GRM® Global Regulation

King of the Audits

27001

Dr. Waldemar Grudzien
Nadine Hofmann
Victoria Denisiuk
Galina Slobodianiuk

May 2024
White paper

Management Summary

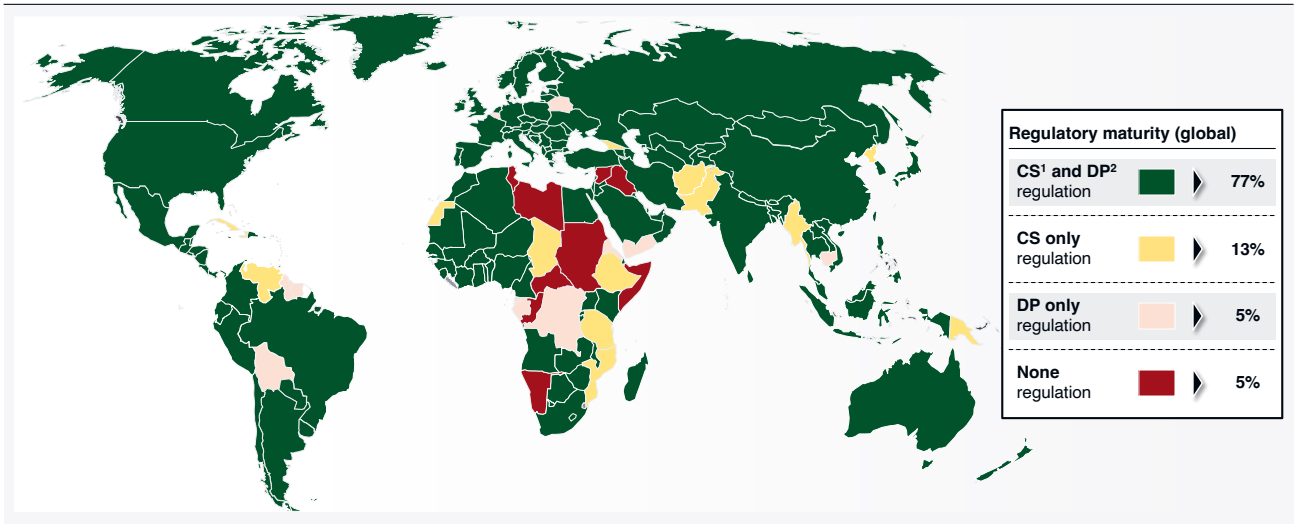
- The European Union (EU) encourages businesses to strengthen their information security and resilience through regulations such as the Network and Information Security 2 (NIS2) Directive, the Critical Entities Resilience (CER) Directive, and Digital Operational Resilience Act (DORA), with a particular focus on companies in critical infrastructures (CRITIS).
- German financial market participants are subject to dual regulatory standards under NIS2 and DORA if they operate critical infrastructure facilities as well.
- Companies must address recurring security requirements from everemerging regulations and continuously demonstrate compliance.
- Information security and resilience must be organised as part of a management system.
- With an information security management system (ISMS) in accordance with the ISO standard 27001, companies achieve legal agility and, if desired, certified security maturity.
- The development of an ISMS should be managed as a project in smaller organisations, or as a program in larger organisations.
- This white paper presents a certificate-proven process model for setting up and operating an ISMS.

EU Security Requirements Pose Challenges for Companies

Regulatory demands for data security and data protection are increasing globally. Data security encompasses cyber security, IT security, information security, and resilience. Data protection ensures the right to informational self-determination. More than 75% of countries have regulations for both cyber security and data protection, while only 5% have no specific regulations for both areas (Figure 1). In this respect, the regulation of both spheres is crucial for the international community of states.

The EU regulation on data protection (GDPR)[1], resilience (DORA[2], CRA[3]) and security (NIS2[4], CER[5]) are influencing jurisdictions worldwide.

Cyber security (CS) and data protection (DP) laws worldwide (2021)



Source: UNCTAD Data Protection and Privacy Legislation Worldwide & Cybercrime Legislation Worldwide I 1: CS = Cyber security I 2: DP = Data protection

Figure 1: Regulation of cyber security and data protection is almost ubiquitous

The EU Directive NIS2, extends cyber security requirements to more companies compared to the NIS1 version: Approximately 2,000 companies in Germany fall under the NIS1 directive, while the Federal Ministry of the Interior estimates around 30,000 companies will fall under the NIS2 directive. The European Commission anticipates that 160,000 companies will fall within the scope of the EU. Consequently, the number of companies under cyber security supervision in Germany multiplies by at least 15-fold.

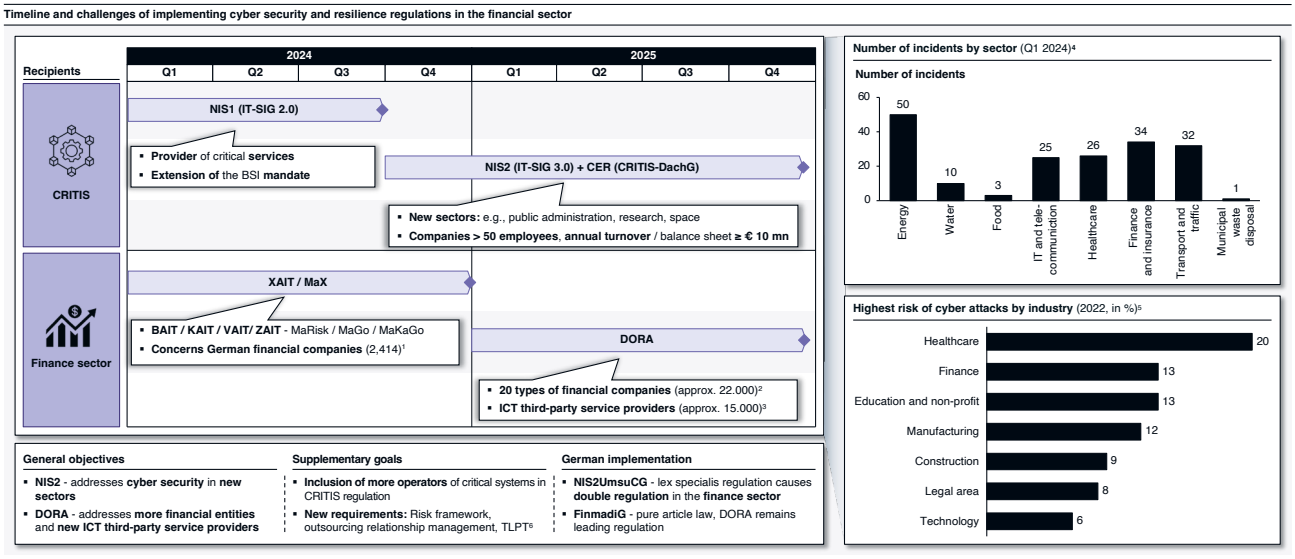
While cyber security is central to the NIS directive, the focus of the CER directive is on enhancing the resilience of critical infrastructure with an emphasis on disaster management. The CER directive obliges member states to identify critical infrastructure and strengthen their physical resilience against threats such as natural disasters, terrorist attacks, or sabotage.

DORA marks the first industry-specific European regulation for cyber security. Under DORA, companies are required to demonstrate digital operational resilience, as it expands the supervisory framework compared to current practices to encompass 20 types of financial entities and additionally includes information and communication technology third-party service providers (ICT-TPSPs). These provide ICT services for financial companies. DORA outlines that, for the first time, critical ICT TPSPs such as hyperscalers, are subject

to direct financial supervision. DORA requires financial organisations to carry out robust, risk-oriented monitoring of third-party ICT risks. The EU estimates that around 22,000 financial institutions and around 15,000 ICT TPSPs in the EU will fall within the scope of DORA (Figure 2).

DORA is a lex specialis for the financial sector compared to NIS2. If a company falls within the scope of both DORA and NIS2, and the requirements in DORA are more specific, they take precedence over the requirements of the NIS2 directive. Particularly, the two regulatory emphases on ICT risk management framework and reporting of ICT incidents are more specific to the financial sector in DORA than in NIS2.

Figure 2 illustrates the transition of the financial IT supervision from national to European oversight of critical sectors (CRITIS), specifically the financial sector: In Germany, the transition from NIS1 to NIS2 and CER for all critical sectors, as well as the transition from the supervisory requirements for IT in diverse institutions (XAIT) and German minimum requirements for different systems and management (MaX) to DORA for the financial sector, is depicted. Financial companies will still be examined nationally; however, national supervisory authorities will collaborate more closely with European supervisory authorities and with each other.



Source: GRM I 1: BaFin I 2: DORA Regulation (EU) 2022/2554 vom 14.12.2022 Recital 3 I 3: ESA 2023 22 of 19.09.2023 I 4: BSI I 5: Healthcare Digital I 6: TLPT = Threat Lead Penetration Testing

Figure 2: 2024 is the transitional year from national to European regulation

Financial companies and ICT TPSPs face additional security requirements for products, services, and offerings from existing effective regulations and from regulatory initiatives in the legislative process. The first group includes the EU GDPR, the Environment, Social, Governance (ESG) legislative canon, and the EU Data Act, while the second group comprises the EU Cyber Resilience Act and the EU Artificial Intelligence Act. These initiatives are not considered in this document but are partially addressed in other publications by Global Regulation Management. It remains uncertain how this dense regulatory environment, often seen by the industry as excessive, will impact security and resilience. It could either enhance these aspects or lead to overburdening accompanied by “fatigue fractures”, ultimately reducing the security and resilience of ICT infrastructures.

This white paper explores the impact of new compliance requirements on the economy, using Germany as a case study. It identifies a suitable ISMS for meeting these regulatory demands and demonstrates its implementation through the example of a bank.

Publication of the Opportunities and Risks

This paper “King of the Audits – 27001” presents cyber security regulation in the EU and the ISMS according to the ISO 27001 standard as an appropriate means of security organisation. The paper fits into the overarching framework of our white paper “The Dark Knight Rises”, whereby the two interrelated dimensions of risk and opportunity deal with the changes in the economic world since the return of bloc formation in risk, regulation, IT, security, and sanctions issues in a superordinate manner (Figure 3).

