GRM® Global Regulation

King of the Audits

27001

Dr. Waldemar Grudzien
Nadine Hofmann
Victoria Denisiuk
Galina Slobodianiuk

Mai 2024
White Paper

Management Summary

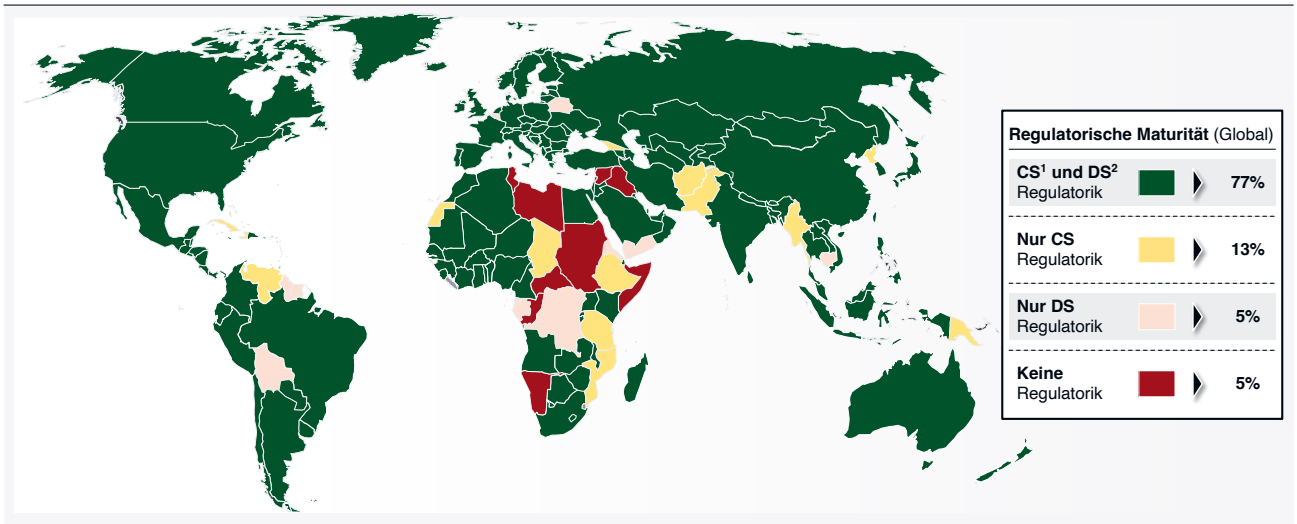
- Die Europäische Union (EU) motiviert die Wirtschaft mit den Regularien Netzwerkinformations- und Sicherheitsrichtlinie (NIS2), Richtlinie über die Resilienz kritischer Einrichtungen (CER) und Richtlinie über die digitale Resilienz operationeller Risiken (DORA) zu mehr Informationssicherheit und Resilienz, insbesondere Unternehmen der kritischen Infrastruktur sind betroffen.
- Deutsche Finanzmarktakteure unterliegen zweifachem Regulierungsstandard aus NIS2 und DORA, wenn sie gleichzeitig Betreiber kritischer Anlagen sind.
- Unternehmen müssen sich zu den selbstähnlichen Sicherheitsanforderungen aus immer neuen Regulierungen verhalten und Konformität neu nachweisen.
- Informationssicherheit und Resilienz sind im Rahmen eines Managementsystems zu organisieren.
- Mit einem Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001-Standard erreichen Unternehmen rechtliche Agilität und auf Wunsch eine zertifizierte Sicherheitsreife.
- Der Aufbau eines ISMS sollte als Projekt, in grösseren Organisationen als Programm durchgeführt werden.
- Das vorliegende Whitepaper zeigt ein zertifikatbewährtes Vorgehensmodell zum Aufbau und Betrieb eines ISMS auf.

Sicherheitsanforderungen der EU stellen Unternehmen vor Herausforderungen

Weltweit steigen Anforderungen der Regulierung von Datensicherheit und Datenschutz. Zur Datensicherheit zählen Cybersicherheit, IT-Sicherheit, Informationssicherheit und Resilienz. Datenschutz steht für Gewährleistung des Rechts auf informationelle Selbstbestimmung. In über 75% aller Länder sind sowohl die Regelung der einen regulatorischen Sphäre als auch der anderen etabliert, während lediglich 5% keine spezifischen Vorschriften zu beiden Segmenten haben (Abbildung 1). Insofern ist die Regulierung beider Sphären für die Staatengemeinschaft essenziell.

Die Regulierungen der EU zu Datenschutz (DSGVO)[1], Resilienz (DORA[2], CRA[3]) und Sicherheit (NIS2[4], CER[5]) sind weltweit prägend für viele Jurisdiktionen.

Gesetze zu Cybersicherheit (CS) und Datenschutz (DS) weltweit (2021)



Quelle: UNCTAD Data Protection and Privacy Legislation Worldwide & Cybercrime Legislation Worldwide I 1: CS = Cybersicherheit I 2: DS = Datenschutz

Abbildung 1: Regulierung von Cybersicherheit und Datenschutz ist weltweit nahezu ubiquitär

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit in der Version 2.0 (NIS2) weitet im Vergleich zur NIS1-Version Cybersicherheitsvorgaben auf mehr Unternehmen aus: Unter die NIS1-Richtlinie fallen ca. 2.000 Unternehmen in Deutschland, für die NIS2-Richtlinie geht das Bundesministerium des Inneren von ca. 30.000 Unternehmen aus. Für die EU rechnet die Europäische Kommission mit 160.000 Unternehmen im Geltungsbereich. Somit vervielfacht sich in Deutschland die Menge der zur Cybersicherheit beaufsichtigten Unternehmen um mindestens das 15-fache.

Während bei der NIS-Richtlinie die Cybersicherheit im Mittelpunkt steht, ist es bei der CER-Richtlinie die Resilienz kritischer Einrichtungen mit Fokus Katastrophenschutz. Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschlägen oder Sabotage zu stärken.

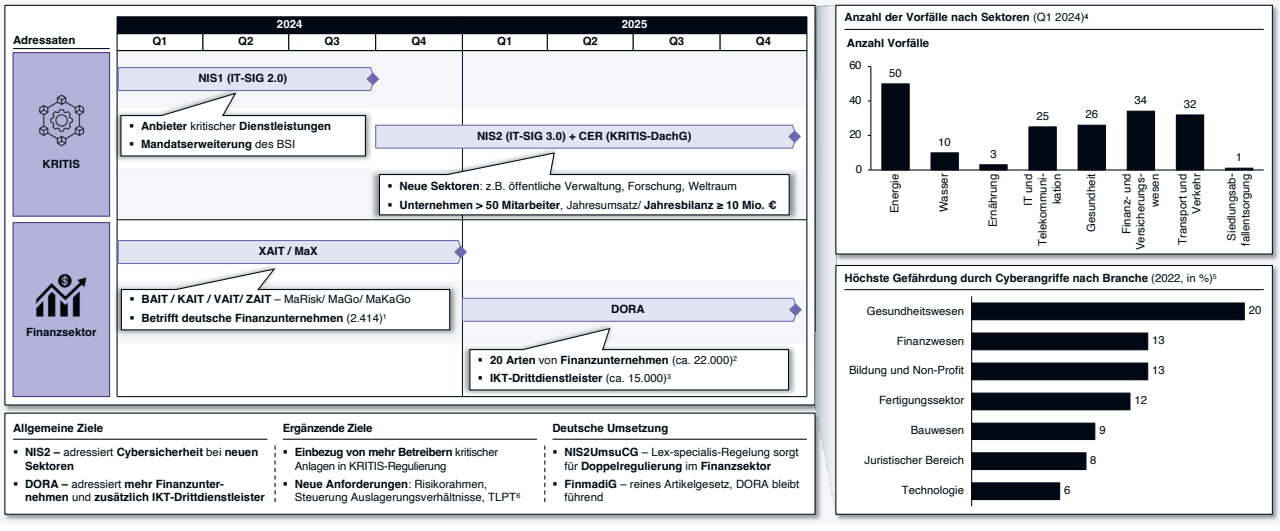
DORA ist die erste branchenspezifische europäische Regulierung der Cybersicherheit. Mit der DORA haben Unternehmen digitale operative Resilienz nachzuweisen, denn sie weitet im Vergleich zur heutigen Anwendung den Aufsichtsrahmen auf 20 Arten von

Finanzunternehmen sowie zusätzlich auf Informations- und Kommunikationstechnologie-Drittdienstleister (IKT-DDL) aus. Diese erbringen IKT-Dienstleistungen für Finanzunternehmen. Durch DORA unterstehen erstmals kritische IKT-DDL wie beispielsweise Hyperscaler der direkten finanzaufsichtlichen Überwachung. DORA fordert von den Finanzunternehmen eine solide risikoorientierte Überwachung der IKT-Drittparteirisiken. Nach Einschätzung der EU werden ca. 22.000 Finanzunternehmen und ca. 15.000 IKT-DDL in der EU in den Anwendungsbereich der DORA fallen (Abbildung 2).

DORA ist für den Finanzsektor lex specialis gegenüber der NIS2: Fällt ein Unternehmen in die Anwendungsbereiche von DORA und NIS2 und sind die Anforderungen in DORA spezifischer, haben diese Vorrang vor den Anforderungen der NIS2-Richtlinie. Insbesondere die zwei Regulierungsschwerpunkte IKT-Risikomanagementrahmen und Meldung von IKT-Vorfällen sind in der DORA spezifischer für den Finanzsektor als in der NIS2 ausgeführt.

In Abbildung 2 wird der Übergang der Finanz-IT-Aufsicht von einer nationalen zu einer europäischen Aufsicht der KRITIS-Sektoren und des Finanzsektors veranschaulicht: In Deutschland der Übergang von NIS1 zu NIS2 und CER für alle KRITIS-Sektoren als auch der Übergang von den aufsichtlichen Anforderungen an die IT verschiedener Finanzentitäten (XAIT) und Mindestanforderungen an das Risikomanagement dieser Entitäten (MaX) zu DORA für den Finanzsektor. Geprüft werden Finanzunternehmen weiterhin national, allerdings werden die nationalen Aufsichtsbehörden enger mit den europäischen Aufsichtsbehörden und untereinander kooperieren.

Zeitplan und Herausforderungen der Umsetzung von Cybersicherheits- und Resilienzregulierungen im Finanzsektor



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

Abbildung 2: 2024 ist Übergangsjahr von nationaler zu europäischer Regulierung

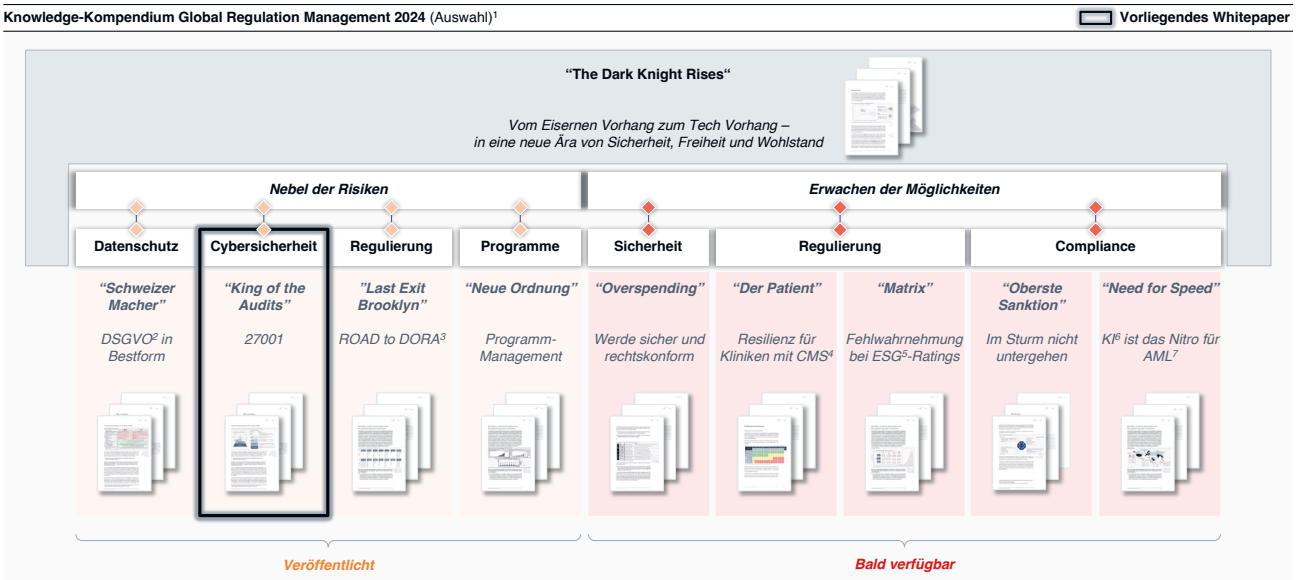
Zusätzliche Anforderungen an die Sicherheit von Produkten, Services und Dienstleistungen erfahren Finanzunternehmen und IKT-Drittdienstleister aus weiteren bereits wirksamen Regulierungen und aus sich im Gesetzgebungsverfahren befindlichen Regulierungsvorhaben. Zur ersten Gruppe gehören die EU-DSGVO, der ESG-Gesetzeskanon (Environment, Social, Governance) und der EU Data Act, zur zweiten Gruppe der EU Cyber Resilience Act und die EU KI-Verordnung. Diese Vorhaben werden in der vorliegenden Ausfertigung nicht betrachtet, sind aber teilweise

Gegenstand weiterer Publikationen von Global Regulation Management (Abbildung 3). Es bleibt abzuwarten, ob und wie sich diese durch die Wirtschaft oft als Überregulierung empfundene Regulierungsdichte auf Sicherheit und Resilienz positiv auswirken wird oder ob sich Überforderungseffekte zeigen, begleitet von „Ermüdungsbrüchen“ in Form von abnehmender Sicherheit und Resilienz der IKT-Infrastrukturen.

