision of other critical services

Impact assessment

Service providers within a federation must perform an impact assessment for their offers as to whether it is worth the effort to comply with the requirements of a KRITIS regulation, even if formally the size of the company does not seem to be sufficient for this.

Effort due to KRITIS regulation

The providers of services registered in the Gaia-X Federated Catalogue must answer the questions that arise in connection with the use of their services by operators of critical infrastructure for themselves: What additional precautions and documentation obligations arise for a service if it is to be used in a KRITIS context? What do audits by clients or supervisory authorities mean, what additional obligations do you enter into when you have clients audit you as part of their contractual minimum requirements? What effort does this entail, and is the federation service provider willing and able to accept this effort to maintain the customer relationship? And then how big is the difference between voluntarily classifying oneself as a critical operator and acting as if one were obliged to do so?

Arrangements, obligations, documentation

Effort due to customer requirements

For those who do not want to be potentially affected as service providers by the classification of their customers as critical infrastructures, the only conceivable but less attractive way out is to draft business and contractual terms and conditions that fundamentally exclude critical infrastructure operators from using the services if they would have to be considered an essential part of the critical service.

Non-compliance only if certain customers are excluded

Risk management for digital services within the framework of Gaia-X

A concrete evaluation of the risk factors must take place for an individual assessment of digital services whose criticality requires a corresponding consideration of the minimum requirements according to KritisV and NIS 2. In principle, the prerequisites for integrating services into the risk management of critical infrastructure operators in compliance with regulation provide for a number of comprehensively defined measures which, according to the first sentence of Article 21 para. 2 sentence 1 NIS 2, must pursue a „cross-hazard approach" and can be systematically classified as follows:

Cross-hazard approach for integration in own risk management

- Concepts related to risk analysis and security for information systems
- Management of security incidents

- Business continuity, such as backup management and disaster recovery, and crisis management
- Supply chain security, including security-related aspects of relationships between individual facilities and their direct vendors or service providers
- Security measures in the acquisition, development, and maintenance of network and information systems, including vulnerability management and disclosure.
- Concepts and procedures for evaluating the effectiveness of cybersecurity risk management measures
- Basic cyber hygiene practices and cyber security training
- Concepts and procedures for the use of cryptography and, if necessary, encryption
- Personnel security, access control concepts and management of facilities
- Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications, and secure emergency communications systems within the facility, as appropriate

Apply the KRITIS compliance checklist

For the providers of services in the GXFS environment, this catalogue of measures represents a checklist, as it were, with which they can check the Federation Services for compliance with the specifications if they are to be used for the operation of critical infrastructures. Always under this premise of the criticality of the service, the following also applies: The implementation of the measures from Article 21 are minimum requirements, the non-observance of which can lead to sanctions in connection with significant disruptions and failures of the critical services.

Documentation and certification of KRITIS services in the GXFS environment

More than just indicators: Certification according to relevant standards

Derived from the classification as ADDs from NIS 1, which fall into the category of essential or important facilities under NIS 2, it can be assumed that all Federation Services that are to be considered cloud computing services are critical infrastructure or UBI. They are thus subject to obligations to demonstrate compliance with corresponding minimum information security requirements, which must not only be provided to the supervisory authorities. In the procurement process of customers who are classified as operators of critical infrastructure, the evidence can also be used to meet the necessary requirements as a third-party service provider that conforms to regulations. One way to simplify this proof is to obtain documented certification in accordance with relevant standards such as EN ISO / IEC 27001, for example on the basis of the BSI IT-Grundschutz Compendium. The obligations that must be complied with vis-à-vis the contractual partners in any case include, for example, the granting of audit rights and the submission of proof of safety - even without a certificate, this should be easy to do if such proof is available from any audits that may have been carried out in accordance with § 8a BSIG. According to the minimum standards of the BSI, public clients are also obliged to demand test reports and test certificates from the cloud service provider in accordance with the C5 catalogue.

