Eine Veröffentlichung des ISACA Germany Chapter e.V.
Fachgruppe Informationssicherheit

Implementierungsleitfaden ISO/IEC 27001:2022

Praxisleitfaden für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001:2022

ISACA Germany Chapter

dpunkt.verlag

Herausgeber
ISACA Germany Chapter e. V.
Storkower Str. 158
10407 Berlin

www.isaca.de
info@isaca.de

Autorenteam 2022

- Erik Gremeyer (CISA, CISM), ATM-Consulting
- Andreas Kirchner (CISM, CISSP), abat AG
- Ralf Knecht (CISM)
- Ying-Yeung John Man (CISA, CISM)
- Dirk Meissner (CISA, CDPSE), Allevio AG
- Nico Müller (CISA, CISM, ITGM)
- Jan Rozek
- Dr. Markus Ruppel, RIMOC GmbH
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CCSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media

Autorenteam 2016

- Gerhard Funk (CISA, CISM), unabhängiger Berater
- Julia Hermann (CISSP, CISM), Giesecke & Devrient GmbH
- Angelika Holl (CISA, CISM), Unicredit Bank AG
- Nikolay Jeliazkov (CISA, CISM), Union Investment
- Oliver Knörle (CISA, CISM)
- Boban Krsic (CISA, CISM, CISSP, CRISC), DENIC eG
- Nico Müller, BridgingIT GmbH
- Jan Oetting (CISA, CISSP), Consileon Business Consultancy GmbH
- Jan Rozek
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CGEIT, CRISC, CISSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media
- Holger Schrader (CISM, CRISC)

Stand: November 2022 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe Informationssicherheit)

Implementierungsleitfaden ISO/IEC 27001:2022

Praxisleitfaden für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001:2022

ISACA
Germany Chapter

Warum dieser Guide?

Informationssicherheit ist unverzichtbar. Sie muss als Bestandteil der Unternehmensführung darauf ausgerichtet sein, die Geschäftsziele optimal zu unterstützen. Auch bzw. gerade in Zeiten sogenannter »Cyberbedrohungen« und der vielerorts aufkommenden Herausforderungen der »Cybersicherheit« bietet ein gut strukturiertes Informationssicherheitsmanagementsystem (ISMS) nach international anerkannten Standards die optimale Grundlage zur effizienten und effektiven Umsetzung einer ganzheitlichen Informationssicherheitsstrategie.

Ob der gewählte Fokus auf die aus dem Internet stammenden Bedrohungen, den Schutz von geistigem Eigentum, die Erfüllung von Regularien und vertraglichen Verpflichtungen oder die Absicherung von Produktionssystemen gelegt wird, hängt von den Rahmenbedingungen (z. B. Branche, Geschäftsmodell oder Risikoappetit) und den konkreten Sicherheitszielen der jeweiligen Organisation ab. In allen Fällen ist entscheidend, sich der in dem jeweiligen Kontext bestehenden Informationssicherheitsrisiken bewusst zu sein bzw. diese aufzudecken und die notwendigen Strategien, Prozesse und Sicherheitsmaßnahmen auszuwählen, umzusetzen und letztlich auch konsequent nachzuhalten.

Die konkrete Umsetzung eines ISMS erfordert Erfahrung, basiert zuvorderst allerdings auf der Entscheidung und Verpflichtung der obersten Leitungsebene gegenüber dem Thema. Ein klarer Managementauftrag und eine an die Geschäftsstrategie angepasste Sicherheitsstrategie sind zusammen mit kompetentem Personal und den letztlich immer erforderlichen Ressourcen die Grundvoraussetzungen, um mit einem ISMS die Erreichung der Geschäftsziele optimal unterstützen zu können.

Der aktualisierte *Implementierungsleitfaden ISO/IEC 27001: 2022* (kurz: Implementierungsleitfaden) enthält praxisorientierte Empfehlungen und Hinweise für Organisationen, die entweder bereits ein ISMS nach der internationalen ISO/IEC-Norm 27001, »Information security, cybersecurity and privacy protection – Information security management systems – Requirements«, betreiben oder ein solches aufbauen wollen, unabhängig von vorhandenen oder etwaig angestrebten Zertifizierungen. Der Leitfaden bietet allen, die mit dem Aufbau und/oder Betrieb eines ISMS betraut sind, pragmatische Hilfestellungen und Herangehensweisen. Die Vorteile eines individuell angepassten und, sofern notwendig, gleichzeitig normkonformen ISMS werden klar herausgestellt. Insbesondere werden Praxisempfehlungen zur Etablierung bzw. Erhöhung des Reifegrads bestehender ISMS-Prozesse und typische Umsetzungsbeispiele verschiedener Anforderungen aufgezeigt.

Danksagung

Das ISACA Germany Chapter e. V. bedankt sich bei der ISACA-Fachgruppe Informationssicherheit und den Autoren für die Erstellung des Leitfadens: Erik Gremeyer, Andreas Kirchner, Ralf Knecht, Ying-Yeung John Man, Dirk Meissner, Nico Müller, Jan Rozek, Dr. Markus Ruppel, Andrea Rupprich, Dr. Tim Sattler, Michael Schmid.

Projektleitung und Redaktion: Andrea Rupprich

Inhaltsverzeichnis

1 Einleitung

Das systematische Management der Informationssicherheit nach ISO/IEC 27001:2022 soll einen effektiven Schutz von Informationen und IT-Systemen in Bezug auf die wesentlichen Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) gewährleisten.

Dieser Schutz ist kein Selbstzweck, sondern dient der Unterstützung der Geschäftsprozesse, der Erreichung der Unternehmensziele und dem Erhalt der Unternehmenswerte durch eine störungsfreie Bereitstellung und Verarbeitung von Informationen. Dazu bedient sich ein ISMS in der Praxis folgender drei Sichtweisen:

- **G – Governance-Sicht**
  - IT-Ziele und Informationssicherheitsziele, die aus den übergeordneten Unternehmenszielen abgeleitet sind (z.B. unterstützt von bzw. abgeleitet aus COSO oder COBIT)
- **R – Risiko-Sicht**
  - Schutzbedarf und Risikoexposition der Unternehmenswerte und IT-Systeme
  - Risikoappetit des Unternehmens
  - Chancen und Risiken
- **C – Compliance-Sicht**
  - Externe Vorgaben durch Gesetze, Regulatorik und Normen
  - Interne Vorgaben und Richtlinien
  - Vertragliche Verpflichtungen

Diese Sichtweisen bestimmen, welche Schutzmaßnahmen angemessen und wirksam sind für

- die Möglichkeiten und Geschäftsprozesse der Organisation,
- den Schutzbedarf in Abhängigkeit von der Kritikalität der jeweiligen Unternehmenswerte sowie
- die Einhaltung geltender Gesetze und Regularien.

Maßnahmen

Maßnahmen zur Erreichung und Aufrechterhaltung einer störungsfreien Informationsverarbeitung müssen einerseits *wirksam (effektiv)* sein, um ein erforderliches Schutzniveau zu erreichen. Andererseits müssen sie auch *wirtschaftlich angemessen (effizient)* sein.

ISO/IEC 27001:2022 und die darin systematisch und ganzheitlich dargelegten Anforderungen und Maßnahmen, die – in unterschiedlicher Ausprägung und Güte – zum Betrieb eines jeden ISMS gehören, unterstützen die Erreichung der eingangs aufgeführten Ziele aus allen drei Sichten (siehe Abbildung 1):

- Die *Governance-Sicht* bezieht sich auf die Steuerungsaspekte des ISMS, wie beispielsweise eine enge Einbeziehung der obersten Leitungsebene (vgl. Kapitel *3.2 Leadership and Commitment*), eine Konsistenz zwischen den Geschäfts- und Informationssicherheitszielen (vgl. Kapitel *3.3 IS Objectives)*, die Festlegung von Strategien und Richtlinien (vgl. Kapitel *3.4 IS Policy)*, eine effektive und zielgruppengerechte Kommunikationsstrategie (vgl. Kapitel *3.9 Communication*), angemessene Verantwortlichkeiten und Organisationsstrukturen (vgl. Kapitel *3.5 Roles, Responsibilities, and Competencies*) sowie eine zielgerichtete Überwachung der Leistung (vgl. Kapitel *3.7 Performance/Risk/Compliance Monitoring*). Weiterführende Informationen zur Governance der Informationssicherheit bietet die ISO/IEC 27014:2020.
- Die *Risiko-Sicht*, die unter anderem als Basis für eine nachvollziehbare Entscheidungsfindung und Priorisierung von technischen und organisatorischen Maßnahmen fungiert, ist einer der Kernpunkte eines ISMS nach ISO/IEC 27001:2022. Sie wird durch das IS-Risikomanagement repräsentiert (vgl. Kapitel *3.6 Risk Management*) und beinhaltet Vorgaben und Methoden für die Identifizierung, Analyse und Bewertung von Risiken im Kontext der Informationssicherheit, d.h. Risiken, die eine potenzielle Gefährdung für die Vertraulichkeit, Integrität und/oder Verfügbarkeit von IT-Systemen und Informationen und letztlich der davon abhängigen Geschäftsprozesse darstellen.

Die *Compliance-Sicht* ist fest in der gesamten Norm verankert. Sie umfasst einerseits die Definition der erforderlichen (Sicherheits-)Vorgaben, was durch die Maßnahmen aus Annex A unterstützt wird. Andererseits bezieht sie sich auf die konkrete Erfüllung genau dieser Vorgaben, was durch eine regelmäßige Kontrolle seitens des Managements und der Informationssicherheitsverantwortlichen (vgl. Kapitel *3.7 Performance/Risk/Compliance Monitoring*) sowie durch interne Audits sichergestellt werden muss (vgl. Kapitel *3.12 Internal Audit* und *3.14 Continual Improvement*). Eine angemessene Dokumentation (vgl. Kapitel *3.8 Documentation*) und das vorhandene Sicherheitsbewusstsein von Mitarbeitern und Führungskräften (vgl. Kapitel *3.10 Awareness*) sind für die Compliance-Sicht ebenfalls von wesentlicher Bedeutung.

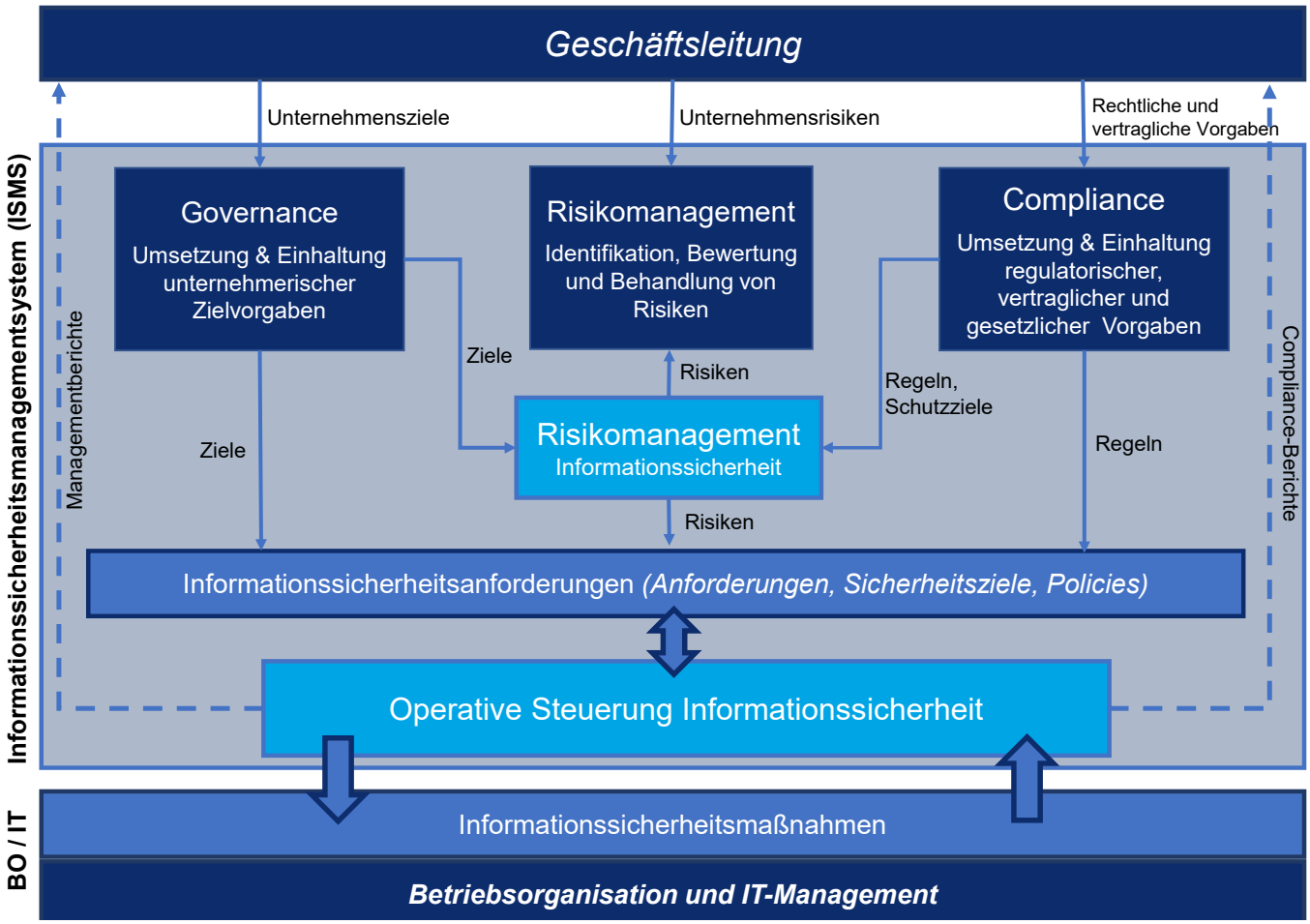


Abbildung 1: Einbindung des ISMS in die Unternehmenssteuerung[1]

1 Quelle: Carmao GmbH.

2 Aufbau des Leitfadens

2.1 Themenbereiche

Der vorliegende Implementierungsleitfaden orientiert sich an den wesentlichen Themenbereichen der Norm ISO/IEC 27001:2022, allerdings ohne erneut die Abschnittsstruktur des Standards identisch wiederzugeben. Vielmehr werden die relevanten Themenbereiche eines ISMS nach ISO/IEC 27001:2022 als »Bausteine« beschrieben, die sich in der Praxis als relevant und erforderlich erwiesen haben. Vor diesem Hintergrund werden die Inhalte der betroffenen Abschnitte der Norm neu strukturiert und zu einzelnen Schwerpunktthemen zusammengefasst. Aus Sicht der Autoren lassen sich auf Basis der Norm im Wesentlichen die nachfolgend aufgeführten 14 »Bausteine« hervorheben, die in Summe das ISMS einer Organisation darstellen (siehe Abbildung 2):

1. Kontext der Organisation (Context of the Organization)
2. Führung und Verpflichtung (Leadership and Commitment)
3. IS-Ziele (IS Objectives)
4. IS-Richtlinie (IS Policy)
5. Rollen, Verantwortlichkeiten und Kompetenzen (Roles, Responsibilities, and Competencies)
6. Risikomanagement (Risk Management)
7. Bewertung der Leistung und KPIs (Performance/Risk/Compliance Monitoring)
8. Dokumentation (Documentation)
9. Kommunikation (Communication)
10. Awareness (Awareness)
11. Lieferantenbeziehungen (Supplier Relationships)
12. Internes Audit (Internal Audit)
13. Vorfallsmanagement (Incident Management)
14. Kontinuierliche Verbesserung (Continual Improvement)

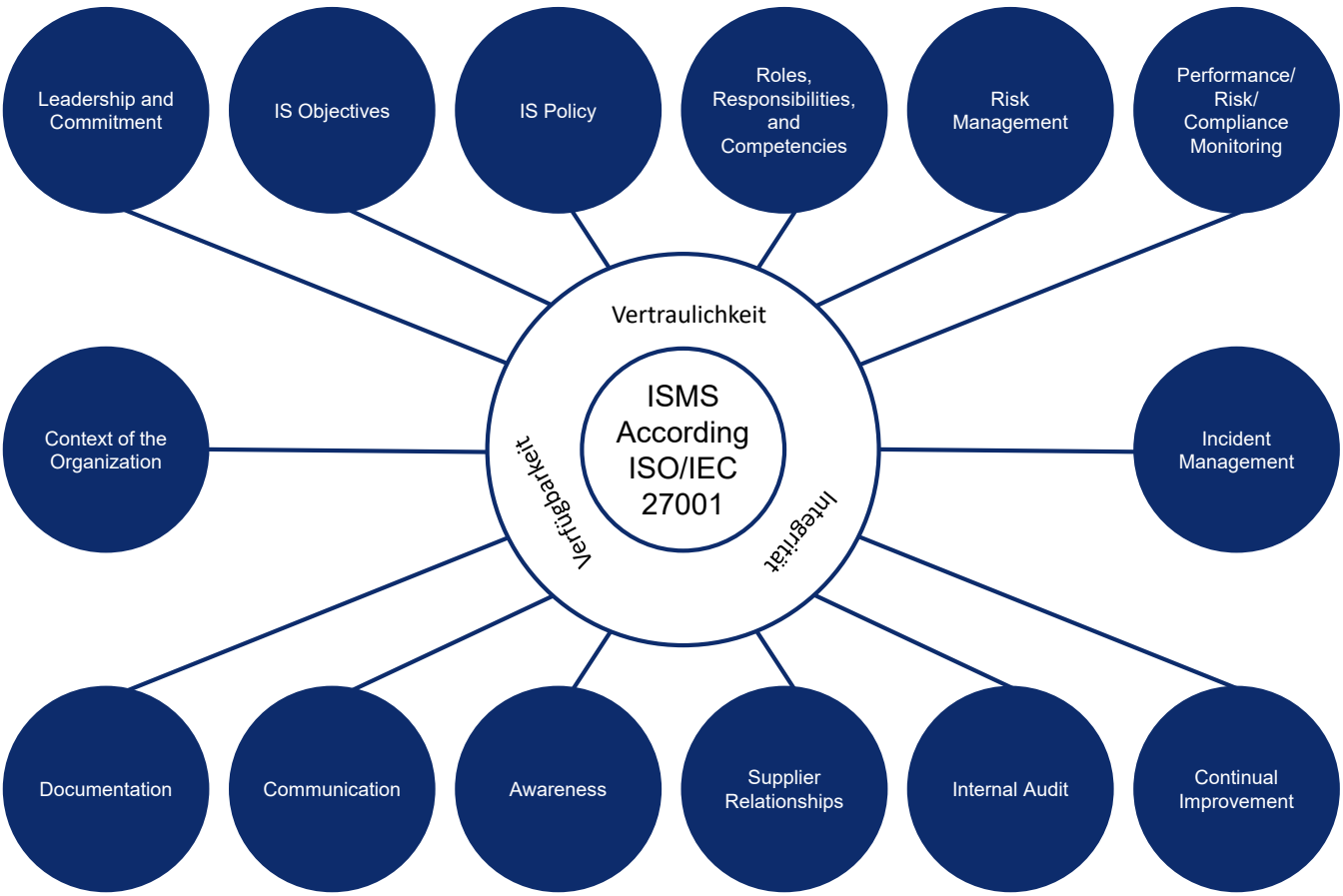


Abbildung 2: Bausteine eines ISMS nach ISO/IEC 27001:2022

In den nachfolgenden Kapiteln werden zu allen Bausteinen wesentliche Erfolgsfaktoren für die normkonforme und praxiserprobte Realisierung aufgezeigt.

Da dieser Leitfaden insbesondere auch praktische Hilfestellung geben soll, gehen die Ausführungen zu den Bausteinen hierbei über die rein normativ geforderten Inhalte der ISO/IEC 27001:2022 (respektive ISO/IEC 27002:2022) hinaus. Das bedeutet im Umkehrschluss allerdings auch, dass nicht jeder Hinweis dieses Dokuments für jedes ISMS bzw. für jede Organisation gleich »gut« geeignet ist.

Der Aufbau eines ISMS, unabhängig ob zur Selbstverpflichtung oder mit Zertifizierungsabsicht, ist ein ambitioniertes Projekt, das – wie jedes andere Projekt auch – »smarte«[1] Ziele, ausreichende und fachkundige Ressourcen, eine(n) passende(n) Projektleiter(in) und ein motiviertes und qualifiziertes Team benötigt. Zudem ist die stetige und sichtbare Unterstützung des Topmanagements für einen erfolgreichen Projektabschluss und den anschließenden Übergang hin zum ISMS-Betrieb von entscheidender Bedeutung.

Der Implementierungsleitfaden umfasst neben Hilfestellungen auch Verweise auf weitere Normen, Standards oder andere hilfreiche Quellen, wobei diese dann als solche gekennzeichnet sind.

2.2 Kapitelstruktur

Die einzelnen Kapitel sind jeweils gleich aufgebaut und in folgende drei Abschnitte gegliedert:

- **Erfolgsfaktoren aus der Praxis**
  Darstellung von – aus Sicht der Autoren – wesentlichen Erfolgsfaktoren für den Aufbau und Betrieb eines ISMS nach ISO/IEC 27001:2022
- **Anforderungen an die Dokumentation**
  Darstellung von Dokumentationsanforderungen, sowohl aus normativen Gesichtspunkten als auch aus Sicht der Praxis
- **Referenzen**
  Angabe der für den Themenbereich relevanten Abschnittsnummern aus ISO/IEC 27001:2022 sowie weitere Quellenangaben, sofern erforderlich und sinnvoll

2.3 Konventionen

Zur besseren Lesbarkeit wird in diesem Leitfaden das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

Sofern im weiteren Verlauf die Begriffe *»Norm«* oder *»Standard«* ohne weitere Konkretisierung verwendet werden, beziehen sich diese stets auf die Norm ISO/IEC 27001:2022.

Der Begriff *»Kapitel«* wird bei Verweisen innerhalb dieses Leitfadens, der Begriff *»Abschnitt«* wird bei Verweisen auf die Norm verwendet.

Der Begriff *»Anhang«* wird bei Verweisen auf Anhänge dieses Leitfadens, die Begriffe *»Annex«* bzw. *»Annex A«* werden bei Verweisen auf den Annex A der Norm verwendet.

Die Begriffe *»Organisation«* und *»Unternehmen«* beziehen sich jeweils auf die Institution bzw. den Bereich, innerhalb derer bzw. dessen das ISMS implementiert wird. Die Begriffe werden im Leitfaden synonym verwendet.

Im Dokument verwendete Abkürzungen und weitere Begriffsdefinitionen befinden sich im Glossar in Kapitel 5.

1 SMART: spezifisch, messbar, akzeptiert, realistisch, terminiert.

3 Bausteine eines ISMS nach ISO/IEC 27001:2022

3.1 Context of the Organization

Eine der ersten Aufgaben bei der Implementierung eines ISMS ist die Festlegung des konkreten Anwendungs- bzw. Geltungsbereichs (engl.: scope) des Managementsystems sowie die Durchführung einer Anforderungs- und Umfeldanalyse im Hinblick auf die Organisation und deren Stakeholder. Durch die Berücksichtigung des Kontexts der Organisation kann eine Organisation sicherstellen, dass ihre Informationssicherheitsmaßnahmen an ihre spezifischen Bedürfnisse und Umstände angepasst und somit effektiv sind. ISO/IEC 27001 fordert daher von Organisationen, dass sie den Kontext der Organisation sorgfältig analysieren und in ihre Informationssicherheitsplanung und -umsetzung einbeziehen.

Festlegung des Geltungsbereichs

Der Geltungsbereich muss laut Norm dokumentiert vorliegen und beschreibt den Umfang des ISMS innerhalb eines Unternehmens, d. h., er legt die Grenzen fest und definiert, welche Assets (Prozesse, Geschäftsbereiche, Standorte, Anwendungen etc.) sich innerhalb und welche sich außerhalb des Geltungsbereichs befinden.

Die Identifizierung des Geltungsbereichs wird üblicherweise mithilfe einer Umfeld- und Anforderungsanalyse durchgeführt.

- Das Scope-Dokument ist im Wesentlichen ein Dokument für die Stakeholder des Managementsystems und sollte bei entsprechender Aufforderung für diese bereitgestellt werden, da die Stakeholder, z. B. Kunden, nur so prüfen können, ob die für sie relevanten Prozesse, Infrastrukturen, Themen oder Anforderungen durch das ISMS abgedeckt sind.
- In der Praxis verweisen Organisationen bei Anfragen oft auf evtl. vorhandene ISO/IEC-27001-Zertifikate, die dann – bei genauerer Betrachtung – oftmals gar nicht für die Anfrage relevant bzw. hinreichend sind, da der angefragte Prozess nicht oder nur teilweise durch das ISMS abgedeckt ist. Zur Vermeidung böser Überraschungen sollte daher zusätzlich zu einem Zertifikat immer das Scope-Dokument bzw. eine *genaue* Beschreibung des Geltungsbereichs angefordert werden.
- Ein weiteres relevantes Dokument zur Darstellung des Scopes und des Umfangs eines ISMS ist die normativ geforderte Erklärung zur Anwendbarkeit (engl.: Statement of Applicability, SoA). In dem SoA werden die begründeten Entscheidungen zur Umsetzung der Maßnahmen (engl.: controls) aus Annex A dokumentiert, d. h., ob die jeweilige Maßnahme innerhalb des ISMS zur Anwendung kommt oder nicht, inklusive der jeweiligen Begründung für die Anwendung oder die Nichtanwendung.
- Es ist üblich, dass in der Information Security Policy (Informationssicherheitsleitlinie) der Scope zumindest grob umrissen wird. Im Gegensatz zum Scope-Dokument sind die Security Policy und das SoA in der Regel interne Dokumente und nicht für die Weitergabe an externe Parteien vorgesehen. Allerdings sollte im Rahmen von Dienstleisterbeziehungen und ggf. Dienstleisteraudits auf die genaue Scope-Definition und die Inhalte des SoA geachtet werden.