Im vorliegenden Whitepaper wird am Beispiel Deutschlands ausgeführt, wie die neuen Compliance-Anforderungen die Wirtschaft tangieren. Zur Umsetzung der regulatorischen Anforderungen wird ein geeignetes ISMS identifiziert und am Beispiel einer Bank der Aufbau des ISMS dargelegt.

Rahmenpublikation der Chancen und Risiken

Die vorliegende Ausarbeitung „King of the Audits - 27001“ stellt die Cybersicherheitsregulierung in der EU und das ISMS nach ISO 27001-Standard als angemessenes Mittel der Sicherheitsorganisation dar. Die Ausarbeitung fügt sich in den übergreifenden Rahmen unseres Whitepapers „The Dark Knight Rises“ ein, wobei in den beiden zusammenhängenden Dimensionen Risiko und Opportunität die Veränderungen der Wirtschaftswelt seit der Rückkehr der Blockbildung in Risiko-, Regulations-, IT-, Sicherheits- und Sanktionsfragen übergeordnet behandelt werden (Abbildung 3).



Quelle: GRM I 1: Weitere Veröffentlichungen auf Anfrage erhältlich I 2: DSGVO = Datenschutz Grundverordnung I 3: DORA = Digital Operational Resilience Act I 4: CMS = Compliance Management System I 5: ESG = Environmental, Social, Governance I 6: KI = Künstliche Intelligenz I 7: AML = Anti-Money Laundering (Geldwäschebekämpfung)

Abbildung 3: Übersicht Kompetenzbereiche

Rechtlicher Abriss

Im folgenden Kapitel wird die deutsche Umsetzung der europäischen drei Regularien NIS2-Richtlinie, CER-Richtlinie und DORA-Verordnung vorgestellt und diskutiert.

Umsetzung der NIS2-Richtlinie durch NIS2UmsuCG

In Deutschland wird die NIS2-Richtlinie durch das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG[6]) bis zum 1. Oktober 2024 umgesetzt.

Das NIS2UmsuCG als Artikelgesetz ändert bestehende Gesetze, so auch das BSI-Gesetz[7] (IT-SiG 2.0), das durch Einbettung der NIS2 zum „IT-SiG 3.0“ wird. Dieses definiert drei Arten von Einrichtungen: „besonders wichtige Einrichtungen“, „wichtige Einrichtungen“ und „Domain Name Registry Diensteanbieter“ (Abbildung 4). Nach § 30 (1) NIS2UmsuCG sind die „Einrichtungen verpflichtet, geeignete, verhältnismässige und wirksame technische und organisatorische Massnahmen zu ergreifen, um Störungen der Vertraulichkeit, Integrität und Verfügbarkeit (engl. CIA) der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.“ Abbildung 4 stellt die wesentlichen Sicherheitsanforderungen an die drei Einrichtungsarten aus dem NIS2UmsuCG dar.

Kategorisierung und Anforderungen an Organisationen nach dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ✓ gilt ✗ gilt nicht

Inhalt NIS2UmsuCG	Besonders wichtige Einrichtung							Wichtige Einrichtung		Domain Name Register – Anbieter
	Einrichtung gem. Anlage 1 NIS2UmsuCG[1]	Qualifizierte Vertrauens-dienstleister	Top Level Domain Name Register	Domain Name System -Diensteanbieter	Telekommuni-kationsdienste[2]	Betreiber kritischer Anlagen	Einrichtung gem. Anlage 3 NIS2UmsuCG	Einrichtung g. Anlagen 1 & 2 NIS2UmsuCG[3]	Vertrauens-diensteanbieter	
§30 (1)(2): Massnahmen	✓	✓	✗	✗	✓	✓	✓	✓	✓	-
§30 (6): Zertifizierte Produkte	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§30 (7): Informationsaustausch	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§30 (9): Recht auf branchenspez. Sicherheitsstand.	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§31: Bes. RM-Anf. von Betreibern krit. Anl.	✗	✗	✗	✗	✗	✓	✗	✗	✗	-
§32: Meldepflichten	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§33: Registrierung	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
§35: Unterrichtung	✓	✓	✗	✗	✓	✓	✓	✓	✓	-
§38: Pflichten der Geschäftsführung	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
§39: Nachweispflichten für Betreiber krit. Anl.	✓	✓	✓	✓	✓	✓	✓	✗	✗	-
§51: Führen einer Datenbank	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
§52: Zugangsgewährung	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓
§53: Kooperationspflicht	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Quelle: NIS2UmsuCG I GRM I 1: ≥250 Mitarbeiter oder >50 Mio. € Umsatz und >43 Mrd. € Bilanz I 2: ≥50 Mitarbeiter oder >10 Mio. € Umsatz und >10 Mio. € Bilanz I 3: ≥ 50 Mitarbeiter oder >10 Mio. € Umsatz und >10 Mio. € Bilanz

Abbildung 4: Wesentliche Sicherheitsanforderungen aus dem NIS2UmsuCG

Die Massnahmen sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen (Artikel 21 NIS und analog § 30 NIS2UmsuCG). Für die Betreiber kritischer Anlagen unter den besonders wichtigen Einrichtungen gelten erhöhte Anforderungen aus § 31 NIS2UmsuCG.

Umsetzung der CER-Richtlinie durch das KRITIS-Dachgesetz

Die CER-Richtlinie wird in Deutschland durch das KRITIS-Dachgesetz (KRITIS-DachG[8]) bis zum 17. Oktober 2024 umgesetzt. In § 3 Abs. 3 KRITIS-DachG werden 18 kritische Dienstleistungen definiert. Den Anwendungsbereich des Gesetzes definiert § 4 Abs. 1 KRITIS-DachG, wonach eine Anlage als kritische Anlage definiert ist, wenn sie einer der durch Rechtsverordnung nach § 16 Abs. 1 festgelegten Anlagenarten in den Sektoren Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung zuzuordnen ist und diese, die durch Rechtsverordnung nach § 16 Abs. 1 KRITIS-DachG festgelegten Schwellenwerte, erreicht. Generell ist eine Anlage ab 500.000 zu versorgenden Einwohnern (sog. Regelschwellenwert) als kritisch einzustufen.

Auch die CER-Richtlinie kennt eine Lex-specialis-Regelung (§ 4 Abs. 6 KRITIS-DachG): Betreiber kritischer Anlagen der Sektoren Bankwesen, Finanz- und Versicherungswesen sowie Informationstechnik und Telekommunikation fallen nicht unter die §§ 7 bis 12 KRITIS-DachG.

Das KRITIS-DachG wird weder sektoren- noch branchenspezifische Regelungen treffen, sondern allen KRITIS-Sektoren geeignete und verhältnismässige Massnahmen zum physischen Schutz vorgeben. Es enthält Resilienzziele in § 10 Abs. 1 KRITIS-DachG, die Betreiber kritischer Anlagen mit ihren Massnahmen erreichen müssen sowie zur Orientierung eine Übersicht von beispielhaften Massnahmen in § 10 Abs. 3 KRITIS-DachG, die Betreiber treffen können (Abbildung 5).

Zur weiteren Konkretisierung von sektorübergreifenden Resilienzmassnahmen wird das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) – voraussichtlich zu Anfang 2026 – einen Katalog mit Mindestanforderungen erarbeiten. Angelehnt an die bekannten branchenspezifischen Sicherheitsstandards bei der IT-Sicherheit (B3S) können die Betreiber kritischer Anlagen und ihre Verbände branchenspezifische Resilienz-Standards entwickeln.

Geschäftsleiter von Betreibern kritischer Anlagen sind inklusive einer Haftungsregelung und Schulungspflicht nach § 11 KRITIS-DachG verpflichtet, die zur Einhaltung von § 10 KRITIS-DachG ergriffenen Massnahmen zu billigen und ihre Umsetzung zu überwachen. Seit der DSGVO ist bekannt, wie wichtig Sanktionsmöglichkeiten für die Durchsetzung einer Regelung sind. Insofern sind die Bussgeldvorschriften nach § 19 KRITIS-DachG für elf Ordnungswidrigkeiten als konsequente Fortschreibung dieser Sanktionspraxis zu verstehen.

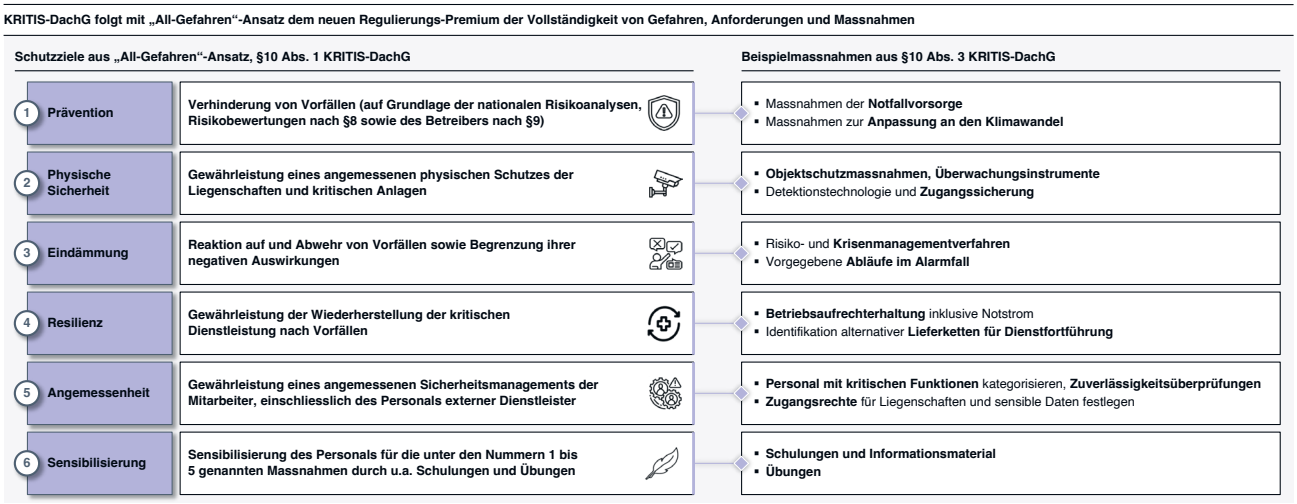


Abbildung 5: Massnahmen zum physischen Schutz für Betreiber kritischer Anlagen

Auf Basis der nationalen Risikoanalysen müssen die Betreiber kritischer Anlagen eigene Risikoanalysen erstellen. Mit § 11 KRITIS-DachG wird das Institut der Sonderprüfung in KRITIS eingeführt: Kann ein Betreiber einer kritischen Anlage nicht den Nachweis der Einhaltung der Resilienzmassnahmen erbringen, kann dies durch die zuständige Aufsichtsbehörde überprüft werden.

Derzeit bestimmen Betreiber eigenständig, ob sie ein Betreiber kritischer Anlagen sind. Hierzu steuert die am 01.01.2024 in Kraft getretene vierte „Verordnung zur Bestimmung Kritischer

Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung, nachfolgend: BSI-KritisV)[9] sowohl die Definition kritischer Dienstleistungen als auch die Schwellenwerte bei.

Um divergierende Bestimmungen zu kritischen Anlagen im Sinne des KRITIS-DachG und im Sinne des BSI-Gesetzes (BSIG) zu vermeiden, werden Betreiber kritischer Anlagen künftig nur noch durch das KRITIS-DachG bestimmt. Darüber hinaus werden für die Registrierung der Betreiber sowie für die Meldung von erheblichen Störungen gemeinsame technische Lösungen angestrebt, sodass in Zukunft beide gesetzlichen Meldepflichten aus dem BSIG und dem KRITIS-DachG im Rahmen einer Meldung erfolgen können.