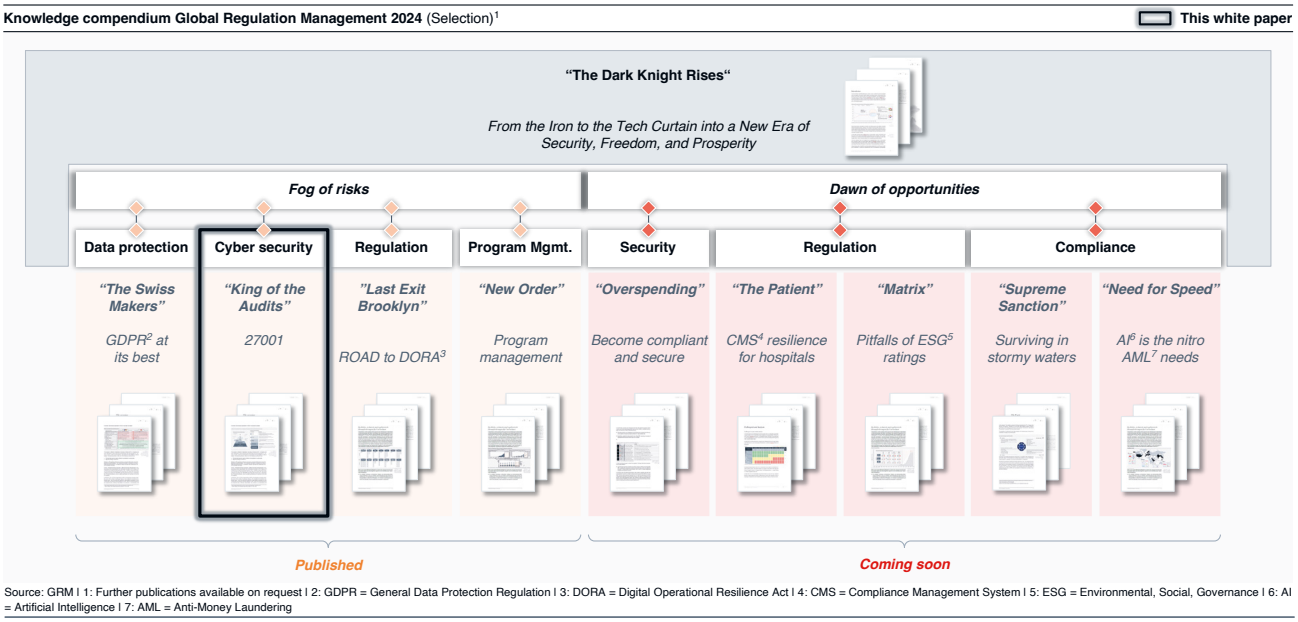


Figure 3: Overview areas of expertise

Legal Outline

The following chapter presents and discusses the German implementation of the three European regulations NIS2 directive, CER directive, and DORA.

Implementation of the NIS2 Directive through NIS2UmsuCG

In Germany, the NIS2 directive will be implemented until the 1st of October 2024 through the “NIS2 Implementation and Cyber Security Strengthening Act” (NIS2UmsuCG[6]). The NIS2UmsuCG as an article law amends existing laws, including the BSI Act[7] (IT-SiG 2.0), which becomes “IT-SiG 3.0” by embedding the NIS2. This defines three types of facilities: “particularly important organisations”, “important organisations” and “domain name registry service providers”.

Categorisation and requirements for organisations according to "NIS2 Implementation and Cyber security Strengthening Act" (NIS2UmsuCG) ✓ applies ✗ does not apply

Content NIS2UmsuCG	Particularly important facility							Important facility		Domain name registry provider
	Facility accord. to Annex 1 NIS2UmsuCG[1]	Qualified trusted service providers	Top level domain name registries	Domain name system service provider	Telecommuni-cation servi-ces[2]	Operators of critical systems	Facility accord. to Annex 3 NIS2UmsuCG	Facility accord. Annexes 1 & 2 NIS2UmsuCG[3]	Trusted service provider	
§30 (1)(2): Measures	✓	✓	✗	✗	✓	✓	✓	✓	✓	-
§30 (6): Certified products	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§30 (7): Exchange of information	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§30 (9): Right to industry-specific security level	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§31: Special risk management requests from operators of critical facilities	✗	✗	✗	✗	✗	✓	✗	✗	✗	-
§32: Reporting obligations	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§33: Registration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
§35: Information	✓	✓	✗	✗	✓	✓	✓	✓	✓	-
§38: Duties of the management	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§39: Obligation to provide evidence for operators of critical facilities	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§51: Maintaining a database	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
§52: Granting of access	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓
§53: Duty to cooperate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Source: NIS2UmsuCG I GRM I 1: ≥250 employees or >€50 mn turnover and >€43 bn balance sheet I 2: ≥50 employees or >€10 mn turnover and >€10 mn balance sheet I 3: ≥50 employees or >€10 mn turnover and >€10 mn balance sheet

Figure 4: Vital security requirements from the NIS2UmsuCG

According to § 30 (1) NIS2UmsuCG, "entities are obliged to take appropriate, proportionate, and effective technical and organisational measures to prevent disruptions to the confidentiality, integrity, and availability (CIA) of the information technology systems, components, and processes they use to provide their services and to minimise the impact of security incidents as much as possible". Figure 4 illustrates the fundamental security requirements for the three facility types from the NIS2UmsuCG.

The measures should comply with the state of the art, take into account relevant European and international standards, and be based on a cross-sectoral approach to threats (Article 21 NIS and analogous to § 30 NIS2UmsuCG). Increased requirements apply to operators of critical infrastructure among the particularly important entities under § 31 NIS2UmsuCG.

Implementation of the CER Directive through the CRITIS Umbrella Act

The CER directive is implemented in Germany through the Critical Infrastructure Act (CRITIS-DachG) by 17 October 2024. In § 3 (3) CRITIS-DachG, 18 critical services are defined. The scope of the law is defined in § 4 (1) CRITIS-DachG, stating that a facility is considered critical if it belongs to one of the types of facilities specified by regulation under § 16 (1) in the sectors of energy, transport and traffic, finance and insurance, healthcare, drinking water, wastewater, food, information technology and telecommunications, space, or municipal waste disposal, and it meets the threshold values specified by regulation under § 16 (1) CRITIS-DachG. Generally, a facility serving over 500,000 inhabitants (so-called standard threshold value) is considered critical.

The CER directive also includes a lex specialis provision (§ 4 (6) CRITIS-DachG): Operators of critical infrastructure in the banking, finance, and insurance sectors, as well as information technology and telecommunications, are not subject to § 7 to 12 CRITIS-DachG.

The CRITIS-DachG will not establish sector-specific or industry-specific regulations but will prescribe appropriate and proportionate measures for physical protection to all critical infrastructure sectors. It includes resilience objectives in § 10 (1) CRITIS-DachG, which

operators of critical infrastructure must achieve with their measures, as well as an overview of exemplary measures in § 10 (3) CRITIS-DachG for orientation, which operators can implement (Figure 5).

To further specify cross-sector resilience measures, the Federal Office of Civil Protection and Disaster Assistance (BBK) is expected to develop a catalogue of minimum requirements, likely at the beginning of 2026. Similar to the well-known industry-specific security standards in IT security (B3S), operators of critical infrastructure and their associations can develop industry-specific resilience standards.

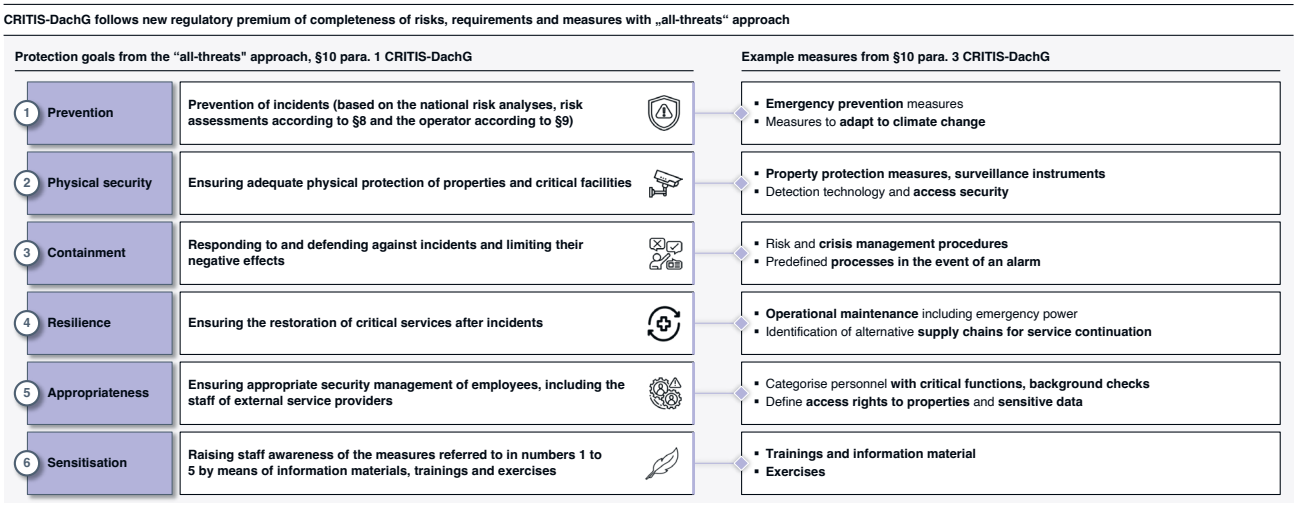


Figure 5: Measures of physical protection for operators of critical infrastructures

Business leaders of operators of critical infrastructure, including liability provisions and training obligations under § 11 CRITIS-DachG, are obligated to approve the measures taken to comply with § 10 CRITIS-DachG and monitor their implementation. Since the GDPR was enacted, the importance of sanction options for enforcing a regulation has been recognised. Therefore, the penalty provisions under § 19 CRITIS-DachG for eleven administrative offenses should be understood as a consistent continuation of this sanctioning practice.