Umfeldanalyse

Die Umfeldanalyse dient der Einordnung des ISMS in das Gesamtumfeld für den betreffenden Scope. Sie sollte neben den für das ISMS relevanten organisatorischen und technischen Schnittstellen insbesondere auch branchentypische bzw. standorttypische Gegebenheiten beschreiben. Hierbei müssen sowohl das Umfeld im Innenverhältnis, z. B. andere Managementsysteme (ISO 9001:2015, ISO 22301:2019 etc.), Schnittstellen zu anderen wichtigen Abteilungen wie Risikomanagement, Personalabteilung, Datenschutz, Facility-Management, Revision und Recht, falls nicht Bestandteil des vorliegenden Geltungsbereichs, sowie das Umfeld im Außenverhältnis, z. B. wichtige Lieferanten und Dienstleister, strategische Partner und ggf. andere Organisationen, betrachtet werden.

Anforderungsanalyse

Die für das Managementsystem verantwortlichen Personen benötigen einen klaren Überblick darüber, welche Interessengruppen (engl.: stakeholder) existieren und welche Anforderungen diese an die Organisation und das Managementsystem haben.

Die Anforderungen interessierter Parteien können gesetzliche und amtliche Vorgaben (z. B. EU-DSGVO, UWG, TMG, Regulierungsbehörden), aber z. B. auch vertragliche Verpflichtungen beinhalten. Die Organisation selbst (oder evtl. eine in der Hierarchie übergeordnete Organisation) könnte ebenfalls über Entscheidungs- und/oder Richtlinienkompetenzen verfügen, was entsprechend zu beachten ist.

Erfolgsfaktoren aus der Praxis

Da die Festlegung des Geltungsbereichs der erste und entscheidende Schritt für den Aufbau und Betrieb eines ISMS ist, sollte diese Phase besonders sorgfältig durchgeführt werden. Das Verständnis des Kontexts ist die Grundlage für alle weiteren Handlungen (z. B. Aufbau und Ablauf der Risikoanalyse, Organisationsstruktur, Definition von Arbeitspaketen und deren Priorisierung, Projektplanung) und ist zudem auch betriebswirtschaftlich eine wesentliche Voraussetzung zur Abschätzung der Machbarkeit und des Aufwands (Ressourcen, Budget, Zeit) für den Aufbau und späteren Betrieb des ISMS.

- In ISO 31000:2018, Abschnitt 5.4.1 »*Understanding the organization and its context*« werden Listen angeboten, mit denen die Vollständigkeit der Darstellung erreicht werden kann.
- Der notwendige Detaillierungsgrad zur Definition des Geltungsbereichs ergibt sich in der Regel aus den internen und externen Anforderungen an die Informationssicherheit der Organisation.

  Es hat sich in der Praxis als hilfreich erwiesen, die vom ISMS maßgeblich betroffenen Bereiche ausreichend detailliert im Geltungsbereich zu beschreiben, da diese Beschreibung ein wichtiges Steuerungswerkzeug darstellt und bei Strategieentscheidungen und (späteren) Abstimmungen relevant sein wird.
- Die gemäß Abschnitt 4.2 der Norm erforderliche Identifikation der Interessengruppen (und deren Anforderungen) ist in jedem Fall sorgfältig und umfassend durchzuführen, denn nur so können klare Ziele und Inhalte des ISMS festgelegt und der bestmögliche Nutzen erreicht werden. Beispiele für Interessengruppen sind: Eigentümer, Anteilseigner, Aufsichtsrat, Betriebsrat, Regulierungsbehörden bzw. Gesetzgeber, Kunden, Klienten, Lieferanten bzw. Zulieferer, Dienstleister, Angestellte etc.
- Als Basis der Erhebung relevanter interner und externer Anforderungen können u. a. Business-Pläne, Verträge sowie Vorgaben von Aufsichtsbehörden und Gesetzgebern zu den betroffenen Geschäftsprozessen dienen. Dies wird in der Praxis oft durch eine Compliance- bzw. IT-Compliance-Funktion wahrgenommen, die bei der Erhebung der Anforderungen unterstützen kann.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Geltungsbereich des ISMS (Abschnitt 4.3)
- Erklärung zur Anwendbarkeit (Abschnitt 6.1.3 d)
- Übersicht aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen, die einen Einfluss auf die Informationssicherheitsstrategie und das ISMS haben (Abschnitt 18.1)
- Übersicht aller für den konkreten Geltungsbereich des ISMS relevanten Interessengruppen (Stakeholder)

Darüber hinaus hat sich in der Praxis folgendes Dokument als zielführend etabliert:

- Schnittstellenvereinbarungen zwischen dem ISMS-Geltungsbereich und den das ISMS unterstützenden internen Bereichen (zur Sicherstellung, dass die Zusammenarbeit mit dem internen Bereich in Übereinstimmung mit ISO/IEC 27001:2022 und den relevanten IS-Anforderungen der Organisation erfolgt). Beispiel: Schnittstellenvereinbarungen mit dem Personalbereich.

Referenzen

ISO/IEC 27001:2022 – Abschnitte 4.3 und 6.1.3

ISO/IEC TR 27023:2015

ISO 22301:2019

ISO 31000:2018

ISO 9001:2015

3.2 Leadership and Commitment

Ein erfolgreiches ISMS wird im Top-down-Ansatz eingeführt und stellt einen Bezug zwischen Geschäftszielen und Informationssicherheit her, indem zum einen die Anforderungen der Stakeholder berücksichtigt und zum anderen die auf die operativen Geschäftsprozesse wirkenden Risiken mit wirksamen Maßnahmen auf ein angemessenes Maß reduziert werden.

Um der genannten Aufgabe gerecht zu werden, müssen also zum einen die Geschäftsziele und die Anforderungen bekannt sein und zum anderen entsprechende organisatorische Rahmenbedingungen, wie z. B. die Einführung bzw. Anpassung von Risikomanagementprozessen in der Organisation, geschaffen werden.

Spätestens bei der notwendigen Anpassung von organisationsweiten Prozessen sind Führung (im Sinne des Vorgebens einer Richtung und Vision), Zustimmung und die Unterstützung (Leadership und Commitment) durch die Leitungsebene unumgänglich, da die eingeführten Prozesse des Managementsystems sonst keinen verbindlichen Charakter haben und somit u. U. keine Akzeptanz finden. Hier sind demnach die Führungskräfte in der Verantwortung, was mit Blick auf ihre Vorbildfunktion auch als »Tone from the Top« beschrieben wird.

Seitens der Norm wird richtigerweise explizit gefordert, dass das Topmanagement nachweislich die Gesamtverantwortung für die Informationssicherheit innerhalb der Organisation übernehmen muss. Ferner muss es die Bedeutung eines effektiven ISMS sowie die Einhaltung der Anforderungen im Rahmen des ISMS an die betroffenen Mitarbeiter kommunizieren. Dies erfolgt in der Regel über die sogenannte Infor-

mationssicherheitsleitlinie (vgl. *Information Security Policy* in Kapitel *3.4 IS Policy*) sowie über eine Anwenderrichtlinie.

- Unter dem Stichwort (IT-)Governance sowie in Zusammenhang mit der Verantwortung der Geschäftsleitung für Strategien wird die nachweisliche Übernahme der Gesamtverantwortung insbesondere in regulierten Bereichen immer stärker auch von den entsprechenden Aufsichtsbehörden gefordert[1].

Erfolgsfaktoren aus der Praxis

Definition »Topmanagement«

Mit »Topmanagement« ist die Leitungsebene gemeint, die für die Steuerung der durch das ISMS zu schützenden Organisation verantwortlich ist und über den Ressourceneinsatz entscheidet.

- Bei großen Unternehmen ist das »Topmanagement«[2] aus Sicht der Norm nicht zwangsläufig die oberste Leitungsebene der gesamten Unternehmensgruppe (z. B. Konzernvorstand). Es kann auch eine lokale Geschäftsführung oder Bereichsleitung sein, die für das ISMS verantwortlich ist. Entscheidend ist immer der konkrete Geltungsbereich des jeweiligen ISMS.
- Bei externen Zertifizierungsaudits kann es vorkommen, dass von der Zertifizierungsstelle dennoch die Einbeziehung der obersten Leitungsebene der gesamten Unternehmensgruppe gefordert wird (z. B. aus Gründen der Risikohaftung). Aus diesem Grund ist es sinnvoll, bei einer angestrebten Zertifizierung diesen Punkt bereits im Vorfeld mit der Zertifizierungsstelle zu klären.

Aufgaben/Verantwortlichkeiten »Topmanagement«

ISO/IEC 27001:2022 fordert vom Topmanagement eine klare Vorbildfunktion hinsichtlich der Informationssicherheit. In der Praxis gehören hierzu neben einem sichtbaren Engagement und einem klaren Bekenntnis (Commitment) zur Informationssicherheit auch die

- vorbildliche Einhaltung der Informationssicherheitsanforderungen,
- hinreichende und nachvollziehbare Bereitstellung von Ressourcen,
- Einforderung einer Vorbildfunktion bei den weiteren Leitungsebenen,
- konsequente Behandlung von und Reaktion auf Nichtkonformitäten,
- Selbstverpflichtung zur kontinuierlichen Verbesserung.

Die zentralen Aufgaben des Topmanagements im Kontext ISMS sind:

- Übernahme der Gesamtverantwortung für Informationssicherheit
- Definition der Informationssicherheitsstrategie und der konkreten IS-Ziele (siehe Kapitel *3.3 IS Objectives*)
- Definition der Entscheidungskriterien und Grundsätze zur Risikobeurteilung und -behandlung und Einführung entsprechender Prozesse (siehe Kapitel *3.6 Risk Management*)
- Integration der Informationssicherheitsanforderungen in Geschäftsprozesse und Projektmanagementmodelle (siehe Kapitel 3.6 *Risk Management*)
- Durchführung regelmäßiger ISMS-(Top-)Managementreviews (siehe Kapitel *3.14 Continual Improvement*)
- Bereitstellung der notwendigen personellen und finanziellen Ressourcen zum Aufbau des ISMS und zur Umsetzung der Informationssicherheitsstrategie
- Sichtbarsein in Awareness-Veranstaltungen oder -Maßnahmen (z. B. Leitvideo-Botschaft)

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Abschnitt 9.3 »*Management Review*« fordert eine Dokumentation der Überprüfung des ISMS durch das Topmanagement, einschließlich der Entscheidungen hinsichtlich Veränderungen und Verbesserungen des ISMS. Diese können als Maßnahmen im Risikobehandlungsplan erfasst werden.
- Beim Managementreview müssen Ergebnisse, wie Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung, als dokumentierte Information aufbewahrt werden.

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Ableitung und Bewertung der aktuellen Risiken aus festgestellten Abweichungen zwischen strategischen IS-Zielen und Zielerreichungsgrad, idealerweise als Risikobehandlungsplan
- Nachweise zur Berichterstattung an das Topmanagement, z. B. in Form von Präsentationen, Protokollen oder Reports

1 Rundschreiben 10/2021 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk *(https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html)*.

2 Siehe Kapitel 3.1 *Context of the Organization und ISO/IEC 27000:2018*, Clause 3.75.

- Reporting über den Umsetzungsstand inklusive dessen Wirksamkeitskontrolle zu festgelegten Maßnahmen (insb. bei Überfälligkeit dieser) aus Audits, Risikobehandlung, Incidents oder der kontinuierlichen Verbesserung

Hinweis: Im Kontext Führungsverantwortung gibt es verschiedene Möglichkeiten zur Dokumentation. Bei den oben aufgeführten Beispielen handelt es sich um Vorschläge für mögliche Aufzeichnungen, die dazu beitragen, die Nachvollziehbarkeit von Berichterstattung und Entscheidungsfindung sicherzustellen. Jede Organisation muss die für sie passende Dokumentationsform und -häufigkeit finden.

Referenzen

ISO/IEC 27001:2022 – Abschnitte 5.1, 9.1 und 9.3, 5.36

3.3 IS Objectives

Das ISMS als Ganzes trägt zum Schutz und zur Aufrechterhaltung der jeweils erforderlichen Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsprozesse und der darin verarbeiteten Informationen bei. Die von der Unternehmensleitung festgelegten Geschäftsziele dienen als Grundlage für die Ausgestaltung bzw. Festlegung der IT-Ziele sowie spezieller Informationssicherheitsziele (IS Objectives) und der daraus resultierenden Maßnahmen.

Erfolgsfaktoren aus der Praxis

Da die Ziele und Grundsätze des ISMS von den übergreifenden Geschäftszielen der Organisation abgeleitet sein sollten, kann das Verfehlen der IS-Ziele einen direkten Einfluss auf die Erreichung der Geschäftsziele haben. Daher ist es unabdingbar, angemessene und messbare IS-Ziele und deren Umsetzung festzulegen.

- Die IS-Ziele müssen im Einklang mit den Inhalten der wesentlichen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, »CIA«) und der IS-Leitlinie stehen (siehe auch Kapitel *3.4 IS Policy*).
- Die IS-Ziele sollten immer an den übergeordneten Unternehmenszielen ausgerichtet werden und regelmäßig auf Aktualität und Angemessenheit überprüft werden. Dies ermöglicht es, die Informationssicherheitsanforderungen in die operative Geschäftstätigkeit so zu integrieren, dass sie nicht zwangsläufig als zusätzlicher (oder ggf. sogar störender) Aufwand empfunden werden und das Thema Informationssicherheit ein integraler Bestandteil der Arbeitsabläufe wird.
- Die Sicherheitsanforderungen des Unternehmens und Ergebnisse aus Risikobetrachtungen (siehe Kapitel *3.6 Risk Management*) stellen eine weitere Basis für die Wahl und Definition von IS-Zielen dar.
- Bei der Planung der IS-Ziele sollte festgelegt werden, wie diese Ziele zu erreichen sind. Dies beinhaltet auch die Definition der Voraussetzungen für die Realisierung. Neben den wesentlichen Tätigkeiten zur Erreichung der Ziele sind die notwendigen Ressourcen und Verantwortlichkeiten sowie ein Zeitrahmen und ein Vorgehen zur Evaluierung der Realisierung festzulegen. In der Praxis erfolgt dies oft durch eine direkte Referenz auf geplante und laufende Projekte. Entscheidend ist, dass nicht funktionale Anforderungen – und Sicherheitsanforderungen sind in der Vielzahl der Fälle nicht funktional – von Beginn an berücksichtigt und sowohl in die Planung von Projekten, Produkten und Systemen als auch in die Weiterbildung der Mitarbeiter (»Awareness-Training«) integriert werden.
- Bei der Formulierung von IS-Zielen ist darauf zu achten, dass ausschließlich echte und langfristig orientierte Ziele/Zielvorgaben beschrieben werden und keine für die Zielerreichung notwendigen operativen technischen/organisatorischen Maßnahmen.
- Wie bei jeder Zielformulierung empfiehlt es sich, auch bei der Festlegung von IS-Zielen »smarte«[3] Ziele zu formulieren und diese mit den jeweils betroffenen Verantwortungsebenen abzustimmen.
- Der Erreichungsgrad der Informationssicherheitsziele soll messbar sein. Die Messung kann idealerweise durch im Vorfeld definierte KPIs erfolgen. Praktische Unterstützung bei dieser Aufgabenstellung liefern beispielsweise der ISACA-Praxisleitfaden »Bewertung der Leistung eines ISMS durch Schlüsselindikatoren« oder COBIT 2019 Focus Area: Information Security.
- Die Formulierung sinnvoll messbarer Ziele und die Umsetzung der dafür erforderlichen Messungen sind in der Praxis ein durchaus herausforderndes Unterfangen. Es empfiehlt sich daher – vor allem zu Beginn einer ISMS-Implementierung –, zunächst wenige, für die jeweilige Organisation jedoch sinnvolle und im Verhältnis von Umsetzungsaufwand und Nutzen ausgewogene IS-Ziele zu definieren.
- Die Messbarkeit von IS-Zielen wird von der Norm »nur« bei Vorliegen einer entsprechenden praktischen Durchführbarkeit gefordert. In der Praxis wird »if practicable« in der Regel »weicher« als »if possible« verstanden. Das heißt nicht, dass Messungen keine normative Anforderung sind, sondern dass die Praktikabilität zur Durchführung von Messungen in die Ausgestaltung immer miteinbezogen werden muss (siehe Abschnitt 6.2 b).

3 SMART: spezifisch, messbar, akzeptiert, realistisch, terminiert.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Eine Dokumentation der IS-Ziele muss vorgehalten werden.

Darüber hinaus haben sich in der Praxis folgende Punkte als zielführend etabliert:

- Die IS-Ziele sind üblicherweise Teil der IS-Leitlinie und können auch als Teil der IS-Strategie formuliert werden.
- Ein Umsetzungsplan, der beschreibt, wie die IS-Ziele durch konkrete Projekte erreicht werden sollen.
- Der Umsetzungsgrad der IS-Ziele wird durch Kennzahlen ausgewiesen (vgl. Kapitel *3.7 Performance/Risk/Compliance Monitoring*).

Referenzen

ISO/IEC 27001:2022 – Abschnitt 6.2 COBIT 2019 Focus Area: Information Security

ISACA Chapter Germany e.V., Praxisleitfaden »Bewertung der Leistung eines ISMS durch Schlüsselindikatoren«

3.4 IS Policy

Das für die Organisation verantwortliche (Top-)Management muss eine Informationssicherheitsleitlinie (engl.: IS Policy; im Deutschen oft auch »Politik«) vorgeben, die die strategische Entscheidung der Organisation zur Einführung eines ISMS dokumentiert und hierbei insbesondere eine Verpflichtung zur Einhaltung der Anforderungen in Bezug auf die Informationssicherheit sowie die Selbstverpflichtung zur laufenden Verbesserung des ISMS beinhaltet.

Die Leitlinie muss für den Zweck der Organisation geeignet sein und die angestrebten Grundsätze und Ziele des ISMS sowie allgemein die Informationssicherheitsziele der Organisation umfassen.

Erfolgsfaktoren aus der Praxis

Die Leitlinie stellt ein wichtiges Werkzeug für die Organisation dar, über das das verantwortliche Management die Bedeutung sowohl eines effektiven ISMS als auch der Einhaltung der ISMS-Anforderungen kommunizieren kann. Zudem sind in der Leitlinie die wesentlichen strategischen und taktischen Ziele verankert, die mithilfe des ISMS erreicht werden sollen. Idealerweise werden auch die Auswirkungen und Anforderungen, die sich für das jeweilige Personal und die jeweiligen Geschäftsbereiche innerhalb des Geltungsbereichs ergeben, dargestellt.

Im Weiteren sollte das verantwortliche Management in der Leitlinie das etablierte ISMS samt seinen Rollen und Verantwortlichkeiten in ausreichender Kürze beschreiben. Dabei sind die nachfolgenden Aspekte zu beachten:

- Die IS-Leitlinie muss von der höchsten Leitungsebene (Topmanagement) verabschiedet sein und den zuständigen Aufsichtsgremien zur Verfügung gestellt werden.
- Die IS-Leitlinie muss als dokumentierte Information verfügbar sein und einer nachvollziehbaren Dokumentenlenkung unterliegen.
- Die IS-Leitlinie kann einen Verweis auf die Unternehmensziele und andere relevante fachspezifische Ziele wie die IT-Ziele beinhalten.
- Die Sprache der IS-Leitlinie muss den Gepflogenheiten des Unternehmens entsprechen und den Stellenwert des Dokuments bestmöglich herausstellen.
- Im Rahmen der Mitarbeitersensibilisierung ist sicherzustellen, dass alle betroffenen Mitarbeiter innerhalb des Geltungsbereichs die IS-Leitlinie kennen. Sie muss den betroffenen Mitarbeitern kommuniziert werden und bei Bedarf auch den Stakeholdern zur Verfügung stehen (vgl. Kapitel *3.10 Competence*).
- Zur praktischen Erreichung der Ziele ist es wichtig, dass die einzelnen Mitarbeiter sich ihrer individuellen Verantwortung und persönlichen Beteiligung in Prozessen im Kontext der Informationssicherheit bewusst sind und die damit verbundenen konkreten Vorgaben kennen (die sich aus der IS-Leitlinie ableiten und z. B. in themenspezifischen Richtlinien und Arbeitsanweisungen widerspiegeln).
- Die IS-Leitlinie sollte nicht mit weiter gehenden Dokumentationen und Umsetzungsvorgaben vermischt werden wie beispielsweise den Inhalten von Sicherheitskonzepten oder Handbüchern. Sehr wohl darf aber in solch »nachgelagerten« Dokumenten auf die Leitlinie (oder andere relevante High-Level-Dokumente des ISMS) verwiesen werden, um so eine Durchgängigkeit der »Vorgabenkette« zu erreichen.
- Je nach gewähltem Ansatz des ISMS und der vorhandenen Struktur und Arbeitsorganisation innerhalb einer Organisation kann es sinnvoll sein, die IS-Leitlinie als ein »mächtiges«, d. h. umfassendes Gesamtdokument zum Thema Informationssicherheit auszugestalten oder ggf. als einen spezifischen »Anker« oder »Startpunkt« für das Thema zu platzieren, der wiederum von weiteren Detaildokumenten vervollständigt wird. Wichtig ist in beiden Fällen, einen den Zielen der IS-Strategie angemessenen Wortlaut und Umfang zu verwenden.
- Bei Aufteilung der ISMS-Dokumentation in ein Hauptdokument und weitere Detaildokumente kann eine Auf-

teilung der Verantwortlichkeit zugunsten eines flexiblen Änderungsmanagements nützlich sein. So wird die IS-Leitlinie vom Topmanagement verantwortet, die Detaildokumente können z. B. vom Informationssicherheitsbeauftragten oder von den zuständigen Fachbereichen verantwortet werden.

- Obwohl bei entsprechender Suche auf eine Vielzahl von Vorlagen und Textbausteinen zurückgegriffen werden kann, empfiehlt es sich, die IS-Leitlinie als neues/eigenes Dokument zu erstellen, das die individuellen Anforderungen der Organisation bestmöglich abdeckt. Vorlagen können Ideen und Anregungen für die Strukturierung und die möglichen Inhalte liefern. Entscheidend für den Umsetzungserfolg und die Identifikation der Mitarbeiter mit dem Thema Informationssicherheit ist jedoch, dass sich die Leitlinie sichtbar an den Unternehmens- und untergeordneten fachspezifischen Zielen orientiert und die Kernaussagen beim Leser einen Bezug zur betroffenen Organisation erkennen lassen.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Informationssicherheitsleitlinie (siehe Abschnitt 5.2 e)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Themenspezifische Informationssicherheitsrichtlinien (siehe Annex 5.1)
- Begleitende Dokumente und Organigramme, beispielsweise zur Verdeutlichung der Aufbauorganisation im Kontext Informationssicherheit (sofern nicht in der Leitlinie enthalten)

Referenzen

ISO/IEC 27001:2022 – Abschnitt 5.2

3.5 Roles, Responsibilities and Competencies

Gemäß Abschnitt 5.3 der Norm ISO/IEC 27001:2022 muss die Organisation die für ein effektives ISMS benötigten Rollen sowie deren Verantwortlichkeiten für den Aufbau, die Aufrechterhaltung und kontinuierliche Verbesserung des ISMS definieren. Hierbei sind insbesondere auch die erforderlichen Ressourcen zu ermitteln und bereitzustellen (siehe ISO/IEC 27001:2022, Abschnitt 7.1).

In diesem Kontext sind vom Management auch die Zuständigkeiten und Befugnisse für Aufgaben, die für die Informationssicherheit relevant sind, zuzuweisen und zu kommunizieren. Hierbei sollte darauf geachtet werden, dass die Verantwortlichkeiten der Rollen klar geregelt und definiert sind und eventuelle Interessenkonflikte vermieden werden (z. B. mithilfe einer RACI[4]- oder SoD[5]-Matrix).

Erfolgsfaktoren aus der Praxis

Konkretisierung der Rollen innerhalb der ISMS-Organisation

Es sollte mindestens die Rolle eines Informationssicherheitsbeauftragten (ISB) bzw. Chief Information Security Officer (CISO) etabliert werden, wenngleich sich die in der Norm beschriebene Anforderung auf alle Zuständigkeiten und Befugnisse bezieht, die für die Informationssicherheit relevant sind (vgl. Abschnitt 7.2 a). Weiterhin sind innerhalb des ISMS die Rollen des Risikoeigentümers (engl.: risk owner) und des Vermögenswerteigentümer (engl.: asset owner) zu definieren und zu etablieren.[6]

Im Kontext der Informationssicherheit sind selbstverständlich weitere Rollen wie Sicherheitsadministratoren, interne Auditoren etc. zu definieren und zu beschreiben.

- Die Rollenbeschreibung des CISO/ISB muss auch die notwendigen Kompetenzen (Erfahrung, Ausbildung, Schulungen, Sozialkompetenz etc.) umfassen, die zur Ausübung der Rolle benötigt werden. Dazu empfiehlt es sich, eine Stellenbeschreibung oder ein Benennungsschreiben mit der Listung der zugewiesenen Aufgaben heranzuziehen.
- Interessenkonflikte, die in der Praxis auf jeden Fall vermieden werden sollten:
  - Informationssicherheitsbeauftragter (ISB bzw. CISO[7]) und IT-Leiter/CIO[8]
  - Datenschutzbeauftragter (DSB) und IT-Leiter/CIO
  - Interner ISMS-Auditor und IT-Administrator
- Die beiden Rollen ISB/CISO und DSB können unter bestimmten Voraussetzungen in der Praxis auch in Personalunion von einem Mitarbeiter ausgeübt werden. Diese Kombination geht allerdings auch mit gewissen (unvermeidbaren) Konfliktpotenzialen einher. Der DSB ist beispielsweise hinsichtlich seines Handelns gesetzlich geschützt und unterliegt der Schweigepflicht. Diesen Schutz bzw. diese Pflicht kann er aber nicht automatisch auf die Rolle des CISO übertragen. Es gibt auch eine juristische Diskussion hinsichtlich der Garantenpflicht des CISO bzw. des Compliance-Officers etc. Diese gilt für den DSB nicht. Eine Personalunion dieser Aufgaben kann daher im schlechtesten Fall in einen substanziellen Interessen-

4 RACI: Responsible (Umsetzungsverantwortung), Accountable (Gesamtverantwortung), Consulted (fachliche Expertise), to be Informed (Informationsrecht), siehe auch Glossar.