Umsetzung der DORA durch das FinmadiG

In Deutschland wird DORA durch das am 23.10.2023 im Entwurf veröffentlichte Finanzmarktdigitalisierungsgesetz (FinmadiG)10 umgesetzt. DORA stärkt die digitale operationale Resilienz des gesamten europäischen Finanzsektors. Die drei Europäischen Aufsichtsbehörden (ESAs, European Supervisory Authorities) EBA (European Banking Authority, deutsch: Europäische Bankenaufsichtsbehörde), EIOPA (European Insurance and Occupational Pensions Authority, deutsch: Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) und ESMA (European Securities and Markets Authority, deutsch: Europäische Wertpapier- und Marktaufsichtsbehörde) erarbeiten gemeinsam technische Regulierungsstandards (RTS) und Implementierungsstandards (ITS) sowie Leitlinien (GL) zur Interpretierung und Konkretisierung der DORA. Im Finanzsektor werden Betreiber kritischer Anlagen durch DORA und NIS2 zweifach reguliert: Zwar bietet die Lex-specialis-Regelung der NIS2 durch § 28 Abs. 5 Nr. 1 NIS2UmsuCG einen Einstieg in die Spezialregulierung der DORA, allerdings verbleiben nach § 28 Abs. 1 Nr. 1 NIS2UmsuCG Finanzunternehmen, die Betreiber kritischer Anlagen sind, parallel im Geltungsbereich der NIS2: Kritisch sind demnach die Dienstleistungen Bargeldversorgung, kartengestützter Zahlungsverkehr, konventioneller Zahlungsverkehr, Handel mit Wertpapieren und Derivaten, die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften, Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende.[9]

Die deutsche Umsetzung von NIS2, CER und DORA resultiert in einer regulatorischen Zweifachbelastung für Anbieter von sechs Zahlungsdienstleistungen.

Der deutsche Finanzsektor ist in einer komfortablen Startposition für die Anwendbarkeit von DORA. Die BaFin hat bereits vor Jahren für den deutschen Finanzplatz Sicherheitsanforderungen aufgestellt als auch überwacht: für die IKT-Sicherheit durch die harmonisierten Anforderungen an das IKT-Risikomanagement für Finanzbereiche (XAIT), für vereinheitlichte Auslagerungsanzeigen, für den Überwachungsrahmen für IT-Mehrmandantendienstleister sowie für die vereinheitlichten Strukturen für das Meldewesen von IKT-bezogenen Vorfällen.

Umsetzungshürden

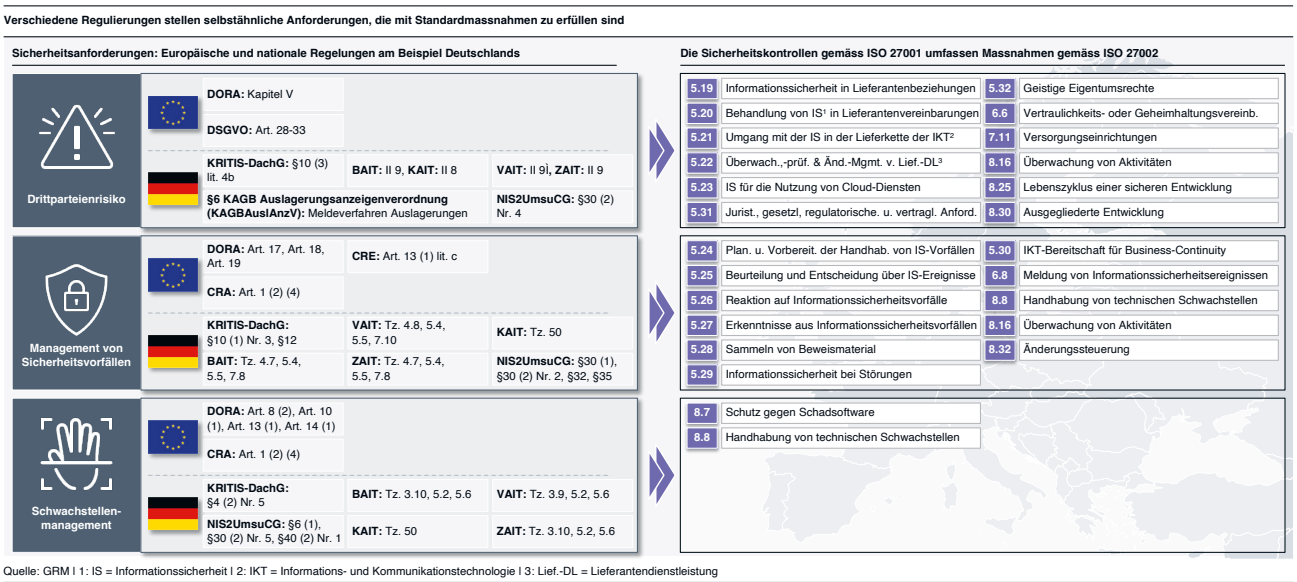
Die Implementierung der Anforderungen stellt Unternehmen vor die Herausforderung des Managements gleicher Anforderungen aus verschiedenen Gesetzen und der Auswahl eines geeigneten Managementsystems der Informationssicherheit.

Management selbstähnlicher Forderungen

Während die NIS2-Richtlinie eine Weiterentwicklung der bereits bekannten und adaptierten NIS1 ist, sind CER und DORA neu. Gleichwohl adressieren alle drei neuen Gesetze mit den Sicherheitsanforderungen die bekannten und bereits durch die aktuell geltenden Regularien adressierten Schutzziele CIA der Informationssicherheit und damit alle Massnahmen zur Erfüllung der Schutzziele. Trotzdem muss die Erfüllung der Anforderungen der neuen Gesetze erneut nachgewiesen werden. Abbildung 6 illustriert diese Aufgabe beispielhaft an den drei Sicherheitszielen „Drittparteienrisiko“, „Management von Sicherheitsvorfällen“ sowie „Schwachstellenmanagement“ und zeigt auf, welche Massnahmen des ISO 27002-Standards diese abdecken.

Durch geltende Regulierungen wie XAIT, DSGVO etc. sind bereits viele Themen der neuen Regulierungen NIS2, CER und DORA adressiert. Trotzdem muss jede neue Regulierung neu in die Organisation integriert werden, was den Aufwand für die Einhaltung von Compliance aus mehreren Gründen erhöht: Oftmals unterscheiden sich die technischen Ausdrücke und Bezeichnungen in den Regelungen, sodass die bisherigen Anforderungen mit den zukünftigen Anforderungen abzugleichen sind. Zweitens zeichnen sich viele Begriffe durch Unklarheit aus und lassen Raum für Interpretation, was Missverständnisse und Fehler in der Ausführungspraxis provoziert.

Drittens kann die Erfüllung der neuen, zu den bereits bestehenden, ähnlichen Anforderungen, zu mehrfachen und redundanten Umsetzungen von Massnahmen führen. Dabei erhöhen NIS2, CER und DORA die Compliance-Aufwände zweidimensional: horizontal durch den erweiterten Anwendungsbereich (Abbildung 2) und vertikal durch erhöhte Sicherheitsanforderungen pro Sicherheitsziel, insbesondere in den Bereichen Berichtspflichten und Meldewesen, Schulung und Sensibilisierung, Risikomanagement, Testen und das Management von Drittanbieterrisiken.



Quelle: GRM I 1: IS = Informationssicherheit I 2: IKT = Informations- und Kommunikationstechnologie I 3: Lief.-DL = Lieferantendienstleistung

Abbildung 6: Verschiedene Gesetze mit gleichen Sicherheitsanforderungen, Kontrollen und Massnahmen

Die Sicherheit eines Geschäftsprozesses, einer Hauptanwendung und eines Unterstützungsprozesses wird durch Schutzziele, Massnahmen und

Sicherheitsanforderungen repräsentiert. Die drei Schutzziele CIA unterliegen nur einem geringen, Massnahmen einem mittleren und die durch Regularien induzierten Sicherheitsanforderungen einem starken Wandel. Die Sicherheitsanforderungen sind das „moving target". Die Schutzziele korrelieren mit den gering variierenden Schutzobjekten Infrastruktur, Anwendungen und Daten. Die Massnahmen unterliegen als rechtliche, organisatorische und technische Massnahmen einer Weiterentwicklung, die insbesondere in der technischen Komponente als jeweiliger Stand der Technik der grössten Dynamik folgt. Somit bildet in einem Geschäftsprozess bestehend aus Infrastruktur, Anwendungen und Daten die Schaffung der Gesetzeskonformität zum „moving target" die grösste Herausforderung. Insgesamt bedarf das Management von Schutzzielen, Massnahmen und Sicherheitsanforderungen eines geeigneten Organisationsrahmens.

Rahmenwerk für das Management der Informationssicherheit

Ein Rahmenwerk für Informationssicherheit strukturiert Dokumente und Prozesse sowie die Verwaltung von Informationssicherheitsrisiken als auch deren Minderung. Gleichzeitig werden Informationsressourcen einer Organisation, einschliesslich ihrer Infrastrukturen, Anwendungen und Daten erfasst. Ermöglicht wird die Organisation der Sicherheit aus mehreren Blickwinkeln, um die Wahrscheinlichkeit von Schwachstellen und Sicherheitsverletzungen aus interner und externer Perspektive zu verringern.

Meistgenutzte Cybersicherheitsrahmenwerke im Vergleich

Empfehlung

	NIST	ISO	ISACA	CIS	CSA	HITRUST	GDPR	PCI DSS	AICPA
Herausgeber	▪ **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)
Anwendung	▪ **Alle Unternehmen** inkl. KRITIS	▪ **Alle Unternehmen**	▪ Unternehmens-IT und **IT-Management**	▪ Unternehmen mit **Schwachstellen in den Cyber-Schutz-mechanismen**	▪ **Cloud**-Dienste/-Unternehmen	▪ **Gesundheitswesen**	▪ Von **EU-Bürgern personenbezogene Daten** verarbeitende Unternehmen	▪ **Regierung** und deren **Auftragsnehmer**	▪ **Dienstleistungs-unternehmen**
Ziele	▪ Verwalten von **CS[1]-Risiken** ▪ Unabhängige Standards und **Best Practices**	▪ **Einrichtung** eines **ISMS[2]** ▪ Kontinuierliche Verbesserung zur **Sicherung der Informationswerte** des Unternehmens	▪ **Angleichung der IT- und Geschäftsziele**, die üblicherweise für die Einhaltung von SOX[3] verwendet werden	▪ **Priorisierung tech-nischer Massnah-men** zur Stärkung der Cybersicherheit ▪ **Verteidigung gegen** bekannte **Cyber-Bedrohungen**	▪ Unterstützung von Cloud-Kunden bei der **systematischen Bewertung des Gesamtsicherheits-risikos** der Implementierung von Cloud-Dienstanbietern	▪ Bereitstellung eines **strukturierten Ansatzes für den Sicherheits- und Datenschutzrahmen** für Organisationen ▪ **Verwaltung** des **Datenschutzes**	▪ **Datenkontrolle** für Betroffene	▪ **Sicherheits-standards** für Kreditkartendaten-Verarbeiter	▪ Sichere **Datenver-waltung** (Lieferkette)
Umfang	▪ Verwalten und behandeln von **Cyberangriffen**	▪ **Informationssicher-heit** (Organisation, Technik, physisch, Personal)	▪ **Gewinnrealisierung** ▪ Management **operat-ionelles Risiko** und **Ressourcen**	▪ **Technische Sicher-heit** und operative Kontrollen ▪ **Risikoreduzierung** ▪ **Resilienzerhöhung**	▪ **17 Sicherheits-domänen** ▪ 197 Kontrollziele	▪ **Risikoanalyse** ▪ **Risikomanagement** ▪ **Operative Anforderungen**	▪ **Personenbezogene Datenverarbeitung** innerhalb als auch ausserhalb der EU	▪ **Standards für Zah-lungstransaktionen**	▪ SOC 1: **Finanzbericht-erstattung** ▪ SOC 2: **NF[4]-Kon-trollen**
Zertifizierung	▪ **Keine Zertifizierung**	▪ **Zertifizierbar** nach ISO 27001 ▪ Erfüllt GDPR, SOC2, PCI DSS, HIPAA ▪ Angleichung an NIST	▪ Nur für **Personen**	▪ **Keine Zertifizierung** ▪ Erfüllt regulatorische Standards wie GDPR, HIPAA, und PCI DSS	▪ Nur für **Personen** ▪ Abgebildet gegen u.a. ISO 27001/-17/, NIST 800-53, C5, COBIT & CIS	▪ **Zertifizierbar** ▪ Selbstvalidierte Bewertung für 19 Bereiche ▪ Integriert HIPAA, NIST, ISO	▪ **Zertifizierbar** nach ISO 27701 (ISO 27001 Zertifizierung ist Vorbedingung)	▪ **Compliance** (gegenüber Kreditkartenunter-nehmen)	▪ **Zertifizierbar** durch CPA-Firma (Report)

Quelle: GRM I 1: CS = Cybersicherheit I 2: ISMS = Informationssicherheitsmanagementsystem I 3: SOX = Sarbanes-Oxley Act (2002) I 4: NF = Nicht-finanzielle

Abbildung 7: Rahmenwerke der Informationssicherheit

Die Implementierung eines Rahmenwerks für Informationssicherheit ist ressourcenintensiv in Personal, Zeit und Geldmitteln. Zudem stellen diese Rahmenwerke keine Einheitslösung dar. Sie müssen auf spezifische Bedürfnisse des jeweiligen Unternehmens zugeschnitten werden, was sich regelmässig als komplexer und zeitaufwändiger Prozess zeigt. Am Markt sind eine Vielzahl an Sicherheitsrahmenwerken verfügbar. 29 Sicherheitsrahmenwerke wurden einer fachlichen Prüfung unterzogen. Die neun am Markt relevanten Rahmenwerke sind in Abbildung 7 in ihren Eigenschaften zusammengestellt. Diese Rahmenwerke enthalten unterschiedliche Best Practices und Industriestandards, die Unternehmen bei der Implementierung robuster Sicherheitsmassnahmen unterstützen.

