ISMS als Führungsinstrument für XAIT

Zertifizierungsfähige ISMS stärken die Cyber-Resilienz und tragen zur Erfüllung der XAIT-Anforderungen bei

Dr. Waldemar Grudzien
Leon Kuhlmann
Moritz Treutwein

August 2022
Blogpost

Öffentlich

Key Facts

- Ein zertifizierungsfähiges Informationssicherheitsmanagementsystem (kurz: ISMS) auf Basis des ISO 27001 trägt einen großen Teil zur Erfüllung der XAIT-Anforderungen[1] (BAIT[2], KAIT[3], VAIT[4], ZAIT[5]) in der Regulation am deutschen Finanzplatz bei
- XAIT-Rundschreiben enthalten über den ISO 27001 hinausgehende branchenspezifische Vertiefungen sowie detaillierte Anforderungen hinsichtlich der Ausgestaltung des ISMS, welche zusätzlich zum Standard berücksichtigt werden müssen
- Mit Einführung der EU-Verordnung Digital Operational Resilience Act (kurz: DORA) wird ein ISMS zu einer EU-weiten Anforderung für betroffene Entitäten
- Ersten Anzeichen zufolge könnte mit kommenden Regulierungszyklen eine ISMS-Zertifizierung für ausgewählte Prozesse verpflichtend eingeführt werden

1. Einleitung

Studien des Digitalverbandes Bitkom zeigen auf, dass Cyber-Angriffe in Form von Sabotage, Datendiebstahl oder Spionage hohen Schaden anrichten: in Deutschland lag dieser in den Jahren 2018/2019 bei rund 100 Milliarden Euro, bevor er sich 2020 mit über 200 Milliarden Euro mehr als verdoppelte[6]. Datenbasis für diese Werte ist eine branchenübergreifende Studie mit Geschäftsführern und Sicherheitsverantwortlichen deutscher Unternehmen. Diese Zahlen verdeutlichen den Stellenwert eines ISMS, schließlich wird die Erfolgswahrscheinlichkeit derartiger Cyber-Angriffe durch den Einsatz von ISMS drastisch minimiert. Konkret erfolgt dies durch die Etablierung von Richtlinien sowie die Implementierung der geforderten Prozesse und Kontrollen für die Gewährleistung der Informationssicherheit.

Darüber hinaus empfiehlt sich für Organisationen aber auch aus regulatorischen Gesichtspunkten die Einführung eines zertifizierungsfähigen ISMS: Institute, welche aufsichtlichen Anforderungen an die IT der BaFin (BAIT, ZAIT, KAIT, VAIT; kurz: *XAIT*) unterliegen, können mithilfe eines ISMS einen Großteil regulatorischer Anforderungen erfüllen (*siehe* Abbildung 1) und anhand des Zertifikats – ausgestellt durch akkreditierte Prüfer – einen am Markt akzeptierten Nachweis zur Gewährleistung der Informationssicherheit erbringen. Darüber hinaus wird der Digital Operational Resilience Act (DORA) als EU-Verordnung EU-weite Anforderungen an ein ISMS stellen.

2. Bestandteile eines ISMS

Informationssicherheitsmanagementsysteme bestehen aus zahlreichen organisationsinternen Richtlinien, Prozessen sowie Kontrollen, welche gesamtheitlich dem Schutz von Informationen

[1] Wortneuschöpfung von CORE, zusammenfassend für die BaFin-Rundschreiben zu Anforderungen an die IT (BAIT, KAIT, ZAIT und VAIT)
[2] BAIT: Bankaufsichtliche Anforderungen an die IT
[3] KAIT: Kapitalverwaltungsaufsichtliche Anforderungen an die IT
[4] VAIT: Versicherungsaufsichtliche Anforderungen an die IT
[5] ZAIT: Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten
[6] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

sowie der strukturierten Erfassung von Informationsrisiken und geeigneten Mitigationsmaßnahmen dienen.

Gemäß BSI[7] umfasst ein Managementsystem alle Regelungen für die zielgerichtete Steuerung und Lenkung einer Institution. Es definiert zunächst in Richtlinien („Policies“) Ziele als Verfahren und Regeln. Diese geben den Rahmen für die in der Praxis umzusetzenden Prozesse („Prozessbeschreibungen“ und „Arbeitsanweisungen“) vor. ISO 27001 gilt dabei als etablierter Standard zum Aufbau und Betrieb eines ISMS, ergänzt um die Umsetzungshinweise und Kontrollen des ISO 27002[8]-Standards. Ein ISMS nach ISO 27001 gliedert sich in eine übergeordnete High Level Structure (HLS) und 14 grundlegende Sicherheitsziele (Security Controls A.5 bis A.18) auf.