5 SoD: Segregation of Duties, Funktionstrennung, siehe auch Glossar.

6 Siehe Abschnitt 6.1.2 c und Control A.5.9 »Ownership of assets«.

7 CISO: Chief Information Security Officer.

8 CIO: Chief Information Officer.

konflikt münden und sollte deshalb ausführlich analysiert und abgewogen werden.

- Je nach Größe und Geschäftsaktivitäten der Organisation sowie des konkret gewählten Geltungsbereichs des ISMS können sich aus der Kombination der Rollen DSB und CISO auch Synergien ergeben, die bei einer Trennung der Rollen nicht gegeben wären (z. B. bzgl. Informationsfluss, Überblick und Ausgestaltung der Maßnahmen). Allerdings muss zum einen immer sorgfältig geprüft werden, ob beim infrage kommenden Kandidaten die fachlichen und persönlichen Kompetenzen im erforderlichen Maß vorhanden sind und das vorliegende Arbeitspensum in den beiden Themengebieten auch tatsächlich erfüllt werden kann. Zum anderen muss wie bereits dargelegt genau geprüft werden, ob die möglicherweise auftretenden Interessenkonflikte »beherrschbar« sind und zu keinen gravierenden Nachteilen der Arbeitserfüllung (einer) der beiden Funktionen führen würden.
- Ein weiteres Beispiel möglicher Interessenkonflikte zwischen DSB und CISO betrifft die Sammlung und Auswertung von Verkehrs- und Protokolldaten. Während der DSB in der Regel das Sammeln und Auswerten von personenbezogenen bzw. -beziehbaren Daten nur unter ganz gewissen Bedingungen und zweckgebunden zulassen wird, möchte der CISO technische Maßnahmen zur Erhöhung des Sicherheitsniveaus (präventiver Schutz) und zur Erkennung und Auswertung potenzieller Schadensereignisse (detektiver Schutz) gerne bestmöglich ausnutzen.

Die Organisation muss sicherstellen, dass alle Personen durch angemessene Ausbildung, Schulung oder Erfahrung über die erforderlichen Kompetenzen (Competencies) verfügen. Der Nachweis über die Kompetenzerreichung muss von der Organisation erbracht werden können, z. B. über entsprechende Weiterbildungszertifikate in der Personalakte (Bildungshistorie) des jeweiligen Mitarbeiters (vgl. Abschnitt 7.2 d).

- ISO/IEC 27001:2022 gibt einen groben Rahmen für die Sicherheitsorganisation von Unternehmen vor (z. B. Topmanagement, Risikoeigentümer, Auditor), beschreibt aber nicht im Detail, wie Rollen und Zuständigkeiten in der Praxis verteilt sein sollen.
- Es hat sich als vorteilhaft erwiesen, für die Besetzung der benötigten Rollen innerhalb des ISMS genau die Mitarbeiter auszuwählen, die bereits »von Haus aus« eine Affinität zum Thema Informationssicherheit mitbringen bzw. über ausreichend intrinsische Motivation verfügen. Neben Fachkenntnissen sind insbesondere für den CISO/ISB Sozialkompetenz, zielführendes Kommunikationsverhalten, integres Auftreten, sachliche Überzeugungsfähigkeit und erfolgreiches Konfliktmanagement erforderlich. Viele der Aufgaben, die sich im Zusammenhang mit der Umsetzung der Informationssicherheitsstrategie und (manchmal auch unangenehmer oder unbeliebter) zugehöriger Maßnahmen ergeben, lassen sich sonst nicht zufriedenstellend lösen.
- Zu den wichtigsten Eigenschaften eines CISO/ISB gehört darüber hinaus die Fähigkeit, zwischen Unternehmenszielen und Compliance-Anforderungen einerseits und Informationssicherheitsrisiken und -maßnahmen andererseits »übersetzen« zu können.
- Die Rolle des CISO/ISB erfordert Führungskompetenzen und sollte im Unternehmen dem Status von Führungskräften gleichgestellt sein.
- Beispiele für die organisatorischen Strukturen hinsichtlich Informationssicherheit finden sich u. a. in » COBIT 2019 Focus Area: Information Security« und dem BSI-Standard 200-2 – IT-Grundschutz-Methodik. Hierin sind u. a. die Rollen und Verantwortlichkeiten des CISO, des Steuerungskomitees, des Informationssicherheitsmanagers, die Rollen im Risikomanagementprozess sowie der fachlichen Dateneigentümer beschrieben.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Nachweis der Kompetenz (Abschnitt 7.2 d)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Rollenbeschreibungen, inklusive des erforderlichen Reportings an das Topmanagement (siehe Abschnitt 5.3 b)
- Stellenprofile/Benennungsschreiben
- Ausgestaltung der strategischen und operativen Zusammenarbeit zwischen DSB, QMB und CISO

Referenzen

ISO/IEC 27001:2022 – Abschnitte 5.3, 7.1 und 7.2

COBIT 2019 Focus Area: Information Security

BSI-Standard 200-2 – IT-Grundschutz-Methodik

3.6 Risk Management[9]

Ein IS-Risiko beschreibt die Möglichkeit, dass eine bestimmte Bedrohung Schwachstellen eines Informationssystems, eines Anwendungssystems oder (von Teilen) der IT-Infrastruktur ausnutzt, was eine Verletzung der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit) darstellt und damit zu negativen Auswirkungen u. a. auf die Geschäftstä-

9 Dieses Kapitel bezieht sich ausschließlich auf das Risikomanagement im Kontext der Informationssicherheit.

tigkeit, finanzielle Zielgrößen, den Ruf oder die Reputation einer Organisation führt.

Das IS-Risiko kann grundsätzlich aus verschiedenen Quellen entstehen, wie zum Beispiel aus Fehlern bei der Konfiguration oder Wartung von Systemen, menschlichem Versagen, Cyberangriffen, Naturkatastrophen oder anderen unvorhersehbaren Ereignissen.

IS-Risikomanagement ist ein wichtiger Aspekt der Unternehmensführung im Allgemeinen und des IS-Managements im Speziellen. IS-Risikomanagement ist ein übergreifender Prozess innerhalb eines Managementsystems, der im Fall eines ISMS zur systematischen Erfassung, Bewertung und transparenten Darstellung von Risiken im Kontext der Informationssicherheit beiträgt und die Gewährleistung eines *akzeptablen* bzw. eine nachhaltige Verbesserung des bestehenden *Sicherheitsniveaus* im Geltungsbereich des ISMS sicherstellen soll.

Ziel ist es, die identifizierten Risiken zu reduzieren und einen nicht tolerierbaren Schaden gegenüber der betrachteten Organisation abzuwenden bzw. so weit zu reduzieren, dass ein für das Unternehmen akzeptables Maß erreicht wird. Was als *akzeptabel* angesehen wird, müssen die jeweiligen Verantwortungsträger im jeweiligen Kontext, manchmal auch in der jeweiligen Situation, entscheiden. Hinzu kommt die Entscheidung darüber, wie mit den identifizierten und bewerteten Risiken umzugehen ist.

Zusammenfassend: Ein nicht tolerierbarer Schaden gegenüber der betrachteten Organisation ist abzuwenden bzw. so weit zu reduzieren, dass ein für das Unternehmen akzeptables Maß erreicht wird.

Die konkreten Ziele des Risikomanagements im Kontext der Informationssicherheit sind:

- Frühzeitiges Erkennen und Beheben von Informationssicherheitsrisiken
- Etablierung einheitlicher Bewertungsmethoden für identifizierte Risiken
- Eindeutige Zuweisung von Verantwortlichkeiten beim Umgang mit Risiken
- Standardisierte und übersichtliche Dokumentation von Risiken, inklusive deren Bewertungen
- Effiziente Behandlung von Risiken[10]

Grundlagen des IT-Risikomanagements und Vorgehen

Wie entstehen Risiken?

Risiken im Kontext der Informationssicherheit ergeben sich u.a. inhärent aus dem Einsatz von IT-Systemen und (aufkommenden) Technologien. Da Informationssicherheit nach ISO/IEC 27001 immer ganzheitlich zu betrachten ist, gibt es weitere Risikoquellen, die auf die Informationen/Daten einer Organisation einwirken (können) und beispielsweise durch folgende Einflussfaktoren entstehen:

- Datenaustausch innerhalb und außerhalb der Organisation
- Anpassung der internen Organisation und Zusammenarbeit (insbesondere bei größeren Unternehmen)
- (Bestands-)Systeme und Anwendungen, die nicht aktualisiert oder abgelöst werden können
- Zusammenarbeit mit externen Partnern/Dienstleistern
- Fernzugriffe in das Unternehmensnetzwerk (z.B. von Partnerunternehmen und Herstellern)
- Naturphänomene/Naturkatastrophen
- Sabotage und Wirtschaftskriminalität
- »Risikofaktor« Mensch (z.B. Social Engineering)
- Einsatz neuartiger Systeme und Technologien (z.B. Cloud und mobile Geräte)
- Eintritt in neue Märkte (geografisch und produktbezogen)

Obwohl grundsätzlich alle Quellen und Einflussfaktoren betrachtet werden müssen, muss jede Organisation auf Basis ihrer jeweiligen Geschäftstätigkeit und der sich daraus ergebenden internen und externen Anforderungen individuelle Schwerpunkte im Risikomanagement festlegen.

- Effizientes Risikomanagement kann nur dann erfolgen, wenn zunächst die Risikoexposition und das Umfeld der jeweiligen Geschäftstätigkeit analysiert werden. Um zu wissen, an welchen Stellen nach Risiken »gesucht« werden muss, muss man wissen, welche Risikofelder insgesamt vorhanden sind und diese einschätzen. Ein guter Ausgangspunkt dafür ist beispielsweise eine Prozesslandkarte oder eine Umfeldanalyse (vgl. Kapitel *3.1 Context of the Organization*).
- Zur Unterstützung der Formulierung und Ausgestaltung des Risikobeurteilungsprozesses kann z.B. die ISO/IEC 27005 herangezogen werden. Neben dem gut ausgearbeiteten Hauptteil beinhalten insbesondere auch die Anlagen wertvolle Hinweise zur Umsetzung.

10 Beispielsweise durch Anpassung der Sicherheitsstrategie oder Umsetzung angemessener Sicherheitsmaßnahmen.

Entdeckung und Bewertung von Risiken

Bevor mit der konkreten Identifizierung und Behandlung von Risiken begonnen wird, müssen in Abstimmung mit der obersten Leitungsebene (Topmanagement) sowohl der generisch formulierte Risikobeurteilungsprozess als auch die unternehmens- bzw. ISMS-weit gültigen Risikoakzeptanzkriterien festgelegt werden (sofern diese nicht bereits aus einem übergeordneten Risikomanagement übernommen werden können bzw. müssen).[11]

Der Risikobeurteilungsprozess beinhaltet u. a. Folgendes:

- Methoden zur Risikoidentifikation
- Kriterien zur Beurteilung von Risiken
- Risikoakzeptanzkriterien

Methoden zur Risikoidentifikation anwenden

Die Identifikation relevanter Risiken erfordert in der Regel, dass die Sichtweisen mehrerer Stakeholder bzw. Abteilungen berücksichtigt und zusammengebracht werden müssen. Als Werkzeuge können verschiedene Techniken und Methoden zum Einsatz kommen, wie beispielsweise:[12]

- Interviews
- Szenarioanalysen/Was-wäre-wenn-Analysen
- Brainstorming
- Business-Impact-Analysen (BIA)
- Checklisten
- Delphi-Methode
- STRIDE Threat Model (Microsoft)

Beispiel

Bei der Risikoanalyse einer neuen E-Commerce-Webanwendung bringen die beteiligten Personen unterschiedliche Risikogesichtspunkte zur Diskussion. Der Softwareentwickler sieht bei der gewählten Programmiersprache einige Schwachstellen, die beispielsweise durch (automatische) Codereviews abgefangen werden können. Der IT-Administrator äußert seine Bedenken bei der geplanten Wartung der Anwendung durch externe Dienstleister und den dafür benötigten Zugriffsrechten in das Unternehmensnetzwerk. Der Datenschutzbeauftragte wirft die Frage nach dem angemessenen Schutz personenbezogener Daten auf und verlangt eine Auflistung der technisch-organisatorischen Maßnahmen zur Erfüllung der Anforderungen nach Art. 32, Abs. 1 EU-DSGVO. Der Informationssicherheitsbeauftragte wiederum erkennt die Reichweite des Projekts (Auswirkung bei Verfügbarkeitseinschränkungen oder Datenabfluss) und fordert daher einen Penetrationstest vor der Produktivsetzung.

- Dieses Beispiel ist keinem Lehrbuch entnommen. Es zeigt aber, dass eine Risikoanalyse auch mit der direkten Formulierung von (Gegen-)Maßnahmen einhergehen kann.
- Bei einer hohen Dynamik des Risikomanagementprozesses kann die direkte Formulierung von (Gegen-)Maßnahmen zur zeitnahen Einleitung der Risikobewältigung genutzt werden. Wird der Risikomanagementprozess hingegen mit einer niedrigen Dynamik umgesetzt, kann dies auch bewusst vermieden werden, um zunächst die Analyse vollständig/umfassend abzuschließen und dann »in Ruhe« weitere Aktivitäten zu definieren.
- Bei einem »kompakt« bzw. »dynamisch« ausgestalteten Risikomanagementprozess, der zügig zur Diskussion und Auswahl der Behandlungsoptionen kommt, besteht die Gefahr, dass der Prozess insgesamt eher reaktiv und maßnahmenzentriert arbeitet und die Analyse der Risiken dadurch ggf. zu kurz kommt.
- Je nach Größe und Umfang einer Organisation bzw. eines konkreten Projekts ist daher der jeweils am besten geeignete Ansatz zu wählen!

Kriterien zur Beurteilung von Risiken definieren

Die Kriterien zur Beurteilung von Risiken sind so auszuformulieren, dass sie für eine möglichst große Variation von Risikotypen bzw. Risikokategorien genutzt werden können. Ob ein Punktemodell oder ein Katalog an qualitativen Parametern herangezogen wird, ist der konkreten Ausgestaltung des Risikomanagementprozesses überlassen.

- Aus Praxissicht empfiehlt es sich, zusätzlich zu klassischen Kriterien (wie z. B. Schutzbedarf für Vertraulichkeit/Integrität/Verfügbarkeit, unterstützte Geschäftsprozesse, Anzahl Benutzer) eine Zusammenstellung an Fragen, die auf die Geschäftstätigkeit der Organisation abgestimmt sind, bereitzustellen, die individuell je Anwendungsfall ergänzt werden kann.
- Die Beurteilung der Eintrittswahrscheinlichkeit (siehe Schritt 2 »Risikoanalyse« weiter unten) ist in der Praxis durchaus herausfordernd. Hier gilt es, dass neben dem »Blick zurück« (Erfahrungswerte, vergleichbare Ereignisse in anderen Organisationen, Kennzahlen, Statistiken etc.) unbedingt auch der »Blick nach vorne« gerichtet wird, um bisher »unbekannte« Erkenntnisse und Entwicklungen, die sich aber ggf. bereits am Horizont abzeichnen, mit berücksichtigen zu können (z. B. das Aufkommen

11 In der ISO 31000:2018 sind diese Aktivitäten in Abschnitt 6 »Process« beschrieben.

12 Siehe auch IEC 31010:2019.

neuer Technologien oder geänderte Gefährdungssituationen)[13]. Oder anders formuliert: »Beim Risikomanagement hängt der Erfolg von den Vorbereitungen ab.«[14]

Risikoakzeptanzkriterien festlegen

Die Festlegung von Risikoakzeptanzkriterien ist eine zentrale Aufgabe im Risikomanagementprozess, denn nur dadurch ergibt sich der volle Nutzen für die Organisation, nicht alle identifizierten und bewerteten Risiken »gleich« kosten- und ressourcenintensiv behandeln zu müssen.

- Risikoakzeptanzkriterien können in Form von Akzeptanzstufen in Abhängigkeit des qualitativen und/oder quantitativen Schadenspotenzials festgelegt werden (z. B. Non-Compliance, finanzieller Schaden, Reputationsschaden, Beeinträchtigung der Aufgabenerfüllung).
- Risikoakzeptanzkriterien können mehrere Schwellwerte umfassen. Jede Schwellwertstufe kann an eine bestimmte Hierarchie-/Managementebene gebunden werden, sodass eine Akzeptanz von Risiken oberhalb einer bestimmten Stufe auch ausschließlich durch die benannten Führungskräfte innerhalb dieser Stufe erfolgt.
- Zur besseren Vergleichbarkeit können qualitative Schadenstufen in quantitative (finanzielle) Beträge umgerechnet werden. Dies ist allerdings in der Regel nur näherungsweise möglich.
- Es kann – insbesondere bei kleinen und mittelständischen Unternehmen – sinnvoll sein, den Risikobeurteilungsprozess mit einem simplifizierten Modell zu beginnen und ihn dann iterativ weiterzuentwickeln. Beispielsweise können in einem ersten Schritt Risiken auch ohne ein vollständig ausgearbeitetes Modell zusammen mit den Fachexperten der IT-Abteilung(en) und Fachabteilung(en) gesammelt und initial beurteilt werden. Die Risikoakzeptanzkriterien können dann nach und nach aus den Ergebnissen abgeleitet und zu einem späteren Zeitpunkt – nach Abnahme durch die Unternehmensleitung – in formale Kriterien überführt werden.
- Bei der Festlegung von Risikoakzeptanzkriterien ist mit Um- und Weitsicht vorzugehen, um einerseits den Risikoappetit[15] des Unternehmens angemessen abzubilden (weder zu hoch noch zu gering) und gleichzeitig die Effizienz und Effektivität des ISMS zu gewährleisten, indem Risiken »flächendeckend« identifiziert und entsprechend ihrer Bewertung und z. B. gemäß rechtlichen oder regulatorischen Vorgaben konsequent behandelt werden können (nicht jedes Risiko kann mit erster Priorität behandelt werden).
- Ein tatsächlich flächendeckend ausgebautes Risikomanagement, das zu jedem Zeitpunkt alle Risiken im Kontext der Informationssicherheit in allen Unternehmensbereichen und Prozessen detailliert ausfindig macht und analysiert, stellt in der Praxis eine hohe Anforderung dar.

Orientierung an einem etablierten Risikomanagementprozess

Nach Festlegung der Risikobeurteilung folgen die jeweils iterativ durchzuführenden Schritte des Risikomanagementprozesses. Sich an einem etablierten Prozess zu orientieren, dient der Transparenz und Nachvollziehbarkeit und macht die Ergebnisse des gesamten Prozesses verlässlicher. In ISO 31000 stehen die folgenden Schritte im Mittelpunkt (siehe Abbildung 3):

1. Risikoidentifikation
2. Risikoanalyse
3. Risikoevaluierung/-bewertung
4. Risikobehandlung

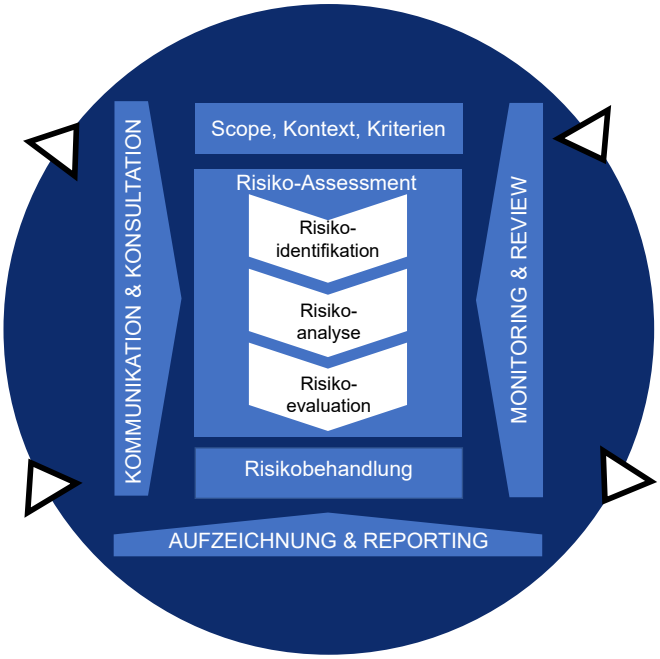


Abbildung 3: Risikomanagementprozess nach ISO 31000[16]

Schritt 1: Risikoidentifikation

Die Risikoidentifikation erfolgt immer anhand von Informationen im Geltungsbereich des ISMS (siehe Abschnitt 6.1.2 c).

13 Beispielsweise durch APTs oder Zero-Day-Schwachstellen.

14 Angelehnt an Konfuzius, chinesischer Philosoph, *551 v. Chr. †479 v. Chr.

15 Je größer der Risikoappetit ist, desto mehr Handlungsspielraum und Chancen sind in der Regel vorhanden.

16 Siehe ISO 31000:2018.

Die Identifizierung konkreter Risiken kann sich beispielsweise aus folgenden Szenarien ableiten:

- Risikoanalysen
  - Für geschäftskritische Prozesse, Anwendungen und Systeme werden explizite Risikoanalysen und -bewertungen durchgeführt, mit deren Hilfe eindeutige Aussagen zur Risikosituation und Risikoexposition der betroffenen Prozesse bzw. der betroffenen Anwendungen/Systeme gemacht werden können.
  - Innerhalb des Projektmanagements sollten Risikoanalysen (mit jeweils angepasstem Umfang) als ein Pflichtelement aufgenommen werden.
- Audits
  - Durchgeführte Audits zeigen, dass Sicherheitsstandards und bekannte Best Practices durch die verantwortlichen Stellen oder in Systemen nicht bzw. nicht ausreichend erfüllt werden.
  - Voraussetzung dafür ist selbstverständlich, dass Audits auch durchgeführt werden (vgl. Kapitel *3.12 Internal Audit*) und der Auditprozess eine eindeutige Vorgehensweise zur Behandlung von Auditfeststellungen beinhaltet (Dokumentation der Feststellungen, Übergabe der Feststellungen an die auditierte Stelle etc.).
- Operativer Betrieb
  - Durch Erkenntnisse im Rahmen des »normalen« operativen Betriebs können neue, bisher unbekannte Risiken zutage treten, die bei entsprechender Einschätzung durch das Fachteam bzw. den Mitarbeiter (zeitnah) an das Risikomanagement berichtet werden sollten/müssen – je nach gewähltem Risikomanagementprozess.
- Sicherheitsvorfälle
  - Durch Sicherheitsvorfälle (wie auch immer die Definition für »Sicherheitsvorfall« aussieht) können zum einen bisher unbekannte Risiken identifiziert werden, die durch den Vorfall sichtbar werden. Zum anderen können bereits bekannte, aber nicht ausreichend behandelte oder bisher akzeptierte Risiken tatsächlich eintreten (beispielsweise durch aktive Ausnutzung einer bereits bekannten Schwachstelle durch einen Angreifer oder durch Ausfall eines Systems aufgrund unzureichender technischer Dimensionierung).

Schritt 2: Risikoanalyse

Bei der Analyse identifizierter Risiken sollten sowohl die Wahrscheinlichkeit als auch die möglichen Folgen/Konsequenzen bei Eintritt der Risiken klar herausgearbeitet und den Entscheidungsträgern verständlich dargestellt werden.

- Bei der sprachlichen Formulierung der Konsequenzen sollte darauf geachtet werden, die Folgen für die Geschäftsprozesse und die Geschäftstätigkeit anstatt technischer Details in den Vordergrund zu stellen.
- Zur Risikoanalyse können standardisierte Bewertungsmatrizen verwendet werden, wobei es je nach Organisation und Anwendungsfall sinnvoll sein kann, Matrizen mit gerader Anzahl an Spalten zu nutzen (z.B. 4x4). Bei Verwendung von Matrizen mit ungerader Spalten-/Zeilenanzahl (z.B. 3x3 oder 5x5) besteht grundsätzlich das Risiko, dass die Entscheidung häufig auf »die Mitte« fällt.

Schritt 3: Risikoevaluierung/-bewertung

Die (finale) Entscheidung über die Behandlung identifizierter Risiken sollte beim Risikoeigentümer des jeweiligen Risikos liegen, da er die Auswirkungen des Risikoeintritts bewerten kann und final die Verantwortung für den/die vom Risiko betroffenen Geschäftsprozesse trägt. In der Regel entscheidet der Risikoeigentümer auch über die Bereitstellung von Ressourcen (z.B. finanzielle Mittel).

- An dieser Stelle wird deutlich, wie wichtig die Identifikation und Festlegung des Risikoeigentümers für den Gesamtprozess des Risikomanagements ist.
- In der Praxis sollte die Rolle des Risikoeigentümers von den entsprechend benannten Verantwortungsträgern bzw. Managern des Unternehmens ausgefüllt werden (z.B. Vorstand, Geschäftsführer, Geschäftsleiter, Bereichsleiter, Abteilungsleiter oder Gruppenleiter). Bei Projekten füllt in der Regel der Projektleiter die Rolle des Risikoeigentümers aus, zumindest für projektspezifische Risiken.

Schritt 4: Risikobehandlung

Die Behandlung von Risiken erfolgt nach dem Risikoappetit der jeweiligen Organisation. Als Ausgangspunkt für die Modellierung der Risikobehandlungsoptionen eignen sich im Kontext der Informationssicherheit insbesondere die Modelle der ISO/IEC 27005[17] (siehe Abbildung 4).