Zudem kann die Nutzung anerkannter Standards die Reputation eines Unternehmens verbessern. Dies kann besonders für Unternehmen wichtig sein, die mit sensiblen Daten agieren oder in stark regulierten Branchen tätig sind. Die Auswahl eines Rahmenwerks hängt wesentlich vom sachlichen und örtlichen Anwendungsbereich eines Unternehmens ab. Bedarf es allerdings einer Zertifizierung, geschäftspolitisch oder regulatorisch motiviert, wird die Auswahl auf drei Rahmenwerke eingeschränkt: SOC 1, SOC 2 und ISO 27001.

Ein ISMS wird in zunehmendem Masse regulatorisch explizit oder implizit gefordert. Explizit durch KRITIS-Verordnung, XAIT und Energiewirtschaftsgesetz (EnWG)[11], wobei der ISO 27001-Standard empfohlen oder vorgeschrieben wird. Implizit durch einen Anforderungskatalog, der am besten geeignet durch ein ISMS nach dem ISO 27001-Standard umgesetzt wird.

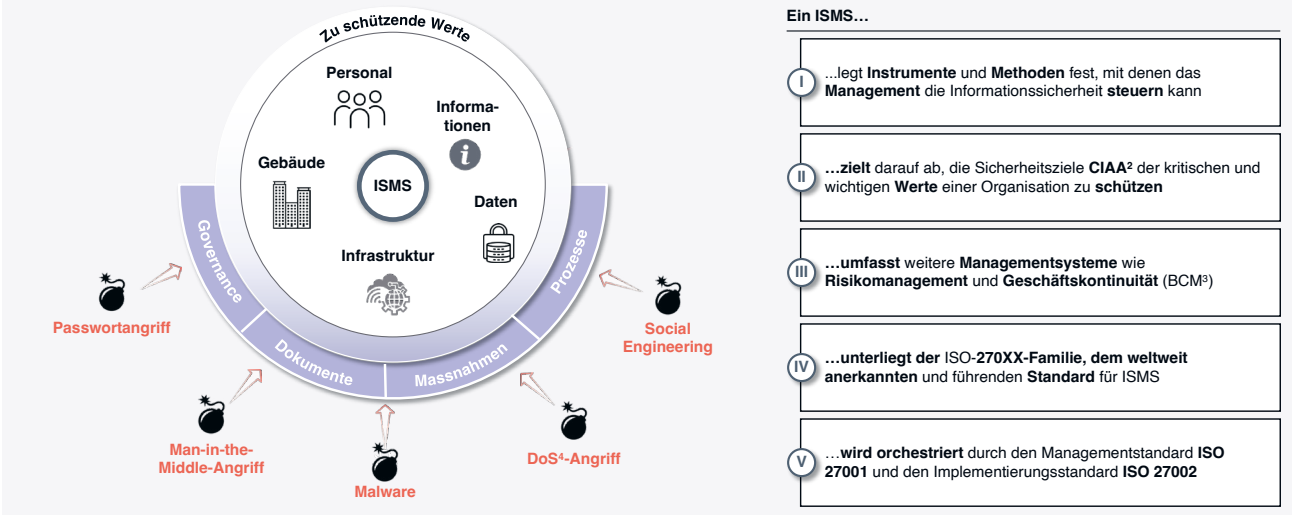
ISMS für mehr Agilität zur Erfüllung regulatorischer Anforderungen

Für die Umsetzung neuer Anforderungen wird betroffenen Organisationen im Folgenden die Implementierung eines Managementsystems anempfohlen.

ISMS nach ISO 27001-Standard: Eigenschaften und Vorzüge

Ein ISMS ist ein Werkzeug zum Schutz der Informationen und Daten einer Organisation. Der weltweit anerkannte Standard für Aufbau und Betrieb eines ISMS ist der ISO 27001-Standard

Komponenten eines ISMS[1], zu schützende Werte und typische Angriffe



Quelle: GRM I 1: ISMS = Informationssicherheitsmanagementsystem I 2: CIAA = Confidentiality, Integrity, Availability and Authenticity (Vertraulichkeit, Integrität, Verfügbargeit und Authentizität) I 3: BCM = Business Continuity Management (Betriebliches Kontinuitätsmanagement) I 4: DoS = Denial of Service (Dienstverweigerungsangriff)

Abbildung 8: ISMS schützt institutionelle Werte vor Gefährdungen

„Information security management systems - Requirements“. Mit Hilfe eines ISMS werden kritische und wichtige Werte einer Organisation vor Bedrohungen und Angriffen interner und externer Angreifer geschützt (Abbildung 8).

Die Werte stellen Personal, Gebäude, Infrastruktur (Hardware, Firmware, Software) sowie die verarbeiteten Informationen und Daten dar. Ein ISMS besteht aus verschiedenen Komponenten: Governance in Form einer Aufbau- und Ablauforganisation der Informationssicherheit, Dokumente (schriftlich fixierte Ordnung – nachfolgend sfO), Prozesse (Umsetzung der in den Dokumenten beschriebenen Prozesse) und rechtliche sowie technisch-organisatorische Massnahmen zum Schutz der Werte.

Obwohl der Standard seit 2005 existiert, erfährt das Thema ISMS erst seit wenigen Jahren eine hohe Aufmerksamkeit, bei weiter steigender Tendenz. Dies hat fünf Gründe: Erstens basieren mehr Geschäftsmodelle auf Internet-Technologien, sodass zweitens mit dieser horizontal und vertikal wachsenden Digitalisierung die Angriffsfläche aus dem Cyberraum grösser wird, dadurch drittens monetäre Verluste als auch nicht-monetäre Schäden steigen, weshalb viertens Organisationen die Sicherheit erhöhen wollen und gleichzeitig fünftens der Regulierer als Gesetzgeber und Aufsicht mit erhöhten als auch neuen regulatorischen Anforderungen reagiert.

Insbesondere die Regulierung motiviert in den letzten Jahren durch verschärfte Sanktionierung die Erhöhung der Sicherheitsreife. Als Beispiele zu nennen sind die Regularien der EU-DSGVO, der EU-CRA und die EU-NIS-Richtlinie. Bei der DSGVO können Bussgelder am Umsatz bemessen werden (bis zu 20 Mio. Euro oder bis zu 4% des weltweiten Jahresumsatzes, orientiert an der höheren Summe). Die im Entwurf des CRA vom 15.09.2022 aufgerufenen Bussgelder können bis zu 15 Mio. EUR oder von bis zu 2,5% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen, je nachdem, welcher Betrag höher ausfällt.

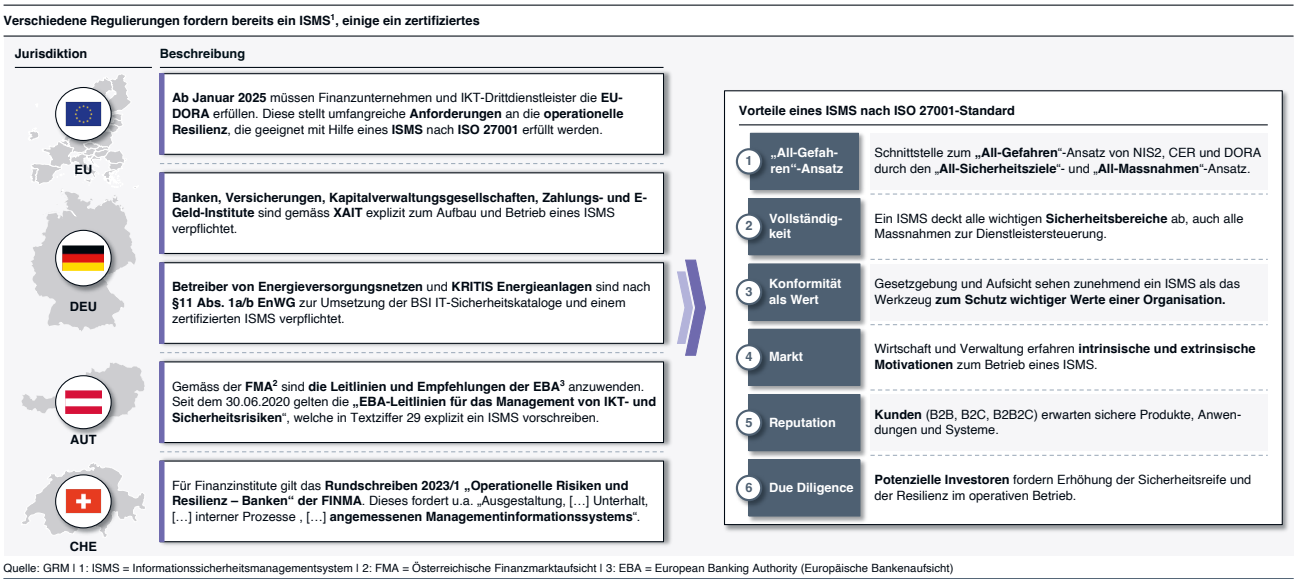


Abbildung 9: Europäische Jurisdiktionen fordern ISMS

Gemäss der NIS2-Richtlinie müssen die Mitgliedsstaaten der Europäischen Kommission bis zum 17. Januar 2025 „wirksame, verhältnismässige und abschreckende Sanktionen“ mitteilen. Bussgelder werden eine zentrale Rolle einnehmen. In Abbildung 9 werden Beispiele der regulatorischen Begründung für ein ISMS in der DACH-Region und der gesamten EU den Vorteilen eines nach ISO 27001-Standard aufgebautem ISMS gegenübergestellt.

Abbildung aller regulatorischen Anforderungen in Massnahmen

Wie hergeleitet ist der bestgeeignete Ordnungsrahmen der Informationssicherheit von Organisationen ein ISMS nach ISO 27001-Standard. Dieses „Rahmen-ISMS“ beinhaltet alle Schutzziele und Massnahmen ohne die regulatorischen Anforderungen, da es kein ISMS zur Erfüllung nur eines bestimmten Sicherheitsgesetzes gibt. Das „Rahmen-ISMS“ wird in der jeweiligen Jurisdiktion zu einem „konformen ISMS“ entwickelt. Dazu werden die Sicherheitsanforderungen der anwendbaren Gesetze und Aufsichtspraktiken der geltenden Jurisdiktion in einem „Rahmen-ISMS“ abgebildet. Konkret werden die jeweiligen Sicherheitsziele eines Gesetzes in die 93 Sicherheitsziele des ISO 27001-Standards integriert, welche mit Massnahmen nach dem ISO 27002-Standard umgesetzt werden (siehe dazu Abbildung 10 mit drei Sicherheitszielen aus Gesetzen: „Drittparteienrisiko“, „Management von Sicherheitsvorfällen und „Schwachstellenmanagement“). Insgesamt wird durch dieses Vorgehen rechtliche Sicherheit bei unternehmerischer Agilität erreicht.

Die weiteren Ausführungen im Whitepaper orientieren sich an Banken, da deren regulatorischer Rahmen als Grundlage dient. Die Ausführungen können durch Bestimmung des regulatorischen Rahmens auf jeden anderen Sektor übertragen werden.