3. Dreistufiger Aufbau eines ISMS

Informationssicherheitssysteme können strukturiert über drei Stufen aufgebaut werden:

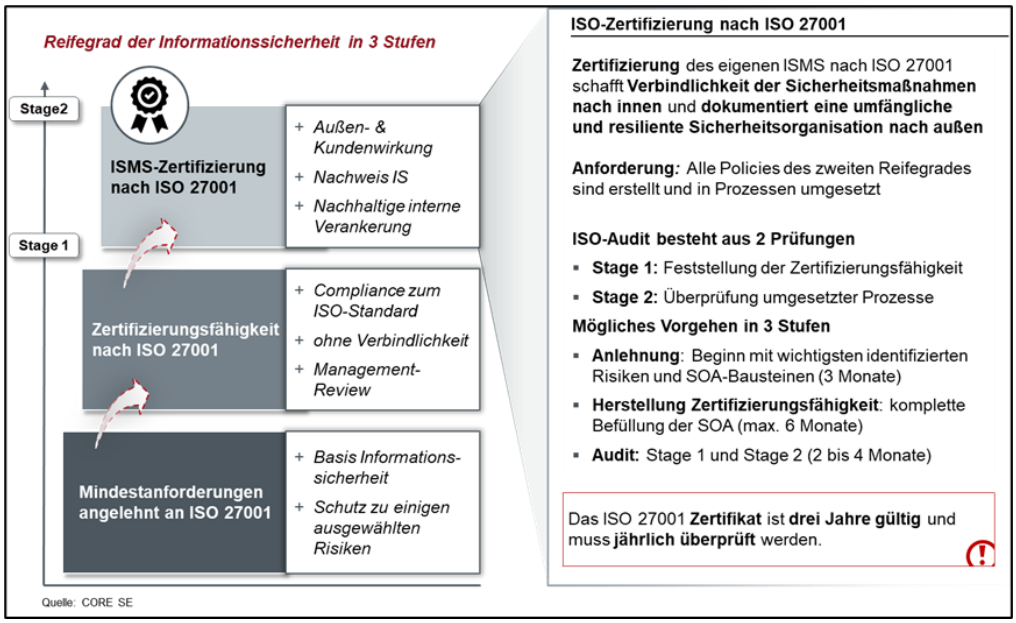

Abbildung 1: Struktur ISO-27001 Standard, Policy-Typen und Aspekte der Umsetzung

Im ersten Schritt werden die für die Zertifizierung wichtigen Prozesse auf relevante Risiken überprüft und anhand von Schutzmaßnahmen adressiert. Unter wichtigen Prozessen werden erstens diejenigen Prozesse verstanden, für die das Zertifikat gelten soll – der Scope des Zertifikats; und zweitens sind es alle Prozesse, die für die Funktionsfähigkeit der erstgenannten Scope-Prozesse notwendig sind. Beispielsweise wird ein Anbieter eines Videoidentifikationsverfahrens dieses Verfahren als zu zertifizierenden Prozess im Scope des Zertifikats deklarieren. Zur Funktionsfähigkeit des Videoidentifikationsverfahrens werden weitere wichtige Subprozesse benötigt wie zum Beispiel die Mustererkennung für hoheitliche Ausweisdokumente und die Bilderkennung für Gesichter.

[7] BSI-Standard 200-1: „Managementsysteme für Informationssicherheit (ISMS)“
[8] Information technology – Security techniques – Code of practice for information security controls

Anhand eines risikoorientierten Ansatzes werden zunächst für die wichtigsten Themenbereiche entsprechende Richtlinien etabliert – gängige Beispiele hierfür sind Vorgaben an das Risikomanagement, Identitäts- und Zugangsmanagement (kurz: IAM) oder auch die Dokumentenlenkung, etwa mit Vorgaben hinsichtlich Freigabe-, Kommunikations- und Veröffentlichungsprozessen von ISMS-relevanten Richtlinien und Prozessen.