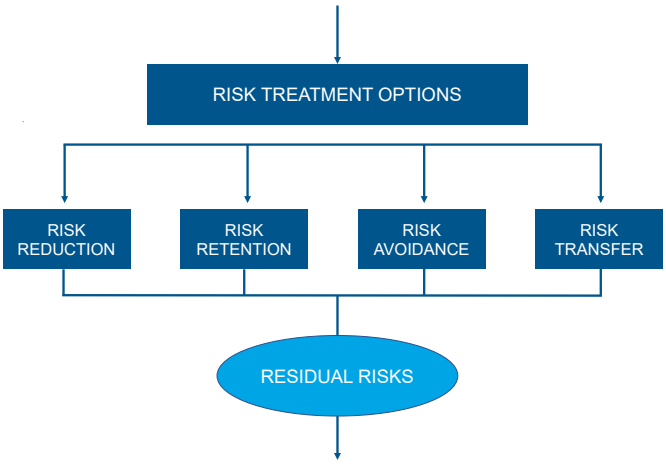


Abbildung 4: Risikobehandlungsoptionen nach ISO/IEC 27005

17 Siehe u.a. Abschnitt 8 der ISO/IEC 27005:2022 – »Information security risk treatment«.

- Maßnahmen zur Risikobehandlung können grundsätzlich aus allen Quellen entnommen werden, müssen aber mit Anhang A der Norm und dem SoA des ISMS abgestimmt werden.
- Risiken müssen den zugehörigen Risikoeigentümern zugeordnet werden. Ohne dediziert verantwortliche Eigentümer werden sowohl die »korrekte« Bewertung als auch die nachhaltig erfolgreiche Behandlung identifizierter Risiken erschwert.
- Risikoeigentümer ist in der Regel die Stelle, die die wirtschaftlichen Auswirkungen bei Eintritt des Risikos tragen muss. In vielen Fällen ist dies der Prozesseigentümer, kann aber – je nach Auswirkung (engl.: impact) und Risikobewertung – auch im höheren Management liegen.
- Auch wenn Risiken beispielsweise durch IT-Systeme hervorgerufen werden, tragen letztlich die jeweils betroffenen Geschäftsbereiche die Auswirkungen. Das heißt, obwohl die Behandlung von (IT-)Risiken durch die jeweilige[18] IT-Abteilung erfolgen muss (engl.: responsibility), befinden sich die Risikoeigentümerschaft und die Gesamtverantwortung nach wie vor in den betroffenen Fachbereichen, die auch über die Bereitstellung von Mitteln entscheiden müssen (engl.: accountability).
- Die Identifizierung der Risiken und die Identifizierung der zugehörigen Risikoeigentümer können getrennt bzw. zeitlich versetzt voneinander ablaufen.

Dokumentation und Reporting

- Es empfiehlt sich, die Ergebnisse aller Risikobeurteilungen an einer zentralen Stelle vorzuhalten, z. B. in Form eines Risikoregisters. Dies ist zwar keine Normforderung, es hilft aber bei der Auswertung und Verwaltung der bekannten Risiken und ihres Bearbeitungsstatus.

  Je nach Größe der Organisation sind Werkzeuge mit unterschiedlichem Funktionsumfang notwendig (Anzahl Risiken, Anzahl Benutzer, Berechtigungskonzept, Mandantenfähigkeit, Onlineverfügbarkeit, Auswertungsmöglichkeiten etc.).
- Die Norm fordert kein zentrales Risikoregister. Allerdings fordert sie, dass der Prozess der Risikobeurteilung von Informationssicherheitsrisiken zu konsistenten, gültigen und vergleichbaren Ergebnissen führt (siehe Abschnitt 6.1.2 b). Je nach Art und Nutzung der eingesetzten Werkzeuge ist der Aufbau eines Registers daher eine logische Konsequenz.
- Da das Risikoregister in der Regel sensible und (streng) vertrauliche Informationen enthält, sollte ein angepasstes Rechte- und Rollenkonzept für den Datenzugriff erstellt und umgesetzt werden.

Erfolgsfaktoren aus der Praxis

- Sofern im Unternehmen oder in der Unternehmensgruppe bereits ein übergeordnetes Risikomanagement vorhanden ist, sollte das Risikomanagement der IS dort integriert werden (z. B. als Bestandteil des operationellen Risikomanagements) oder zumindest über definierte Schnittstellen verfügen.
- Das Risikomanagement sollte nach Möglichkeit prozessorientiert sein, anstatt die einzelnen Vermögenswerte (Assets) in den Vordergrund zu stellen. Damit wird zum einen gewährleistet, dass Risiken und Gefährdungen (geschäfts-)prozessorientiert formuliert werden und so leichter von den Risikoeigentümern, also in der Regel den Prozesseigentümern, verstanden werden, und zum anderen können so die potenziellen (Schadens-)Auswirkungen (engl.: damaging impacts) sehr zutreffend ermittelt werden.
- Das Vorgehensmodell für die Durchführung von Projekten im Unternehmen sollte so angepasst bzw. erweitert werden, dass eine (je nach Projektart und -umfang unterschiedlich intensive) Risikoanalyse und -bewertung durchgeführt werden muss. Das Projektteam muss die Analyseergebnisse dokumentieren und – je nach Ausgestaltung des Risikomanagements – müssen Risiken, die einen definierten Schwellwert überschreiten, weitergemeldet werden. Eine formale Risikoübernahme des jeweiligen Risikoeigentümers muss bei fehlenden Maßnahmen oder bei Risikoakzeptanz ebenfalls erfolgen und dokumentiert werden.
- Auch bei (umfangreichen) Änderungen an Prozessen, Anwendungen oder Systemen empfiehlt es sich, Risikoanalysen und -bewertungen als verpflichtenden Teil des Change-Managements einzuführen.
- Werden Nichtkonformitäten oder Schwachstellen identifiziert (z. B. durch das Monitoring oder andere operative IT-Prozesse wie Change-, Problem- oder Incident-Management), die innerhalb des Regelbetriebs nicht bzw. nicht fristgerecht behoben werden können, sind diese im Risikomanagement zu bewerten und durch den Risikoeigentümer zu behandeln.
- Bei Risikoanalysen und -bewertungen wird immer das Spezialisten-Know-how des jeweiligen Prozesseigentümers benötigt. Die IS-Beauftragten der Organisation können bei der Durchführung unterstützen und beispielsweise im Rahmen von Interviews oder Workshops die Risiken erfassen und Vorschläge zur Bewertung geben. Eine

18 Dies beinhaltet auch Fachabteilungen und Softwareentwicklungsabteilungen, die ggf. außerhalb der IT angesiedelt sind, eigene IT-Risiken zu verantworten haben und für deren Risikobehandlung verantwortlich sind.

weitere Methode ist der Einsatz von Fragebögen/Self-Assessments. Je nach gewähltem Ansatz können diese Selbsteinschätzungen anschließend von einem »zweiten Augenpaar« zusätzlich bewertet werden. Entscheidend ist, dass es einen formalen und pragmatischen Prozess gibt, der die Fachbereiche und Projektverantwortlichen optimal bei ihrer Arbeit unterstützt und gleichzeitig gewährleistet, dass Risiken frühzeitig erkannt und angemessen behandelt werden.

- Der BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz – liefert Ansatzpunkte, wie mithilfe der im IT-Grundschutz-Kompendium aufgeführten Gefährdungen eine Risikoanalyse für die Informationsverarbeitung durchgeführt werden kann. Die BSI-Methodik verlangt allerdings, dass zunächst die Schritte der IT-Grundschutz-Vorgehensweise durchgeführt worden sind (u. a. Informationsverbund, Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, IT-Grundschutz-Check, ergänzende Sicherheitsanalyse), bevor entschieden werden kann, für welche Zielobjekte eine Risikoanalyse durchgeführt wird und für welche Zielobjekte dies dagegen entbehrlich ist.
- Das schützenswerte Gut bleibt im Kontext eines ISMS immer die Information an sich. Es ist die Aufgabe der jeweiligen Verantwortungsträger (Unternehmensleitung, Management, Prozesseigentümer), dieses Gut hinsichtlich seines »Wertes« für das Unternehmen bzw. den jeweiligen Prozess zu bewerten. Das Informationsgut wird dadurch zum Informationswert. Die Aufgabe der Risikoeigentümer ist es, innerhalb aller Prozessschritte angemessene, wirksame und effiziente Maßnahmen zu etablieren. Die ISMS-Verantwortlichen sind »Wächter« für die Umsetzung der Informationssicherheitsstrategie und u. a. verantwortlich für eine wahrheitsgemäße Berichterstattung hinsichtlich Risikoexposition und Sicherheitsvorfällen.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Risikobeurteilungsprozess (Abschnitt 6.1.2)
- Risikobehandlungsprozess (Abschnitt 6.1.3)
- Aufzeichnungen und Ergebnisse von Risk Assessments bzw. Risikoanalysen (Abschnitt 8.2)
- Aufzeichnungen und Ergebnisse von Risikobehandlungen (Abschnitt 8.3)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Aufzeichnungen und Ergebnisse von Risk Assessments und Risikoanalysen

Referenzen

ISO/IEC 27001:2022 – Abschnitte 6.1, 8.2, 8.3

ISO/IEC 27005:2022

ISO 31000:2018

COBIT 2019 Focus Area: Information Security

BSI-Standards 200-2 und 200-3

3.7 Performance/Risk/Compliance Monitoring

Im Kontext des ISMS wird eine Reihe an Vorgaben definiert, z. B. Informationssicherheitsziele oder Richtlinien und Konzepte zu ihrer Umsetzung in der Praxis. Es wird erwartet, dass kontinuierlich sichergestellt wird, dass diese Vorgaben erfüllt sind, was mittels eines entsprechenden »Monitorings« sicherzustellen ist. »Performance/Risk/Compliance Monitoring« bezieht sich damit auch auf die kontinuierliche Überwachung und Verbesserung des Informationssicherheitsmanagementsystems (ISMS).

- Performance-Monitoring umfasst die Bewertung der Wirksamkeit des ISMS im Hinblick auf die Erreichung der Sicherheitsziele und die Erfüllung der Anforderungen der ISO/IEC 27001.
- Risikomonitoring bezieht sich auf die Bewertung und Überwachung von Sicherheitsrisiken im Unternehmen und im ISMS (siehe auch Kapitel 3.6).
- Das Compliance-Monitoring bezieht sich auf die Überwachung der Einhaltung von rechtlichen Anforderungen und regulatorischen Vorgaben, aber auch von internen Richtlinien und Standards.

Mit der Durchführung von Performance-, Risiko- und Compliance-Monitoring sollen Organisationen sicherstellen, dass ihr ISMS effektiv und effizient arbeitet und die Anforderungen der ISO/IEC 27001 sowie die gesetzlichen und regulatorischen Vorgaben erfüllt werden. Es beinhaltet, dass die ISMS-Prozesse, Verfahren und Kontrollen regelmäßig geprüft werden, um sicherzustellen, dass sie den relevanten Anforderungen entsprechen.

Um Vergleichbarkeit, Kontinuität und Nachvollziehbarkeit herzustellen, sollten alle Ziele, deren Erreichung anhand von Kennzahlen gemessen werden soll, den SMART-Kriterien genügen:

- Spezifisch
- Messbar
- Attraktiv/Akzeptiert
- Realistisch
- Terminiert

Dadurch wird sichergestellt, dass diese Ziele exakt, eindeutig und für jeden verständlich beschrieben werden.

Der Informationssicherheitsbeauftragte ist nun in der Lage, anhand der unterschiedlichen Kennzahlen, z. B. mithilfe einer Dashboard-Ansicht, die Informationssicherheit zu bewerten und zu steuern. Aus der Vielzahl der Kennzahlen konzentrieren wir uns im Hinblick auf die Informationssicherheit auf die folgenden Kennzahlklassen:

Schlüsselindikatoren KxIs (Key-Performance/Risk/Control-Indikatoren)

KPI – Key-Performance-Indikatoren
Ein Key-Performance-Indikator ist ein Wert (Soll-Ist-Vergleich), der anzeigt, wie **erfolgreich** ein Unternehmen die relevanten Maßnahmen sowie die Informationssicherheitsprozesse in Bezug auf die Erreichung der Informationssicherheitsziele umsetzt. Erfolgreich ist eine Maßnahme, wenn das gewünschte Leistungsniveau innerhalb der vorgegebenen Zeit und mit möglichst geringem Aufwand erreicht wird.

KRI – Key-Risk-Indikatoren
Ein Key-Risk-Indikator ist ein Wert (Soll-Ist-Vergleich), der anzeigt, ob Veränderungen im Risikoprofil die gewünschten Toleranzgrenzen potenziell überschreiten und damit die Zielerreichung gefährden. Er ist damit ein Maß dafür, wie **risikoorientiert** ein Unternehmen die relevanten Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Eine Situation, die den Risikoappetit des Unternehmens überschreitet, wird durch gegensteuernde Maßnahmen wieder in den akzeptablen Risikobereich gebracht.

KCI – Key-Control-Indikatoren
Ein Key-Control-Indikator ist ein Wert (Soll-Ist-Vergleich), der anzeigt, wie **effektiv** in Bezug auf die Zielerreichung ein Unternehmen die relevanten Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Effektiv ist eine Maßnahme, wenn die Steuerungsziele zuverlässig innerhalb der gewünschten Toleranzgrenzen erreicht werden.

Um die Effektivität und Effizienz der ISMS-Prozesse und der etablierten Maßnahmen kontinuierlich zu überprüfen, sollten in der Praxis diese Indikatoren verwendet werden (siehe Abbildung 5). Sie geben Auskunft über den Leistungsstand des gesamten ISMS und dienen als Auslöser für ein notwendiges Eingreifen des Managements.

Dies bedeutet, die Istsituation im Verhältnis zu der durch die Vorgaben beschriebenen Sollsituation zu erfassen und ggf. steuernd einzugreifen. Diese Leistungsindikatoren werden in Bezug auf die zu erreichenden Unternehmensziele, gesetzliche Vorgaben und Schutzbedürfnisse hin zusammengefasst.

Der Mehrwert der KxIs liegt in der Möglichkeit, grundlegende Aussagen über das Schutzsystem zu geben. Sie dienen dem

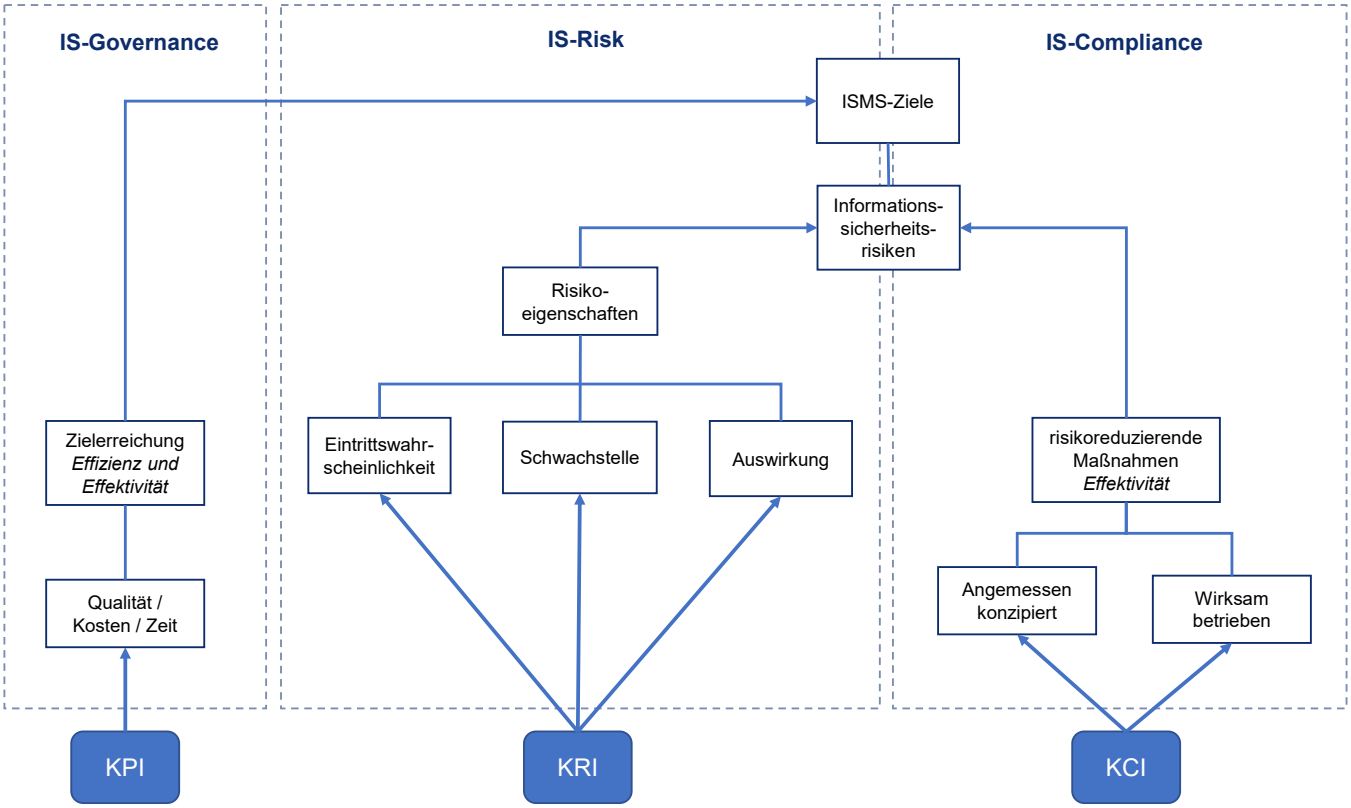


Abbildung 5: Aufbau und Beziehung von KPI, KRI und KCI

Management als nachvollziehbare und verständliche Grundlage für fundierte Entscheidungen zur Steuerung der Informationssicherheit. Neben den klassischen Performance-Analysen können durch KxIs sowohl Indizien auf (neue) Risiken bzw. Veränderungen innerhalb der Risikolandschaft als auch Nichtkonformitäten in Bezug auf die Umsetzung von Sicherheitsvorgaben und Richtlinien aufgedeckt werden.

Erfolgsfaktoren aus der Praxis

Schlüsselindikatoren sind nur dann sinnvoll zur Darstellung der Istsituation und Steuerung einsetzbar, wenn sie bestimmte Voraussetzungen erfüllen:

- Jeder Schlüsselindikator muss messbar, wiederholbar und vergleichbar sein, sowohl entlang der Zeitachse als auch branchen- oder zumindest organisationsübergreifend.
- Indikatoren sollten systematisch aufgebaut sein und auf soliden und geeigneten statistisch-mathematischen Grundlagen mit zuverlässigen Messungen in einem ausreichenden Umfang basieren.
- Die Indikatoren sollen zeitgerecht sein und aktuelle Informationen wiedergeben. Die Häufigkeit der Datenerhebung und die Dauer der Verarbeitung bis zur Präsentation beim Management sollen die Steuerung ermöglichen, ähnlich den Anzeigen auf dem Armaturenbrett eines Autos, die dem »Lenkenden« des Systems mitteilen, ob alle »wichtigen« Parameter im gewünschten, ordnungsgemäßen Bereich liegen.
- Leistungsindikatoren müssen für die Ziele des Informationssicherheitsmanagements relevant sein, steuernde Eingriffe ermöglichen und die Entscheidungsfindung praktisch unterstützen.
- Die Auswahl der Indikatoren soll risikobasiert erfolgen und die Wirtschaftlichkeit der Datenerhebung ins Verhältnis zur Aussagekraft und Nutzbarkeit für die Entscheidungsfindung stellen.
- Die Auswahl von KxIs soll eine Bewertung des ISMS als Ganzes ermöglichen. Das heißt, es ist nicht ausreichend, nur einzelne Teilaspekte und Indikatoren zu erfassen. Diese müssen vielmehr zu einem sinnvollen Ganzen zusammengefasst werden und die Performance des gesamten ISMS erfassen.
- Leistungsindikatoren können auch zur Bewertung und Steuerung von Dienstleisterverhältnissen genutzt werden und beispielsweise als Vertragsbestandteil oder in ein (Security-)SLA aufgenommen werden.
- Siehe auch Anhang 8.3 *Ganzheitliche Absicherung der Wertschöpfungskette*, Seite 66

Relevante KxIs für das ISMS

Es gibt viele Quellen für Leistungsindikatoren der Informationssicherheit, die eine riesige Auswahl bieten, so etwa COBIT 2019 for Information Security[19], The CIS Security Metrics[20] oder Performance Measurement Guide for Information Security[21], um nur einige davon zu nennen.

Natürlich wollen wir an dieser Stelle auch auf den ISACA-Praxisleitfaden »Bewertung der Leistung eines ISMS durch Schlüsselindikatoren (für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016)« hinweisen.

Die konkrete Auswahl von KxIs soll auf den Gegebenheiten der jeweiligen Organisation basieren, die bereits beschriebenen Qualitätskriterien erfüllen und kontinuierlich optimiert werden.

Nachfolgend einige Beispiele für solche Schlüsselindikatoren aus dem ISACA-Praxisleitfaden für die Bewertung der Leistung eines ISMS durch Schlüsselindikatoren:

Key-Performance-Indikatoren

- Benötigte Zeit im Vergleich zur geplanten Zeit bei der vorgegebenen Umsetzungsrate (z.B. 80% der Mitarbeiter) einer Awareness-Kampagne
- Benötigtes Budget im Vergleich zum geplanten Budget für die Umsetzung einer Awareness-Kampagne

Key-Risk-Indikatoren

- Prozentsatz der Mitarbeiter, die einen präparierten Phishing-Link während einer Awareness-Kampagne klicken
- Prozentsatz der IT-Systeme mit Schwachstellen, die nicht im vorgesehenen Zeitfenster geschlossen wurden
- Prozentsatz der produktiven IT-Systeme, für die kein Herstellersupport mehr besteht

Key-Control-Indikatoren

- Verhältnis der bisher geschulten Mitarbeiter im Vergleich zu den Planzahlen der zu schulenden Mitarbeiter bei einer Awareness-Kampagne
- Anzahl der Mitarbeiter, die die Lernkontrolle am Ende der Awareness-Kampagne bestanden haben, im Vergleich zu den bereits geschulten Mitarbeitern bei einer Awareness-Kampagne

19 ISACA, COBIT 2019 for Information Security, 2019.

20 The Center for Internet Security, »The CIS Security Metrics«.

21 »Performance Measurement Guide for Information Security«, NIST Special Publication SP 800-55.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Dokumentation der Messstruktur für alle KxIs. Sie beantwortet die folgenden Fragen:
  - Was wurde gemessen und bewertet?
  - Welche Methoden wurden zur Messung, Analyse und Bewertung herangezogen und führen diese zu reproduzierbaren Ergebnissen?
  - Wann wurde durch wen gemessen?
  - Wann wurde durch wen analysiert und bewertet?
- Ergebnisse der Messungen und die daraus abgeleiteten Managementberichte zur Eskalation

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Alle Aufzeichnungen und Nachweise, die für den Kontext der Wirksamkeitsüberwachung relevante Informationen enthalten, da die Organisation dokumentierte Nachweise über die Überwachung und gemessenen Ergebnisse aufbewahren muss.

Referenzen

ISO/IEC 27001:2022 – Abschnitt 9.1

ISO/IEC 27004:2009 – Abschnitte 5, 6, 7, 8, 9, 10 und Annex A

COBIT 2019 Focus Area: Information Security

3.8 Documentation

Im Kontext der Dokumentation ist als zentrale Anforderung innerhalb des Managementsystems sicherzustellen, dass (zumindest) für die ISMS-Dokumentation nachfolgende Aspekte geregelt sind:

- Die Erstellung und Aktualisierung sowie die Genehmigung und ggf. Kommunikation von Dokumenten müssen nach einem definierten Verfahren (Workflow) ablaufen.
- Hierbei muss eine eindeutige Kennzeichnung von Dokumenten erfolgen, z. B. Titel, Datum, Autor, Version, Ablage sowie eine angemessene Eignungs- und Tauglichkeitsprüfung (QS) und abschließende Freigabe.
- Klassifizierung der Dokumente bzw. deren Inhalte bzgl. der Vertraulichkeit
- Erstellung ausreichender und inhaltlich relevanter Aufzeichnungen im Rahmen der operativen Tätigkeiten zur Sicherstellung der Nachvollziehbarkeit

Die Inhalte und die Detailtiefe der seitens der Norm geforderten Dokumente werden u.a. vom gewählten Geltungsbereich des ISMS, von der Größe der Organisation, von den eingesetzten Technologien und von der Organisationsstruktur beeinflusst und unterscheiden sich daher von Organisation zu Organisation.

Die Anzahl und die Art der Dokumente variieren ebenfalls. Aus Praxissicht kann es für eine Organisation sinnvoll sein, ein Set von (vielen) Einzeldokumenten zu erstellen und granular zu pflegen. Für eine andere Organisation wiederum kann es geeigneter sein, ein zentrales Ablagemedium zu nutzen, das organisationsweit zugreifbar ist. Dies kann in der Praxis auch bedeuten, ein Wiki oder ein anderes Onlinesystem als Dokumentationsbasis zu verwenden.

Sofern keine spezifischen Dokumente gefordert werden, verwendet die Norm ISO/IEC 27001:2022 den Begriff »documented information« im Zusammenhang mit Dokumentation und Aufzeichnungen. In diesem Fall wird dem Unternehmen freigestellt, in welchen zugehörigen Dokumenten diese Informationen geführt werden, wobei der Begriff »Dokument« beliebige Formate beinhaltet.

Die innerhalb des ISMS erforderliche Dokumentation ist fortlaufend zu kontrollieren, damit Folgendes sichergestellt ist:

- Verfügbarkeit und Eignung für die Verwendung, unabhängig von Ort und Zeitpunkt
- Angemessener Schutz, z. B. vor Verlust der Vertraulichkeit, unsachgemäßer Verwendung oder vor unerlaubter Manipulation/Verlust der Integrität

Erfolgsfaktoren aus der Praxis

Die Erfüllung der Anforderung an eine Dokumentenlenkung kann in der Praxis grundsätzlich mit einer Dokumentenrichtlinie unterstützt werden. Entscheidend für den Umsetzungserfolg ist allerdings nicht die Quantität der Dokumentation, sondern deren Güte, Akzeptanz und Verfügbarkeit sowie deren effiziente Steuerung (Stichwort: Dokumentenlenkung).

Praktische Aspekte zur Einschätzung der Dokumentationsqualität und der Dokumentenlenkung ergeben sich aus folgenden Fragestellungen:

- Wie werden Inhalte und Änderungen der Dokumentation an die betroffenen Mitarbeiter kommuniziert oder geschult?
- Wie gut sind die Mitarbeiter mit den Inhalten vertraut und wie werden die Anforderungen der Dokumente von den Betroffenen im Alltag »gelebt«?
- Wer kennt die Ablageorte und Ablagemedien, an denen die aktuellen Dokumente zu finden sind?