Sicherheitsziele (“security controls”) gemäss ISO 27001:2022-Standard

Drittparteienrisiko | Management von Sicherheitsvorfällen | Schwachstellenmanagement

5. Organisatorische Maßnahmen				**8. Technologische Maßnahmen**			
5.1	Informationssicherheitspolitik und -richtlinien	5.26	Reaktion auf Informationssicherheitsvorfälle	8.1	Endpunktgeräte des Benutzers	8.13	Sicherung von Informationen
5.2	IS¹-Rollen und -verantwortlichkeiten	5.27	Erkenntnisse aus Informationssicherheitsvorfällen	8.2	Privilegierte Zugangsrechte	8.14	Redundanz v. Inform.-verarbeitenden Einrichtungen
5.3	Aufgabentrennung	5.28	Sammeln von Beweismaterial	8.3	Informationszugangsbeschränkung	8.15	Protokollierung
5.4	Verantwortlichkeiten der Leitung	5.29	Informationssicherheit bei Störungen	8.4	Zugriff auf den Quellcode	8.16	Überwachung von Aktivitäten
5.5	Kontakt mit Behörden	5.30	IKT-Bereitschaft für Business-Continuity	8.5	Sichere Authentisierung	8.17	Uhrensynchronisation
5.6	Kontakt mit speziellen Interessensgruppen	5.31	Jurist., gesetzl., regulat. u. vertragl. Anforderungen	8.6	Kapazitätssteuerung	8.18	Gebrauch v. Hilfsprogrammen m. privilege. Rechten
5.7	Informationen über die Bedrohungslage	5.32	Geistige Eigentumsrechte	8.7	Schutz gegen Schadsoftware	8.19	Installation von Software auf Systemen im Betrieb
5.8	Informationssicherheit im Projektmanagement	5.33	Schutz von Aufzeichnungen	8.8	Handhabung von technischen Schwachstellen	8.20	Netzwerksicherheit
5.9	Inventar der Inform. u. anderen damit verbund. Werte	5.34	Datenschutz und Schutz v. personenbez. Daten	8.9	Konfigurationsmanagement	8.21	Sicherheit von Netzwerkdiensten
5.10	Zul. Gebrauch von Inform. u. and. damit verb. Werten	5.35	Unabhängige Überprüfung der Informationssicherheit	8.10	Löschung von Informationen	8.22	Trennung von Netzwerken
5.11	Rückgabe von Werten	5.36	Einhalt. v. Richtl., Vorschriften und Normen für die IS	8.11	Datenmaskierung	8.23	Webfilterung
5.12	Klassifizierung von Informationen	5.37	Dokumentierte Betriebsabläufe	8.12	Verhinderung von Datenlecks	8.24	Verwendung von Kryptographie
5.13	Kennzeichnung von Informationen	**6. Personenbezogene Maßnahmen**				8.25	Lebenszyklus einer sicheren Entwicklung
5.14	Informationsübermittlung	6.1	Sicherheitsüberprüfung	6.5	Verantwortlichk. bei Beend. o. Änd. d. Beschäftigung	8.26	Anforderungen an die Anwendungssicherheit
5.15	Zugangssteuerung	6.2	Beschäftigungs- und Vertragsbedingungen	6.6	Vertraulichkeits- o. Geheimhaltungsvereinbarungen	8.27	Sich. Systemarchitektur u. Entwicklungsgrundsätze
5.16	Identitätsmanagement	6.3	IS-Bewusstsein, -Ausbildung und -Schulung	6.7	Remote-Arbeit	8.28	Sichere Codierung
5.17	Authentisierungsinformationen	6.4	Massregelungsprozess	6.8	Meldung von Informationssicherheitsereignissen	8.29	Sicherheitsprüfung bei Entwicklung und Abnahme
5.18	Zugangsrechte	**7. Physische Maßnahmen**				8.30	Ausgegliederte Entwicklung
5.19	Informationssicherheit in Lieferantenbeziehungen	7.1	Physische Sicherheitsperimeter	7.8	Platzierung u. Schutz von Geräten u. Betriebsmitteln	8.31	Trennung von Entw.-, Test- und Prod.-umgebungen
5.20	Behandlung von IS in Lieferantenvereinbarungen	7.2	Physischer Zutritt	7.9	Sicherheit von Werten ausserhalb Räumlichkeiten	8.32	Änderungssteuerung
5.21	Umgang mit der IS in der Lieferkette der IKT²	7.3	Sichern von Büros, Räumen und Einrichtungen	7.10	Speichermedien	8.33	Testdaten
5.22	Überwach., Überprüf. & Änd.-Mgmt. Lieferanten-DL³	7.4	Physische Sicherheitsüberwachung	7.11	Versorgungseinrichtungen	8.34	Schutz d. Inform.systeme während Tests i.R.v. Audits
5.23	IS für die Nutzung von Cloud-Diensten	7.5	Schutz vor phys. und umweltbedingten Bedrohungen	7.12	Sicherheit der Verkabelung		
5.24	Plan. u. Vorbereit. d. Handhab. v. IS-vorfällen	7.6	Arbeiten in Sicherheitsbereichen	7.13	Instandhaltung von Geräten und Betriebsmitteln		
5.25	Beurteilung und Entscheidung über IS-Ereignisse	7.7	Aufgeräumte Arbeitsumgebung u. Bildschirmsperren	7.14	Sich. Entsorg. o. Wiederverw. v. Geräten u. BM⁴		

Quelle: ISO.org I 1: IS = Informationssicherheit I 2: IKT = Informations- und Kommunikationstechnologie I 3: DL = Dienstleistung I 4: BM = Betriebsmittel

Abbildung 10: Massnahmen am Beispiel von drei Sicherheitszielen

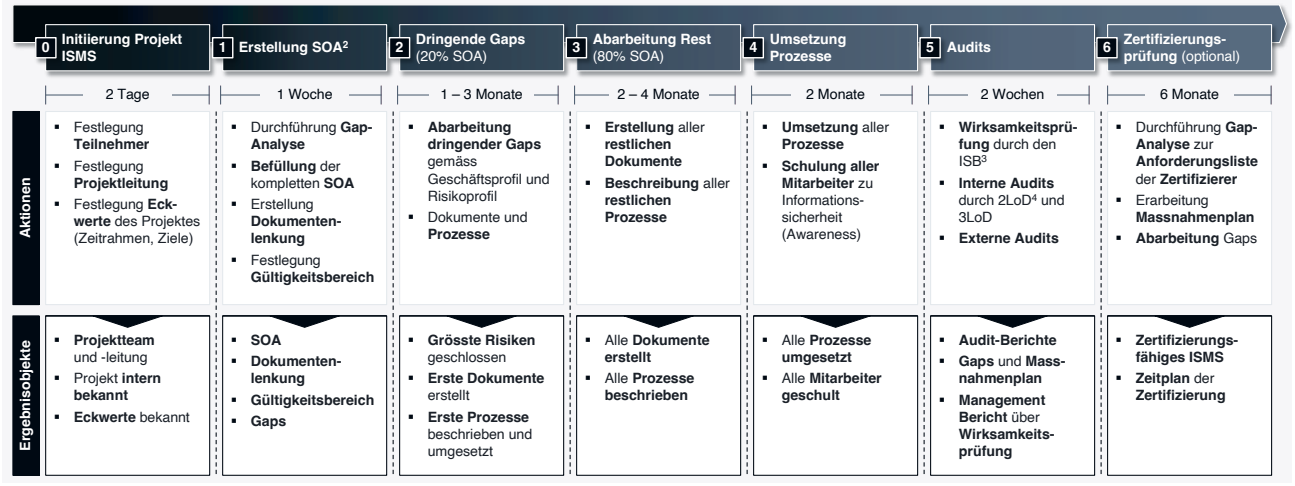
Hinweise zum Aufbau eines ISMS

Während es beim Datenschutz um Informationen geht, die auf eine natürliche Person zurückzuführen sind, umfasst Informationssicherheit auch alle anderen strukturierten und unstrukturierten verarbeiteten Informationen einer Organisation. Es kann sich um analoge Informationen handeln, die in physischen Medien wie Papierdokumenten, Visitenkarten oder Ausdrucken festgehalten werden, oder um digitale Informationen, die auf Datenträgern gespeichert oder von Software und Geräten verarbeitet werden. Die Informationen werden mit detektiven, präventiven und reaktiven Sicherheitsmassnahmen geschützt. Diese Massnahmen orientieren sich an den grundlegenden vier Zielen der Informationssicherheit:

- Vertraulichkeit: Schutz von Informationen vor nicht autorisierter Offenlegung
- Integrität: Korrektheit der Daten
- Verfügbarkeit: Jederzeitige bestimmungsgemässe Nutzung von IT-Systemen und Daten
- Authentizität: Verifizierte Herkunft von Daten und IT-Systemen (bei Nutzung von
- kryptographischen Primitiven sind integre Daten gleichzeitig authentisch)

Der ISO 27001-Standard besteht aus den zwei Teilen „High Level Structure“ (HLS) und Anhang A mit den „Security Controls“. Das HLS besteht aus den Kapiteln 4 bis 10 des Standards und es stellt die organisatorischen Rahmenbedingungen für die Einführung und den Betrieb des ISMS. Anhang A nennt 93 Kontrollen, die in die vier Gruppen organisatorische, personelle, physische und technische Kontrollen gegliedert sind (Abbildung 10). Eine „Security Control“ ist dabei kontextbezogen gleichbedeutend mit „Kontrolle“ und „Sicherheitsziel“.

Aufbau eines ISMS[1] in sechs Phasen plus optionale Zertifizierung



Quelle: GRM I 1: ISMS = Informationssicherheitsmanagementsystem I 2: SOA = Statement of Applicability (Erklärung der Anwendbarkeit) I 3: ISB = Informationssicherheitsbeauftragter I 4: LoD = Line of Defence

Abbildung 11: Sechs Phasen zum Aufbau eines ISMS, Zertifizierung des ISMS ist optional

Aufbau eines ISMS mit einem Projekt

Der Aufbau des ISMS sollte im Rahmen eines Projektes erfolgen (Abbildung 11, Schritt 0). Es sollte früh im Projekt bekannt sein, welche Gesetze und Verordnungen auf die Organisation anwendbar sind (sfO-Dokument „Anwendbare Gesetze und sonstige Vorschriften“).

Das Projekt sollte durch die Leitungsebene initiiert und mit strategischen Zielstellungen unterlegt sein. Die aus den strategischen Zielstellungen abzuleitenden Eckwerte bilden sich aus der Geschäftsstrategie, der IT-Strategie und den Anforderungen an die Informationssicherheit. Zu den Projektteilnehmern zählen mindestens die Funktionen Informationssicherheitsbeauftragter (ISB), Datenschutzbeauftragter (DSB), Auslagerungsverantwortlicher und alle weiteren Stakeholder entsprechend dem Geltungsbereich des ISMS wie zum Beispiel IT-Betrieb, Personalabteilung und Anwendungsentwicklung.

Es gibt verschiedene Möglichkeiten, die Arbeiten an der schriftlich fixierten Ordnung zu beginnen: Identifikation der zu schützenden Werte, Aufnahme des Informationsverbundes, Feststellung der Schutzbedarfe der wichtigen Werte oder auch Durchführung von Risikoanalysen für diese. Die Autoren empfehlen jedoch ein anderes Vorgehen: Befüllung der Statement of Applicability (SOA, deutsch: Erklärung der Anwendbarkeit), Schritt 1 in Abbildung 11. Dieser Ansatz hat sich in vielen ISMS- und Prüfungs-Projekten erfolgreich bewährt. Die SOA stellt das Skelett eines ISMS dar, an dem die Einzelteile zu einem in sich schlüssigen System zusammengeführt werden. In Abbildung 10 finden sich die 93 Sicherheitsziele. Zu jeder einem Sicherheitsziel zugeordneter Kontrolle muss die Relevanz und Anwendung beschrieben werden. Hierzu gehören eine Begründung, ob und wie ein bestimmtes Sicherheitsziel durch diese Kontrollen erreicht wird. Trifft eine Kontrolle nicht zu, muss dies ebenfalls erklärt werden. Kontrollen, gleichbedeutend mit Sicherheitszielen, können durch Dokumente (Richtlinien, Arbeitsanweisungen etc.) und Massnahmen erreicht werden. Die Relevanz der SOA zeigt sich an der Tatsache, dass sie das einzige im Zertifikat referenzierte Dokument ist – mit Titel, Version und Datum.

Die Bezos Pizza Regel gilt beim Aufbau eines ISMS: Das Kernteam sollte von zwei Pizzas satt werden.