In einer zweiten Stufe wird das ISMS gemäß ISO 27001 ganzheitlich aufgesetzt. Das führende und zugleich für die Zertifizierung verpflichtende Dokument ist hierbei das Statement of Applicability (kurz: SoA; Erklärung zur Anwendbarkeit), in welchem die Organisation die Anwendbarkeit der einzelnen Domäne des ISO-Standards erläutert. Diese Erklärung der Anwendbarkeit basiert auf Anhang A des ISO 27001 – respektive ISO 27002, welcher in der aktuellen Fassung von 2022 noch insgesamt 93 sogenannte Kontrollen beinhaltet.

Zum Zusammenhang dieser Standards sei kurz Folgendes erläutert:

ISO 27001 ist ein sogenannter Management-Standard (da er den Standard für den Betrieb eines ISMS beschreibt) und ermöglicht somit auch eine Zertifizierung. Grundsätzlich finden sich die in Anhang A des ISO 27001 beschriebenen Controls mit gleichem Namen und Nummerierung im ISO 27002 wieder, sind dort aber wesentlich ausführlicher beschrieben. Aktuell ergibt sich hinsichtlich der Nummerierung jedoch eine Diskrepanz, da ISO 27002:2022 – anders als die erwartete Aktualisierung ISO 27001:2022 – bereits mit folgenden Änderungen veröffentlicht wurde:

Gegenüber der zuletzt gültigen Version hat die Anzahl der Kontrollen von 114 auf 93 abgenommen, wobei 11 neue Kontrollen hinzugefügt wurden. Zahlreiche bestehende Kontrollen wurden zusammengefügt und auch die Zahl der Hauptdomänen wurde von 14 auf 4 reduziert und beinhaltet nun Controls für die Domäne *Organizational, People, Physical und Technological*.

Deklarieren Organisationen in ihrem SoA einzelne Maßnahmen als nicht anwendbar, ist das – auch in Vorbereitung für eine etwaige Zertifizierung – mit einer nachvollziehbaren Begründung zu erläutern. Ziel der Anwendbarkeitserklärung ist somit auch, etwaige, bestehende Defizite hinsichtlich Richtlinien, Prozessen oder Kontrollen in einem ersten Schritt sichtbar zu machen, um sie anschließend strukturiert erstellen und implementieren zu können. Auch die Art und Weise der Implementierung der jeweiligen Maßnahmen sollte in der Anwendbarkeitserklärung dargelegt werden, sodass das SoA sowohl für den Aufbau des ISMS als auch die etwaige Zertifizierung eine zentrale Rolle einnimmt.

Durch den Aufbau des vollständigen Policy-Konvoluts mit den enthaltenen Prozessen und Kontrollen wird die Zertifizierungsfähigkeit hergestellt. Diese Fähigkeit kann in der dritten, optionalen Stufe im Rahmen eines Audits, aufgeteilt auf zwei Stages, bewiesen werden.

4. Informationssicherheitszertifizierung

Für die Informationssicherheitszertifizierung nach ISO 27001 ist zunächst anzumerken, dass diese lediglich für einzelne Prozesse nicht jedoch pauschal für eine ganze Firma durchgeführt

wird. Aus diesem Grund wird im Rahmen des Audits zunächst der avisierte Geltungsbereich der Zertifizierung festgelegt.

Die im Vorhinein erwähnten Stages für eine Erstzertifizierung sind folgendermaßen aufgebaut:

- **Stage 1**: In dieser Stufe wird die Zertifizierungsfähigkeit bestätigt, konkrete Überprüfungshandlungen umfassen ein Review des SoA sowie des Policy-Konvoluts, um den sogenannten „Test of Design“ zu bestätigen.
- **Stage 2**: Daran anknüpfend folgt der „Test of Effectiveness”, in welchem die Umsetzung der Prozesse und Kontrollen gemäß SoA überprüft werden.

Nach einem erfolgreich durchgeführten Audit wird für den definierten Geltungsbereich ein ISO 27001-Zertifikat mit einer Gültigkeit von drei Jahren ausgestellt. In den Jahren zwei und drei finden im Rahmen von sogenannten Überwachungsaudits jährliche Überprüfungen statt, bevor nach Ablauf der drei Jahre ein Rezertifizierungsaudit notwendig wird. Das Programm beginnt von vorn mit einer großen Prüfung aller Domänen.

Abbildung 2 zeigt eine Übersicht der Dokumentenhierarchie für den vollständigen Nachweis des in der sfO zu verankernden „Soll“ (Test of Design).