Based on national risk assessments, operators of critical infrastructure must conduct their own risk analyses. Section 11 of the Critical Infrastructure Act (CRITIS-DachG) introduces the concept of special audits in critical infrastructure: If an operator of critical infrastructure fails to provide evidence of compliance with resilience measures, this can be verified by the competent supervisory authority.

Currently, operators independently determine whether they are operators of critical infrastructure. To this end, the fourth “Regulation on the Determination of Critical Infrastructures according to the BSI Act (BSI-Kritisverordnung, hereinafter referred to as BSI-KritisV)[9]”, which came into force on 1 January 2024, both controls the definition of critical services and sets the thresholds.

To avoid divergent provisions regarding critical infrastructure under the CRITIS-DachG and the BSI Act (BSIG), operators of critical infrastructure will in the future only be determined by the CRITIS-DachG. Furthermore, common technical solutions are being pursued for

the registration of operators and for reporting significant disruptions, so that in the future, both legal reporting obligations under the BSIG and the CRITIS-DachG can be fulfilled within one report.

Implementation of DORA Through the FinmadiG

In Germany, DORA will be implemented by the Financial Market Digitisation Act (FinmadiG)[10] published in draft form on 23 October 2023. DORA enhances the digital operational resilience of the entire European financial sector. The three European Supervisory Authorities (ESAs), namely the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA) collaborate to develop regulatory technical standards (RTS) and implementation technical standards (ITS), as well as guidelines (GL) for the interpretation and specification of DORA. In the financial sector, operators of critical infrastructure are subject to dual regulation by DORA and NIS2: Although the lex specialis provision of NIS2 through § 28 (5) No. 1 NIS2UmsuCG provides an entry into the specialised regulation of DORA, financial companies that are operators of critical infrastructure remain within the scope of NIS2 in parallel, according to § 28 (1) No. 1 NIS2UmsuCG: Critical services include cash supply, card-based payment transactions, conventional payment transactions, trading in securities and derivatives, clearing and settlement of securities and derivative transactions, insurance services, social security services, and basic security for job seekers.[9]

The German implementation of NIS2, CER, and DORA results in a regulatory double burden for providers of six payment services.

The German financial sector is in a comfortable position for the applicability of DORA. The BaFin has already established and monitored security requirements for the German financial market for years: for ICT security through harmonised requirements for ICT risk management for financial sectors (XAIT), for standardised outsourcing notifications, for the surveillance framework for IT multi-tenant service providers, and for unified structures for reporting ICT-related incidents.

Implementation Hurdles

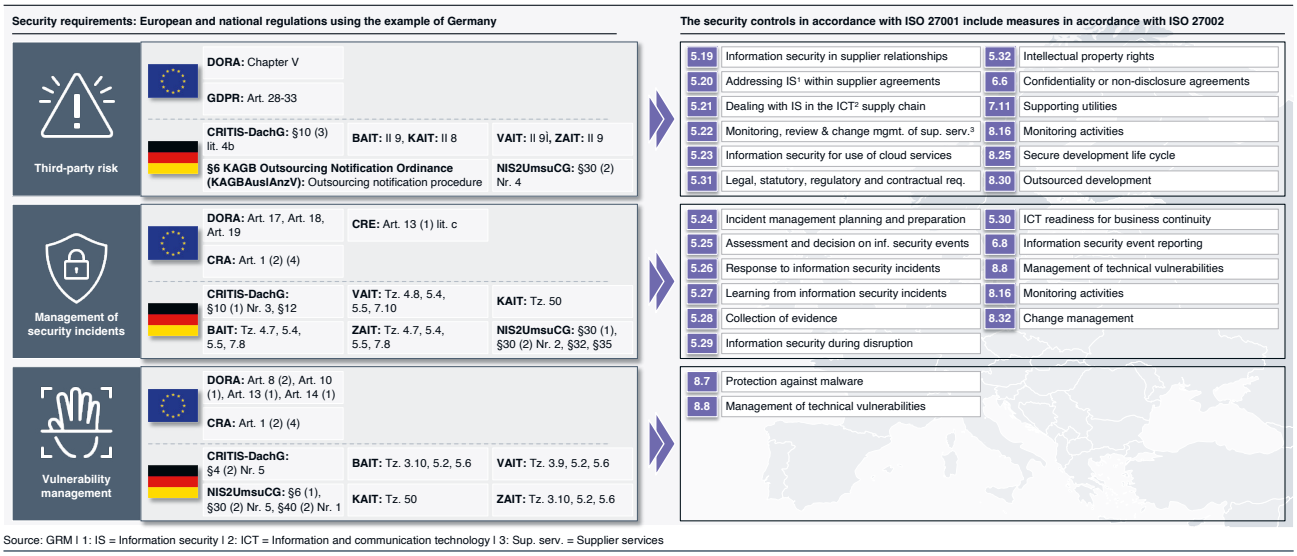
Implementing the requirements poses a challenge for companies in managing identical requirements from different laws and selecting an appropriate information security management system.

Management of Self-similar Stipulations

While the NIS2 directive builds upon the existing NIS1, CER and DORA are entirely new regulations. However, all three initiatives focus on achieving the well-established security objectives of Confidentiality, Integrity, and Availability (CIA) in information security, which are already addressed by existing regulations. However, compliance with the new laws' requirements must be demonstrated anew. Figure 6 exemplifies this task by illustrating the three security goals "Third-Party Risk," "Incident Management," and "Vulnerability Management," and shows which measures of ISO 27002 cover these areas.

Existing regulations like XAIT and GDPR already address many aspects of the new regulations NIS2, CER, and DORA. Each new regulation still needs to be integrated into the organisation, increasing the compliance burden for several reasons: Often, the technical terms and designations in the regulations differ, requiring alignment of current requirements with future ones. Secondly, many terms are ambiguous and open to interpretation, leading to potential misunderstandings and errors in implementation.

Thirdly, fulfilling the new requirements, which are similar to existing ones, can lead to multiple and redundant implementations of measures. NIS2, CER, and DORA increase compliance efforts in two dimensions: horizontally through the expanded scope (see Figure 2) and vertically through heightened security requirements per security objective. This is particularly evident in areas such as reporting and notification obligations, training and awareness, risk management, testing, and third-party risk management.



Source: GRM I 1: IS = Information security I 2: ICT = Information and communication technology I 3: Sup. serv. = Supplier services

Figure 6: Various laws with the same security requirements, controls and measures

The security of a business process, a main application, and a support process is represented by security objectives, measures, and security requirements. The three security objectives CIA undergo minimal change, measures experience moderate change, and the security requirements induced by regulations are subject to significant change. These security requirements are the “moving target.” The security objectives correlate with the relatively stable protection objects: infrastructure, applications, and data. Measures, including legal, organisational, and technical measures, evolve, particularly the technical component, which follows the most dynamic development as the state of the art. Therefore, in a business process comprising infrastructure, applications, and data, achieving legal compliance as a “moving target” poses the greatest challenge. Overall, managing security objectives, measures, and security requirements necessitates an appropriate organisational framework.

Framework for the Management of Information Security

An information security framework structures documents and processes as well as the management of information security risks and their mitigation. At the same time, an organisation's information resources, including its infrastructures, applications and data, are captured. It enables the organisation of security from multiple perspectives to reduce the likelihood of vulnerabilities and security breaches from both internal and external perspectives.

A comparison of the most widely used cyber security frameworks — Recommendation

	NIST	ISO	ISACA	CIS	CSA	HITRUST	GDPR	PCI DSS	AICPA
Publisher	▪ **NIST** (National Institute of Standards and Technology)	▪ **ISO** (International Organization for Standardization)	▪ **ISACA** (Information Systems Audit and Control Association)	▪ **CIS** (Center for Internet Security)	▪ **CSA** (Cloud Security Alliance)	▪ **CSF** (Common Security Framework)	▪ **EU** (European Union) Parliament	▪ **PCI SSC** (Payment Card Industry Security Standards Council)	▪ **AICPA** (American Institute of Certified Public Accountants)
Application	▪ **All companies** including CRITIS	▪ **All companies**	▪ Corporate IT and **IT management**	▪ Companies with **weaknesses in their cyber protection mechanisms**	▪ **Cloud** services/companies	▪ **Healthcare**	▪ Companies processing **personal data** from **EU citizens**	▪ **Government** and its **contractors**	▪ **Service company**
Goals	▪ Managing **CS[1] risks** ▪ Independent standards and **best practices**	▪ **Establishment** of an **ISMS** ▪ Continuous improvement to **safeguard the** company's **information assets**	▪ **Alignment of IT and business objectives** commonly used for SOX[2] compliance	▪ **Prioritisation of technical measures** to strengthen cyber security ▪ **Defence against** known **cyber threats**	▪ Supporting cloud customers in **systematically assessing the overall security risk of** cloud service providers' implementations	▪ Providing a **structured approach to the security and privacy framework** for organisations ▪ **Data protection management**	▪ **Data control** for data subjects	▪ **Security standards** for credit card data processors	▪ Secure **data management** (supply chain)
Scope	▪ Manage and handle **cyber attacks**	▪ **Information security** (organisation, technology, physical, personnel)	▪ Profit **realisation** ▪ Management of **operational risk** and **resources**	▪ **Technical security** and operational controls ▪ **Risk reduction** ▪ **Increasing resilience**	▪ **17 Security domains** ▪ 197 Control objectives	▪ **Risk analysis** ▪ **Risk management** ▪ **Operational requirements**	▪ **Processing of personal data** within and outside the EU	▪ **Standards for payment transactions**	▪ SOC 1: **Financial reporting** ▪ SOC 2: **NF[3]-controlling**
Certification	▪ **No certification**	▪ **Certifiable** according to ISO 27001 ▪ Complies with GDPR, SOC2, PCI DSS, HIPAA ▪ Alignment with NIST	▪ For **persons** only	▪ **No certification** ▪ Complies with regulatory standards such as GDPR, HIPAA, and PCI DSS	▪ For **persons** only ▪ Illustrated against ISO 27001/-17/, NIST 800-53, C5, COBIT & CIS, among others	▪ **Certifiable** ▪ Self-validated assessment for 19 areas ▪ Integrated HIPAA, NIST, ISO	▪ **Certifiable** in accordance with ISO 27701 (ISO 27001 certification as a basis)	▪ **Compliance** (vis-à-vis credit card companies)	▪ **Certifiable** by CPA firm (report)

Source: GRM I 1: CS = Cyber security I 2: SOX = Sarbanes-Oxley Act (2002) I 3: NF = Non-financial

Figure 7: Framework of information security

Implementing a security framework is resource-intensive, requiring significant personnel, time, and financial investment. Additionally, these frameworks are not one-size-fits-all solutions. They need to be tailored to the specific needs of each company, a process that is often complex and time-consuming. There are numerous security frameworks available on the market. A professional review was conducted on 29 security frameworks, with the nine most relevant frameworks summarised in Figure 7. These frameworks encompass various best practices and industry standards that assist companies in implementing robust security measures.