Governance eines ISMS

Zur Governance eines ISMS gehören Zielvorgaben, Ressourcenausstattung und ein Modus Operandi. Für Aufbau und Betrieb des ISMS ist die ISB-Funktion verantwortlich. Die Ziele werden mindestens jährlich oder anlassbezogen auch unterjährig durch die Leitungsebene vorgegeben und gesteuert. Die Ausstattung mit den Aufgaben und dem Umfang des ISMS angemessenen personellen, technischen und organisatorischen Ressourcen obliegt der Geschäftsführung und basiert auf der jährlichen Aufwandsplanung der ISB-Funktion. Zum Modus Operandi gehören ebenso der Turnus, der Inhalt und die Mitglieder von Ausschüssen und Projektgruppen, die Berichts- und Meldewege sowie -formate. Dabei agieren viele Ebenen und Beschäftigte im Rahmen des ISMS zum Schutz der wichtigen Infrastrukturen vor Bedrohungen und Angriffen zusammen. Für diese Kooperation hat sich bei Banken das Modell der drei Verteidigungslinien, den sogenannten „3LoD“ (Lines-of-Defence) etabliert:

- 1LoD: Umsetzung von Massnahmen durch Geschäftsbereiche und Service-Bereiche wie IT und Betrieb sowie Durchführung eigener 1LoD-Kontrollen
- 2LoD: Anforderungen der ISB-Funktion, unabhängige Bewertung der Informationssicherheitsrisiken und Durchführung eigener 2LoD-Kontrollen der 1LoD
- 3LoD: Überprüfung der Effektivität des internen Kontrollsystems (IKS) durch die interne Revision

Sollen kritische Infrastrukturen geschützt werden wie bspw. bankeigene Zahlungssysteme, wird das 3LoD-Modell um den Staat als vierte Verteidigungslinie (4LoD) erweitert:

- 4LoD: Staat in seiner Doppelfunktion als Gesetzgeber (Setzer von Anforderungen) und als Aufsicht (Überprüfungsorgan).

Awareness

Das Bewusstsein (engl. Awareness) für Informationssicherheit ist ein fundamentaler Pfeiler im Rahmen der Unternehmenssicherheit und essenziell für deren Erfolg. Bei zunehmend komplexer werdender Bedrohungslandschaft ist es unabdingbar, dass alle Mitarbeiter neben dem Verstehen der Prinzipien der Informationssicherheit auch ihre individuelle Rolle im Schutzprozess kennen. Dieses Bewusstsein schafft eine robuste Verteidigung der 1LoD gegen potenzielle interne und externe Sicherheitsbedrohungen. Die kontinuierliche Schulung und Sensibilisierung der Belegschaft beispielsweise mit Trainings, Übungen und wöchentlichen Sprechstunden über Risiken, wie Phishing, Social Engineering und andere Cyberbedrohungen, tragen wesentlich dazu bei, die Wahrscheinlichkeit von Sicherheitsvorfällen zu verringern. Darüber hinaus stärkt eine hohe Awareness das Verständnis für Richtlinien und Verfahren, was zu einer besseren Einhaltung von Sicherheitsregeln führt. Dieser Ansatz fördert eine Unternehmenskultur, in der Sicherheit als gemeinsame Verantwortung verstanden wird und jeder Einzelne zum Schutz von Unternehmenswerten beiträgt.

Übergeordnete Dokumente des ISMS

Das ISMS besteht aus Dokumenten mehrerer Hierarchiestufen. Vielfach verwendet werden die fünf Dokumentenebenen Strategien, Leitlinien, Richtlinien, Prozesse, Arbeitsanweisungen und Beweisdokumente (Abbildung 12). Alle Dokumente müssen regelmässig und anlassbezogen überprüft und erforderlichenfalls angepasst werden.

Ein ISMS[1] strebt einen ganzheitlichen Ansatz an, der alle geltenden Gesetze und Normen entlang einer logischen Dokumentenhierarchie umfasst

Beschreibung der Dokumentenarten

Dokumentenart	Beschreibung
I Leitlinie	▪ Verpflichtungserklärung des Managements zur Informationssicherheit und Einbettung der Organisation in das ISMS ▪ Muss allen Mitarbeitern zur Kenntnis gebracht werden
II Richtlinie	▪ Beinhaltet Rollen und Verantwortlichkeiten sowie Anforderungen ▪ Enthält Sicherheitskontrollen der 2LoD[2]
III Prozess	▪ Bildet vornehmlich in grösseren Organisationen das Bindeglied zwischen Richtlinie und Arbeitsanweisung, wird bei kleineren Entitäten obsolet ▪ Beschreibung einer einzelnen Aktivität als Prozess, der im Rahmen der 1LoD-Tätigkeit umgesetzt wird
IV Arbeitsanweisung	▪ Spezifische Anleitungen zur effektiven Umsetzung der Verfahren ▪ Schrittweise Beschreibung der Vorgehensweisen zur Umsetzung der Sicherheitskontrollen
V Beweisdokument	▪ Aufzeichnungen und Dokumente zum Nachweis der Einhaltung der ISMS-Anforderungen ▪ Nachweis, dass Sicherheitsmassnahmen eingeführt wurden und befolgt werden

Quelle: „Non-financial Risk Managemen in the Financial Industry" (Frankfurt School Verlag) I GRM I 1: ISMS = Informationssicherheitsmanagementsystem I 2: LoD = Line of Defense

Abbildung 12: Dokumentenhierarchie im ISMS

Die Geschäftsleitung definiert in Strategien Unternehmensziele und beschreibt Massnahmen zu deren Erreichung. Deutsche Banken müssen die informationssicherheitsrelevanten Strategien für Geschäft, Risiko, IT und Auslagerung erstellen. Österreichische Institute müssen EBA-Leitlinien[12] folgen und zumindest eine Geschäftsstrategie und eine Gesamtrisikostrategie erstellen. Schweizer Institute müssen gemäss Bankengesetz, dem Finanzmarktaufsichtsgesetz und konkretisierendem Rundschreiben[13] Strategien für Geschäft, Risiko und IT erstellen.

Richtlinien sind Dokumente der 2LoD, im Falle eines ISMS somit der ISB-Funktion. Sie spezifizieren Anwendungsbereiche, Verantwortlichkeiten und Mindestanforderungen, können aber auch Vorgehensweisen und Prozesse umfassen.

Prozesse stellen die Umsetzung der in den übergeordneten Dokumenten genannten Aktivitäten durch die 1LoD dar. Arbeitsanweisungen geben detaillierte Anleitungen zur Prozessdurchführung und zum Einsatz spezifischer IT-Anwendungen. Die Tiefe der Dokumente ist den Unternehmen nach eigenem Ermessen überlassen. So kann auch ein Prozess generisch beschrieben sein, welcher im weiterführenden Dokument detailliert dargestellt wird. Auch Dokumentenvorlagen sind Arbeitsanweisungen.

Beweisdokumente dienen dem Nachweis der effektiven Implementierung der Prozesse, indem sie Ergebnisse zusammenfassen und allgemein Zustände beschreiben: Auditberichte, Risikoanalysen, Rechnungen, Sitzungsprotokolle und ausgefüllte Vorlagen. Auch die Prüfprotokolle der Internen Revision (3LoD) über das IKS, d.h. über die Effektivität der Arbeiten von 1st und 2nd LoD sind Beweisdokumente.

Dokumentenerstellung folgt Pareto-Prinzip

Parallel zur Erstellung der SOA sollte der Geltungsbereich (Umfang) des ISMS festgelegt, die Dokumentenlenkung begonnen und eine Gap-Analyse durchgeführt werden. Die Dokumentenlenkung beschreibt einerseits, wie Dokumente des ISMS in ihrem Lebenszyklus erstellt, geprüft, genehmigt, gekennzeichnet, verteilt, aktualisiert und zurückgezogen werden und andererseits gibt sie einen Überblick über alle Dokumente des ISMS, sie ist die „schriftlich fixierte Ordnung“. Ein effektives ISMS sollte gemäss den spezifischen Domänen der Informationssicherheit strukturiert sein, die sowohl klassische Abteilungen (Bsp. Human Resources, IT) als auch dedizierte Sicherheitsbereiche (Bsp. Security Information and Event Management Identitäts- und Zugriffsmanagement) umfassen können. Diese Domänen eignen sich dementsprechend zur Strukturierung der Dokumente des ISMS in der Dokumentenlenkung.

Für den Zuschnitt der Domänen empfehlen die Autoren folgende Einordnung: Da der aktuelle Standard aus dem Jahr 2022 die 93 Kontrollen in nur vier Domänen (organisatorische, personelle, physische und technische Kontrollen) einordnet, entstehen vier sehr grosse Bereiche des ISMS mit vielen verschiedenen Einzelthemen. Am anderen Ende der Skala des Domänenzuschnitts liegt die direkte Einordnung in 93 Domänen, was zu feingranular wäre und die Effektivität des ISMS reduziert. Als Mittelweg eignet sich die Einordnung der 93 Kontrollen der Version 2022 des ISO 27001-Standards in die 14 Domänen der Version 2013. Diese Kombination beider Versionen des Standards ist in Abbildung 13 vollzogen.

Ohne Dokumentation ist alles andere nichts

Die Gap-Analyse identifiziert die Lücken zwischen dem Soll-Zustand eines zertifizierungsfähigen ISMS und dem Ist-Zustand. Ergebnis der Gap-Analyse ist der Massnahmenplan zur Schliessung der Lücken in den drei Schritten 2 bis 4 in Abbildung 11. In Schritt 2 werden nach dem Pareto-Prinzip zuerst die dringlichsten 20% der identifizierten Lücken geschlossen. Diese Lücken stellen die grössten Sicherheitsrisiken für Informationen dar und sind dementsprechend priorisiert zu behandeln. Mit Schritt 3 folgen die weiteren 80% der notwendigen Arbeiten zum Aufbau des ISMS. Die Umsetzung aller Prozesse im Schritt 4 erfolgt unmittelbar.

Das aufgebaute ISMS muss initial und nach Inbetriebnahme laufend in seiner Funktionsfähigkeit überprüft werden. Dem dient der Schritt „Wirksamkeitsprüfung“, in dem das Management das ISMS jährlich zu dessen Eignung, Angemessenheit und Wirksamkeit misst. Die Datenlage liefert die ISB-Funktion über kontinuierlich durchzuführende interne Audits (2LoD-Kontrollen) zur

- Eignung (Test of Design, ToD),
- Angemessenheit (Test of Implementation, ToI) und
- Wirksamkeit (Test of Effectiveness, ToE)

Zuordnung der 93 Sicherheitsziele aus ISO 27001:2022 zu den 14 Domänen gemäss Annex A ISO 27001:2013

Quelle: GRM, auf Basis von ISO 27001:2013 und 27001:2022 I 1: BCM = Business Continuity Management (Betriebliches Kontinuitätsmanagement)

Abbildung 13: Vorschlag zur Strukturierung der 93 Sicherheitsziele in 14 Domänen

von Massnahmen zur Erreichung der Sicherheitsziele. Das Themenspektrum des ISMS sollte in einem Zeitraum von drei Jahren geprüft werden, die als kritisch identifizierten Aspekte einer Organisation öfter (jährlich bis halbjährlich). Zur Unterstützung der 2LoD-Kontrollen (ISB), der 3LoD (internen Revision) sowie der 1LoD (IT-Betrieb) kann sich eine Organisation auch externer Audits bedienen. Penetrationstests sind das klassische Beispiel einer ausgelagerten Audittätigkeit.

Dokumentenhierarchie am praktischen Beispiel

Die übergeordneten Dokumente eines ISMS sind die bereits genannten SOA und Dokumentenlenkung, die Informationssicherheitsleitlinie, die Richtlinie zu Wirksamkeitsprüfung des ISMS und die „Anwendbaren Gesetze und sonstigen Vorschriften“.

Die Informationssicherheitsleitlinie (IS-Leitlinie) ist zentral für das ISMS und die Organisation. Sie muss allen Mitarbeitern zur Kenntnis gebracht werden und sollte nach dem HLS, d.h. den Kapiteln 4 bis 10 des ISO 27001-Standards aufgebaut sein. Das HLS ist das Instrument für das Management ein ISMS kontrolliert zu betreiben und die notwendige Weiterentwicklung sicherzustellen. Es erfordert die Positionierung des Managements zum

ISMS in den Aspekten Kontext der Organisation (Kapitel 4), Führung (Kapitel 5), Planung (Kapitel 6), Unterstützung (Kapitel 7), Betrieb (Kapitel 8), Bewertung der Leistung (Kapitel 9) und Verbesserung (Kapitel 10).

Die IS-Leitlinie vereint somit weitere wichtige Inhalte, wie beispielsweise den Anwendungsbereich des ISMS, Sicherheitsrollen und Verantwortlichkeiten, IT-Sicherheitspolitik und -ziele, das Risikomanagement und die Wirksamkeitsprüfung. Neben dem Bekenntnis der Leitung, Informationssicherheit aktiv zu unterstützen, und der Verpflichtung der Mitarbeiter zur dessen Einhaltung, werden in der IS-Leitlinie insbesondere allgemeine Grundsätze der Organisation festgelegt. Beispiele sind die kontinuierliche Erhöhung des Sicherheitsniveaus oder die Aufrechterhaltung einer hohen Reputation.