- Sind die Inhalte zielgruppenorientiert aufbereitet und eindeutig formuliert?
- Wie leicht fällt es neuen Mitarbeitern, die Inhalte der Dokumente zu erfassen und im eigenen Arbeitsumfeld umzusetzen? Welche Art von Nachfragen gibt es?
- Werden die Dokumente regelmäßig bzw. nach Anforderung aktualisiert? Wie gut funktionieren die Aktualisierung und die Freigabe der Dokumente?
- Gibt es je Dokument dedizierte Dokumenteigentümer?

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation (Abschnitte 4-10):

- Geltungsbereich des ISMS (*Scope of the ISMS*, Abschnitt 4.3)
- Informationssicherheitsleitlinie (*Information security policy*, Abschnitt 5.2 e)
- Beschreibung des Risikobeurteilungsprozesses (*Information security risk assessment process*, Abschnitt 6.1.2)
- Beschreibung des Risikobehandlungsprozesses (*Information security risk treatment process*, Abschnitt 6.1.3)
- Erklärung zur Anwendbarkeit (*Statement of Applicability*, Abschnitt 6.1.3 d)
- Risikobehandlungsplan (*Information security risk treatment plan*, Abschnitt 6.1.3 e)
- Sicherheitsziele (*Information security objectives and planning to achieve them*, Abschnitt 6.2)
- Monitoring zur Erreichung der Sicherheitsziele (*Information security objectives and planning to achieve them*, Abschnitte 6.2 d, 6.2 g)
- Kompetenznachweise (*Evidence of competence*, Abschnitt 7.2 d)
- Nachweise zur korrekten Ausführung sowie Änderungen der ISMS-Prozesse[22] (*Operational planing and control*, Abschnitt 8.1 d; *Planning of cha*nges, Abschnitt 6.3)
- Ergebnisse der Risikobeurteilung (*Results of the Information security risk assessment*, Abschnitt 8.2)
- Ergebnisse der Risikobehandlungen (*Results of the Information security treatment*, Abschnitt 8.3)
- Nachweis von Kontrolle und Leistungsmessung des ISMS (*Evidence of the monitoring and measurement results*, Abschnitt 9.1)
- Nachweis über die Durchführung von Audits und deren Resultate (*Evidence of the audit programme(s) and the audit results*, Abschnitt 9.2)
- Nachweis über die Ergebnisse von Managementreviews (*Evidence of the results of management reviews*, Abschnitt 9.3)
- Festgestellte Abweichungen von ISMS-Vorgaben sowie Maßnahmen zur Behebung (*Evidence of the nature of the nonconformities and any subsequent actions taken*, Abschnitt 10.1 f)
- Nachweis über die Resultate von Korrekturmaßnahmen (*Evidence of the results of any corrective action*, Abschnitt 10.1 g)

Darüber hinaus muss die Organisation für sich selbst festlegen, welche Dokumentation und Aufzeichnungen zusätzlich zum normativ Geforderten nötig sind, um »ein ausreichendes Vertrauen zu haben, dass die Prozesse wie geplant durchgeführt wurden« (siehe Abschnitt 8.1).

Die ISMS-Prozesse zum Risikomanagement, Incident Management und zur kontinuierlichen Verbesserung des ISMS sollten über geeignete Prozessdarstellungen (z.B. ereignisgesteuerte Prozessketten, EPKs) visualisiert und über Prozessbeschreibungen bzw. konkrete Arbeitsanweisungen den Mitarbeitern verständlich kommuniziert werden.

Hinzu kommen noch die Dokumente und Aufzeichnungen aus Annex A, sofern diese Maßnahmen gemäß »Statement of Applicability« angewendet werden.

Referenzen

ISO/IEC 27001:2022

3.9 Communication

Beim Betrieb eines ISMS ist eine Zusammenarbeit mit anderen Organisationen und Abteilungen erforderlich (z.B. Lieferanten, Personalabteilung, Rechtsabteilung, Revision). Die wesentliche Aufgabe im Rahmen des Bausteins »Communication« besteht darin, den Bedarf an interner und externer Kommunikation zu bestimmen und zu beschreiben.

Mit externer Kommunikation ist hierbei die Kommunikation mit (externen) Stakeholdern und anderen Organisationen gemeint (siehe auch Umfeldanalyse in Kapitel *3.1 Context of the Organization*). Unter interner Kommunikation ist der Kommunikationsbedarf innerhalb des Managementsystems und innerhalb der Organisation zu verstehen, also z.B. mit internen Stakeholdern wie Vorstand, Führungskräften und Mitarbeitern.

Im Rahmen einer Analyse sollte bestimmt werden, welche Informationen im Kontext des ISMS (Abschnitt 7.4 a der Norm) von wem (Abschnitt 7.4 d) an wen (Abschnitt 7.4 c) kommuniziert werden müssen. Darüber hinaus sollte festgelegt werden, wann kommuniziert wird (Abschnitt 7.4 b) und

22 Die Norm spricht in diesem Kontext von »dokumentierte Information im notwendigen Umfang«.

über welche Kommunikationskanäle/-prozesse (Abschnitt 7.4 e) dies erfolgen soll.

Die Ergebnisse der Analyse werden im Idealfall in einem Kommunikationsplan zusammengefasst. Dieser wird üblicherweise formal in fünf konkreten Schritten erarbeitet (siehe Abbildung 6):

Abbildung 6: Ausarbeitung eines Kommunikationsplans

- Prozess- und Kommunikationsschnittstellen sollten im Sinne der Effizienz eindeutig definiert sein und in die organisatorischen bzw. operativen Abläufe integriert werden. Es ist eindeutig zu regeln, welche Informationen zu welchem Zeitpunkt von wem an wen geliefert werden müssen, beispielsweise im Rahmen des Change- oder Incident-Managements.
- Die Norm fordert, dass die Organisation interne und externe Kommunikation im Kontext des ISMS bestimmt. Sie fordert nicht explizit, dass dies im Rahmen einer Analyse erfolgen muss. Der Praxisnutzen einer Analyse besteht aber darin, dass mit ihrer Hilfe klar identifiziert werden kann, welche Anforderungen an eine passgenaue Kommunikationsstruktur existieren.

Erfolgsfaktoren aus der Praxis

Ein Kommunikationsplan, auch Kommunikationsmatrix genannt, kann beispielhaft im Ergebnis wie in den Tabellen 1 und 2 aussehen.

Interne Kommunikation				
Kommunikationsgrund	*Initiator*	*Empfänger*	*Häufigkeit*	*Medium*
Managementreview	CISO	Topmanagement	jährlich	Managementbericht gemäß Template per Mail + Präsentation
Reporting	CISO	Topmanagement	quartalsweise	KPI-Bericht gemäß Template per E-Mail + Präsentation
Awareness-Training	CISO	Alle Mitarbeiter im Geltungsbereich	jährlich	Schulung (Präsenz/Online)
IS-Newsletter	CISO	Alle Mitarbeiter im Geltungsbereich	quartalsweise sowie fallbezogen bei akuter Bedrohung	E-Mail
Risikomanagement	CISO	Topmanagement	quartalsweise, fallbezogen bei akuter Bedrohung, projektbezogen	Balanced-Scorecard-Bericht, ggf. per E-Mail
Sicherheitsvorfall	Support	CISO *(ggf. weitere gemäß SIRP)*	fallbezogen	Eskalation gemäß SIRP (Security Incident Response Process)
Sicherheitsvorfall	CISO	Topmanagement	fallbezogen	E-Mail, ggf. mündlich
Sicherheitsvorfall mit personenbezogenen Daten	CISO	Datenschutzbeauftragter	fallbezogen	E-Mail, ggf. telefonisch oder mündlich
Sicherheitsvorfall mit Compliance-Bezug	CISO	Justiziariat	fallbezogen	E-Mail, ggf. telefonisch oder mündlich

Tabelle 1: Kommunikationsplan – interne Kommunikation

Externe Kommunikation				
Kommunikationsgrund	*Initiator*	*Empfänger*	*Häufigkeit*	*Medium*
Report Betriebsdienstleister	Betriebsdienstleister	CISO	quartalsweise	SLA-Report gemäß Template per E-Mail
Extern beauftragtes CERT/ Vulnerability Analysis	CERT	CISO/IT-Leiter	wöchentlich/fallbezogen	Report gemäß Vertrag per E-Mail
Sicherheitsvorfall	CISO, ggf. Topmanagement	betroffene Kunden/Partner	fallbezogen	gemäß SIRP, auf Website, Brief, E-Mail, telefonisch
Sicherheitsvorfall mit strafrechtlichem Hintergrund	CISO	Ermittlungsbehörden	fallbezogen	gemäß SIRP

Tabelle 2: Kommunikationsplan – externe Kommunikation

- Wenn die Kommunikationsmatrix ausgearbeitet ist, hat sich in der Praxis gezeigt, dass diverse Schnittstellen zwischen Kommunikationspartnern und/oder Abteilungen bereits existieren. Diese zu identifizieren, ist ein wichtiger Erfolgsfaktor, um die Kommunikation im Kontext des ISMS in der Organisation effizient zu gestalten. Es kann sinnvoll sein, den IS-Kommunikationsplan in einen übergreifenden Kommunikationsplan zu integrieren.
- Um mit allen Ebenen der Organisation kommunizieren zu können, sollte eine Plattform bereitgestellt werden, damit die umfassenden Sicherheitsinformationen des ISMS für verschiedene Zielgruppen zugänglich sind. Kollaborationsplattformen zur besseren Kommunikation bzw. zum Reporting könnten z. B. Intranet, Confluence, Wiki o.Ä. sein.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen keine normativen Anforderungen an die Dokumentation des ISMS in Bezug auf Kommunikation.

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Verfahren zur internen und externen Kommunikation
- Kommunikationsmatrix
- Kommunikationsplan

Referenzen

ISO/IEC 27001:2022 – Abschnitt 7.4

3.10 Awareness

»Informationssicherheit ist der Betrieb von Firewalls und Antivirus« – dies ist eine der häufigen und großen Fehleinschätzungen, die die Sicherheit von Informationen und IT-Systemen eines Unternehmens gefährden, denn eine Vielzahl von sicherheitsrelevanten Ereignissen und Sicherheitsvorfällen im operativen Betrieb fällt in die Kategorien »fehlendes Verantwortungsbewusstsein«, »fehlende oder unausgereifte Prozesse« und »mangelhafte Ausbildung und/oder Sensibilität der Mitarbeiter«.

Die Schaffung eines »gesunden« Risikobewusstseins ist daher ein wesentlicher Bestandteil eines praxistauglichen ISMS, das einen Nutzen für die Organisation erzeugt, indem Bedrohungen frühzeitig erkannt, Sicherheitsvorfälle vermieden und die Aufwände, die für deren Behandlung notwendig wären, »eingespart« werden.

Sicherheitssensibilisierung (Security Awareness) ist hierbei kein Selbstläufer, sondern muss vom Unternehmen aktiv – über entsprechende Awareness-Kampagnen – gefördert und gefordert werden, unter anderem durch folgende wichtige Aspekte (vgl. Abschnitt 7.3):

- Die Kenntnis der Informationssicherheitsleitlinie und Anwenderrichtlinie sowie der relevanten Informationssicherheitsrichtlinien aufseiten der Vorgabenempfänger (Mitarbeiter, Führungskräfte, externe Partner) muss sichergestellt werden.
- Der Beitrag eines jeden Mitarbeiters innerhalb des ISMS-Geltungsbereichs sollte sich an den in der Anwenderrichtlinie dokumentierten Maßnahmen orientieren. Die für Awareness-Maßnahmen eingesetzten Materialien unterstützen idealerweise die Vermittlung dieser Inhalte. Eine erfolgreiche Vermittlung durch Tests nachzuweisen ist empfohlen.
- Auswirkungen und ggf. Sanktionen bei Nichteinhaltung von Sicherheitsbestimmungen sollten aus den Materialien, die im Rahmen einer Awareness-Maßnahme verwendet werden, hervorgehen. Gleichzeitig sollte die Meldung eines Benutzers zu einer Sicherheitsverletzung (z. B. Whistleblower) durch eigenes Fehlverhalten in der Regel nicht zu einer Sanktionierung führen.

Erfolgsfaktoren aus der Praxis

Informationssicherheits-Awareness-Kampagnen lassen sich in der Praxis üblicherweise in verschiedene Phasen gliedern. Man startet zunächst mit einer Bedarfsermittlung und versucht dann zielgruppengerecht und auf Basis von konkreten Gefährdungspotenzialen eine Sensibilisierungskampagne zu planen und umzusetzen. Informationssicherheits-Awareness darf hierbei nicht als einmaliges Projekt gesehen werden, sondern sollte über entsprechend in der Kampagne eingeplante Mechanismen nachhaltig etabliert werden. Die Analyse der Wirksamkeit einer Kampagne sollte bereits im Vorfeld bedacht werden. In der Praxis haben sich die nachfolgenden Phasen für eine Security-Awareness-Kampagne als sinnvoll erwiesen (siehe Abbildung 7):

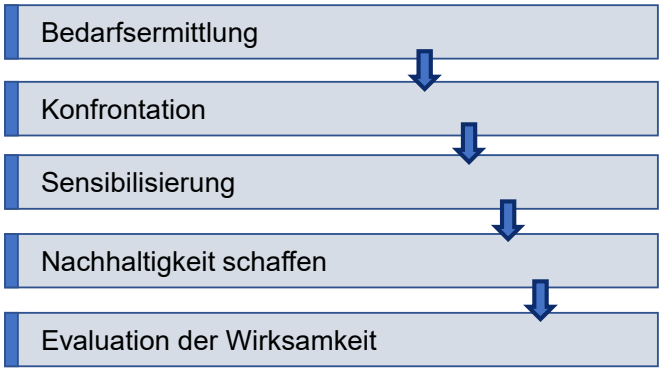


Abbildung 7: Phasenmodell für Security-Awareness-Kampagnen

Phase 1: Bedarfsermittlung (auf Basis von Gefahrenpotenzialen)

Eine erfolgreiche Umsetzung von Security-Awareness-Kampagnen setzt voraus, dass man seine Zielgruppe und deren Bedarf kennt. Aus diesem Grund sollten Awareness-Kampagnen zunächst immer mit einer Bedarfsermittlung starten.

- Sicherheitssensibilisierung ist in allen Unternehmensbereichen sinnvoll, jedoch nur in einem der tatsächlichen Gefährdung und der Zielgruppe entsprechenden Umfang.
- Die Kenntnis von Sicherheitsvorgaben kann z. B. durch Awareness-Maßnahmen mit aktiver Beteiligung und Teilnehmerprotokollen nachgewiesen werden.

Bevor mit der Definition und Planung von Awareness-Maßnahmen begonnen wird, sollte sich ein Unternehmen folglich Gedanken über seine individuellen Gefahrenpotenziale (Risiken) bezogen auf die Anwender machen. Es ist wenig hilfreich, die Anwender mit Gefahren und Situationen zu konfrontieren, die nicht auf ihren Bereich zutreffen.

Phase 2: Konfrontation mit der Thematik

In der Phase der »Konfrontation« soll die Aufmerksamkeit der Mitarbeiter für das Thema geweckt, Betroffenheit erzeugt und die Akzeptanz für die Phase 3, also die eigentliche Sensibilisierung, gefördert werden. Dies erfolgt in der Regel am besten durch eine direkte Konfrontation der Mitarbeiter mit dem Thema (»erfahrungsbasiertes Lernen«).

- Durch Eigenerfahrung werden die Mitarbeiter hinsichtlich ihrer Wichtigkeit für die Informationssicherheit sensibilisiert und sind im Normalfall anschließend dankbar und offen für Weiterbildungsmaßnahmen zum Thema.

Nachfolgend sind einige Simulationen von Angriffen aufgelistet, um Mitarbeiter mit dem Thema zu konfrontieren:

- Social-Engineering-Angriffe auf Mitarbeitende, beispielsweise mit Fake-Anrufen, um vertrauliche Informationen (wie z. B. Passwörter) zu erhalten, und Fake-E-Mails (z. B. mit der Aufforderung der Eingabe des Passworts in ein Onlinesystem mit dem vorgeblichen Zweck, die Passwortstärke für ein anstehendes Audit zu prüfen).
- Präparierte USB-Sticks unternehmensintern auslegen (Parkplatz, Besprechungsraum, WCs etc.), die bei Nutzung Warnmeldungen generieren, die anonymisiert registriert und zur Auswertung genutzt werden können (»Ich hätte ein Virus sein können«).
- Altpapiertonne oder Papierkörbe nach vertraulichen Dokumenten durchsuchen (»dumpster diving«).

Die Praxis hat gezeigt, dass die oben genannten Angriffsszenarien in den meisten Unternehmen zu – in diesem Kontext – »wertvollen« Sicherheitsvorfällen und verwertbaren Informationen führen. Die »anonyme« Auflösung der Aktion in Verbindung mit der Darstellung von möglichen Konsequenzen für das Unternehmen sorgen üblicherweise für einen »Hallo-wach-Effekt« bei den Mitarbeitern, der als Einstieg in die eigentliche IS-Kampagne (»Wissensvermittlung«) genutzt werden kann. Auch aus ethischen Gründen empfiehlt es sich, simulierte »Angriffe« auf die Mitarbeiter nur nach vorheriger Ankündigung und in enger Abstimmung mit dem ggf. vorhandenen Betriebsrat durchzuführen, um Unmut bei den Betroffenen zu vermeiden, der den gewünschten Lerneffekt konterkarieren könnte.

Alternativ zu solchen Kampagnen kann die »Konfrontation« auch passiv, etwa am Anfang einer Präsenzschulung, erfolgen. Als Demonstrationen wären z. B. Live-Hacking-Sessions, anonymes Prüfen von Passwortstärken oder auch Rollenspiele denkbar.

- Ein essenzieller Aspekt in dieser Phase ist es, einen positiv gestalteten Einstiegspunkt für das Thema zu erzeugen und so den Kontakt mit den Mitarbeitern »auf Augenhöhe«

herzustellen. Bei aller Konfrontation muss die Grundrichtung immer dahin gehen, die Mitarbeiter dort »abzuholen«, wo sie gerade stehen (Welche IS-Vorgaben gibt es bereits? Wie wurden diese bisher kommuniziert? Welche Vorfälle gab es bereits? Etc.), und sie aktiv einzubinden.

- Es ist auch wichtig, sich über die Rahmenbedingungen im Klaren zu sein und die ggf. bestehenden Informationslücken zu kennen. Der Umfang der durchgeführten Aktivitäten und bereitgestellten Informationen muss mit der »Aufnahmekapazität« aufseiten der Adressaten abgeglichen werden. Nur so kann die Kampagne ihre volle Wirkung entfalten und wird weder als zu banal noch als zu überzogen/überladen wahrgenommen.

Phase 3: Sensibilisierung

Die eigentliche Sensibilisierung stellt bestenfalls einen Mix von Wissensvermittlung, Demonstration und aktiver Beteiligung der Mitarbeiter dar. Für die Wissensvermittlung können hierbei verschiedene Methoden zum Einsatz kommen (Präsenzschulungen, E-Learning etc.).

Die Kategorisierung von Sensibilisierungsmaßnahmen in Themengebiete oder Maßnahmen hat sich bewährt, insbesondere die folgende:

- **Physische Sicherheit/Sicherheit am Arbeitsplatz**
  - Worauf muss beim Zutritt zu den Gebäuden und Räumlichkeiten geachtet werden?
  - Wie wird verhindert, dass sich Unbefugte Zutritt verschaffen, z. B. falsche Anlieferungen oder ein Unbekannter hängt sich an eine Gruppe von Mitarbeitern an und kommt unbemerkt mit in das Gebäude (»piggybacking«)?
- **Datenschutz**
  - Der Datenschutzteil sollte die gesetzlichen Anforderungen herausstellen, z. B. Datengeheimnis, Löschprozeduren und Verpflichtung der Mitarbeiter.
- **IT-Sicherheit**
  - Was ist beim Umgang mit IT-Systemen und Computern zu beachten, z. B. Umgang mit E-Mails, Surfen im Internet, Handhabung von Wechselmedien (CDs, USB-Sticks), Schutz und Werkzeuge gegen Malware?
- **Telefonie**
  - Was kann passieren, wenn schützenswerte Informationen oder Prozesse über das Telefon preisgegeben werden?
- **Meldung von und Umgang mit Sicherheitsvorfällen**
  - Welche (zentralen) Anlaufstellen gibt es?
  - Was sind relevante Erstmaßnahmen?

Zusätzlich müssen besonders gefährdete Zielgruppen (z. B. IT-Administratoren, Mitarbeiter und Führungskräfte mit weitreichenden Zugangs-, Zugriffs- und Informationsrechten, mobile Mitarbeiter, aber auch Callcenter-Mitarbeiter oder andere Gruppen mit Außenkontakt) berücksichtigt werden, um abzuwägen, ob diese besonders geschult werden müssen.

Zur Unterstützung der Trainings sollten Awareness-Materialien erstellt und bei Bedarf verteilt werden. Das können z. B. einseitige oder mehrseitige Broschüren oder Newsletter mit Trainingsinhalten, aber auch Poster, Aufkleber oder andere Medien mit hohem Wiedererkennungseffekt (Plakate, Flyer, Videos etc.) sein.

- Optimalerweise erfolgt die Erstellung von Awareness-Materialien durch die eigenen Mitarbeiter im Rahmen der IS-Kampagne. Eine zusätzliche Motivation zur Mitarbeit kann über ein Incentive-System[23] erreicht werden.
- Ein Leitvideo des Topmanagements kann die Wichtigkeit des Themas mit entsprechender Aufforderung an die Mitarbeiter zum achtsamen Umgang mit Informationen besonders herausheben.

Phase 4: Nachhaltigkeit schaffen

Einmalige Awareness-Maßnahmen sind nicht ausreichend, um eine nachhaltige Verhaltensänderung bei den Mitarbeitern zu bewirken. Es ist zwar notwendig, eine umfangreiche Erstsensibilisierung vorzunehmen, aber nur eine regelmäßige Wiederholung der Themen auf Basis eines Schulungsplans und die regelmäßige Kommunikation der zentralen Botschaften im Alltag können eine dauerhafte Awareness gewährleisten. Möglichkeiten zur Schaffung einer unbewussten Präsenz des Themas im Alltag sind beispielsweise:

- Regelmäßiger Versand von simulierten Phishing-E-Mails (z. B. zur Preisgabe von Zugangsdaten)
- Veröffentlichung aktueller News (z. B. über das Intranet, Mitarbeiterzeitung)
- Einbindung eines Onlinequiz zum Thema IS im Intranet oder über eine App (evtl. mit Incentivierung)
- Nutzung eines Bildschirmschoners mit ansprechenden Sicherheitsbotschaften
- Jährliche Durchführung eines Cyber-Sicherheits-Monats mit z. B. internen oder externen Vorträgen, Live-Hackings

23 Incentive = Anreiz, Leistungsanreiz.

Phase 5: Evaluation der Wirksamkeit

In dieser Phase wird – in regelmäßigen Abständen – der Reifegrad der Mitarbeitersensibilisierung erhoben. Ziel ist die Schaffung von Transparenz in Bezug auf den Reifegrad der Mitarbeitersensibilisierung. Als mögliche KPIs zur Messung dienen beispielsweise:

- Anzahl der Sicherheitsvorfälle, die durch Fehlverhalten ausgerufen wurden, im Verhältnis zu allen Sicherheitsvorfällen
- Anzahl/Verhältnis der Klickraten oder Kennworteingaben auf simulierte Phishing-E-Mails
- Ergebnisse eines Quiz oder Tests zum Thema Informationssicherheit
- Net Promoter Score (NPS) bei Schulungsinhalten

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Nachweise der Kompetenz von Mitarbeitern im Geltungsbereich des ISMS (Abschnitt 7.2)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Awareness-/Schulungskonzept
  - Welche Themen werden behandelt?
  - Wie werden Awareness-Maßnahmen durchgeführt, z. B. Präsenztrainings und/oder Onlineschulungen?
  - Wie werden die Inhalte der Informationssicherheitsrichtlinie vermittelt?
- Awareness-/Schulungsprogramm
  - Wann werden welche Themen behandelt?
  - Finden Updates zu Maßnahmen, wie im Standard gefordert, regelmäßig statt?
- Schulungsunterlagen, die die Inhalte der Informationssicherheitsleitlinie knapp und prägnant wiedergeben und auf Gefahren und Schwachstellen in der Informationsverarbeitung hinweisen
- Nachweis der Teilnahme: Namen der teilgenommenen Personen, Inhalte und Datum der Awareness-Maßnahme

Referenzen

ISO/IEC 27001:2022 – Abschnitte 7.2 und 7.3

3.11 Supplier Relationships

Die starke Vernetzung und Standardisierung in der Informationsverarbeitung haben den Einsatz externer Dienstleister/Lieferanten stark gefördert. Umgekehrt wirken sich Sicherheitsrisiken beim Dienstleister/Lieferanten auch auf die eigene Infrastruktur aus. Dies belegen etliche öffentlichkeitswirksame Vorfälle der letzten Jahre, bei denen Sicherheitsmängel bei Dienstleistern/Lieferanten zu Datendiebstählen oder anderen Sicherheitsvorfällen bei namhaften Firmen führten.

Der Begriff »Dienstleister« bzw. »Lieferant«

Im Selbstverständnis der Norm ISO/IEC 27001:2022 umfasst der Begriff »Supplier« eine große Bandbreite von Geschäftsbeziehungen zu externen Firmen und Partnern. Er schließt Beziehungen aus dem IT-Umfeld, wie Softwarehersteller, IT-Dienstleister, Outsourcing-Partner oder Cloud Service Provider, aber auch aus anderen Bereichen mit ein. Dazu gehören zum Beispiel Logistik, Versorgungseinrichtungen, Facility-Management, Reinigungsdienstleister und viele weitere.

Die Anforderungen von ISO/IEC 27001:2022 fokussieren auf verschiedene Schutzmaßnahmen, beispielsweise die Festlegung von Prozessen und Verfahren (Abschnitt 5.19) sowie die Vereinbarung vertraglicher Regelungen mit dem Lieferanten (Abschnitt 5.20), z. B. Anbindung an Protokollierung oder Sicherheitslogging, CERT-Anbindung, Meldewege zu Sicherheitsvorfällen, Integration in ein bestehendes Identity Management System. Dabei sind auch Risiken aus dessen ITK-Infrastruktur, Lieferketten und sonstige Weiterverlagerungen (Abschnitt 5.21) sowie Regelungen zur Überwachung und Änderung der Dienstleistungserbringung (Abschnitt 5.22) zu berücksichtigen.