Additionally, using recognised standards can enhance a company's reputation, which is particularly important for businesses handling sensitive data or operating in highly regulated industries. The choice of a framework largely depends on the specific and regional scope of a company. If certification is required, whether for business policy or regulatory reasons, the selection is narrowed down to three frameworks: SOC 1, SOC 2, and ISO 27001.

An ISMS is increasingly required, either explicitly or implicitly, by regulations. Explicit requirements come from the CRITIS Regulation, XAIT, and the Energy Industry Act (EnWG)11, where the ISO 27001 standard is recommended or mandated. Implicit requirements are found in a catalogue of demands that are best met through an ISMS according to the ISO 27001 standard.

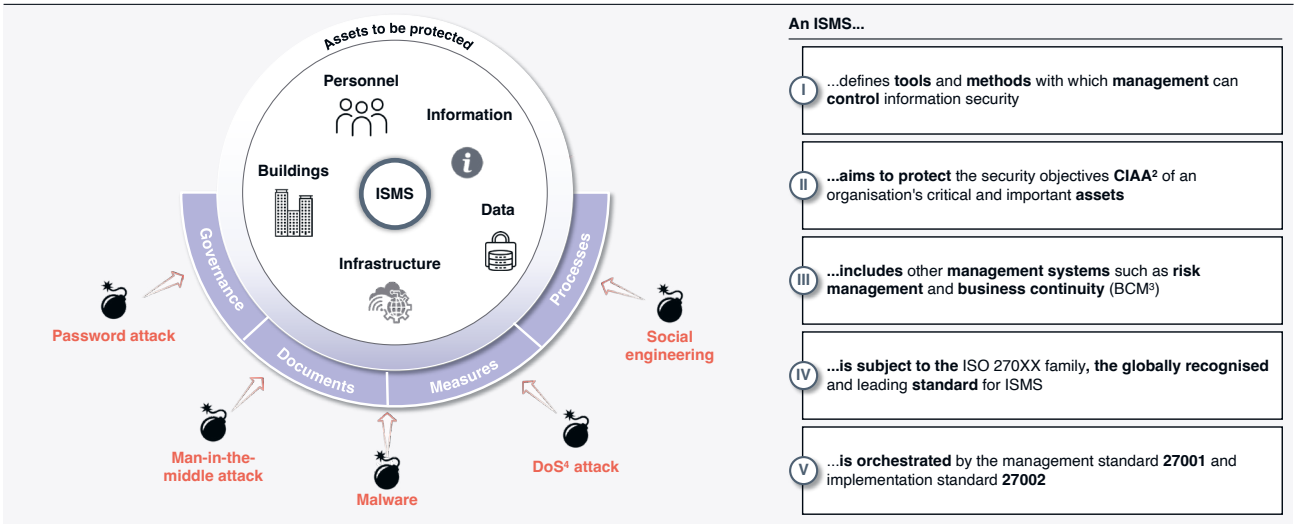
ISMS for More Agility to Fulfil Regulatory Requirements

For the implementation of new requirements, affected organisations are recommended to adopt a management system.

ISMS According to ISO 27001 Standard: Characteristics and Benefits

An Information Security Management System (ISMS) is a tool for protecting an organisation's information and data. The globally recognised standard for establishing and operating an ISMS is the ISO 27001 standard, "Information Security Management Systems – Requirements." An ISMS helps safeguard an organisation's critical and important assets from threats and attacks by internal and external actors (Figure 8).

Components of an ISMS[1], assets to be protected and typical attacks



Source: GRM I 1: ISMS = Information security management system I 2: CIAA = Confidentiality, integrity, availability and authenticity I 3: BCM = Business continuity management I 4: DoS = Denial of service

Figure 8: An ISMS protects institutional values from threats

The assets include personnel, buildings, infrastructure (hardware, firmware, software), as well as processed information and data. An ISMS comprises various components: governance in the form of organisational structures and processes for information security, documents (written order of the ISMS), processes (implementation of the processes described in the documents), and legal as well as technical and organisational measures for protecting the assets.

Despite being around since 2005, the concept of ISMS has only recently garnered significant attention, a trend that continues to grow. This surge in interest can be attributed to several factors. Firstly, an increasing number of business models are heavily reliant on internet technologies. Consequently, the expanding digital landscape has led to a broader attack surface in cyber space, both horizontally and vertically. This has resulted in a rise in both financial losses and intangible damages. As a result, organisations are increasingly inclined to bolster their security measures. Simultaneously, regulatory bodies and lawmakers are responding to these trends by introducing new and heightened regulatory requirements.

In recent years, regulations, particularly through stricter enforcement, have been a significant motivator for enhancing security maturity. Examples include regulations of the EU GDPR, the EU CRA, and the EU NIS Directive. Under GDPR, fines can be calculated based on the revenue (up to €20 million or up to 4% of the worldwide annual turnover, whichever is higher). Similarly, fines outlined in the draft CRA from 15th September, 2022, can reach up to €15 million or up to 2.5% of the total worldwide annual turnover of the preceding financial year, depending on which amount is higher.

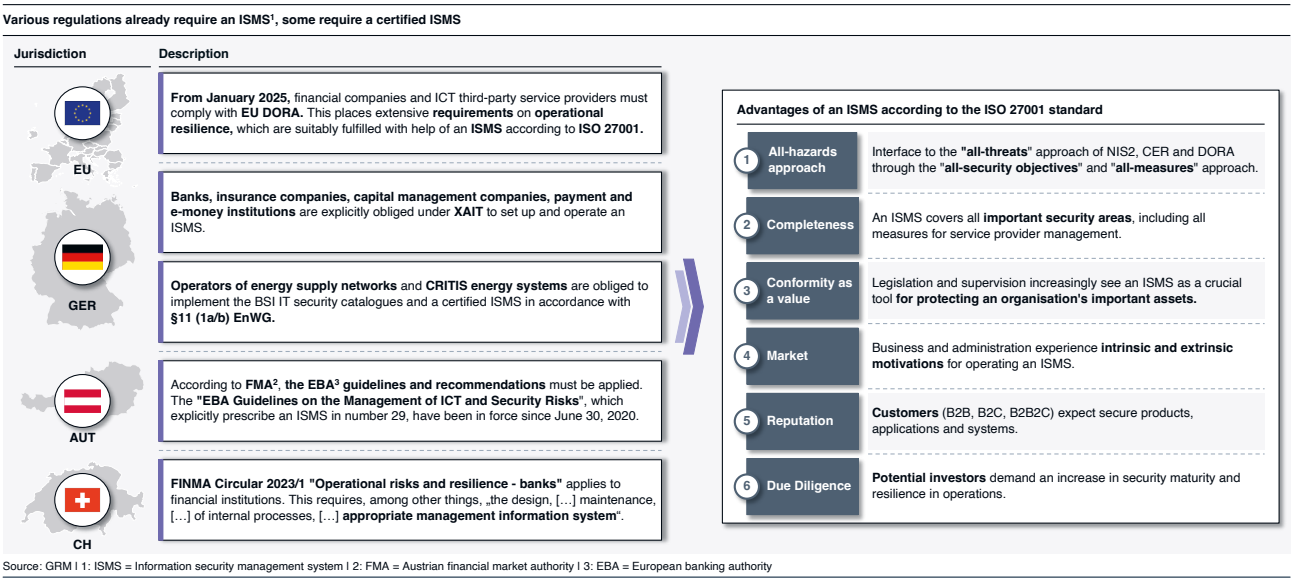


Figure 9: European jurisdictions require an ISMS

According to the NIS2 Directive, member states must notify the European Commission of "effective, proportionate, and dissuasive sanctions" by 17th January, 2025. Fines will play a central role. In Figure 9, examples of the regulatory justification for an ISMS in the DACH region and the entire EU are compared to the benefits of an ISMS based on ISO 27001.

Mapping of all Regulatory Requirements in Measures

The most suitable framework for information security in organisations is derived from an ISMS based on ISO 27001 standard. This "Framework ISMS" encompasses all security objectives and measures without the regulatory requirements, as there is no ISMS designed to fulfil only specific security laws. The "Framework ISMS" is then developed into a "compliant ISMS" within the respective jurisdiction. This involves mapping the security requirements of applicable laws and supervisory practices of the jurisdiction in a "Framework ISMS". Specifically, the security objectives of a law are integrated into the 93 security objectives of the ISO 27001 standard, which are implemented with measures according to the ISO 27002 standard (see Figure 10 for three security objectives from laws: "Third-party risk", "Management of security incidents", and "Vulnerability management"). Overall, this approach ensures legal certainty while maintaining entrepreneurial agility.

Further elaborations in the white paper are oriented toward banks, with a banks' respective regulatory framework serving as the foundation. Explanations can be applied to any other sector by determining the regulatory framework accordingly.