Des Weiteren spielt die Geschäftsstrategie eine tragende Rolle im ISMS: Wenn die Bank Anwendungen in eigener Verantwortung entwickelt, folgt das Dokumentenset im ISMS zum Thema Anwendungsentwicklung und sicheres Coding einem anderen Paradigma, als wenn Anwendungen extern bezogen werden. Gleiches gilt für strategische Geschäftsentscheidungen wie zum Beispiel die Auslagerung des IT-Betriebs in eine inländische oder Drittstaaten-Cloud. Dem Ergebnis der Gap-Analyse folgend werden, beginnend mit den dringlichen, alle Dokumente des ISMS erstellt. Für alle Anforderungsdokumente des ISMS, d.h. Richtlinien, empfiehlt sich die Verwendung der Anforderungen aus den Kontrollen im ISO 27001-Standard. Mit dieser Vorgehensweise wird das Ziel des Dokumentes vorgegeben und zusätzlich bereits das ToD erfüllt.

Implementierung des ISMS durch automatisierte Prozesse

Ein wirksames ISMS wird im besten Falle mit Tools umgesetzt. Grundsätzlich müssen zwei Arten von ISMS-Tools unterschieden werden: Tools zur Organisation des ISMS selbst und Tools zum Management einzelner Themen des ISMS wie zum Beispiel das Identitäts- und Zugriffsmanagement (IAM), das Asset-Management und das Risiko-Management.

Der PDCA-Zyklus als Organisationsform empfohlen

Abbildung 14 gibt einen Überblick zum Tooling der Themenstellungen zum ISMS mit typischen Toolbeispielen je Thema.

Die Prozesse der Informationssicherheit sind parallel zu den Dokumenten zu beschreiben und in gemeinsamer Verantwortung der 1LoD mit Unterstützung der 2LoD umzusetzen. Die Dokumentation ihrer Inbetriebnahme liefert den Nachweis der erfüllten Anforderungen durch implementierte Prozesse. Einzig die Beschreibung der Umsetzung in einer Arbeitsanweisung genügt nicht als Nachweis der Wirksamkeit.

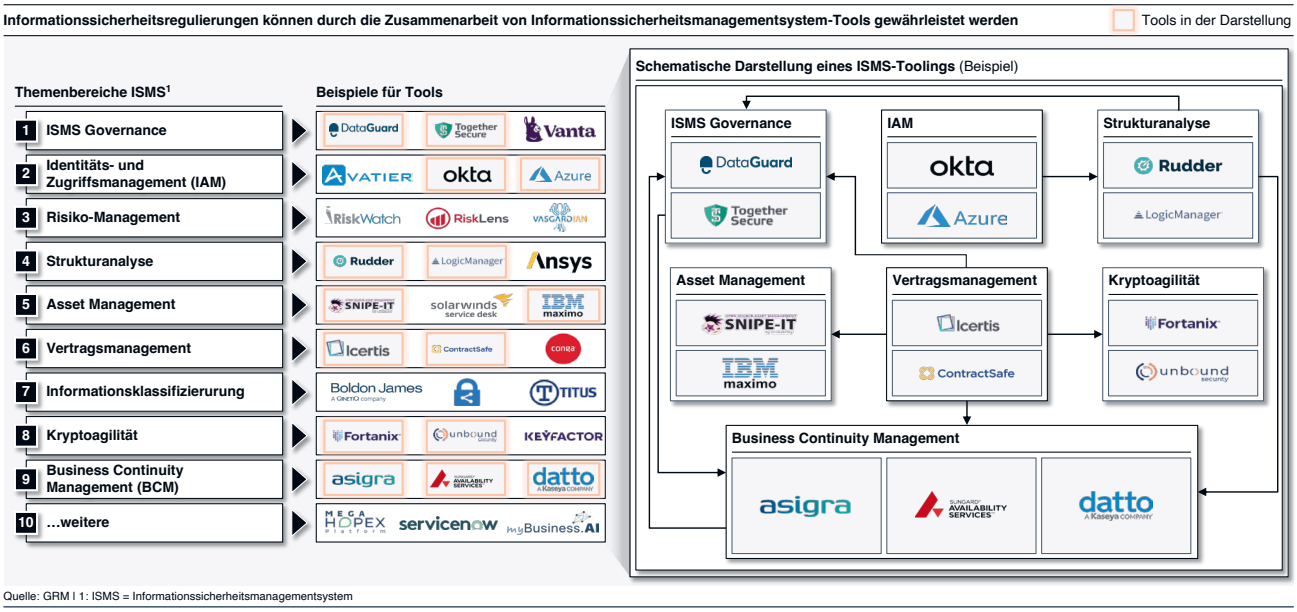


Abbildung 14: Themenstellungen eines ISMS mit Tool-Beispielen

Prozesse werden im Plan-Do-Check-Act (PDCA)-Zyklus bearbeitet:

- **Plan (planen):** Der Beispielprozess Informationsklassifizierung wird in der gleichnamigen Richtlinie beschrieben. Massnahmen und die Umsetzung müssen mit den verantwortlichen Experten vorab auf Machbarkeit geprüft werden.
- **Do (tun):** Prozesse, Massnahmen und Kontrollen werden umgesetzt. Dazu gehören auch Schulungs- und Sensibilisierungsprogramme für Mitarbeiter. Die Wirksamkeit ist über 1LoD-Kontrollen sicherzustellen.
- **Check (prüfen):** Die Wirksamkeit der Informationsklassifizierung wird überwacht und regelmässig geprüft. Hierzu erfolgen regelmässige Kontrollen innerhalb der 1LoD als auch durch Kontrollen der 2LoD und 3LoD.
- **Act (handeln):** Auf Basis der Erkenntnisse der Check-Phase ergreifen ISB-Funktion und 1LoD Korrektur- und Präventivmassnahmen wie Aktualisierung von Richtlinien und Arbeitsanweisungen, Verbesserung des Prozesses oder des Berichtswesens.

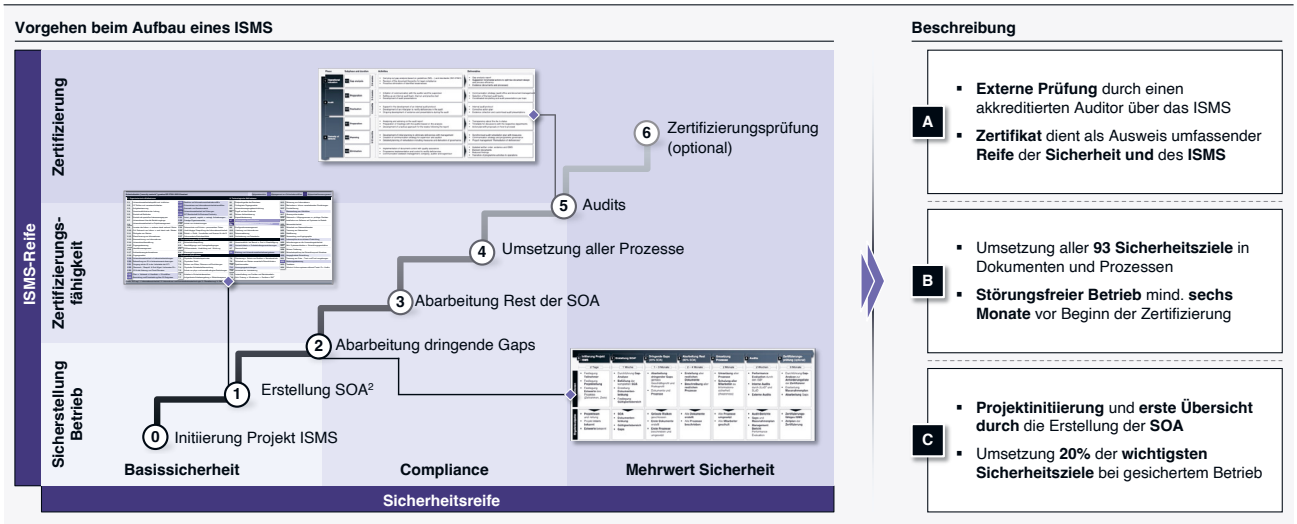
Das Zusammenwirken der vier Phasen ist entscheidend zur Sicherstellung der Wirksamkeit der Prozesse und damit des ISMS als Ganzes, das an Änderungen in der Organisation, an neue Angriffe und Bedrohungen und neue Compliance-Anforderungen angepasst werden muss.

Der Weg zum zertifizierten ISMS

Grundsätzlich muss die Funktionsfähigkeit und Wirksamkeit des ISMS kontinuierlich überprüft werden. Wird das ISMS aufgebaut, muss es erstmalig auditiert werden. Dies erfolgt in Phase 5 aus Abbildung 11. Soll das ISMS zertifiziert werden, sind verschiedene Audits vor der Zertifizierungsprüfung unabdingbar (Phase 5 in Abbildung 15): Die ISB-Funktion stellt die jährlich durchgeführte Wirksamkeitsprüfung der Leitungsebene vor. Diese kontinuierliche Evaluation wird über KXI (KPIs, KRIs und KCIs; Key Indicators für Performance, Risk und Compliance) gemessen. Im ersten Jahr eines aufgebauten ISMS kann mit einer Gesamtzahl für KXI von zehn gearbeitet werden, nach dem finalen Ausbau sollten zur Praktikabilität maximal 30 KXI verwendet werden. Sowohl die 2LoD als auch die 3LoD müssen eigene Prüfungshandlungen der Wirksamkeit durchführen. Die ISB-Funktion muss dabei in einem Zyklus von drei Jahren das komplette Themenspektrum des ISMS, d.h. alle 93 Sicherheitsziele der 14 Domänen aus Abbildung 13 auditieren. Besonders wichtige Bereiche müssen öfter geprüft werden. Die interne Revision prüft stichprobenartig und von allen anderen Funktionen und Verteidigungslinien unabhängig.

Die steigende Zahl der regulatorischen Forderungen nach einem ISMS und die Beweislast auf Seiten der Betreiber, den Schutz von Informationen nachzuweisen, bedingen eine transparente und nachweisbare Verwaltung der Informationssicherheit in einem Managementsystem.

Steigerung der ISMS[1]- und Sicherheitsreife in drei Stufen



Quelle: GRM I 1: ISMS = Informationssicherheitsmanagementsystem I 2: SOA = Statement of Applicability (Erklärung der Anwendbarkeit)

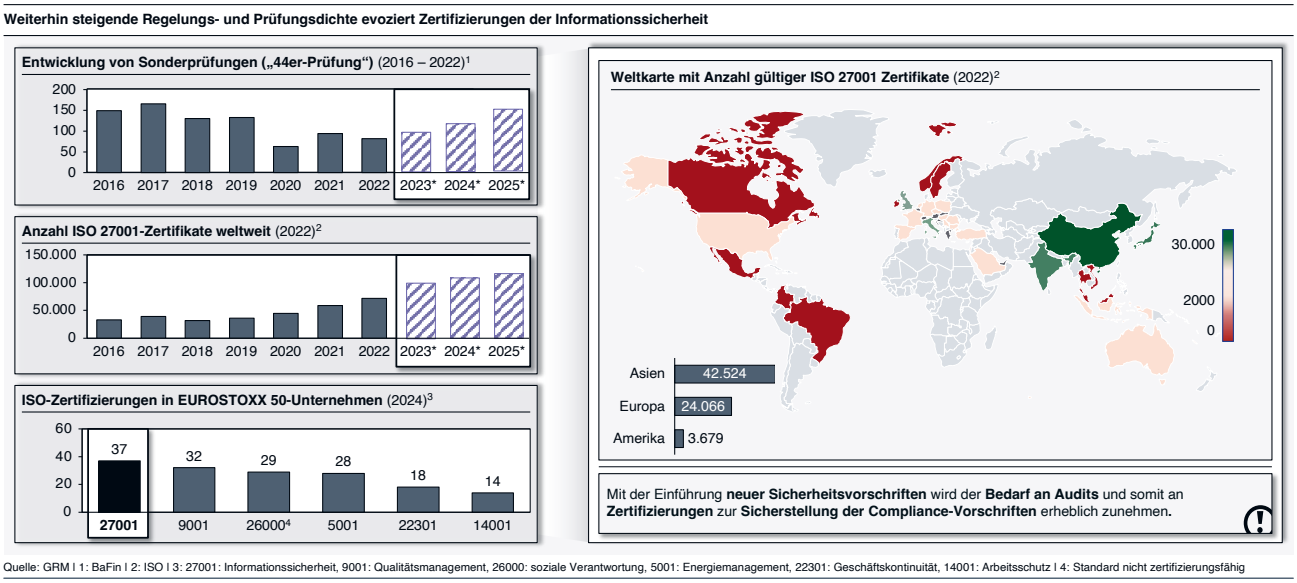
Abbildung 15: Ausbaustufen eines ISMS und korrespondierende Sicherheitseigenschaften

Die erste Ausbaustufe des ISMS umfasst die ersten drei Phasen 0 bis 2 in Abbildung 15 und stellt den Betrieb gegen die dringlichsten identifizierten Lücken sicher. Dieses ISMS ist weder gesetzeskonform, noch bietet es bereits einen Mehrwert der Sicherheit zum Beispiel gegenüber Investoren.