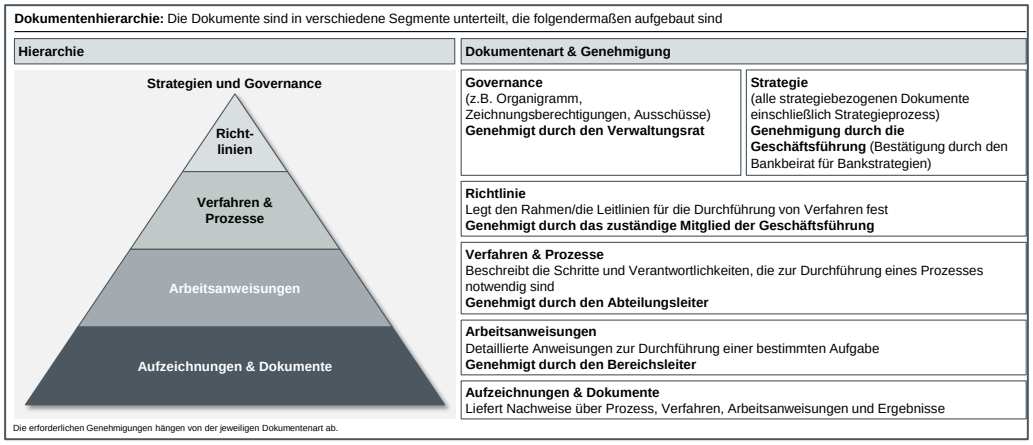

Abbildung 2: Beispiel für eine Dokumentenhierarchie für ein „Test of Design“

5. ISMS-relevante regulatorische Anforderungen im Finanzsektor

Regulatorische Anforderungen an die Zertifizierung eines ISMS gibt es indes – noch – nicht. Daher ist es auch nicht überraschend, dass die Zahl der ISO 27001-zertifizierten Unternehmen in Deutschland im niedrigen vierstelligen Bereich verharrt. Im Finanzsektor werden zumindest inhaltliche Anforderungen an entsprechende ISMS im Rahmen der XAIT-Rundschreiben BAIT (Bankaufsichtliche Anforderungen an die IT, Vorbemerkung 3), ZAIT (Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten, Vorbemerkung 3), KAIT (Kapitalverwaltungsaufsichtliche Anforderungen an die IT, Vorbemerkung 2) sowie VAIT (Versicherungsaufsichtliche Anforderungen an die IT, Vorbemerkung 6) formuliert und stellen damit auch

die Grundlage für aufsichtliche Audits dar. Die letzt- und diesjährigen Aktualisierungen der ZAIT im Vergleich zur BAIT[9] sowie VAIT[10] haben wir in vorherigen Blogposts bereits erörtert.

Im Nachfolgenden beziehen sich die Verfasser auf einzelne Rundschreiben der BaFin. Diese Rundschreiben wurden gesammelt ausgewertet, in XAIT zusammengeführt und beschreiben eine von den Verfassern präferierte Lösung eines gemeinsamen IT-Anforderungskatalogs für Banken, Kapitalverwaltungsgesellschaften, Zahlungs- und E-Geld-Institute sowie Versicherungsunternehmen mit branchenspezifischen Ergänzungen.

Die regulatorische Einordnung dieser Rundschreiben erfolgt in den jeweiligen Vorbemerkungen und wird im Folgenden beispielhaft anhand der BAIT dargestellt: „Dieses Rundschreiben gibt auf der Grundlage des § 25a Abs. 1 des Kreditwesengesetzes (KWG) einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute insbesondere für das Management der IT-Ressourcen, das Informationsrisikomanagement und das Informationssicherheitsmanagement - vor.“[11] Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass sich Rechtsgrundlagen für die ZAIT, VAIT und KAIT durch das Zahlungsdiensteaufsichtsgesetz (kurz: ZAG) respektive das Versicherungsaufsichtsgesetz (kurz: VAG) und das Kapitalanlagegesetzbuch (kurz: KAGB) ergeben.