Security objectives ("security controls") in accordance with ISO standard 27001:2022

Third-party risk | Management of security incidents | Vulnerability management

5. Organisational Controls				8. Technological Controls			
5.1	Policies for information security	5.26	Response to information security incidents	8.1	User end point devices	8.13	Information backup
5.2	Information security roles and responsibilities	5.27	Learning from information security incidents	8.2	Privileged access rights	8.14	Redundancy of information processing facilities
5.3	Segregation of duties	5.28	Collection of evidence	8.3	Information access restriction	8.15	Logging
5.4	Management responsibilities	5.29	Information security during disruption	8.4	Access to source code	8.16	Monitoring activities
5.5	Contact with authorities	5.30	ICT readiness for business continuity	8.5	Secure authentication	8.17	Clock synchronisation
5.6	Contact with special interest groups	5.31	Legal, statutory, regulatory and contractual req.	8.6	Capacity management	8.18	Use of privileged utility programs
5.7	Threat intelligence	5.32	Intellectual property rights	8.7	Protection against malware	8.19	Installation of software on operational systems
5.8	Information security in project management	5.33	Protection of records	8.8	Management of technical vulnerabilities	8.20	Networks security
5.9	Inventory of inf. and other associated assets	5.34	Privacy and protection of pers. identifiable infor. (PII)	8.9	Configuration management	8.21	Security of network services
5.10	Acceptable use of inf. and other associated assets	5.35	Independent review of information security	8.10	Information deletion	8.22	Segregation of networks
5.11	Return of assets	5.36	Compliance with policies, rules and standards for IS	8.11	Data masking	8.23	Web filtering
5.12	Classification of information	5.37	Documented operating procedures	8.12	Data leakage prevention	8.24	Use of cryptography
5.13	Labeling of information	6. People Controls				8.25	Secure development life cycle
5.14	Information transfer	6.1	Screening	6.5	Resp. after termination or change of employment	8.26	Application security requirements
5.15	Access control	6.2	Terms and conditions of employment	6.6	Confidentiality or non-disclosure agreements	8.27	Sec. system architecture and engineering princples
5.16	Identity management	6.3	Inf. security awareness, education and training	6.7	Remote working	8.28	Secure coding
5.17	Authentication information	6.4	Disciplinary process	6.8	Information security event reporting	8.29	Security testing in development and acceptance
5.18	Access rights	7. Physical Controls				8.30	Outsourced development
5.19	Information security in supplier relationships	7.1	Physical security perimeters	7.8	Equipment siting and protection	8.31	Separation of development, test and production
5.20	Addressing inf. security w/in supplier agreements	7.2	Physical entry	7.9	Security of assets off-premises	8.32	Change management
5.21	Managing IS[1] in the ICT[2] supply chain	7.3	Securing offices, rooms and facilities	7.10	Storage media	8.33	Test information
5.22	Monitoring, review and change mgmt. of supplier	7.4	Physical security monitoring	7.11	Supporting utilities	8.34	Protection of inf. systems during audit testing
5.23	Information security for use of cloud services	7.5	Protecting against phys. and environmental threats	7.12	Cabling security		
5.24	IS Incident management planning and preparation	7.6	Working in secure areas	7.13	Equipment maintenance		
5.25	Assessment and decision on IS events	7.7	Clear desk and clear screen	7.14	Secure disposal or re-use of equipment		

Source: ISO.org I 1: IS = Information security I 2: ICT = ICT = Information and communication technology

Figure 10: Security objectives: using the example of three security targets

Instructions on Setting up an ISMS

While data protection concerns information relating to natural persons, information security encompasses all other structured and unstructured information processed by an organisation. This can include analogue information recorded on physical media such as paper documents, business cards, or printouts, as well as digital information stored on data carriers or processed by software and devices. Information is protected using detective, preventive, and reactive security measures. These measures are guided by the fundamental four goals of information security:

- Confidentiality: Safeguarding information from unauthorised disclosure
- Integrity: Accuracy of the data
- Availability: Ensuring IT systems and data are usable whenever required
- Authenticity: Ensuring verified origin of data and IT systems (when using cryptographic primitives, integrity of data implies authenticity)

The ISO 27001 standard consists of two parts: the "High-Level Structure" (HLS) and Annex A with the "Security Controls". The HLS comprises chapters 4 to 10 of the standard and provides the organisational framework for the implementation and operation of the ISMS. Annex A lists 93 controls divided into four groups: organisational, personnel, physical, and technical controls (see Figure 10). A "Security Control" is contextually synonymous with "control" and "security objective".

Setting up an ISMS With a Project

The implementation of the ISMS should be part of a project (see Figure 11, Step 0). It is of essence to determine early in the project which laws and regulations are applicable to the organisation (written order document “Applicable Laws and Other Regulations”).

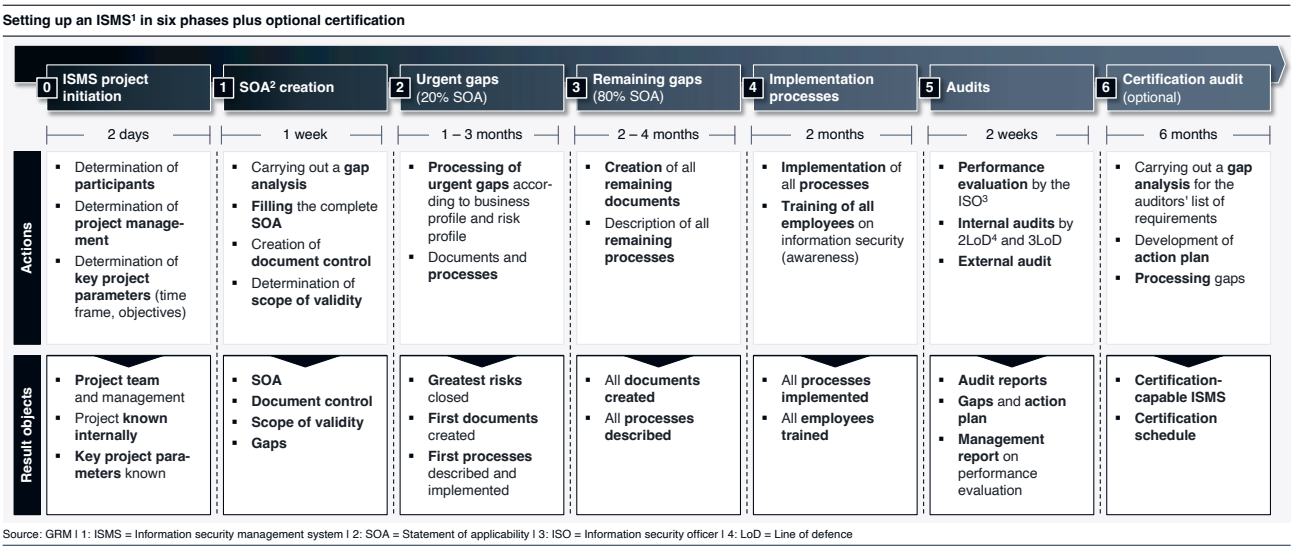


Figure 11: Six phases for setting up an ISMS, certification of the ISMS is optional

The project should be initiated by the management level and supported by strategic objectives. Key parameters derived from strategic objectives are determined by the business strategy, IT strategy, and information security requirements. Project participants should include at least the roles of Information Security Officer (ISO), Data Protection Officer (DPO), Outsourcing Officer, and all other stakeholders relevant to the scope of the ISMS, such as IT operations, human resources, and application development.

There are several ways to start work on the written order: identifying the values to be protected, recording the information network, determining the protection needs of the important values, or conducting risk analyses for them. The authors recommend a different approach: filling out the Statement of Applicability (SOA), as shown in Step 1 in Figure 11. This approach has proven successful in many ISMS and auditing projects. The SOA forms the skeleton of an ISMS, where the individual parts are brought together to form a coherent system. In Figure 10, 93 security objectives are listed. For each control associated with a security objective, the relevance and application must be described. This includes an explanation of whether and how a specific security objective is achieved by these controls. If a control does not apply, this must also be explained. Controls, synonymous with security objectives, can be achieved through documents (policies, procedures, etc.) and measures. The importance of the SOA is highlighted by the fact that it is the only document referenced in the certificate – including title, version, and date.

Governance of an ISMS

The governance of an ISMS includes goal setting, resource allocation, and a mode of operation. The Information Security Officer (ISO) function is responsible for the establishment and operation of the ISMS. The goals are set and managed by the management level at least annually or as needed, even intra-annually. The provision of personnel, technical, and organisational resources appropriate to the tasks and scope of the ISMS is the responsibility of the management, based on the annual workload planning of the ISO function. The mode of operation also includes the frequency, content, and members of committees and project groups, as well as reporting and communication channels and formats. Many levels and employees collaborate within the ISMS framework to protect critical infrastructures from threats and attacks. For this cooperation, banks have established the model of the three lines of defence, known as the "3LoD" (lines of defence):

The Bezos Pizza rule applies when building an ISMS: the core team should get satisfied from two pizzas.

- 1LoD: Implementation of measures by business units and service areas such as IT and operations, as well as conducting their own 1LoD controls
- 2LoD: Requirements from the ISO function, independent assessment of information security risks, and conducting their own 2LoD controls over the 1LoD
- 3LoD: Reviewing the effectiveness of the internal control system (ICS) by the internal audit

If critical infrastructures such as bank-owned payment systems are to be protected, the 3LoD model is expanded to include the state as the fourth line of defence (4LoD):

- 4LoD: The state in its dual role as legislator (setting requirements) and regulator (supervisory body).