Die zweite Ausbaustufe (Phasen 3 bis 5) stellt die Zertifizierungsfähigkeit des ISMS her: Das ISMS ist vollständig aufgebaut. Eine Zertifizierung wird nur in der dritten Ausbaustufe mit Phase 6 erreicht. Damit wird ein Mehrwert an Sicherheit gegenüber Investoren, Regulator, Aufsicht und Kunden generiert. Das ISO 27001-Zertifikat ist ein

begehrtes Gütesiegel der Informationssicherheitsreife einer Organisation, nach innen wie nach aussen. Abbildung 15 verfügt über keine Zeitskala. Grundsätzlich kann von einem zeitlichen Aufwand von 6 bis 12 Monaten für die Schritte 0 bis 5 ausgegangen werden. Die Zertifizierung selbst ist an zeitliche Vorgaben der externen Auditoren gebunden und kann mit mindestens 6 Monaten veranschlagt werden. Diese Zeitangaben gelten unter der Voraussetzung einer intensiven und eng abgestimmten Zusammenarbeit aller Beteiligten während der gesamten Projektlaufzeit. Die Maturität der zu Beginn der Zertifizierung erreichten Informationssicherheit nach Schritt 5 bestimmt massgeblich den personellen, organisatorischen und zeitlichen Aufwand zur Erlangung des Zertifikats im Schritt 6. Die Entscheidung pro oder contra Zertifizierung ist aus den in der Geschäftsstrategie festgelegten Zielen abzuleiten.

Abbildung 16 stellt den Zusammenhang her zwischen Anzahl der ISO 27001-Zertifikate weltweit, der Zunahme von finanzaufsichtlichen Prüfungen („§ 44er Prüfung“) in Deutschland und der Anzahl der ISO-Zertifikate der EUROSTOXX 50-Unternehmen.



Quelle: GRM I 1: BaFin I 2: ISO I 3: 27001: Informationssicherheit, 9001: Qualitätsmanagement, 26000: soziale Verantwortung, 5001: Energiemanagement, 22301: Geschäftskontinuität, 14001: Arbeitsschutz I 4: Standard nicht zertifizierungsfähig

Abbildung 16: Neue Regulierung erzwingt höhere Prüfungs- und Zertifizierungsaufwände

Zu den Prognosen in Abbildung 16: Die Sonderprüfungen werden zunehmen da die DORA die Anzahl der Aufsichtsobjekte erhöht. Die Anzahl der ISO 27001-Zertifikate wird ebenso zunehmen da ein zertifiziertes ISMS durch weitere Gesetze gefordert wird. Die Relevanz der Informationssicherheit zeigt sich auch bei den EUROSTOXX 50 Unternehmen: mit 37 ISO 27001-Zertifikaten bilden sie die grösste Gruppe. Kurzgefasst: Je mehr Unternehmen unter ein Sicherheitsgesetz fallen, desto mehr ISMS werden zertifiziert.

Die neuesten Veröffentlichungen von ISO-Standards und die Ausweitung der zu beaufsichtigten Sektoren sind hinweisgebend für zukünftig mehr Sicherheitszertifizierungen, wie u.a. der ISO 21434 „Road vehicles – Cybersecurity engineering“ oder TISAX14 der deutschen Automobilindustrie, angelehnt an den ISO 27001-Standard. Allgemein müssen Betreiber kritischer Infrastrukturen gemäss IT-Sicherheitsgesetz eine Mindestsicherheit vorweisen, hierfür bietet ein funktionsfähiges und wirksames ISMS die beste Evidenz.

Fazit

Wirtschaft, Gesellschaft und Verwaltung finden verstärkt im digitalen Raum statt und alle drei Sphären sind in zunehmendem Mass abhängig von sicheren digitalen Infrastrukturen. Hiernach vergrössert sich die Cyberangriffsfläche horizontal und vertikal. Unternehmen haben ein intrinsisches Interesse daran, das Vertrauen der Kunden zu erhalten und versuchen, die Reife ihrer Informationssicherheitsorganisation zu erhöhen. Parallel begegnen Gesetzgeber und Aufsichten den steigenden monetären und nicht-monetären Verlusten aus erfolgreichen Angriffen mit mehr Sicherheitsgesetzen und Prüfungen der Sicherheitsreife der Organisationen. Mit steigender Tendenz wird regulatorisch implizit oder gar explizit ein ISMS gefordert.

Im Whitepaper wurde zunächst der kommende Regulierungskanon aus NIS2, CER und DORA sowie dessen nationale Umsetzung in Deutschland vorgestellt. Dabei wurde eine Zweifachbelastung für Betreiber kritischer Anlagen unter den Finanzunternehmen identifiziert. Auf Basis der neuen Regulierung wurde das Informationssicherheitsmanagementsystem nach ISO 27001-Standard als grundlegendes Strukturelement der Sicherheitsorganisation ausgeführt, dies am Beispiel einer Bankorganisation im Aufbau eines ISMS. Für den Tool-gestützten Betrieb eines ISMS wurden Beispiele zu verschiedenen Themenstellungen eines ISMS gegeben. Der Aufbau sollte als Projekt ausgeführt werden, bevor der Betrieb an die Linie übergeben wird. Das vorgestellte Vorgehen besteht aus sieben Phasen inklusive Zertifizierung. Für den Schutz der Unternehmenswerte wurde, inspiriert aus der Finanzindustrie, das Modell der drei Verteidigungslinien (3LoD) eingeführt, das im Falle einer kritischen Infrastruktur durch die Autoren um den Staat als vierte Verteidigungslinie (4LoD) erweitert wurde.

Zwar müssen mehr Unternehmen ein ISMS aufbauen und betreiben, für einige Branchen ist bereits ein zertifiziertes ISMS mandatorisch, jedoch bietet das Strukturelement ISMS auch ohne regulatorischen Zwang überzeugende Vorteile beim Management der Sicherheitsorganisation: Erstens kann ein sicherheitskritisches Thema nicht mehr übersehen werden (Funktion Checkliste). Zweitens sichert ein ISO 27001-ISMS als weltweit anerkannter Standard, der durch viele Experten durchdacht, in Unternehmen exerziert, von Gesetzgeber gefordert und Aufsichten geprüft wurde (Funktion anerkannt gute Praxis) den Zugang zum weltweiten Erfahrungswissen. Drittens fungiert dieses Managementsystem als Hub für die verschiedenen Kommunikationskanäle zwischen IT-Betrieb, Überwachungsfunktionen, Leitungsebene sowie Aufsicht und vereint so operative, taktische und strategische Sicherheitsaspekte in einem Organisationsrahmen (Funktion Kommunikations-Hub). Viertens eignet sich ein ISMS als Strukturierungsvorlage für weitere Compliance-Aufgaben wie Datenschutz, Geldwäscheprävention und ESG (Funktion Modell). Dies bedeutet, dass Unternehmen mit einem ISMS nach ISO 27001-Standard zukunftssicher(er) werden. Und fünftens ist der Ausweis der Sicherheitsreife eine relevante Evidenz der Unternehmensreife für potenzielle Investoren (Funktion Attraktivität für Investments). Als Managementsystem verstanden trägt ein ISMS massgeblich zum Unternehmenserfolg bei.

Quellen

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. Deutschland (BMI). Diskussionspapier Bearbeitungsstand: 07.05.2024, des Bundesministeriums des Innern und für Heimat
7. Deutschland (BMI). Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
8. Deutschland (BMI). Referentenentwurf des Bundesministeriums des Innern und für Heimat zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITISDachG)
9. Deutschland (BMI). Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)
10. Deutschland (BMF). Gesetzesentwurf der Bundesregierung Entwurf eines Gesetzes über die Digitalisierung des Finanzmarktes (Finanzmarktdigitalisierungsgesetz – FinmadiG)
11. Deutschland. Gesetz über die Elektrizitäts- und Gasversorgung (EnWG)
12. EBA. Leitlinien für das Management von IKT- und Sicherheitsrisiken
13. Schweiz (FINMA). Operationelle Risiken und Resilienz – Banken
14. Trusted Information Security Assessment Exchange (TISAX)

Abkürzungsverzeichnis

Abkürzung	Bezeichnung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAIT, KAIT, VAIT, ZAIT	BaFin: Bankaufsichtliche / Kapitalverwaltungsaufsichtliche / Versicherungsaufsichtliche / Zahlungsdiensteaufsichtliche Anforderungen an die IT
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER	Resilience of Critical Entities Directive
CIA	Confidentiality, Integrity, Availability
CRA	Cyber Resilience Act
DORA	Digital Operational Resilience Act
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
EnWG	Energiewirtschaftsgesetz
ESMA	European Securities and Markets Authority
FINMA	Eidgenössische Finanzmarktaufsicht
FMA	Österreichische Finanzmarktaufsicht
HLS	High Level Structure
IKS	Internes Kontrollsystem
ISB	Informationssicherheitsbeauftragter

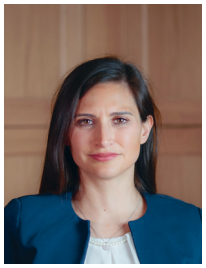
Abkürzung	Bezeichnung
KPI, KRI, KCI	Key Performance Indicators, Key Risk Indicators, Key Compliance Indicators
KRITISDachG	KRITIS-Dachgesetz
KritisV	BSI-Kritisverordnung
MaX	Zusammenfassung der Mindestanforderungen der BaFin an das Risikomanagement MaRisk, MaGo, KAMaRisk
NIS	Netz- und Informationssicherheit
NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
sfO	schriftlich fixierte Ordnung
SOA	Statement of Applicability (Erklärung der Anwendbarkeit)
TISAX	Trusted Information Security Assessment Exchange
ToD, ToI, ToE	Test of Design, Test of Implementation, Test of Effectiveness
XAIT	Zusammenfassung der aufsichtlichen Anforderungen der BaFin BAIT, KAIT, VAIT und ZAIT

Autoren

Dr. Waldemar Grudzien | Managing Director

Waldemar ist Experte für finanzaufsichtliche Prüfungen, Informationssicherheit und Datenschutz. Er unterstützt Klienten bei Prüfungen sowie der Einhaltung entsprechender Anforderungen. Als promovierter Elektroingenieur und studierter Wirtschaftswissenschaftler war er bei einem Verband der Kreditwirtschaft als Experte für Sicherheit im Retail- und Online-Banking tätig.

Mail: wgr@globalregulation.com



Nadine Hofmann | Director

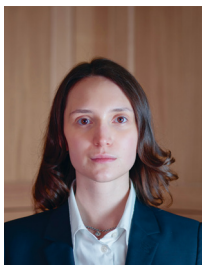
Nadine ist Expertin für Managementsysteme der Informationssicherheit und des Datenschutzes nach den ISO-Standards. Dies beinhaltet die Implementierung von Maßnahmen für Finanzinstitute über die Definition von Anforderungen und Prozessen bis hin zur Vorbereitung von Audits, und der Migration von Prüfungsergebnissen. Sie schloss das Studium zu Luft- und Raumfahrttechnik an der TU Braunschweig und TU Dresden ab.

Mail: nho@globalregulation.com

Victoria Denisiuk | Manager

Victoria ist Managerin bei GRM. Sie ist spezialisiert auf digitale Transformation, einschließlich strategischer Modernisierung, intelligenter Automatisierung und der Optimierung von Informationssystemen. Mit ihrer Expertise in den Bereichen Business Analysis, Projektmanagement und Technologieimplementierung treibt sie die operative Effizienz voran und entwickelt sichere Lösungen für Unternehmen.

Mail: vde@globalregulation.com



Galina Slobodianiuk | Associate

Galina ist Consultant bei GRM. Sie verfügt über einen Bachelor in Finanzwesen und einen Master in Betriebswirtschaftslehre der Humboldt-Universität zu Berlin, mit dem Schwerpunkt Datenanalyse. Ihre fundierte Erfahrung in den Bereichen Finanzen und Datenanalyse verleiht ihr ein ausgeprägtes Verständnis für das Geschäftsprozessmanagement und die Durchführung von Marktanalysen.

Mail: gsl@globalregulation.com

Über Global Regulation Management AG

GRM hebelt Regulierung. Unsere Mission ist der Aufbau regelkonformer Unternehmensstrukturen für global agierende Organisationen. Dabei setzen wir auf ein tiefes Verständnis von Geschäftsprozessen, den rechtlichen Anforderungen in Zielmärkten sowie den gezielten Einsatz moderner Softwarelösungen. Die enge Verzahnung von Geschäftsentwicklung, Risikomanagement und regulatorischen Vorgaben in einer globalisierten Wirtschaftswelt stehen im Mittelpunkt. Das Ergebnis unserer Arbeit sind sichere, rechtskonforme und international operierende Unternehmensstrukturen.

Global Regulation Management AG
Baarerstrasse 52
6300 Zug
Schweiz

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