Grant audit rights for customers

Supply chain perspective: KRITIS operator must always be able to provide services

If services are no longer available: KRITIS operators need exit strategy

KRITIS operators that outsource critical services to a contractor's cloud as a contracting authority must protect themselves against a failure of those services. Above all, they must ensure that their critical services remain available even if the cloud service fails. If the risk analysis shows that certain services may no longer be used - best example: data processing with American cloud operators, even if the data does not leave European data centres, after the Safe Harbor agreement between the EU and the USA has expired - an exit strategy must be in place: The KRITIS operator must prove that it can move the entire operation to its own on-premise server or the cloud of a GDPR-compliant provider, even at short notice.

KO criteria portability, geo-redundancy, resilience

For particularly innovative services, which may even be considered a unique selling point of the GXFS environment, this can have fatal consequences: If the service is so exclusive or only possible in a certain

environment, the customer's prescribed exit strategy will be futile. The operators of critical infrastructures must be able to continue operating a service they have used on another platform without interruption at any time in order to meet the legal requirements placed on them. Concepts are needed here to ensure the necessary level of resilience in the GXFS environment, either through geo-redundancy of server operations and resilient network architecture within Gaia-X, or through support services for the portability of critical services to other operators, private clouds or on-premise platforms.

Conclusion and recommendations

Check measures before authority decision

Anyone who is potentially one of the operators of critical infrastructure in Germany and other countries in Europe needs to make sure on all sides whether and in what way external reporting and notification obligations and regulations of their information security management and other regulations are to be applied. In case of doubt, the decision is up to the supervisory authorities, but every company is well advised to already consider appropriate measures before the BSI officially determines that it belongs to the group of critical infrastructure operators, so that they can be initiated without delay as soon as the obligation arises. This also applies to operators whose services in the area of critical infrastructure are still being planned or implemented, because the effort required to comply with the relevant provisions of KritisV and industry-specific regulations should already be assessed at this point in time in order to make the resources required available.

Need to comply with minimum requirements irrespective of whether national or European regulation is involved

For most companies, it should be irrelevant whether in the future the risk-based identification of KRITIS operators will remain, as is expected at the moment, or whether there will be a switch to a NIS-2-compliant classification as „essential facilities" with a rigid orientation to company size - it is more likely anyway that both scales will be run in parallel. Many German companies are also active in other European member states as operators of critical infrastructures or make their services available to other public services. In both cases, it will be necessary to demonstrate compliance with the minimum standards. This requires an information security management system that functions across countries in order to be able to serve the reporting and notification obligations that apply in each case.

Certification is an aid

Certifications are a useful tool for implementing the security requirements given to critical infrastructure operators, but are rarely mandatory: They are helpful in fulfilling the obligations to provide evidence, but they do not protect against inspections and interventions by the supervisory authorities.

Observing further development across Europe

In any case, the constantly changing legal framework must be carefully observed. The specific implementations into the respective national laws of the EU member states, especially of the two directives NIS 2 and CER, will gradually become apparent by the set implementation deadline at the end of 2024. For example, there will be more or less significant deviations in terms of the role and powers of the national supervisory authorities. The conditions in Germany are of a predominantly foreseeable nature, even if there are no draft bills yet for the implementations in the KritisDG and a future IT-SiG 3.0. However, for a consortium operating on a Europe-wide basis, such as the operators of the Gaia-X environment, it is not only the regulation of critical infrastructures in the German market that will be relevant in the future.