Für die Nutzung von Cloud-Diensten sollten eine themenspezifische Richtlinie etabliert sowie Prozesse für den gesamten Lebenszyklus des Dienstes entwickelt sein (Abschnitt 5.23). So werden von der Beschaffung, Nutzung, Verwaltung und Ausstieg aus dem Cloud-Dienst relevante Aspekte der Informationssicherheit adressiert.

ISO/IEC 27036 und weitere relevante Standards

Eine deutlich detailliertere Betrachtung bietet die Norm ISO/IEC 27036 »Information Security for supplier relationships«. Sie geht auf die notwendigen Prozesse ein und beschreibt die im jeweiligen Prozess erforderlichen Aktivitäten. Eine Zertifizierung nach diesem Standard ist nicht möglich, jedoch wird eine gemeinsame Terminologie geschaffen, die u.a. viele konkrete Hilfestellungen zur Umsetzung gibt.

Abbildung 8 zeigt eine Übersicht der in diesem Kontext relevanten Standards, unterteilt in Überblick, Anforderungen und Leitfäden, sowie ergänzende Dokumente, die auf Prozesse und Techniken fokussieren.

In regulierten Branchen sind ggf. weitere konkrete Anforderungen zu berücksichtigen, beispielsweise MaRisk AT 9 bei Banken. Des Weiteren findet sich vermehrt die ISO 28001 »Sicherheitsmanagementsysteme für die Lieferkette« als Be-

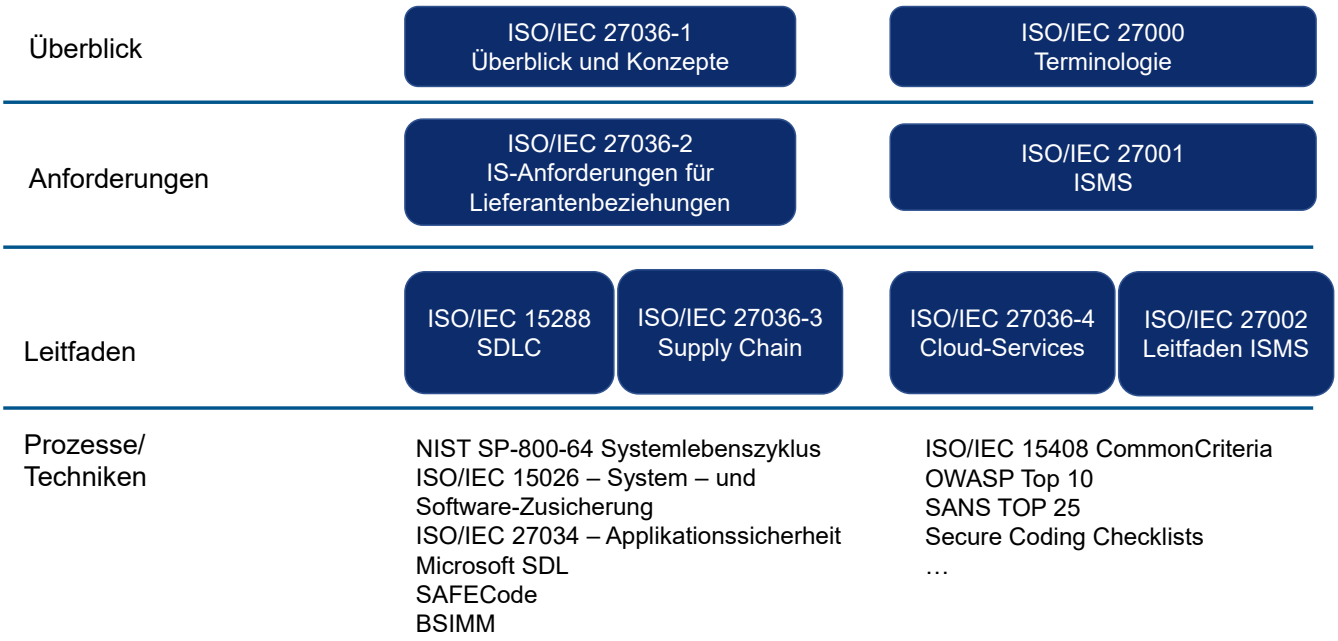


Abbildung 8: IS-Normenübersicht zu Lieferantenbeziehungen

standteil von Kundenverträgen wieder. Auch in dieser Norm sind Anforderungen an die Informationssicherheit (z. B. physische Sicherheit, Personalsicherheit, IT-Sicherheit) festgelegt.

Erfolgsfaktoren aus der Praxis

Ganzheitliche Risikobetrachtung

Es ist wichtig, auf alle Risiken einzugehen, denen die eigene Organisation durch die Zusammenarbeit mit externen Dienstleistern ausgesetzt ist. Die Norm fordert an dieser Stelle, dass alle ausgelagerten Prozesse klar festgelegt und nachhaltig gesteuert werden (siehe Abschnitt 8.1).

Eine mögliche Einteilung der Lieferantenbeziehungen bietet die ISO/IEC 27036-1. Sie unterscheidet zwischen:

- Lieferantenbeziehungen für Produkte
- Lieferantenbeziehungen für Services
- Lieferkette für Informationstechnologie
- Cloud Computing

Einsatz von Software

Auch der Einsatz von Software jeglicher Art sollte unter dem Aspekt des Lieferantenmanagements beurteilt werden. Sowohl selbst entwickelte Software als auch fertige Produkte und Dienstleistungen binden häufig Frameworks, Pakete oder andere Bibliotheken mit ein. In der Vergangenheit haben Angriffe auf diese hinter der eigentlichen Anwendung liegenden Komponenten zu erfolgreichen Kompromittierungen geführt. Verfahren zur Identifikation und Kontrolle dieser Komponenten sollten Bestandteil des IT-Betriebs bzw. der Softwareentwicklung sein.

Recht auf Auditierung

Das Recht zur Auditierung sollte grundsätzlich in jedem Vertrag vorgesehen sein.

- In Standardverträgen mit Cloud-Anbietern wird dieses Recht üblicherweise jedoch nicht eingeräumt. In diesem Fall sind Alternativen zu prüfen, beispielsweise die Einsichtnahme in Ergebnisberichte externer Audits oder die Bereitstellung von Zertifikaten inklusive der jeweiligen Geltungsbereiche.

Zertifizierungen

Das Verlangen nach Informationssicherheit bei Kunden wird durch Lieferanten zunehmend mittels Zertifizierungen beantwortet. Hierfür geeignet sind insbesondere die ISO/IEC 27001:2022 oder der IT-Grundschutz. Aber auch die ISO/IEC 27018 für die Verarbeitung personenbezogener Daten in der Cloud oder – in Teilen – der internationale Standard ISAE 3402 »Assurance Reports on Controls at a Service Organization« werden dazu herangezogen. Im Automobil-Sektor hat sich TISAX® etabliert. Die Grundlage für das Prüfverfahren ist das VDA Information Security Assessment, das sich an der ISO/IEC 27001 orientiert.

- In allen Fällen ist ein vollständiger Bericht über das Audit und seine Ergebnisse sehr wichtig, da der Scope einer Prüfung und die jeweils geprüften Kontrollen ggf. variieren können. Für kritisch eingestufte Lieferanten sollte ein SOC Type II Report gemäß ISAE 3402 eingefordert wer-

den. Weiterhin sollten potenzielle Abweichungen durch den Auftraggeber gemäß eigenem Risikoappetit bewertet werden.

- Bei personenbezogenen Daten ist der Einsatz von Dienstleistern, insbesondere von solchen, die außerhalb des deutschen Rechtsraums oder außerhalb des EWR[24] agieren, sehr kritisch zu prüfen.
- In diesen Kontext fällt ebenfalls das Thema Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO[25] unabhängig davon, wo der Dienstleister angesiedelt ist.

Kennzahlen

Folgende Kennzahlen[26] können beispielsweise zur Auswertung der Informationssicherheit in Bezug auf Dienstleister genutzt werden:

- Anzahl der fristgerecht gelieferten Dienstleister-Reports im Verhältnis zur Gesamtanzahl der vereinbarten Reports
- Durchschnittliche Zeit vom Entdecken bis zum Melden von Sicherheitsvorfällen durch Dienstleister
- Anzahl der Dienstleister, die IS-Maßnahmen vertraglich zusichern, im Verhältnis zu allen Dienstleistern
- Anzahl der Sicherheitsvorfälle bei Dienstleistern im vergangenen Berichtszeitraum

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Festlegung des Geltungsbereichs unter Berücksichtigung der Abhängigkeiten von externen Partnern und Dienstleistern (Abschnitt 4.3)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Prozesse und Verfahren für Dienstleisterbeziehungen (vgl. ISO/IEC 27001:2022, Abschnitte 5.19–5.22). Dort sollten Vorgaben, die sich aus der Beschaffungsstrategie und jeglicher Dienstleisterbeziehung ergeben, definiert werden. Außerdem sollten Informationssicherheitsrisiken innerhalb der ICT-Dienstleistungs- und Produktlieferkette adressiert werden.
- Vereinbarungen zu Informationssicherheitsanforderungen mit Lieferanten. Hier sollten die unterschiedlichen Kategorien von Lieferanten berücksichtigt werden.
- Themenspezifische Richtlinie zur Nutzung von Cloud-Services (vgl. ISO/IEC 27001:2022, Abschnitt 5.23)
- Branchenspezifische Sicherheitsanforderungen wie z. B. das BDEW-Whitepaper aus dem Energiesektor

Referenzen

ISO/IEC 27001:2022 – Abschnitte 4.3 und 8.1 sowie 5.19 – 5.23

ISO/IEC 27036-1:2021

BDEW-Whitepaper »Anforderungen an sichere Steuerungs- und Telekommunikationssysteme«

3.12 Internal Audit

Die primären Ziele interner ISMS-Audits sind die Überprüfung, inwieweit das ISMS den eigenen Anforderungen der Organisation sowie den Anforderungen nach ISO/IEC 27001:2022 gerecht wird (Konformitätskontrolle), und die Überprüfung der Umsetzung und der Wirksamkeit ergriffener Maßnahmen (Umsetzungs- und Wirksamkeitskontrolle).

Hierfür muss ein Auditprogramm geplant und eingeführt werden, das Aspekte wie Häufigkeit, Verfahren, Zuständigkeiten und Verantwortlichkeiten, Planungsanforderungen, Nachverfolgung und Berichterstattung regelt. Ferner muss festgelegt werden, wie mit Korrektur- und Vorbeugemaßnahmen (also den aus den Audits direkt abgeleiteten Maßnahmen) umgegangen wird und wo diese zur weiteren Bearbeitung »nachgehalten« werden.

Mit dem Auditprogramm soll sichergestellt werden, dass alle durch das ISMS abgedeckten Geschäftsprozesse (laut Scope) mindestens einmal in drei Jahren hinsichtlich der zum Zeitpunkt des Audits geltenden Vorgaben und Richtlinien zur Informationssicherheit und bzgl. Konformität zum ISMS auditiert werden. Dies ist nachzuweisen.

Mit internen Audits im Sinne der Norm ist nicht die Tätigkeit der internen Revisionsfunktion im engeren Sinne gemeint, wobei diese auch eine Stelle sein kann, die interne Audits durchführt. In der Praxis sind die internen ISMS-Audits eine zentrale Aufgabe des ISMS-Verantwortlichen/CISO, der – ggf. zusammen mit einem internen Auditteam oder mithilfe externer Unterstützung und unter Berücksichtigung der ISO 19011:2018 – Audits plant und verwaltet.

Erfolgsfaktoren aus der Praxis

Bei der Umsetzung interner Audits können zwei Bereiche unterschieden werden (siehe Abbildung 9):

- Das »Auditprogramm« bzw. »Auditrahmenwerk«, das als ein organisatorischer Überbau zur Steuerung und

24 EWR: europäischer Wirtschaftsraum.

25 EU-DSGVO: EU-Datenschutz-Grundverordnung.

26 Siehe auch: Bewertung der Leistung eines ISMS durch Schlüsselindikatoren (ISACA Germany Chapter).

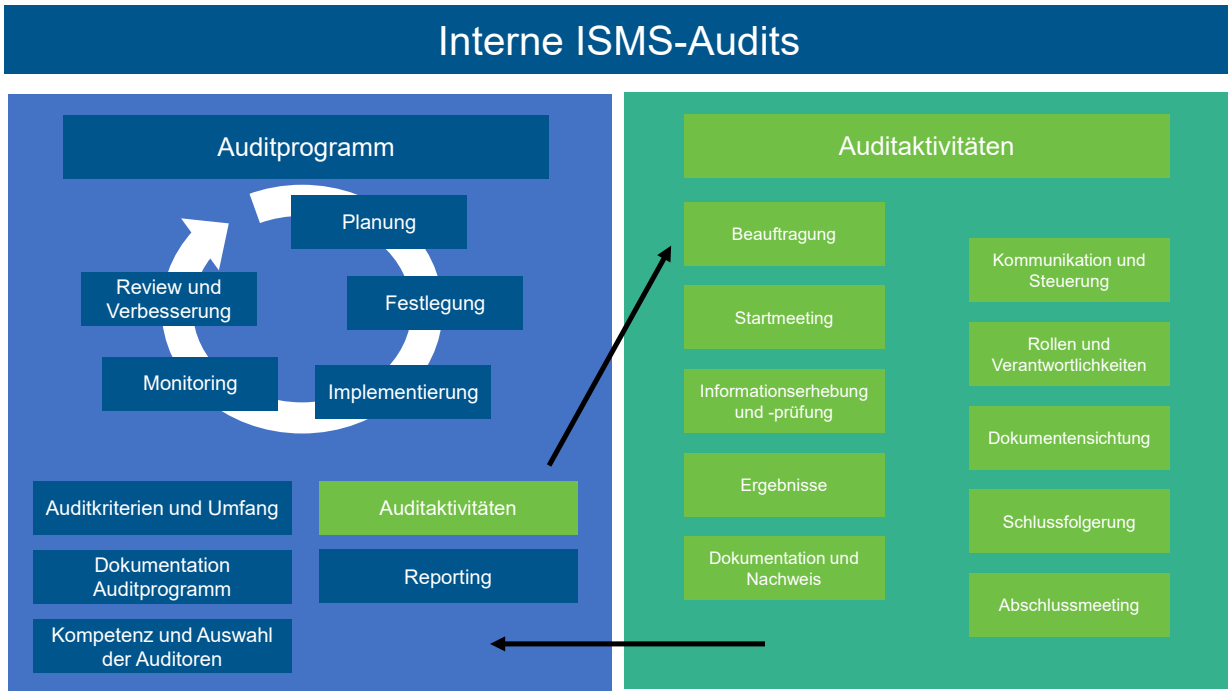


Abbildung 9: Struktur für interne ISMS-Audits (Auditprogramm vs. Auditaktivitäten)

Überwachung aller Aktivitäten im Kontext interner Audits dient und die Schnittstelle zu anderen Prozessen im ISMS bildet.

- Die konkreten »Auditaktivitäten«, die die jeweilige Planung und praktische Durchführung einzelner interner Audits beinhalten.

Die Auditaktivitäten dienen der betrieblichen Umsetzung des Auditprogramms, eine Abstimmung mit der internen Revisionsfunktion der Organisation ist daher sinnvoll.

In größeren Organisationen ist eine organisatorische Aufteilung zwischen diesen Bereichen sinnvoll, wobei ein Auditteamleiter für das Auditprogramm verantwortlich ist und ein Team von Auditoren die internen Audits praktisch durchführt. Es ist sicherzustellen, dass sowohl die gesamtheitliche Ausgestaltung als auch die operative Steuerung des Auditprogramms optimal auf die Erreichung der IS-Ziele hinwirken. Dadurch erhält die Organisation den bestmöglichen Return on Investment (ROI) für den Ressourceneinsatz im Auditbereich.

Das Auditprogramm

Das Auditprogramm besteht aus einem Zyklus mit den Teilprozessen Planung, Festlegung, Implementierung, Monitoring sowie Review und Verbesserung des Auditprogramms selbst (siehe Abbildung 10).

- Im Auditprogramm und bei der risikobasierten Planung konkreter Auditaktivitäten sollten sowohl die Bedeutung der betroffenen Prozesse (Kernprozesse, Schadensauswirkungen, Geschäftskritikalität) und IT-Systeme als auch die Ergebnisse vorangegangener Audits berücksichtigt werden.
- Im Auditprogramm müssen die allgemeinen Kriterien für Audits festgelegt sein. Je nach Größe der Organisation, Anzahl durchgeführter Audits und gewünschtem Detaillierungsgrad des Auditprogramms kann hier auch direkt der konkrete Umfang einzelner Audits definiert werden.
- Durchgeführte Audits müssen dokumentiert werden und entsprechende Informationen (z. B. in Form von Auditberichten) müssen als Nachweis der Umsetzung des Auditprogramms vorhanden sein.
- Es sind regelmäßig Managementreports mit Informationen über die Leistungsfähigkeit des Auditprogramms und zu den Auditaktivitäten und deren Ergebnisse zu erstellen.

Teilprozess »Planung«

Das Auditprogramm sollte auf den individuellen Anforderungen der jeweiligen Organisation basieren (siehe Abschnitte 4.2 und 4.3 der Norm und Kapitel *3.1 Context of the Organization* dieses Leitfadens). Ferner sollte aus den definierten Zielen des Auditprogramms hervorgehen, dass

- die Audits an den festgestellten Risiken orientiert sind,
- die Wichtigkeit der einzelnen Geschäftsprozesse berücksichtigt wird und
- das Auditprogramm den Gültigkeitsbereich des zugehörigen ISMS abdeckt.

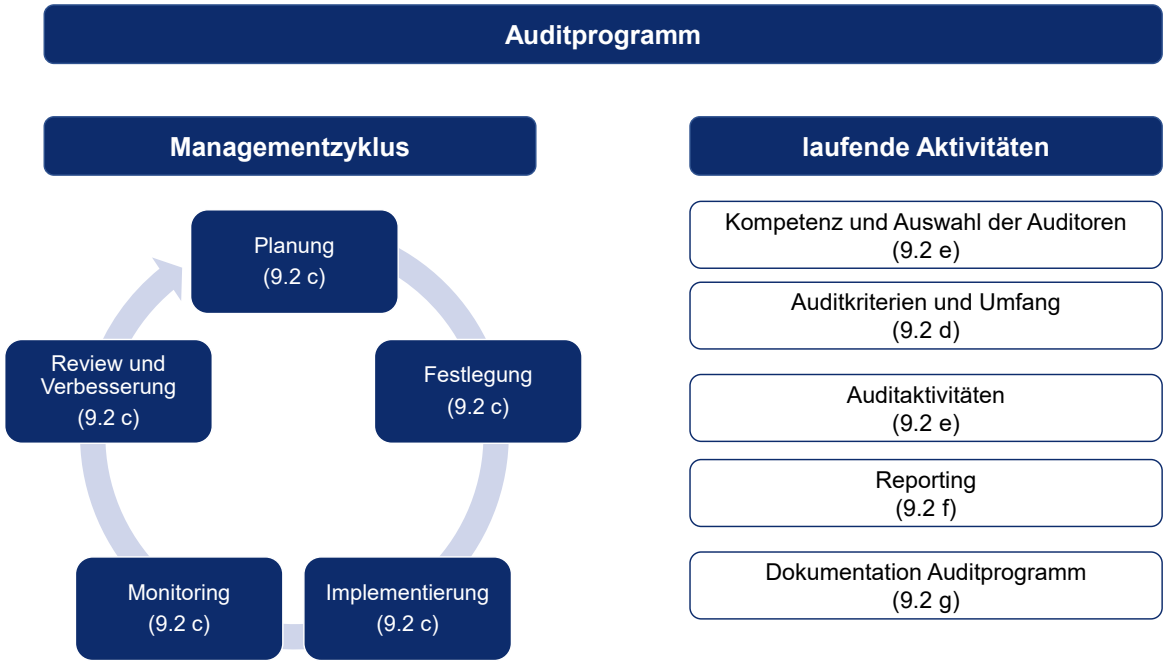


Abbildung 10 - Anforderungen an das Auditprogramm[27]

Teilprozess »Festlegung«

Der für das Auditprogramm verantwortliche Mitarbeiter muss u.a. folgende Aufgaben erfüllen:

- Festlegung und Implementierung des gesamten Auditprogramms
- Identifikation, Bewertung und Behandlung der direkt auf das Auditprogramm wirkenden Risiken (z.B. zu knappe Ressourcen, Lücken in der Qualifikation der Auditoren, zu große Betrachtungsbereiche für einzelne Audits)
- Etablierung von Prozessen für die Durchführung von Audits
- Bestimmung und Beschaffung der erforderlichen Ressourcen
- Bestimmung der Audits und Festlegung der Bereiche und Kriterien für die einzelnen Audits
- Festlegung der anzuwendenden Methoden und Werkzeuge
- Auswahl der Auditoren mit Sicherstellung ihrer Qualifikation und Erfahrung
- Gewährleistung, dass Unterlagen zum Auditprogramm stets aktuell geführt werden
- Laufende Überwachung und Verbesserung des Auditprogramms selbst

Teilprozess »Implementierung«

Zur Implementierung und Durchführung des Auditprogramms sind die während der Festlegung getroffenen Entscheidungen umzusetzen.

Ob hier bereits Ziele und der Umfang für einzelne Audits festgelegt werden, hängt von der jeweiligen Ausgestaltung bzw. dem Detaillierungsgrad des Auditprogramms ab. Ziele und Umfang von Audits ergeben sich generell aus den individuellen Anforderungen und dem Schutzbedarf der betroffenen IT-Systeme.

Es ist sehr empfehlenswert, die zu auditierenden Bereiche so zu wählen, dass sie einzeln und mit überschaubarem Aufwand auditiert werden können. Weitere Faktoren für die Auswahl der zu auditierenden Bereiche sind Kritikalität der Geschäfts- bzw. Serviceprozesse und der jeweils als tolerabel festgelegte Zeitraum zwischen zwei Audits. Die Summe der auditierten Bereiche muss (innerhalb von drei Jahren) selbstverständlich mit dem Geltungsbereich des ISMS übereinstimmen.

Teilprozess »Monitoring«

Im Teilprozess »Monitoring« ist das Auditprogramm selbst fortlaufend hinsichtlich Qualität und Effizienz zu überwachen. Es ist u.a. zu hinterfragen, ob

- das Auditprogramm nach wie vor am Geltungsbereich des ISMS und den Geschäftsanforderungen ausgerichtet ist,
- die Zeit- und die Ressourcenplanung passend bzw. angemessen ausgelegt sind,

27 Verweise in Klammern beziehen sich auf den Abschnitt 9.2 der Norm ISO/IEC 27001:2022.

- die »richtigen« Prozesse/Bereiche/Anwendungen/Systeme/Daten auditiert werden und
- die Prüftiefe sowie die Art der Prüfungen geeignet sind, die Ziele optimal zu unterstützen.

Es ist hilfreich, den Aufwand je Audit zu dokumentieren. Da der Aufwand je nach Eigenschaft des IT-Systems und/oder der betroffenen Organisationseinheit variieren kann, werden so Daten gesammelt, um die Aufwände für zukünftige Audits besser abschätzen zu können.

Bei der Überwachung der Leistungen der Mitglieder des Auditteams ist es wichtig, auf die Qualität, beispielsweise die Sachlichkeit, die Übersichtlichkeit und die Nachvollziehbarkeit, der Auditergebnisse zu achten. Relevant ist hier u.a., ob die für ein IT-System zuständige Fachabteilung zu festgestellten Mängeln nachvollziehbare, geeignete und vollständige Maßnahmenempfehlungen erhalten hat. Sind Maßnahmenempfehlungen nicht verstanden worden, weil z.B. Informationen fehlen oder Handlungsempfehlungen nicht passend sind, so sind dies Hinweise darauf, dass die Mitglieder des Auditteams zusätzliche fachliche oder methodische Unterstützung benötigen.

Zu diesem Teilprozess gehört auch die Erfassung und Auswertung des Feedbacks des Managements, der auditierten Bereiche bzw. Organisationseinheiten, der Auditoren und anderer Stakeholder.

Teilprozess »Review und Verbesserung«

Im Teilprozess »Review und Verbesserung« prüfen die für das Auditprogramm verantwortlichen Personen regelmäßig, ob die Erwartungen der Stakeholder nach wie vor erfüllt werden. Ausgangsbasis sind die Informationen, die im Teilprozess »Monitoring« gesammelt wurden. Weiterhin ist die kontinuierliche fachliche und methodische Weiterentwicklung der Auditoren festzustellen und zu steuern.[28]

Der Status des Auditprogramms ist an das verantwortliche Management zu berichten. Zweckmäßig ist hier zudem die Einführung von KPIs, um das Qualitätsniveau des Auditprogramms und der internen Audits insgesamt messbar und vergleichbar zu machen. Qualitätsaussagen wie z.B. »Anteil der von Fachbereichen akzeptierten und zur Umsetzung eingeleiteten Maßnahmen« sind gegenüber reinen Zeitaussagen wie z.B. »pro Audit aufgewendete Arbeitszeit« zu bevorzugen.

Kompetenz und Auswahl der Auditoren

- Die Auswahl der ISMS-Auditoren sollte so erfolgen, dass die notwendige Objektivität, Expertise und Unparteilichkeit im Auditprozess sichergestellt sind.
- Die notwendigen Kompetenzen eines internen Auditors sollten beschrieben sein (z.B. in einer Rollen- bzw. Stellenbeschreibung).

Planung und Durchführung von Audits

Durch Audits werden sowohl Nichtkonformitäten zu bestehenden Vorgaben als auch potenzielle bisher unbekannte Schwachstellen und Gefährdungen identifiziert.