Awareness

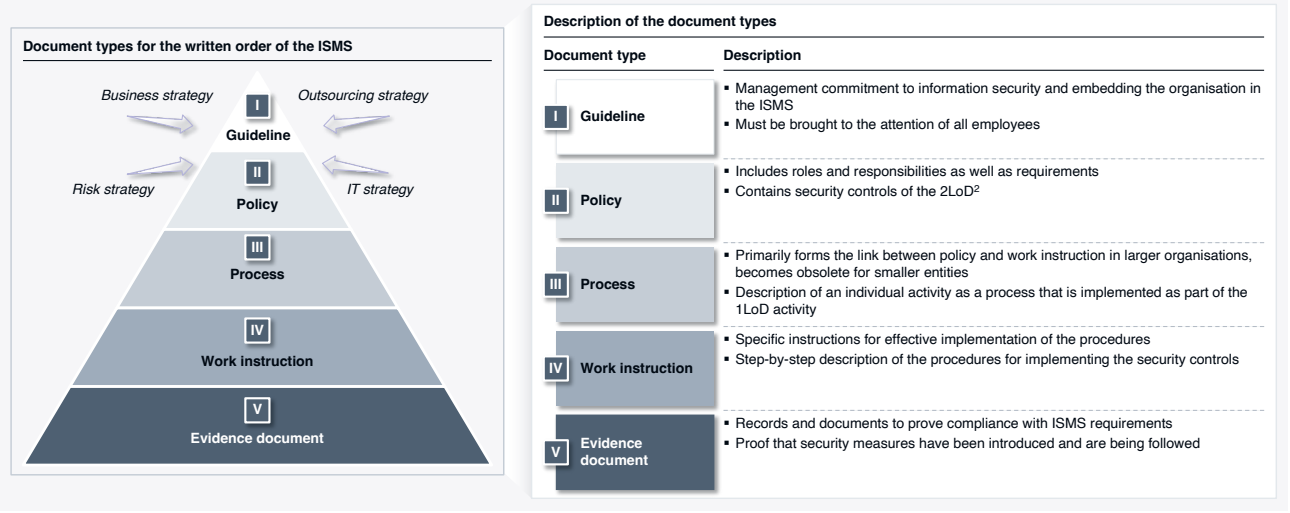
Awareness of information security is a fundamental pillar within corporate security and essential for its success. In an increasingly complex threat landscape, it is essential that all employees not only understand the principles of information security but also recognise their individual roles in the protection process. This awareness creates a robust defence within the 1LoD against potential internal and external security threats. Continuous training and awareness-raising among the workforce, for example through trainings, exercises, and weekly sessions on risks such as phishing, social engineering, and other cyber threats, significantly reduce the likelihood of security incidents. Furthermore, high awareness strengthens understanding of policies and procedures, leading to better compliance with security rules. This approach promotes a corporate culture where security is understood as a shared responsibility, with each individual contributing to the protection of company assets.

Superordinate Documents of the ISMS

The ISMS consists of documents spanning several hierarchical levels. Commonly used are the five document levels: strategies, guidelines, policies, processes, work instructions, and evidence documents (see Figure 12). All documents must be regularly reviewed and adjusted as needed, both periodically and on an ad-hoc basis.

The executive management defines corporate objectives and outlines measures to achieve them in strategies. German banks are required to develop information security-related strategies for business, risk, IT, and outsourcing. Austrian institutions must follow EBA guidelines and create at least one business strategy and one overall risk strategy. Swiss institutions must develop strategies for business, risk, and IT in accordance with banking laws, financial market supervision laws, and specific circulars.

An ISMS[1] aims for a comprehensive approach that encompasses all applicable laws and standards along a logical document hierarchy



Source: "Non-financial Risk Management in the Financial Industry" (Frankfurt School Verlag) I GRM I 1: ISMS = Information security management system I 2: LoD = Line of defence

Figure 12: Document hierarchy of an ISMS

Policies are documents of the 2LoD, in the case of an ISMS, thus of the ISO function. Policies specify scope, responsibilities, and minimum requirements, but can also encompass procedures and processes.

Processes represent the implementation of activities mentioned in the overarching documents by the 1LoD. Work instructions provide detailed guidance for process execution and the use of specific IT applications. The depth of the documents is left to the discretion of the companies. For example, a process can also be described generically, which is detailed in the subsequent document. Document templates are also work instructions.

Evidence documents serve as proof of the effective implementation of processes by summarising results and describing general conditions: audit reports, risk analyses, invoices, meeting minutes, and completed templates. The audit reports of the Internal Audit (3LoD) on the ICS, i.e., on the effectiveness of the work of the 1st and 2nd LoD, are also evidence documents.

Document Creation Follows the Pareto Principle

Alongside the creation of the SOA, the scope of the ISMS should be defined, document control initiated, and a gap analysis conducted. Document control describes how ISMS documents are created, reviewed, approved, labelled, distributed, updated, and withdrawn throughout their lifecycle. It also provides an overview of all ISMS documents, serving as the “written order”. An effective ISMS should be structured according to the specific domains of information security, which can encompass both traditional departments

(e.g., Human Resources, IT) and dedicated security areas (e.g., Security Information and Event Management, Identity and Access Management). These domains are suitable for structuring ISMS documents in the document control process.

The authors recommend the following classification for the delineation of domains: since the current standard from 2022 categorises the 93 controls into only four domains (organisational, personnel, physical, and technical controls), there are four very large areas of the ISMS with many different individual topics. At the other end of the domain classification scale is the direct categorisation into 93 domains, which would be too granular and reduce the effectiveness of the ISMS. A middle ground is to classify the 93 controls of the 2022 version of the ISO 27001 standard into the 14 domains of the 2013 version. This combination of both versions of the standard is depicted in Figure 13.

The gap analysis identifies the gaps between the desired state of a certification-ready ISMS and the current state. The result of the gap analysis is the action plan to close the gaps in the three steps 2 to 4 in Figure 11. In step 2, according to the Pareto principle, the most urgent 20% of identified gaps are closed first. These gaps represent the greatest security risks for information and should therefore be prioritised accordingly. Step 3 involves the remaining 80% of the necessary work to establish the ISMS. The implementation of all processes in step 4 occurs immediately.

The established ISMS must be initially and continuously assessed for its functionality after commissioning. This is achieved through the “Effectiveness Review” step, in which management annually evaluates the ISMS for its suitability, adequacy, and effectiveness. The ISO function gathers data through continuously conducted internal audits (2LoD controls) to assess

- Design (Test of Design, ToD),
- Implementation (Test of Implementation, ToI) and,
- Effectiveness (Test of Effectiveness, ToE)

of measures to achieve the security objectives. The range of topics covered by the ISMS should be audited every three years, while the aspects of an organisation identified as critical audited more frequently (annually to semi-annually). An organisation can also make use of external audits to support the 2LoD controls (ISO), the 3LoD (internal audit) and the 1LoD (IT operations). Penetration tests are the classic example of an outsourced audit activity.

Document Hierarchy With a Practical Example

The overarching documents of an ISMS include the aforementioned SOA and document control, the information security policy, the ISMS effectiveness review policy, and the “Applicable Laws and Other Regulations” document.

The PDCA cycle is recommended as a form of organisation.

The Information Security Policy (IS Policy) is central to the ISMS and the organisation. It must be communicated to all employees and should be structured according to the HLS, i.e., chapters 4 to 10 of the ISO 27001 standard. The HLS serves as the instrument for the management to operate an ISMS in a controlled manner and ensure its necessary development. It requires management’s positioning on the ISMS in aspects such as the

organisation's context (Chapter 4), leadership (Chapter 5), planning (Chapter 6), support (Chapter 7), operation (Chapter 8), performance evaluation (Chapter 9), and improvement (Chapter 10).

The IS policy thus combines other important contents, such as the scope of the ISMS, security roles and responsibilities, IT security policies and objectives, risk management, and effectiveness testing. In addition to management's commitment to actively support information security and employees' obligation to comply with it, the IS Policy particularly establishes general principles of the organisation. Examples include continuously enhancing the security level or maintaining a high reputation.

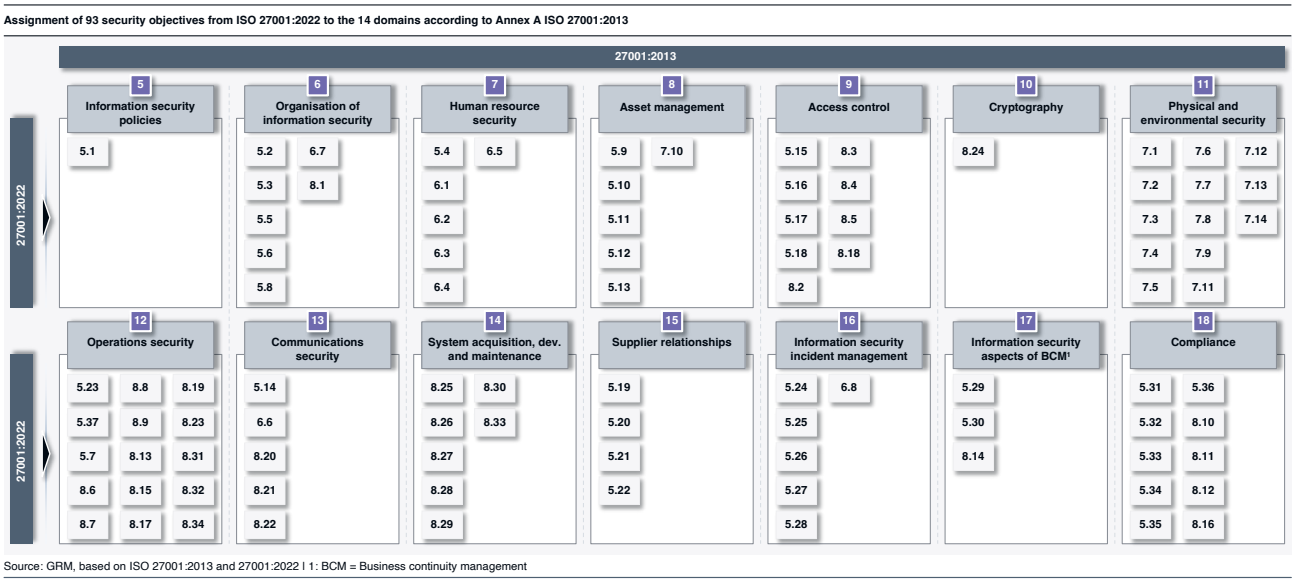


Figure 13: Proposal for the structuring of the 93 security objectives in 14 domains

Additionally, the business strategy plays a pivotal role in the ISMS: When the bank develops applications in-house, the document set in the ISMS concerning application development and secure coding follows a different paradigm than when applications are obtained externally. The same applies to strategic business decisions such as outsourcing IT operations to a domestic or third-country cloud. Following the results of the gap analysis, starting with the urgent ones, all documents of the ISMS are created. For all requirement documents of the ISMS, i.e., policies, it is advisable to use the requirements from the controls in the ISO 27001 standard. This approach sets the document's goal and additionally fulfils the ToD.