List of abbreviations

Digital Service Providers (ADD)	Digital Service Providers
AS	Autonomous Systems
AtG	Law on the peaceful use of nuclear energy and protection against its dangers ("Atomic Law")
AWV	The German Foreign Trade and Payments Ordinance
B3S	Industry-specific security standards
BaFin	Federal Financial Supervisory Authority
BAIT	Bank supervisory requirements for IT
BBK	Federal Office for Civil Protection and Disaster Assistance
BDSG	Federal Data Protection Act
BImSchV, StöV	Twelfth Ordinance on the Implementation of the Federal Immission Control Act (Major Accidents Ordinance - 12 BImSchV)
BNetzA	Federal Network Agency
BSI	Federal Office for Security in Information Technology
BSIG	Law on the Federal Office for Information Security (BSI Law)
BSZ	Accelerated security certification
C5	Cloud Computing Compliance Criteria Catalogue
CC	Common Criteria for Information Technology Security Evaluation
CDN	Content delivery networks
CE Identification	Conformité Européenne (European conformity), identifies products that comply with the product-specific applicable European directives
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardisation)
CER (directive)	Critical Entities Resilience Directive („Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical facilities and repealing Council Directive 2008/114/EC").
CNC	Computer numerical control
CPU	Central processing unit
CRA	Cyber Resilience Act („Regulation on cybersecurity requirements for products with digital elements")
DIN	German Institute for Standardisation

DNS	Domain Name System
DORA	Digital Operational Resilience Act („Directive(EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience in the financial sector and amending directives (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011").
GDPR	General Data Protection Regulation („Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing directive 95/46/EC").
EBA	European Banking Association
ECI (directive)	European Critical Infrastructure Directive („Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection")
EECC (directive)	European Electronic Communication Codex („Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 on the European Electronic Communications Code").k
EC	European Community
eIDAS (-directive)	Electronic Identification, Authentication and Trust Services („Directive (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC").
EN	European standard
EnWG	Electricity and Gas Supply Act (Energy Industry Act)
ESSIF	European Self-Sovereign Identity Framework
EU	European Union
Gaia-X	Project to build a networked, open data infrastructure
gematik	Telematics company
GG	Basic Law for the Federal Republic of Germany
GXFS	Gaia-X Federated Services
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IKT	Information and communication technology
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information technology
IT-SiG, IT-SiG 2.0	IT Security Act (Article Law)
ITS	Implementing Technical Standards
IXP	Internet Exchange Point
KRITIS	Critical infrastructures
KritisDG	KRITIS umbrella law (in preparation)
KritisV	Ordinance for determining critical infrastructures according to the BSI Act (BSI-Kritis Ordinance - BSI-KritisV)
KWG	Banking Act
MaRisk	Minimum requirements for risk management

MW	Megawatt
NESAS CCS-GI	NESAS (Network Equipment Security Assurance Scheme) Cybersecurity Certification Scheme - German Implementation
NIC	INetwork Information Center
NIS 2 (directive)	Directive on measures for a high common level of cyber security in the Union („Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security in the Union, amending Directive (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148", NIS-2 Directive).
NIS (directive)	IDirective to ensure a high level of network and information security („Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security for network and information systems in the Union", NIS Directive)
NPSI	National Information Infrastructure Protection Plan
RAN	Radio Access Network
RTS	Regulatory Technical Standards
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SGB V	Social Code (SGB) Fifth Book (V) - Statutory health insurance
SGB X	Social Code (SGB) Tenth Book (X) - Social administration procedures and social data protection
SSI	Self-Sovereign Identity
StöV	see BImSchV
TKG	Telecommunications Act
TLD, gTLD, ccTLD, nTLD	Top Level Domain, generic TLD, country TLD, new TLD
TMG	Telemedia Act
TR	Technical directive
UBI	Companies in special public interest
UP Bund	Implementation plan for the federal administration
UP KRITIS	Implementation plan for the critical infrastructures
VAG	German Insurance Supervision Act
VAIT	Insurance law requirements for IT
ZAG	Payment Services Supervision Act

Publisher:
eco – Association of the Internet Industry
Point of Contact: Emma Wehrwein, Vivien Witt, Lauresha Memeti – Project Team GXFS-DE
E-Mail: pmo@gxfs.de
Adress: Lichtstraße 43h, 50825 Cologne, Germany

Commissioned study author:
nGENn GmbH
Point of Contact: Ulrich Plate, Senior Information Security Consultant
E-Mail: plate@ngenn.net
Adress: nGENn GmbH, Erdfunkstelle 1, 61250 Usingen, Germany