- Bei der Auditplanung gilt: Ohne dedizierten Auditauftrag kein Audit. Das heißt, die eigentlichen Arbeiten werden erst dann aufgenommen, wenn die Beauftragung gesichert und formal kommuniziert ist. Zudem sollte der zu auditierende Bereich aktiv in die Auditplanung einbezogen werden, beispielsweise zur Abstimmung des Scopes (gegen was wird geprüft), der zeitlichen Planung und der Verfügbarkeit von Ansprechpartnern während des Audits.
- Sofern möglich sind bereits im Audit (Sofort-)Maßnahmen für die angemessene Behandlung von Gefährdungen abzuleiten. Die Umsetzung muss allerdings formal mit den jeweiligen Service-, System- und/oder Risikoeigentümern abgestimmt werden.
- Werden bisher unbekannte prozessimmanente Defizite oder Risiken identifiziert, deren Behandlung kurzfristig nicht möglich ist, sind diese im zentralen Risikoinventar aufzunehmen.
- Auditergebnisse müssen der Leitungsebene des ISMS (zumindest in konsolidierter Form) regelmäßig gemeldet werden.
- In Auditberichten ist eindeutig zu vermerken, welche Systeme und Dokumente geprüft bzw. gesichtet und als Basis für die Audits verwendet wurden.
- Eine offene und über die gesamte Dauer eines Audits aufrechterhaltene Kommunikation trägt wesentlich dazu bei, Vorbehalte beim auditierten Bereich abzubauen, und senkt damit das Risiko, dass Informationen zurückgehalten oder nicht realitätsgetreu dargestellt werden.[29]
- Um die Eignung, Vollständigkeit und Wirksamkeit der umgesetzten Maßnahmen festzustellen, werden in der Regel durch den Auditor die maßgeblich mit dem Betrieb und der Überwachung dieser Maßnahmen beauftragten Mitarbeiter direkt befragt, die Dokumentation geprüft und/oder praktische Vorführungen veranlasst und beurteilt. Von den Auditoren werden dabei ein umfangreiches technisches Wissen und methodisches Können gefordert. Es ist daher angebracht, die Auditoren auf Basis der Ziele und Inhalte des jeweiligen Audits auszuwählen.

28 Siehe auch Abschnitt 7 der ISO/IEC 19011:2018.

29 Siehe auch »Communication – The Missing Piece«, ISACA Journal 3/2012 *(https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/archives/journal-volume-3-2012.pdf).*

- Im Kontext der Planung einzelner Audits, d. h. vor Beginn der Durchführung, muss durch die verantwortlichen Leitungsebenen die Übernahme der entstehenden Kosten geklärt werden.
- Spätestens im Abschlussmeeting eines Audits sind die Ergebnisse gemeinsam mit dem auditierten Bereich durchzusprechen, da dieser die Feststellungen und Maßnahmenempfehlungen verstehen und akzeptieren sollte. Eine formale Abnahme des Auditberichts sollte angestrebt werden. Meinungsverschiedenheiten, die nicht aufgelöst werden können, sind im Bericht zu dokumentieren.
- Es ist sicherzustellen, dass die relevanten Informationen und Auditberichte vertraulich behandelt und vor unberechtigtem Zugriff geschützt aufbewahrt bzw. archiviert werden.
- Die Anforderungen aus Abschnitt 9.2 an interne Audits können durch die Umsetzung der Empfehlungen aus Abschnitt 6.4 der ISO/IEC 19011:2018 und ISO/ IEC 27007:2020 (siehe Kapitel 8.5 *Durchführung interner ISMS-Audits (Prozessschaubild)*, Seite 62) erfüllt werden, wobei zu beachten ist, dass die normativen Anforderungen nach ISO/IEC 27001:2022 bei Weitem nicht so umfangreich sind, wie in gängigen Best Practices beschrieben.
- Weitere Informationen bzgl. interner Audits sind z. B. im QAR-IT-Leitfaden der ISACA zu finden. Dieser Leitfaden ist zwar auf die interne IT-Revision ausgerichtet, kann jedoch sinngemäß auch für die internen ISMS-Audits angewendet werden.[30]

Abgrenzung interner ISMS-Audits zu Zertifizierungsaudits

Interne (ISMS-)Audits sind ein wesentliches Instrument im kontinuierlichen Verbesserungsprozess des Managementsystems. Über sie wird geprüft, ob das Managementsystem den eigenen Anforderungen der Organisation gerecht wird und wo Verbesserungspotenziale bestehen. Über das Auditprogramm wird sichergestellt, dass alle Bereiche des Geltungsbereichs wirksam durch das Managementsystem gesteuert werden.

Zertifizierungsaudits sind immer externe Audits. Sie werden von qualifizierten externen Auditoren im Namen einer Zertifizierungsstelle durchgeführt. Externe Auditoren arbeiten in der Regel auf der Basis der beiden Normen ISO/IEC 27006:2015 »Requirements for bodies providing audit and certification of information security management systems« und ISO/IEC 17021-1:2015 »Conformity assessment – Requirements for bodies providing audit and certification of management systems«.

Abgrenzung interner ISMS-Audits zum internen Kontrollsystem (IKS)

Das interne Kontrollsystem eines Unternehmens (IKS) stellt ein wesentliches Steuerungs- und Überwachungsinstrument dar. Aspekte des ISMS können ein Bestandteil des internen Kontrollsystems sein, jedoch geht das IKS in der Regel weit über das ISMS hinaus und umfasst vor allem auch fachliche Prozesskontrollen.

Bei einem IKS unterscheidet man zwischen prozessintegrierten und prozessunabhängigen Kontrollaktivitäten. Bei den erstgenannten handelt es sich üblicherweise um Kontrollmaßnahmen, die aus der Risikoanalyse, aus guten Managementpraktiken oder internen und externen Vorgaben resultieren (z. B. Vieraugenprinzip bei Buchungsfreigabe, Multifaktor-Authentifizierung für kritische Benutzer usw.) und somit die Empfehlungen der ISO/IEC 2700x als Ursprung haben können. Hierbei handelt es sich um die sogenannte »erste Verteidigungslinie«, die die Ordnungsmäßigkeit von Prozessen und Aktivitäten im Unternehmen sicherstellen soll und durch die direkte Leitungsebene wahrgenommen wird.

Die Wirksamkeit der Kontrollmaßnahmen kann weiterhin beispielsweise durch ein ISMS außerhalb der IT oder eine Compliance-Funktion prozessunabhängig überprüft werden. Dies wird in der Praxis oft als »zweite Verteidigungslinie« bezeichnet. Diese Überprüfung ersetzt nicht die Tätigkeit der Internen Revision, die wiederum die Wirksamkeit des gesamten IKS als sogenannte »dritte Verteidigungslinie« prüfen soll.

- Sofern ein IKS bereits etabliert ist oder sich im Aufbau bzw. in Veränderung befindet, lohnt es sich zu prüfen, ob und inwieweit die Kontroll- und Auditanforderungen des ISMS dort berücksichtigt oder ggf. sogar teilweise integriert werden können. Eine vollständige Integration wird in der Praxis nicht möglich sein, da sich die Ziele der beiden Systeme substanziell unterscheiden. Organisatorische Schnittstellen zum IKS und zur Internen Revision sind allerdings in jedem Fall empfehlenswert.
- Zur Modellierung eines IKS kommen in der Praxis z. B. COSO oder COBIT zum Einsatz.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Dokumentation des Auditprogramms bzw. der Auditprogramme (Abschnitt 9.2 g)
- Dokumentation der Auditergebnisse (Abschnitt 9.2 g)

30 Siehe *https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf.*

Referenzen

ISO/IEC 27001:2022 – Abschnitt 9.2

ISO/IEC 19011:2018

ISO/IEC 27006:2015

ISO/IEC 27007:2020

ISO/IEC 17021-1:2015

3.13 Incident Management

Obwohl es im normativen Teil der Norm nicht explizit erwähnt wird, ist das Management von Informationssicherheitsvorfällen ein weiterer elementarer Baustein eines gut funktionierenden ISMS.

Sicherheitsrelevante Vorfälle sind in der Regel Nichtkonformitäten, die, sofern ihren Ursachen auf den Grund gegangen wird, einen entscheidenden Einfluss auf den kontinuierlichen Verbesserungsprozess (KVP) und den Reifegrad des ISMS haben. Denn letztlich gilt: Nur wer Fehler erkennt und aus ihnen lernt, d.h. seine Aktivitäten und Strategien überdenkt und beispielsweise unwirksame Maßnahmen entfernt oder ersetzt, bestehende (Sicherheits-)Konzepte anpasst oder neue (Sicherheits-)Maßnahmen umsetzt, der erhält langfristig auch den bestmöglichen Nutzen eines innerhalb »unvorhersehbarer« Rahmenbedingungen (= Risiken) betriebenen Managementsystems.

Erfolgsfaktoren aus der Praxis

Um die Informationssicherheit im operativen Betrieb aufrechtzuerhalten, ist es unumgänglich, die Behandlung von Informationssicherheitsvorfällen bestmöglich zu antizipieren, d.h. bereits im Vorfeld Verantwortlichkeiten, Abläufe und Behandlungsoptionen festzulegen und auch einzuüben.

Das grundsätzliche Ziel des Prozesses zur Behandlung von Informationssicherheitsvorfällen ist ein weitgehend koordiniertes, zielgerichtetes und damit effizientes Handeln beim Eintreten einer tatsächlichen Sicherheitsverletzung oder eines gezielten Cyberangriffs (siehe Abbildung 11).

- In diesem Kapitel wird »nur« das Thema »Informationssicherheitsvorfälle« adressiert. Für die Erarbeitung eines ganzheitlichen Notfallvorsorgesystems wird auf die ISO 22301:2019 »Security and resilience – Business continuity management systems – Requirements« verwiesen.
- Die Organisation muss eine für sich sinnvolle Kategorisierung für Vorfälle festlegen, die eine praktikable und vernünftige Abgrenzung des Schweregrads ermöglicht, beispielsweise Unterscheidung zwischen Störungen, Sicherheitsvorfällen, Notfällen und Krisen.
- Es sollte ein entsprechender »Incident Response Plan« (Behandlungsplan) entwickelt werden, in dem die wesentlichen Abläufe festgeschrieben werden (siehe ISO/IEC 27001:2022, Annex 5.24). Dieser kann zwar nicht jede Eventualität abdecken, dient aber beim Eintritt eines Vorfalls als Orientierung und sorgt für ein zielgerichtetes Vorgehen.
- Im Notfall funktioniert nur das, was bereits zuvor kommuniziert und mehrfach geübt wurde. Wer sich stattdessen darauf verlässt, dass die jeweils betroffenen Mitarbeiter (welche sind das?) »im Falle eines Falles« noch wissen, an welcher Stelle sie in ihrem Behandlungsplan nachschlagen müssen (wo war der noch mal abgelegt?), um ohne Umschweife den dortigen Anweisungen sofort und sachgerecht Folge zu leisten, und dass die laut Plan verantwortlichen Führungskräfte ebenfalls wissen, was mit den auf sie einströmenden Informationen zu tun ist, der ist bei Eintritt eines echten Sicherheitsvorfalls nur wenig besser vorbereitet als jemand »ohne Plan« – zumindest für die ersten Minuten bzw. Stunden. Allerdings kommt es »im Falle eines Falles« genau auf die an. Daher reicht es nicht aus, den Plan in der Schublade zu haben – er muss bekannt sein und das Vorgehen muss trainiert werden.
- Der Prozess zur Sicherheitsvorfallbehandlung und dessen Detaillierungsgrad sollte dem Risikoappetit der Organisation und den Rahmenbedingungen des ISMS Rechnung tragen.

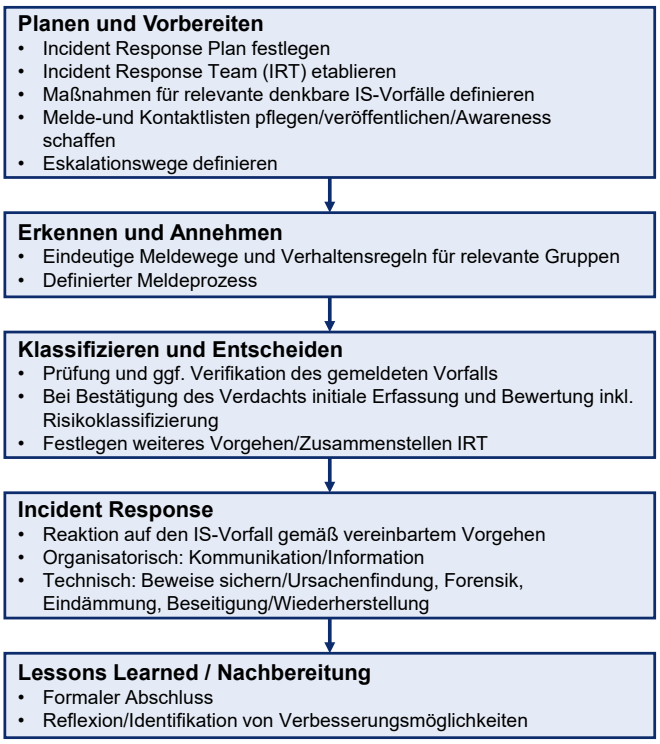


Abbildung 11: Incident Response Management – Phasenmodell angelehnt an ISO/IEC 27035-1:2023

Planen und Vorbereiten

Um das grundsätzliche Ziel des Prozesses zu erreichen, sind für alle operativen Phasen des Prozesses Präventivmaßnahmen zu treffen, die die Organisation und die Mitarbeiter auf einen solchen Fall bestmöglich vorbereiten. Neben generischen Problemlösungsstrategien sind vorab insbesondere Ansprechpartner und Eskalationswege zu definieren.

Erkennen und Annehmen

- Sicherheitsvorfälle sollten (unabhängig vom Eingangskanal) immer an einer zentralen Meldestelle eingehen. Allen relevanten Gruppen, bei denen IS-Vorfälle auftreten können, ist ein eindeutiger Meldeweg anzubieten, etwa Mitarbeitern, IT-Lieferanten, Kunden, Partnern.
- Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten inklusive Anlaufstellen/Meldeplänen sollten zielgerichtet bereitgestellt werden.

Klassifizieren und Entscheiden

- Die Meldestelle entscheidet, ob das gemeldete Ereignis tatsächlich ein Sicherheitsereignis darstellt oder ob es sich um ein Ereignis ohne Sicherheitsbezug, einen sogenannten »Known Error« (»Problem«), handelt, für den bereits eine Lösungsbeschreibung vorliegt, oder gar um einen Notfall, für den evtl. ein Notfallplan existiert. Im Zweifelsfall muss hier eine Eskalation (ggf. über einen »Manager on Duty«) erfolgen. Die Meldestelle ist entsprechend zu schulen.
- Alle einkommenden Vorfallsmeldungen sollten dokumentiert werden. Es sollten mindestens die nachfolgenden Informationen erfasst werden:
  - Eindeutige Identifikationsnummer
  - Datum der Annahme und Eintritt des Security Incident
  - Name(n) des/der Meldenden, Name(n) der betroffenen Person(en) und Identifikation(en) der Informationen/IT-Systeme
  - Beschreibung des Sicherheitsvorfalls (Wie ist der Angreifer vorgegangen, welche Schwachstellen wurden ausgenutzt? Bisher entstandener Schaden)
  - Gegebenenfalls bereits vorgenommene Sofortmaßnahmen
- Alle Sicherheitsvorfälle müssen nach einem vorab abgestimmten Klassifizierungsschema (initial) klassifiziert werden, sodass eine Priorität abgeleitet werden kann. Abhängig von der Priorität sind vorab definierte Sofortmaßnahmen einzuleiten und die verantwortlichen Personen (z. B. Informationssicherheitsbeauftragter, CISO) zu informieren.
- Die im (Ticket-)System dokumentierten Sicherheitsvorfälle sollten ggf. einem Monitoring unterliegen, sodass sichergestellt ist, dass auch niedrig klassifizierte Ereignisse bearbeitet werden.

Incident Response

In Bezug auf die Incident Response hat sich in der Praxis folgendes Vorgehen als effektiv erwiesen:

1. **Eindämmung und (initiale) Beweissicherung:** Analyse der Ausdehnung und Eindämmung des Sicherheitsvorfalls sowie (initiale) Sicherung potenzieller Hinweise und Belege, ggf. durch forensische Analysen und im Vorfeld festgelegte und geübte (!) Vorgehensweisen (siehe auch Control 5.28).

   Beispiele für lokale Maßnahmen zur Eindämmung:
   - Sperrung kompromittierter Benutzerkonten
   - Abschaltung angegriffener bzw. gefährdeter Dienste
   - Nutzung von Malware-Tools (Virenscanner, Anti-Spyware oder ähnliche Programme), um Systeme oberflächlich zu säubern
   - Beispiele im Netzwerk:
     - Kompromittierte Systeme vom restlichen Netzwerk isolieren und Zugriff auf ein Quarantänenetz beschränken
     - Sperren bestimmter Dienste und/oder Protokolle und ausgewählter IP-Adressen
2. **Beseitigung und Wiederherstellung:** Maßnahmen zur Wiederherstellung des Sollzustands einer Information/eines IT-Systems: In vielen Fällen kann dies über ein Restore des Backups erfolgen. Die Daten und Software werden in diesem Fall von »sauberen« Datensicherungsdateien auf »neuen« Systemen wiederhergestellt, wobei darauf zu achten ist, dass alle (im Backup evtl. noch vorhandenen) Schwachstellen geschlossen werden (ggf. Updates und Patches einspielen) und die Sicherungsdateien frei von Veränderungen durch einen Angreifer sind.

   Eine weitere Maßnahme kann z. B. die Aktualisierung von Systemsoftware und die Härtung der betroffenen Systeme sein.
3. **Ursachenfindung und (erweiterte) Beweissicherung:** Feststellung des Ursprungs (»root cause«) des Ereignisses und Sicherung potenzieller Hinweise und Belege, ggf. durch weiter gehende forensische Analysen

Lessons Learned/Nachbereitung

- Die Nachvollziehbarkeit zu einem Sicherheitsvorfall soll zu jeder Zeit gegeben sein. Das bedeutet, dass zu jedem Vorfall ersichtlich sein muss,
  - wie der aktuelle Status der Bearbeitung ist (z. B. Neu, Akzeptiert, In Arbeit, Angehalten, Gelöst, Abgeschlossen),

  - wer die mit der Bearbeitung beauftragten, ggf. zuständigen Mitarbeiter sind,
  - welche Maßnahmen zur Problemlösung (aktuell) geplant sind,
  - wann die Umsetzung der erforderlichen Maßnahmen vorgesehen ist.
- Alle dokumentierten Sicherheitsvorfälle müssen (nach Bearbeitung) einer Prüfung unterzogen werden, ob durch eine Optimierung im »Incident Response Plan« oder durch Änderungen in der Aufbau- und Ablauforganisation (u.a. Erstellung bzw. Anpassung von Handlungsanweisungen) in Zukunft ein besseres Handling ähnlich gelagerter Vorfälle erreicht werden kann.
- Bei der Bearbeitung von Sicherheitsvorfällen muss zum Abschluss immer dokumentiert werden, wie derartige Vorfälle in Zukunft zu vermeiden bzw. in ihrer Auswirkung zu minimieren sind. Daraus können ggf. weitere Maßnahmen abgeleitet werden, die in den Regelbetrieb zu überführen sind.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen keine Mindestanforderungen an die Dokumentation.

Jedoch haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Incident Response Plan (IRP), inklusive aktueller (!) Kontaktlisten und Eskalationspläne
- Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten
- Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen
- IS-Vorfallsberichte

Referenzen

ISO/IEC 27001:2022 – Abschnitte 5.24 – 5.28 und 6.8

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

ISO 22301:2019

3.14 Continual Improvement

Unabhängig davon, wie viele Leitfäden und Bücher bzgl. »optimaler« Managementsysteme geschrieben werden, wird es solche in der Praxis vermutlich nie geben, da Organisationen zu unterschiedlich sind, um diese mit einem einheitlichen »Kochrezept« zu bedienen. Darüber hinaus ändern sich ständig die Rahmenbedingungen, sodass es nie eine »für immer beste Lösung« geben kann.

Die Organisationen sind daher aufgefordert, die vorhandenen Best Practices zu analysieren und stetig an ihre Bedürfnisse angepasst anzuwenden. Insbesondere sind sie aufgefordert, aus ihren Nichtkonformitäten Verbesserungspotenziale abzuleiten und dadurch ihr ISMS stetig zu verbessern. Dieser Prozess wird kontinuierlicher Verbesserungsprozess (KVP) genannt.

Eine Organisation, die ein normkonformes ISMS betreiben möchte, muss folglich organisatorische Maßnahmen festlegen, auf deren Basis eine kontinuierliche Verbesserung gezielt und planmäßig stattfindet. Die Durchführung dieser Maßnahmen und die jeweiligen Ergebnisse sind hierbei zu überwachen und angemessen zu dokumentieren. Darüber hinaus hat die Organisation nachzuweisen, wie sie bei festgestellten Mängeln dafür sorgt, dass sich diese nicht wiederholen.

PDCA-(Plan-Do-Check-Act-)Zyklus

Die empfohlene Herangehensweise zur nachhaltigen Sicherstellung der kontinuierlichen Verbesserung des ISMS kann nach wie vor dem PDCA-Zyklus folgen, der die Basis vieler Managementsysteme darstellt.

- **Plan**
  - Etablierung von IS-Zielen und Verantwortlichkeiten für deren Erreichung
  - Etablierung der Sicherheitsmaßnahmen zur Erreichung der IS-Ziele und der operativen Prozessverantwortlichen für diese Maßnahmen
  - Definition der Leistungsindikatoren, die eine Leistungsmessung gegen die IS-Ziele erlauben, und zugehöriger Monitoring-Maßnahmen
  - Definition des Prozesses zur Messung der Leistung inklusive der Messpunkte, Berechnungsmethode des Indikators und der Norm- und Toleranzbereiche
  - Definition der Korrekturmaßnahmen, um die Sicherheitsmaßnahme im Normbereich zu regeln
- **Do**
  - Kontinuierliche Messung der IS-Zielerreichung
  - Einleitung von Korrekturen bei festgestellten Mängeln oder Nichtkonformitäten
- **Check**
  - Überwachen der einzelnen Sicherheitsmaßnahmenindikatoren und Vergleichen der einzelnen Leistungsfähigkeiten mit den IS-Zielen
  - Überwachung der eingeleiteten Maßnahmen hinsichtlich Umsetzung und ihrer Effektivität
  - Erstellen von Sicherheitsberichten mit Key-Performance-Indikatoren für das Management, basierend auf den IS-Zielen. Diese Berichte sollten Handlungsoptionen für notwendige Managemententscheidungen zur Stärkung der Sicherheitsmaßnahmen, die regelmäßig in den Toleranzbereich laufen oder den Schwellwert zur Ineffektivität überschreiten, enthalten.

- **Act**
  - Treffen von notwendigen Managemententscheidungen, um die Effektivität von Sicherheitsmaßnahmen wiederherzustellen. Entscheidungen werden an den operativen Betrieb zur Umsetzung weitergegeben.
  - Die getroffenen Entscheidungen werden mit Begründungen angemessen dokumentiert, beispielsweise über das Security Controlling.

Erfolgsfaktoren aus der Praxis

Die Verbesserung des ISMS erfolgt in der Regel durch die Identifikation von Abweichungen zu den Anforderungen sowie durch daraus abgeleitete Korrekturmaßnahmen. Es ist allerdings auch denkbar, dass Verbesserungsvorschläge direkt bewertet und umgesetzt werden, also ohne eine vorliegende Abweichung.

Mögliche Quellen für Abweichungen und Verbesserungsvorschläge

- Schlussfolgerungen aus KPIs – Analysen und Messungen
- Nachbereitung von Sicherheitsvorfällen
- Ergebnisse von (internen) Audits
- Managementreview und Steuerung durch die Leitung
- Betriebliches Vorschlagswesen (Verbesserungsvorschlag)
- Abgeleitete Maßnahmen aus der Risikobehandlung
- Maßnahmen aus dem KVP sollten in einen übergreifenden Umsetzungsplan aufgenommen werden, sodass eine zentrale konsolidierte oder zumindest eine geschäftsbereichsweite Liste mit Maßnahmen existiert.
- Des Weiteren führen die regelmäßig vorzunehmenden Risikoanalysen zu einer ständigen Verbesserung des ISMS. Die Ergebnisse der Risikobehandlung stellen einen wesentlichen Bestandteil der Verbesserung des ISMS dar, da hierbei risikominimierende Maßnahmen identifiziert und in Risikobehandlungspläne zur Umsetzung aufgenommen werden.
- Der übergreifende Umsetzungsplan erleichtert das Monitoring zum Umsetzungsstatus und zur Fälligkeit von Umsetzungsterminen sowie die erforderliche Überprüfung der Wirksamkeit einer umgesetzten Maßnahme.
- Korrektur vs. Korrekturmaßnahme: Bei Feststellung von Mängeln und Nichtkonformitäten muss die Organisation reagieren und diese korrigieren bzw. abstellen (siehe Abschnitte 10.1 a und b). Durch Korrekturen werden nichtkonforme Situationen bereinigt bzw. beseitigt. Um das erneute Auftreten desselben Fehlers zu verhindern, ist es erforderlich, eine nachhaltige Ursachenforschung zu betreiben und Korrekturmaßnahmen festzulegen (engl.: corrective actions; siehe Abschnitte 10.1 c bis g).

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2022 bestehen folgende Mindestanforderungen an die Dokumentation:

- Nachweise über die Art von Nichtkonformitäten sowie über umgesetzte Maßnahmen (Abschnitt 10.1 f)
- Nachweise über die Wirksamkeit einer Maßnahmenumsetzung (Abschnitt 10.1 d)
- Nachweise über die Resultate zu sämtlichen korrigierenden Maßnahmen (Abschnitt 10.1 g)

Darüber hinaus haben sich in der Praxis folgende Dokumente als zielführend etabliert:

- Verfahren für Korrekturmaßnahmen (ab Abschnitt 10.1 c)
- Beschreibung des Incident-Managements und der Verfolgung von Korrekturmaßnahmen
- Dokumentations-Tool für die Nachverfolgung des Umsetzungsstatus und Überprüfung der Wirksamkeit von Maßnahmen

Referenzen

ISO/IEC 27001:2022 – Abschnitt 10

ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2021 – Annex SL

4 Integration und Operationalisierung von Managementsystemen

Integration von bestehenden Managementsystemen

Der bisherige Leitfaden konzentriert sich auf die Einführung eines ISMS, betrachtet aber nur am Rande die hierbei oft sinnvolle Integration des Managementsystems in bereits vorhandene Governance-Strukturen samt den damit einhergehenden Chancen und Herausforderungen, wie z. B. der Nutzung von Synergieeffekten durch Bündelung von Maßnahmen bzw. Control Sets.