Implementation of the ISMS Through Automated Processes

An effective ISMS is ideally implemented using tools. Fundamentally, two types of ISMS tools need to be distinguished: tools for organising the ISMS itself and tools for managing specific aspects of the ISMS, such as Identity and Access Management (IAM), Asset Management, and Risk Management.

Figure 14 provides an overview of the tooling of the ISMS topics with typical tool examples for each topic.

The processes of information security should be described in parallel with the documents and implemented jointly by the 1LoD with the support of the 2LoD. Documenting their implementation provides evidence of meeting requirements through implemented processes. Merely describing the implementation in a work instruction is not sufficient as proof of effectiveness.

Security objectives ("security controls") in accordance with ISO standard 27001:2022

Third-party risk | Management of security incidents | Vulnerability management

5. Organisational Controls				8. Technological Controls			
5.1	Policies for information security	5.26	Response to information security incidents	8.1	User end point devices	8.13	Information backup
5.2	Information security roles and responsibilities	5.27	Learning from information security incidents	8.2	Privileged access rights	8.14	Redundancy of information processing facilities
5.3	Segregation of duties	5.28	Collection of evidence	8.3	Information access restriction	8.15	Logging
5.4	Management responsibilities	5.29	Information security during disruption	8.4	Access to source code	8.16	Monitoring activities
5.5	Contact with authorities	5.30	ICT readiness for business continuity	8.5	Secure authentication	8.17	Clock synchronisation
5.6	Contact with special interest groups	5.31	Legal, statutory, regulatory and contractual req.	8.6	Capacity management	8.18	Use of privileged utility programs
5.7	Threat intelligence	5.32	Intellectual property rights	8.7	Protection against malware	8.19	Installation of software on operational systems
5.8	Information security in project management	5.33	Protection of records	8.8	Management of technical vulnerabilities	8.20	Networks security
5.9	Inventory of inf. and other associated assets	5.34	Privacy and protection of pers. identifiable infor. (PII)	8.9	Configuration management	8.21	Security of network services
5.10	Acceptable use of inf. and other associated assets	5.35	Independent review of information security	8.10	Information deletion	8.22	Segregation of networks
5.11	Return of assets	5.36	Compliance with policies, rules and standards for IS	8.11	Data masking	8.23	Web filtering
5.12	Classification of information	5.37	Documented operating procedures	8.12	Data leakage prevention	8.24	Use of cryptography
5.13	Labeling of information	6. People Controls				8.25	Secure development life cycle
5.14	Information transfer	6.1	Screening	6.5	Resp. after termination or change of employment	8.26	Application security requirements
5.15	Access control	6.2	Terms and conditions of employment	6.6	Confidentiality or non-disclosure agreements	8.27	Sec. system architecture and engineering princples
5.16	Identity management	6.3	Inf. security awareness, education and training	6.7	Remote working	8.28	Secure coding
5.17	Authentication information	6.4	Disciplinary process	6.8	Information security event reporting	8.29	Security testing in development and acceptance
5.18	Access rights	7. Physical Controls				8.30	Outsourced development
5.19	Information security in supplier relationships	7.1	Physical security perimeters	7.8	Equipment siting and protection	8.31	Separation of development, test and production
5.20	Addressing inf. security w/in supplier agreements	7.2	Physical entry	7.9	Security of assets off-premises	8.32	Change management
5.21	Managing IS[1] in the ICT[2] supply chain	7.3	Securing offices, rooms and facilities	7.10	Storage media	8.33	Test information
5.22	Monitoring, review and change mgmt. of supplier	7.4	Physical security monitoring	7.11	Supporting utilities	8.34	Protection of inf. systems during audit testing
5.23	Information security for use of cloud services	7.5	Protecting against phys. and environmental threats	7.12	Cabling security		
5.24	IS Incident management planning and preparation	7.6	Working in secure areas	7.13	Equipment maintenance		
5.25	Assessment and decision on IS events	7.7	Clear desk and clear screen	7.14	Secure disposal or re-use of equipment		

Source: ISO.org I 1: IS = Information security I 2: ICT = ICT = Information and communication technology

Figure 14: Topics of an ISMS with tool examples

Processes are handled in the Plan-Do-Check-Act (PDCA) cycle:

- **Plan:** The example process of information classification is described in the corresponding guideline. Measures and implementation must be checked for feasibility in advance with the responsible experts.
- **Do:** Processes, measures and controls are implemented. This also includes training and awareness programs for employees. Effectiveness must be ensured through 1LoD controls.
- **Check:** The effectiveness of the information classification is monitored and regularly reviewed. To this end, regular checks are carried out within the 1LoD as well as through checks of the 2LoD and 3LoD.
- **Act:** A Based on the findings of the check phase, the ISO function and 1LoD take corrective and preventive measures such as updating guidelines and work instructions, improving the process or the reporting system.

The interaction of the four phases is crucial to ensure the effectiveness of the processes and thus of the ISMS as a whole, which needs to be adjusted to changes in the organisation, new attacks and threats, and new compliance requirements.

The Path to a Certified ISMS

Generally, the functionality and effectiveness of the ISMS must be continuously assessed. During the establishment of an ISMS, it should undergo an initial audit. This occurs in Phase 5 in Figure 11. If the ISMS is to be certified, various audits are obligatory before the certification examination (Phase 5 in Figure 15): The ISO function presents the annual effectiveness review to the management level. This continuous evaluation is measured through KPIs, KRIs, and KCIs (Key Indicators for Performance, Risk, and Compliance). In the first year of an established ISMS, a total of ten KXIs can be used, and after final expansion, a maximum of 30 KXIs should be employed for practicality. Both the 2LoD and the 3LoD must conduct their own effectiveness audits. The ISO function must audit the entire spectrum of ISMS topics, i.e., all 93 security objectives of the 14 domains from Figure 13, in a cycle of three years. Particularly important areas must be audited more frequently. The internal audit checks on a sample basis and independently of all other functions and lines of defence.

The increasing number of regulatory demands for an ISMS and the burden of proof on the operators to demonstrate the protection of information necessitate a transparent and demonstrable management of information security within a management system.

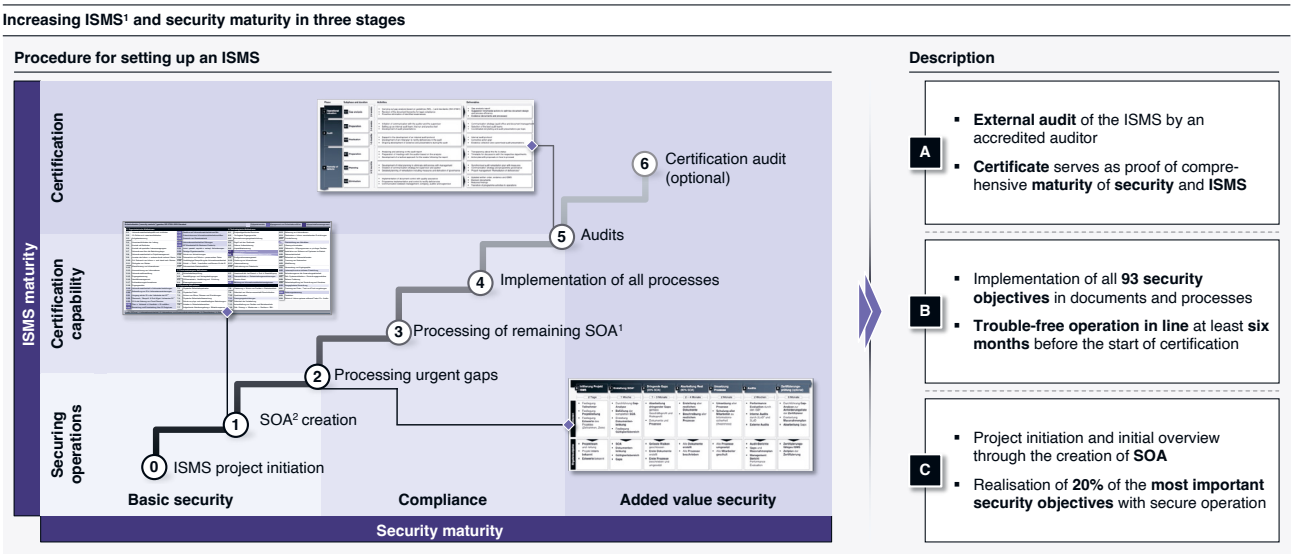


Figure 15: Expansion stages of an ISMS and corresponding security properties

The initial stage of the ISMS encompasses the first three phases (0 to 2) in Figure 15 and ensures operation against the most urgent identified gaps. This ISMS is neither compliant with regulations nor does it yet provide added security value, for instance, to investors.

The second stage of development (phases 3 to 5) establishes the certification readiness of the ISMS: the ISMS is fully developed. Certification is achieved only in the third stage with phase 6. This provides added security value to investors, regulators, supervisors, and customers. The ISO 27001 certification is a coveted hallmark of an organisation's information security maturity, both internally and externally. Figure 15 does not include a timeline. Generally, a timeframe of 6 to 12 months can be expected for steps 0 to 5. The certification itself is subject to deadlines set by external auditors and may take at

least 6 months. These timeframes are based on the assumption of a closely coordinated collaboration between all stakeholders throughout the entire project duration. The maturity of information security achieved at the start of certification in step 5 significantly influences the personnel, organisational, and time investment required to obtain the certificate in step 6. The decision for or against certification should be derived from the goals set forth in the business strategy.

Figure 16 depicts the relationship between the number of ISO 27001 certificates worldwide, the increase in financial regulatory audits ("§ 44 audits") in Germany, and the number of ISO certificates of EUROSTOXX 50 companies.