Gleichermaßen relevant ist Nummer 3 der BAIT-Vorbemerkungen, welche klarstellt, dass die Rundschreiben unter anderem als Konkretisierung der Mindestanforderungen an das Risikomanagement (MaRisk) zu verstehen sind, deren Anforderungen aber davon grundsätzlich unberührt bleiben. Ebenso erwähnenswert ist der Zusatz, dass Institute weiterhin verpflichtet sind, „(…) bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Zu diesen zählen beispielsweise der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization.“

Zwar sind Institute in der Wahl der Standards grundsätzlich frei, in der IT-Strategie müssen sie jedoch die zur Orientierung ausgewählten Standards für die Bereiche IT sowie Informationssicherheit benennen und auch den avisierten Implementierungsumfang darlegen. Neben der Anforderung einer quantitativ wie qualitativ angemessenen Ressourcen-Ausstattung des Informationssicherheitsmanagements fordern die Rundschreiben weiterhin auch die Benennung von Informationssicherheitsbeauftragten (kurz: ISB), welche den Informationssicherheitsbereich in letzter Konsequenz verantworten.

6. Erfüllung von XAIT-Anforderungen mithilfe eines ISMS

Ein ISMS nimmt eine zentrale Rolle bei der Erfüllung von XAIT-Anforderungen ein. An früherer Stelle haben wir den Aufbau eines ISMS bereits in drei Stufen skizziert: beginnend mit der Erfüllung von Mindestanforderungen, dann die Erstellung der Anwendbarkeitserklärung mit anschließender Lückenschließung sowie die abschließende, optionale Zertifizierung. Für XAIT-regulierte

[9] https://core.se/de/blog/zait-vergleich-zur-bait
[10] https://core.se/de/blog/vait-aktualisierung-2022
[11] BAIT, 1, Nr. 2

Organisationen ergibt sich bei diesem Vorgehensmodell mit einer Gap-Analyse vom ISO 27001 zum jeweilig anwendbaren XAIT-Rundschreiben ein zusätzlicher Schritt.

Die Notwendigkeit der Gap-Analyse ergibt sich daraus, dass ISO- und BSI-Standards keine branchenspezifischen Vorgaben enthalten. Vereinfacht gesagt: Die Standards definieren ein grundsätzliches Setting der Organisation in Bezug auf die Domäne Organisation-Technologie-Personal-Recht, haben jedoch den Anspruch, für sämtliche Organisationen unabhängig des Geschäftsmodells gleichermaßen anwendbar zu sein.

So wird im ISO 27001 beispielsweise die Funktion des Informationssicherheitsbeauftragten gefordert. Die branchenspezifischen, aufsichtlichen Rundschreiben definieren nachfolgend die geforderte Ausgestaltung mit klaren, Finanzsektor-spezifischen Auf- und Vorgaben an die Position des Informationssicherheitsbeauftragten.

Dieser Zirkelschluss aus ISO-Standard und XAIT ergibt sich unter anderem über das Sicherheitsziel A.18 (Compliance) des ISO-Standards, durch welchen Organisationen angehalten sind, für sie geltende rechtliche Verpflichtungen zu identifizieren, um Verletzungen von rechtlichen, vertraglichen, satzungsgemäßen oder regulatorischen Verpflichtungen zu vermeiden.

Diese – im Fall der XAIT – branchenspezifische Anforderungen sorgen somit für die Notwendigkeit einer Gap-Analyse. Um dem Ergebnis einer solchen Analyse bereits ein Stück weit vorwegzugreifen: in Abbildung 3 haben die Verfasser einen BAIT-ISO-27001-Abgleich verbildlicht. Es wird deutlich, dass eine hohe Anzahl (grün gekennzeichnet) der BAIT-Anforderungen als Spezifizierung von bestehenden ISO-Anforderungen und nicht als zusätzliche Anforderungen zu verstehen sind.

Hellrot gekennzeichnet sind BAIT-Anforderungen, welche sich aufgrund ihres starken branchenspezifischen Charakters gar nicht im ISO-Standard wiederfinden, konkret betrifft das die Themenbereiche *Management der Beziehungen mit Zahlungsdienstnutzern* sowie *kritische Infrastrukturen (kurz: KRITIS)*. Die grau markierten BAIT-Anforderungen gehen über eine reine Branchenspezifizierung hinaus. Sie sind in dieser Form teilweise im ISO-Standard reflektiert und können als zusätzliche Anforderungen verstanden werden:

	von ISO 27001 weitestgehend abgedeckt, BAIT enthält lediglich Spezifizierung	von ISO 27001 teilweise abgedeckt, BAIT enthält zusätzliche Anforderungen	von ISO 27001 nicht abgedeckt
BAIT-Anforderungen	**BAIT-Kapitel**		
1. IT-Strategie	1.1 1.2		
2. IT-Governance	2.1 2.2 2.3 2.4 2.5		
3. Informationsrisikomanagement	3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8 3.9 3.10 3.11		
4. Informationssicherheitsmanagement	4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10		
5. Operative Informationssicherheit	5.1 5.2 5.3 5.4 5.5 5.6		
6. Identitäts- und Rechtemanagement	6.1 6.2 6.3 6.4 6.5 6.6 6.7 6.8		
7. IT-Projekte und Anwendungsentwicklung	7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 7.10 7.11 7.12 7.13 7.14		
8. IT-Betrieb	8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8		
9. Auslagerungen & sonstiger IT-Fremdbezug	9.1 9.2 9.3 9.4 9.5		
10. IT-Notfallmanagement	10.1 10.2 10.3 10.4 10.5		
11. Zahlungsdienstleister-Management	11.1 11.2 11.3 11.4 11.5 11.6 11.7 11.8		
12. Kritische Infrastrukturen	12.1 12.2 12.3 12.4 12.5		

Quelle: CORE

Abbildung 3: Abdeckung von BAIT-Anforderungen in ISO 27001

Es wird deutlich, dass bei einer vollständigen Implementierung eines ISMS auf Basis des ISO 27001-Standards zahlreiche BAIT-Anforderungen unmittelbar mit erfüllt werden. Im Rahmen der Gap-Analyse ergeben sich – kurz zusammengefasst – darüberhinausgehende Anforderungen insbesondere in den folgenden Bereichen:

- *BAIT Kapitel 1* – ***IT-Strategie***: Aufgrund des Informationssicherheits-Scope kein Teil von ISO 27001
- *BAIT Kapitel 3* – ***Informationsrisikomanagement (IRM)***: Auch wenn sich ein Großteil der IRM-Anforderungen im ISO-Standard wiederfinden, gibt es Ausnahmen für die Kapitel 3.4 bis 3.6, welche sogenannte Schutzbedarfe sowie den Begriff des Informationsverbundes einführen. Zwar sind Unternehmen gemäß ISO-Standard dazu angehalten, entsprechende Assets zu identifizieren und zu inventarisieren. Eine Forderung zur Einstufung von Schutzbedarfen sowie die Klassifizierung als Informationsverbund findet sich im ISO-Standard jedoch nicht
- *BAIT Kapitel 3 und 4* – ***Informationsrisikomanagement (IRM)*** *und* ***Informationssicherheitsmanagement (ISM)***: Eine weitere Abweichung ergibt sich in den Themenbereichen IRM (Kapitel 3.11) und ISM (Kapitel 4.10) für das Reporting an die Geschäftsführung, welches in der BAIT mindestens vierteljährlich gefordert wird
- *BAIT Kapitel 4* – ***Informationssicherheitsmanagement (ISM)***: Während der ISO 27001-Standard lediglich die Benennung eines Informationssicherheitsbeauftragten fordert, geht die XAIT-Anforderung (BAIT: Kapitel 4.6) einen Schritt weiter und fordert, dass diese Position im Institut vorgehalten werden muss – ein Outsourcing wird damit ausgeschlossen
- *BAIT Kapitel 7* – ***IT-Projekte***: Die XAIT formulieren für IT-Projekte sowie Anwendungsentwicklungen zahlreiche Anforderungen, welche sich so aufgrund der thematischen Abgrenzung nicht im ISO-Standard 27001 finden (BAIT-Kapitel 7.2 bis 7.7, 7.10, 7.11). ISO 27001 formuliert diesbezüglich lediglich informationssicherheitsbezogene Anforderungen, während sich die XAIT explizit auf jegliche IT-Projekte beziehen und auch allgemeine Mindestinhalte zur Projektsteuerung definieren
- *BAIT Kapitel 8* – ***IT-Betrieb***: Ein Großteil der Anforderungen der XAIT hinsichtlich des IT-Betriebs lassen sich aus ISO 27001 ableiten, Ausnahmen gibt es hinsichtlich Funktionsprüfungen: ISO 27001 fordert lediglich die Überprüfung von IS-relevanten Aspekten sowie von Leistungsstörungen
- *BAIT Kapitel 10* – ***IT-Notfallmanagement***: ISO 27001 formuliert in A.17 Maßnahmen für Informationssicherheitsaspekte als Teil des Business Continuity Managements. Explizite Anforderungen zum Thema IT-Notfallmanagement analog zur XAIT lassen sich im ISO-Standard nicht finden, hier sei stattdessen auf BSI 200-4 verwiesen