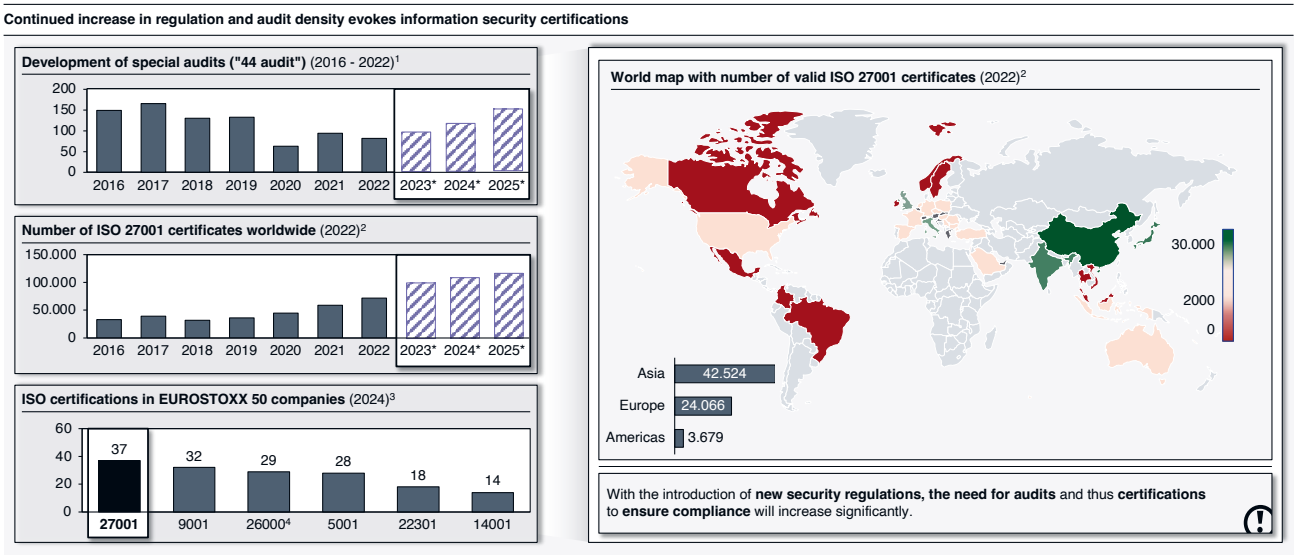


Figure 16: New regulation enforces higher audit and certification efforts

Regarding the forecasts in Figure 16: special inspections will increase as DORA raises the number of supervisory objects. The number of ISO 27001 certificates will also increase as a certified ISMS is required by further laws. The importance of information security is also evident among EUROSTOXX 50 companies: with 37 ISO 27001 certificates, they form the largest group. In summary: The more companies fall under a security law, the more ISMS will be certified.

The latest releases of ISO standards and the expansion of supervised sectors indicate a future increase in security certifications, such as ISO 21434 "Road vehicles – Cybersecurity engineering" or TISAX14 in the German automotive industry, based on ISO 27001. Generally, operators of critical infrastructures must demonstrate minimum security according to the IT Security Act, for which a functional and effective ISMS provides the best evidence.

Summary

The increasingly digital nature of economy, society, and governance expands the cyberattack surface both horizontally and vertically. As businesses strive to maintain customer trust, they inherently seek to enhance the maturity of their information security. Simultaneously, legislators and regulators respond to the escalating monetary and non-monetary losses from successful attacks with more security laws and assessments of organisational security maturity. There is a growing trend towards regulatory demands for an ISMS, either implicitly or explicitly.

The white paper initially introduces the upcoming regulatory framework of Network and Information Security 2 (NIS2) Directive, the Critical Entities Resilience (CER), and Digital Operational Resilience Act (DORA), along with their national implementation in Germany. Within this context, a dual burden for operators of critical infrastructure within the financial sector is highlighted. Leveraging the new regulations, the information security management system (ISMS) based on ISO 27001 standard is described as a fundamental structural element of the security organisation, using a banking organisation as an example in the development of an ISMS. Various ISMS topics are illustrated with examples for tool-supported ISMS operations. This emphasises the necessity for the setup to be treated as a project before transitioning to operational status. The proposed approach consists of seven phases, including certification. Inspired by the financial industry, the model of the three lines of defence (3LoD) is introduced for safeguarding corporate assets, further expanded by the authors to include the government as a fourth line of defence (4LoD), particularly in critical infrastructure scenarios.

While more companies are required to establish and operate an ISMS, for certain industries, a certified ISMS is already mandatory. The ISMS structural element offers compelling benefits for managing the security organisation even without regulatory pressure: Firstly, it ensures that critical security issues cannot be overlooked (Function Checklist). Secondly, an ISO 27001-ISMS, as a globally recognised standard, provides access to worldwide expertise, thoroughly considered by experts in the past, practiced in companies, mandated by legislators, and scrutinised by regulators (function recognised good practice). Thirdly, this management system serves as a hub for various communication channels between IT operations, monitoring functions, management, and oversight, thus integrating operational, tactical, and strategic security aspects within an organisational framework (function communication hub). Fourthly, an ISMS serves as a template for structuring additional compliance tasks such as data protection, anti-money laundering, and ESG, meaning that companies with an ISMS based on the ISO 27001 standard become future proof (function model). Lastly, demonstrating security maturity serves as relevant evidence of corporate maturity for potential investors (function attractiveness for investments). Defined as a management system, an ISMS significantly contributes to the success of a company.

Sources

1. EU-General Data Protection Regulation (GDPR).
2. EU Digital Operational Resilience Act (DORA).
3. EU Cyber Resilience Act (CRA).
4. EU Directive on measures for a high common level of cybersecurity (NIS2).
5. EU Directive on the resilience of critical entities (CER).
6. Germany (BMI). Discussion Paper, Status: 07.05.2024, of the Federal Ministry of the Interior and Community.
7. Germany (BMI). Law on the Federal Office for Information Security (BSI-Gesetz - BSIG).
8. Germany (BMI). Draft Bill of the Federal Ministry of the Interior and Community for the Implementation of Directive (EU) 2022/2557 and for Strengthening the Resilience of Operators of Critical Facilities (KritisDachG).
9. Germany (BMI). Ordinance on the Determination of Critical Infrastructures according to the BSI Act (BSI-Kritisverordnung - BSI-KritisV).
10. Germany (BMF). Draft Law of the Federal Government: Draft Law on the Digitalization of the Financial Market (Finanzmarktdigitalisierungsgesetz - FinmadiG).
11. Germany. Law on Electricity and Gas Supply (EnWG).
12. EBA. Guidelines for the Management of ICT and Security Risks.
13. Switzerland (FINMA). Operational Risks and Resilience - Banks.
14. Trusted Information Security Assessment Exchange (TISAX).

List of Abbreviations

Abbreviations	Description
BaFin	German federal financial supervisory authority
BAIT, KAIT, VAIT, ZAIT	BaFin: Banking supervisory / capital management supervisory / insurance supervisory / payment services supervisory IT requirements
BSI	German federal office for information security
CER	Resilience of critical entities directive
CIA	Confidentiality, integrity, availability
CRA	Cyber resilience act
DORA	Digital operational resilience act
DPO	Data protection officer
GDPR	General data protection regulation
EBA	European banking authority
EIOPA	European insurance and occupational pensions authority
EnWG	Energy industry act
ESMA	European securities and markets authority
FINMA	Swiss financial market supervisory authority
FMA	Austrian financial market authority
HLS	High level structure
ICS	Internal control system

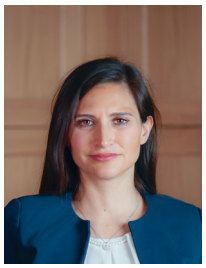
Abbreviations	Description
ISO	Information security officer
KPI, KRI, KCI	Key performance indicators, Key risk indicators,
Key compliance indicators	KRITIS-Dachgesetz
CRITISDachG	CRITIS umbrella law
CritisV	BSI criticality ordinance
MaX	Summary of BaFin's minimum requirements for risk management MaRisk, MaGo, KAMaRisk
NIS	Network and information security
NIS2UmsuCG	NIS-2 implementation and cybersecurity strengthening act
SOA	Statement of applicability
TISAX	Trusted information security assessment exchange
ToD, ToI, ToE	Test of Design, Test of Implementation, Test of Effectiveness
XAIT	Summary of the supervisory requirements of BaFin BAIT, KAIT, VAIT and ZAIT

Authors

Dr. Waldemar Grudzien | Managing Director

Waldemar is an expert in financial supervisory audits, information security, and data protection. He supports clients with audits and compliance with relevant requirements. As an electrical engineer with a doctorate and a qualified economist, he worked for an association in the credit industry as an expert in security for retail and online banking.

Mail: wgr@globalregulation.com



Nadine Hofmann | Director

Nadine is an expert in information security and data protection management systems according to ISO standards. This includes the implementation of measures for financial institutions, from defining requirements and processes to preparing for audits and migrating audit results. She completed her aerospace engineering studies at TU Braunschweig and TU Dresden.

Mail: nho@globalregulation.com

Victoria Denisiuk | Manager

Victoria is a Manager at GRM. She specialises in digital transformation, including strategic modernisation, intelligent automation, and the optimisation of information systems. With her expertise in business analysis, project management, and technology implementation, she drives operational efficiency and develops secure solutions for businesses.

Mail: vde@globalregulation.com

Galina Slobodianiuk | Associate Consultant

Galina is a Consultant at GRM. She holds a Bachelor‘s degree in Finance and a Master‘s degree in Business Administration from Humboldt University of Berlin, with a focus on data analysis. Her solid experience in finance and data analysis gives her a strong understanding of business process management and the execution of market analyses.

Mail: gsl@globalregulation.com

About Global Regulation Management AG

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

Copyright Notice

The information provided serves exclusively for general informational purposes. It makes no claim to be current or complete and is subject to individual interpretation. An independent verification of the information is expressly recommended.

We assume no liability for any errors, omissions, or inaccuracies, or for consequences arising from the use of the information. Likewise, we are not responsible for content on linked third-party websites.

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

Global Regulation Management AG
Baarerstrasse 52
6300 Zug
Schweiz

info@globalregulation.com
https://globalregulation.com