7. EU-weite Regulierung eines ISMS durch DORA

Mit dem Digital Operational Resilience Act wird das Ziel der Stärkung von Cybersicherheit und Resilienz im Finanzsektor außerdem zusätzlich zu den EBA Guidelines auf europäischer Ebene

verankert, schließlich wird die Verordnung für sämtliche EU-regulierte Finanzunternehmen Anwendung finden. Diese zusätzliche EU-Anforderungen dürfte zu einer weiter verstärkten Verbreitung von ISMS beitragen.

Konkret fordert die Verordnung in Artikel 5 (IKT-Risikomanagementrahmen), Absatz 4 die Anwendung eines „Systems für die Steuerung der Informationssicherheit“ – sprich: ein ISMS in Reinform; in ähnlicher Form bereits regulatorisch gefordert in den XAIT-Rundschreiben. Es bleibt jedoch zu konstatieren, dass derartige, vollumfängliche ISMS in der Praxis bei Weitem nicht etabliert sind.

Und auch wenn DORA analog zu XAIT noch keine Anforderung an die Zertifizierung eines ISMS beinhaltet, gibt es Anzeichen, dass sich dies im Rahmen der nächsten Iterationen der Regulierung in circa drei bis fünf Jahren – zumindest für ausgewählte Prozesse – ändern könnte. Für betroffene Institute ist es daher naheliegend, den Aufbau respektive die Anpassung des ISMS mit dem Ziel einer entsprechenden Zertifizierung zu gestalten.

Bei exakter Umsetzung können Organisationen erreichen, dass ein ISMS zum einen zertifizierungsfähig ist und zum anderen gleichzeitig alle XAIT-Anforderungen erfüllt. Eine ganzheitliche Betrachtung und Implementierung eines ISMS ist ein Wettbewerbsvorteil für Finanzunternehmen.

Fazit

Die Einführung eines zertifizierungsfähigen Informationssicherheitsmanagementsystems ist derzeit nicht verpflichtend. Im XAIT-Rundschreiben formuliert die BaFin jedoch Anforderungen an die IT von entsprechenden Organisationen. Diese müssen die XAIT als ergänzende Branchen-Spezifikation sowie den ISO 27001-Standard als vertiefende Anforderungen verstehen. Mithilfe eines zertifizierungsfähigen ISMS lässt sich ein Großteil der XAIT-Anforderungen unmittelbar erfüllen.

Mit Blick auf die Zukunft ist ein zertifizierungsfähiges ISMS aus mehreren Gründen erstrebenswert: zum einen fordern stetig steigende Zahlen an Cyber-Angriffen eine höhere Cyber-Resilienz von Instituten und Akteuren im deutschen Finanzplatz, wofür ein ISMS das zentrale Managementsystem darstellt. Zum anderen wird ein ISMS mit dem Digital Operational Resilience Act obligatorisch für betroffene Organisationen. Und auch wenn derzeit noch keine Zertifizierung des ISMS gefordert wird, existieren erste Anzeichen, dass sich dieser Umstand – zumindest für geschäftskritische Prozesse – mittelfristig ändern könnte.

Verfasser

Waldemar Grudzien ist Expert Director bei CORE. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientenstrukturen.

Mail: waldemar.grudzien@core.se

Moritz Treutwein ist Transformation Manager bei CORE. Sein Beratungsschwerpunkt ist Banking & Capital Markets, dabei umfasst seine Expertise unter anderem die Steuerung und Umsetzung von Geschäftsfelderweiterungen im Rahmen von IT-Implementierungsprojekten, Audit Remediations, sowie die Entwicklung digitaler Geschäftsmodelle. Darüber hinaus ist er Informationssicherheitsbeauftragter bei CORE.

Mail: moritz.treutwein@core.se

Leon Kuhlmann ist Transformation Director bei CORE. Mit seinem „International Business“ Hintergrund und Erfahrung im agilen und klassischen Projektmanagement begleitet er Klienten bei der Umsetzung komplexer IT-Transformationen. Sein Fokus reicht von der Strategieentwicklung bis zum „Go-Live“. Seine aktuellen Tätigkeiten umfassen Programminitiativen für IT-Compliance sowie Core-Banking-Transformationen.

Mail: leon.kuhlmann@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se