In der Praxis besteht meist nicht die Möglichkeit oder besser gesagt die Notwendigkeit, ein ISMS isoliert als Insel einzuführen. Neben bereits anderen in der Organisation etablierten Managementsystemen, einschließlich ihrer Maßnahmen und Prozesse, sind auch weitere operative oder organisatorische Gegebenheiten zu berücksichtigen.

Alle Managementsysteme haben große Überschneidungen im Aufbau, internen und externen Anforderungen und damit auch Möglichkeiten, Synergien zu nutzen. Durch harmonisierte Anforderungen an die Managementsysteme können einzelne Maßnahmen managementsystemübergreifend eingesetzt werden, wie z. B. die Dokumentenlenkung oder eine integrative Anwendung von Risk Assessments. Damit lassen sich Aufwand und Risiko bei Einführung, Betrieb und Nachweisführung des Managementsystems reduzieren.[1]

In diesem Kapitel werden einige in den Unternehmen häufig wiederkehrende Herausforderungen sowie zugehörige sinnvolle Ansätze aufgezeigt. Es werden dabei explizit nicht nur neu einzuführende Managementsysteme, sondern auch mögliche Verbesserungspotenziale für etablierte Systeme adressiert. Denn aufgrund der immensen Zunahme von Cybersicherheitsbedrohungen in den letzten Jahren sowie der stark wachsenden Compliance-Anforderungen, insbesondere für international tätige Organisationen, müssen sich auch etablierte Systeme fragen, ob die aktuellen Regelungen/Prozesse noch zeitgemäß sind, um den wachsenden Aufgaben nicht nur effektiv, sondern auch effizient gerecht zu werden.

Anfragen der folgenden Art sind mittlerweile in ISMS-Abteilungen an der Tagesordnung:

- Bitte prüfen Sie, ob wir konform zum »China's Cyber Security Law« sind.
- Welche Sicherheitsmaßnahmen sind für die OT-Sicherheit relevant?[2]
- Ein Stakeholder/Großkunde möchte eine Sicherheits-Selbstbewertung nach ISO/NIST/BSI/VDA-ISA/EU-DSGVO durchführen lassen.

Eine neue Herausforderung ist demnach die Notwendigkeit, zeitnah auf eine wachsende Zahl von Compliance-Anforderungen zu reagieren, die oftmals im Wesentlichen gleiche oder zumindest ähnliche Maßnahmen wie die aus uns geläufigen Standards beinhalten.

In der Folge – als eine Art Bugwelle der Compliance-Anforderungslisten – wachsen auch die Mapping-Tabellen, in denen die jeweiligen Kontrollen, Benchmarks etc. miteinander in Beziehung gesetzt werden, um so bereits bewertete Umsetzungen in anderen Managementsystemen, wie z. B. dem IKS oder dem Datenschutz-Managementsystem, nutzen zu können.

In der Zwischenzeit haben einige Risikomanagement/Compliance/ISMS-Tool-Anbieter ihre Lösungen dahingehend angepasst, dass eigene Kontrollziele definiert werden können, die auf die Kontrollziele der diversen Standards verlinkt werden.

Dadurch kann man jederzeit den Reife- bzw. Erfüllungsgrad eines Standards prüfen und erkennt sofort, bei welchen Kontrollen des gewählten Standards noch offene Punkte bzw. Risiken existieren.

1 Siehe Annex SL.

2 Siehe *https://www.isaca.de/sites/default/files/isaca_leitfaden_cyber-sicherheits-check_ot.pdf, Seite 17 ff.*

Operationalisierung durch Etablierung einer »Corporate-Control-Datenbank«

Basierend auf dem Ansatz aus dem vorherigen Kapitel stellt die Einführung einer zentral gepflegten »Corporate-Control-Datenbank« ein Handlungsfeld im Sinne einer stetigen Verbesserung aller vorhandenen Managementsysteme dar.

In den meisten Organisationen haben die verantwortlichen Manager eines Managementsystems derzeit noch ihre eigenen Maßnahmen definiert, was dazu führt, dass viele Steuerungsmaßnahmen, z. B. sichere Löschung von Informationen, doppelt – wenn nicht sogar dreifach – an verschiedenen Stellen in der Organisation gepflegt werden, inklusive aller Folgemaßnahmen, wie z. B. Erhebung des Umsetzungsstatus, Auditierung, Prüfung der Wirksamkeit etc. Dies führt unweigerlich zu einem Mehraufwand und insbesondere beim fachlich für das Thema Verantwortlichen zu einem Unverständnis, da dieselben Fragestellungen von diversen Revisoren/Auditoren gestellt werden.

Auf die Verantwortlichen wirken auch branchen-, produkt- bzw. leistungsspezifische Normen, Standards und Best Practices ein, die sich oft schon untereinander konterkarieren. Diesen Anforderungen gerecht zu werden, wird insbesondere durch eine Vielzahl unterschiedlicher, manueller und isolierter Prozesse erschwert.

Durch die harmonisierte Struktur der Managementsysteme (nach Annex SL) wurden viele ISO-Managementsysteme integrationstauglich. Prominente Beispiele sind die ISO/IEC 27001, die ISO/IEC 27701, die ISO 22301. Auch weitere, nicht direkt IT-relevante Managementsysteme, wie z. B. Qualitätsmanagement, Arbeitsschutz und Umweltschutz, folgen der neuen Struktur und ermöglichen damit ein organisationsweites integriertes Managementsystem im Kontext GRC.

Eine Corporate-Control-Datenbank harmonisiert für den Nutzer Regeln über verschiedene Vorgaben und Richtlinien hinweg auf Basis eines gemeinsamen Rahmenwerks. Damit geht auch eine geänderte Vorgehensweise einher, bei der die Steuerungsmaßnahmen nicht mehr an Normen, sondern nach Themen ausgerichtet sind. Die Ausrichtung an Domänen (siehe unten) ist dafür zielführend.

Die Normen werden mithilfe einer Metaebene zugeordnet und gepflegt. Diese Metaebene ermöglicht somit für die gesamte Organisation konsolidiert vorliegende Maßnahmen[3]. Dies bringt den Vorteil, dass die Antworten zu anderen, vorher nicht betrachteten »Standards/Gesetzen/Best Practices« ersichtlich werden, selbst wenn man sich vorher nie mit der neuen Compliance-Anforderung auseinandergesetzt hat. Zugleich ermöglicht dies den Nutzern eine individualisierte branchen-, produkt- bzw. leistungsbezogene Zusammenstellung der Anforderungen sowie Kontrolle über deren Einhaltung.

Ergänzend beinhalten sie entsprechende Workflows und Schnittstellen, sodass Änderungen automatisiert eingebunden werden. Somit werden Governance-Vorgaben konsolidiert und in ein ganzheitliches Risiko- und Compliance- Management integriert. Die Qualität der Datenbank wächst dabei mit jeder neuen Bewertung eines Standards bzw. einer Norm.

Operationalisierung durch Ausrichtung der »Central Corporate Controls« an Domänen

In der Praxis hat es sich als sinnvoll erwiesen, die in der Organisation zu steuernden Aspekte in Domänen zu gruppieren und auszurichten, um eine thematisch klare Zuordnung und Verantwortlichkeit zu schaffen. Diese Domänen sollten sich in das übergeordnete Modell der Organisation in Bezug auf dessen Managementsysteme integrieren, wobei sich COBIT als Orientierung anbietet.

Zugrunde liegende Domänen aus dem Bereich Informationssicherheit könnten beispielsweise aus der ISO/IEC 27002 entnommen werden. Mit der neuen Version könnte etwa die Gruppierung nach der neuen Property »Cybersecurity Concepts« erfolgen. Alternativ wäre eine Gruppierung nach dem BSI IT-Grundschutz-Kompendium oder der NIST Special Publication 800-53 denkbar. Wichtig ist, dass alle im Fokus stehenden Bereiche abgedeckt werden.

Die Wahl der Control-Frameworks ist hierbei zweitrangig und sollte von der Organisation für ihre Zwecke, die letztendlich auch durch externe Vorgaben oder des Geschäftsmodells variieren können, angemessen gewählt werden. Ein Automobilhersteller bedient sich eher TISAX, für einen SaaS-Anbieter eignet sich z. B. eher die Cloud Control Matrix (CCM) der Cloud Security Alliance (CSA), wobei im behördlichen Umfeld primär das BSI-Kompendium dienlich sein wird.

Wie auch immer sich die Organisation entscheidet, mit entsprechender Softwareunterstützung oder manuellem Fleiß kann der letztendlich gewählte Standard über eine Metaebene gepflegt werden, sodass viele Standards zu großen Teilen berücksichtigt werden können. In diesem Ansatz ist der Domänenverantwortliche zuständig, Neuerungen, Anforderungskonflikte oder Unklarheiten an zentraler Stelle aufzulösen. Die Qualität der Datenbank wächst damit zunehmend mit jeder neuen Bewertung eines Standards bzw. einer Norm.

3 Siehe beispielhaft die Controls aus den Normen IDW PS 951, EU-DSGVO (ISO/IEC 27701:2019), ISMS (ISO/IEC 27002:2022), BCMS (ISO 22301:2019), QMS (ISO 9001:2015) bis hin zu IT/OT Operations Controls.

5 Glossar

ADV Auftragsdatenverarbeitung – die Verarbeitung von personenbezogenen Daten durch Dienstleister (extern oder intern durch rechtlich eigenständige Einheiten einer Unternehmensgruppe) gemäß Art. 28 EU-DSGVO

APT Advanced Persistent Threat

Asset Alles, was Wert für die Organisation hat, auch Informationsgut oder Informationswert genannt. Es gibt viele Asset-Typen, etwa: Informationen, Software, Hardware, Services, Menschen und ihre Qualifikationen, Kompetenzen und Erfahrungen sowie immaterielle Werte, wie Reputation und Image. ISO/IEC 27005:2022 unterscheidet zwischen primären und sekundären Assets, wobei die primären Assets Geschäftsprozesse und Geschäftsaktivitäten sowie Informationen umfassen. Sekundäre Assets unterstützen die primären Assets: etwa Einrichtungen, Räume, Hardware, Software, Netzwerk, Personal, Websites.

BCMS Business Continuity Management System

BCS Business Criticality Scorecard

BDEW Bundesverband der Energie- und Wasserwirtschaft

BIA Business Impact Analysis

BO Betriebsorganisation

BSI Bundesamt für Sicherheit in der Informationstechnik

BSIMM Building Security in Maturity Model

CCM Cloud Control Matrix

CERT Computer Emergency Response Team

CIO Chief Information Officer

CIS Center for Internet Security

CISO Chief Information Security Officer

COBIT Control Objectives for Information and Related Technology – ein international anerkanntes Framework zur IT-Governance mit Fokus auf IT-Prozesse und Kontrollziele

COSO Committee of Sponsoring Organizations of the Treadway Commission – eine US-amerikanische Organisation, die u.a. den anerkannten Standard für interne Kontrollen, das sogenannte COSO-Modell, entwickelt hat.

CSA Cloud Security Alliance

DSB Datenschutzbeauftragter

DSGVO siehe EU-DSGVO

EU Europäische Union

EU-DSGVO EU-Datenschutz-Grundverordnung

EWR Europäischer Wirtschaftsraum

GRC Governance, Risk and Compliance

ICT Information and Communications Technology

IEC International Electrotechnical Commission – eine internationale Normungsorganisation, die unter anderem den Standard ISO/IEC 2700x zusammen mit der ISO entwickelt hat.

IKS Internes Kontrollsystem

IRP Incident Response Plan

IRT Incident Response Team

IS Informationssicherheit, Information Security

ISA Information Security Assessments

ISAE International Standard on Assurance Engagements

ISB Informationssicherheitsbeauftragter

ISMS Information Security Management System – Teil des übergreifenden Managementsystems, basierend auf einem Geschäftsrisiko-Ansatz, zur Etablierung, Implementierung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit. Das Managementsystem beinhaltet die Organisationsstruktur, Policies, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Prozesse und Ressourcen.

ISO International Organization for Standardization – Herausgeber von internationalen Normen, u.a. der ISO/IEC 2700x-Familie

ISO Information Security Officer, synonym zum ISB

KCI Key-Control-Indikator

KPI Key-Performance-Indikator – ein Leistungsindikator

KRI Key-Risk-Indikator

KVP Kontinuierlicher Verbesserungsprozess

MaRisk Mindestanforderungen an das Risikomanagement – eine Verwaltungsanweisung zur Ausgestaltung des Risikomanagements in deutschen Kreditinstituten von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

NIST National Institute of Standards and Technology

NPS (Net Promoter Score) Kennzahl, die misst, inwiefern Konsumenten ein Produkt oder eine Dienstleistung weiterempfehlen würden.

OT Operational Technology

OWASP Open Web Application Security Project

PDCA Plan-Do-Check-Act-Zyklus – ein kontinuierlicher Verbesserungsprozess

QAR-IT ISACA-Leitfaden zur Durchführung eines Quality Assurance Review der internen IT-Revision (QAR-IT)

QMB Qualitätsmanagementbeauftragter

QMS Qualitätsmanagementsystem

QS Qualitätssicherung

RACI-Matrix Organisationen nutzen die Kategorisierung nach RACI, um zu beschreiben, welche Rolle für welche Aktivitäten verantwortlich ist und welche Rollen zu beteiligen sind. So kann man zu einer klaren Beschreibung der Verantwortlichkeiten und Zuständigkeiten gelangen. Dabei werden die Begriffe wie folgt interpretiert:

- *Responsible* – zuständig für die eigentliche Durchführung (Umsetzungsverantwortung). Die Person, die die Initiative für die Durchführung an andere gibt. Wird auch als Verantwortung im disziplinarischen und qualitativen Sinne interpretiert.
- *Accountable* – rechenschaftspflichtig (Gesamtverantwortung), verantwortlich im Sinne von »genehmigen«, »billigen« oder »unterschreiben«. Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt. Wird auch als Verantwortung aus Kostenstellensicht interpretiert.
- *Consulted* – konsultiert (fachliche Expertise). Eine Person, deren Rat eingeholt werden soll oder muss. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
- *to be Informed* – zu informieren (Informationsrecht). Eine Person, die Informationen über den Verlauf bzw. das Ergebnis der Tätigkeit erhält oder die Berechtigung besitzt, Auskunft zu erhalten.

In der Regel sollte pro Aktivität nur eine Person (Rolle) *accountable* sein. Dagegen können mehrere Personen bei einer Aktivität *responsible*, *consulted* oder *informed* sein. Ebenso kann es vorkommen, dass eine Person für eine Aktivität gleichzeitig *accountable* und *responsible* ist.

Risiko Wirkung von Ungewissheit auf Ziele (Definition nach ISO 31000:2018)

RPO Recovery Point Objective

RTO Recovery Time Objective

SaaS Software as a Service

Scope Geltungsbereich

SDLC Software Development Life Cycle

SIRP Security Incident Response Process

SLA Service Level Agreement – Vereinbarung zwischen Auftraggeber und Dienstleister

SMART Spezifisch, messbar, akzeptiert, realistisch, terminiert

SoA Statement of Applicability – dokumentierte Erklärung über die relevanten sowie anwendbaren Kontrollziele und Maßnahmen im ISMS der Organisation

SoD-Matrix Segregation-of-Duties-Matrix – Übersicht der zu berücksichtigenden Funktionstrennungen zwischen Rollen innerhalb der Organisation

TISAX Trusted Information Security Assessment Exchange

TMG Telemediengesetz

UWG Gesetz gegen den unlauteren Wettbewerb

VDA Verband der Automobilindustrie e.V.

Zero-Day-Schwachstelle Eine bislang nicht veröffentlichte und nicht korrigierte Schwachstelle, die ausgenutzt werden könnte, um Computeranwendungen, Daten oder andere Netzwerkdienste zu manipulieren oder anzugreifen.

6 Referenzen

Normen und Standards

ISO 9001:2015 Quality management systems – Requirements

ISO 19011:2018 Guidelines for auditing management systems

ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements

ISO 31000:2018 Risk management – Guidelines

IEC 31010:2018 Risk management – Risk assessment techniques

ISO Guide 73:2009 Risk management – Vocabulary

ISO/IEC 17021-1:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements

ISO/IEC 17021-2:2016 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 2: Competence requirements for auditing and certification of environmental management systems

ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls

ISO/IEC 27003:2017 Information technology – Security techniques – Information security management system – Guidance

ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks

ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2020 Information security, cybersecurity, and privacy protection – Guidelines for information security management systems auditing

ISO/IEC 27014:2020 Information security, cybersecurity, and privacy protection – Governance of information security

ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1:2021 Cybersecurity – Supplier relationships – Part 1: Overview and concepts

ISO/IEC 27036-2:2022 Cybersecurity – Supplier relationships – Part 2: Requirements

ISO/IEC 27036-3:2014 Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedure for the technical work – Procedures specific to ISO –, Annex SL, 2021

ISO/IEC TR 27023:2015 Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

Weitere Quellen

COBIT 2019 for Information Security, ISACA 2019

BDEW-Whitepaper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Version 2.0, Mai 2018

BSI-Standard 200-2, IT-Grundschutz-Vorgehensweise, Version 1.0, 2017

BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, 2017

IT-Grundschutz-Kompendium 2022, BSI, 2022

Leitfaden Cyber-Sicherheits-Check, Version 2, BSI/ISACA, 2020

SC27 Platinum Book – Twenty Years of ISO/IEC JTC1/SC27

Weblinks

www.bsi.bund.de

www.enisa.europa.eu

www.esma.europa.eu

www.isaca.de

www.isaca.org

www.iso27001security.com

www.iso.org

www.jtc1sc27.din.de

7 Abbildungs-/Tabellenverzeichnis

Abbildungen

Tabellen

8 Anlagen

8.1 Mapping Annex ISO/IEC 27001:2022 vs. Annex ISO/IEC 27001:2013

Die folgende Tabelle zeigt die Übereinstimmung der Maßnahmen aus ISO/IEC 27001:2022 mit ISO/IEC 27001:2013.

Mapping: ISO/IEC 27001:2022 vs. ISO/IEC 27001:2013		
ISO/IEC 27001:2022		**ISO/IEC 27001:2013**
5	**Organizational controls**	
5.1	Policies for information security	A.5.1.1, A.5.1.2
5.2	Information security roles and responsibilities	A.6.1.1
5.3	Segregation of duties	A.6.1.2
5.4	Management responsibilities	A.7.2.1
5.5	Contact with authorities	A.6.1.3
5.6	Contact with special interest groups	A.6.1.4
5.7	Threat intelligence	Neu
5.8	Information security in project management	A.6.1.5, A.14.1.1
5.9	Inventory of information and other associated assets	A.8.1.1, A.8.1.2
5.10	Acceptable use of information and other associated assets	A.8.1.3, A.8.2.3
5.11	Return of assets	A.8.1.4
5.12	Classification of information	A.8.2.1
5.13	Labelling of information	A.8.2.2
5.14	Information transfer	A.13.2.1, A.13.2.2, A.13.2.3
5.15	Access control	A.9.1.1, A.9.1.2
5.16	Identity management	A.9.2.1
5.17	Authentication information	A.9.2.4, A.9.3.1, A.9.4.3
5.18	Access rights	A.9.2.2, A.9.2.5, A.9.2.6
5.19	Information security in supplier relationships	A.15.1.1
5.20	Addressing information security within supplier agreements	A.15.1.2
5.21	Managing information security in the ICT supply chain	A.15.1.3
5.22	Monitoring, review and change management of supplier services	A.15.2.1, A.15.2.2
5.23	Information security for use of cloud services	Neu
5.24	Information security incident management planning and preparation	A.16.1.1
5.25	Assessment and decision on information security events	A.16.1.4
5.26	Response to information security incidents	A.16.1.5
5.27	Learning from information security incidents	A.16.1.6
5.28	Collection of evidence	A.16.1.7
5.29	Information security during disruption	A.17.1.1, A.17.1.2, A.17.1.3
5.30	ICT readiness for business continuity	Neu
5.31	Identification of legal, statutory, regulatory, and contractual requirements	A.18.1.1, A.18.1.5

→

5	Organizational controls (Fortsetzung)	
5.32	Intellectual property rights	A.18.1.2
5.33	Protection of records	A.18.1.3
5.34	Privacy and protection of PII	A.18.1.4
5.35	Independent review of information security	A.18.2.1
5.36	Compliance with policies and standards for information security	A.18.2.2, A.18.2.3
5.37	Documented operating procedures	A.12.1.1
6	**People controls**	
6.1	Screening	A.7.1.1
6.2	Terms and conditions of employment	A.7.1.2
6.3	Information security awareness, education and training	A.7.2.2
6.4	Disciplinary process	A.7.2.3
6.5	Responsibilities after termination or change of employment	A.7.3.1
6.6	Confidentiality or non-disclosure agreements	A.13.2.4
6.7	Remote working	A.6.2.2
6.8	Information security event reporting	A.16.1.2, A.16.1.3
7	**Physical controls**	
7.1	Physical security perimeter	A.11.1.1
7.2	Physical entry controls	A.11.1.2, A.11.1.6
7.3	Securing offices, rooms and facilities	A.11.1.3
7.4	Physical security monitoring	Neu
7.5	Protecting against physical and environmental threats	A.11.1.4
7.6	Working in secure areas	A.11.1.5
7.7	Clear desk and clear screen	A.11.2.9
7.8	Equipment siting and protection	A.11.2.1
7.9	Security of assets off-premises	A.11.2.6
7.10	Storage media	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5
7.11	Supporting utilities	A.11.2.2
7.12	Cabling security	A.11.2.3
7.13	Equipment maintenance	A.11.2.4
7.14	Secure disposal or re-use of equipment	A.11.2.7
8	**Technological controls**	
8.1	User endpoint devices	A.6.2.1, A.11.2.8
8.2	Privileged access rights	A.9.2.3
8.3	Information access restriction	A.9.4.1
8.4	Access to source code	A.9.4.5
8.5	Secure authentication	A.9.4.2
8.6	Capacity management	A.12.1.3
8.7	Protection against malware	A.12.2.1
8.8	Management of technical vulnerabilities	A.12.6.1, A.18.2.3
8.9	Configuration management	Neu
8.10	Information deletion	Neu

→

8	Technological controls (Fortsetzung)	
8.11	Data masking	Neu
8.12	Data leakage prevention	Neu
8.13	Information backup	A.12.3.1
8.14	Redundancy of information processing facilities	A.17.2.1
8.15	Logging	A.12.4.1, A.12.4.2, A.12.4.3
8.16	Monitoring activities	Neu
8.17	Clock synchronization	A.12.4.4
8.18	Use of privileged utility programs	A.9.4.4
8.19	Installation of software on operational systems	A.12.5.1, A.12.6.2
8.20	Network controls	A.13.1.1
8.21	Security of network services	A.13.1.2
8.22	Segregation in networks	A.13.1.3
8.23	Web filtering	Neu
8.24	Use of cryptography	A.10.1.1, A.10.1.2
8.25	Secure development lifecycle	A.14.2.1
8.26	Application security requirements	A.14.1.2, A.14.1.3
8.27	Secure system architecture and engineering principles	A.14.2.5
8.28	Secure coding	Neu
8.29	Security testing in development and acceptance	A.14.2.8, A.14.2.9
8.30	Outsourced development	A.14.2.7
8.31	Separation of development, test and production environments	A.12.1.4, A.14.2.6
8.32	Change management	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
8.33	Test information	A.14.3.1
8.34	Protection of information systems during audit and testing	A.12.7.1

Die folgende Tabelle zeigt die Übereinstimmung der Maßnahmen aus ISO/IEC 27001:2013 mit ISO/IEC 27001:2022.

Mapping: ISO/IEC 27001:2013 vs. ISO/IEC 27001:2022		
ISO/IEC 27001:2013		**ISO/IEC 27001:2022**
A.5	**Information security policies**	
A.5.1.1	Policies for information security	5.1
A.5.1.2	Review of the policies for information security	5.1
A.6	**Organization of information security**	
A.6.1.1	Information security roles and responsibilities	5.2
A.6.1.2	Segregation of duties	5.3
A.6.1.3	Contact with authorities	5.5
A.6.1.4	Contact with special interest groups	5.6
A.6.1.5	Information security in project management	5.8
A.6.2.1	Mobile device policy	8.1
A.6.2.2	Teleworking	6.7
A.7	**Human Resource Security**	
A.7.1.1	Screening	6.1
A.7.1.2	Terms And Conditions Of Employment	6.2
A.7.2.1	Management Responsibilities	5.4
A.7.2.2	Information Security Awareness, Education And Training	6.3
A.7.2.3	Disciplinary Process	6.4
A.7.3.1	Termination Or Change Of Employment Responsibilities	6.5
A.8	**Asset Management**	
A.8.1.1	Inventory of assets	5.9
A.8.1.2	Ownership of assets	5.9
A.8.1.3	Acceptable use of assets	5.10
A.8.1.4	Return of assets	5.11
A.8.2.1	Classification of information	5.12
A.8.2.2	Labelling of information	5.13
A.8.2.3	Handling of assets	5.10
A.8.3.1	Management of removable media	7.10
A.8.3.2	Disposal of media	7.10
A.8.3.3	Physical media transfer	7.10
A.9	**Access Control**	
A.9.1.1	Access Control Policy	5.15
A.9.1.2	Access To Networks And Network Services	5.15
A.9.2.1	User Registration And De-Registration	5.16
A.9.2.2	User Access Provisioning	5.18
A.9.2.3	Management Of Privileged Access Rights	8.2
A.9.2.4	Management Of Secret Authentication Information Of Users	5.17
A.9.2.5	Review Of User Access Rights	5.18
A.9.2.6	Removal Or Adjustment Of Access Rights	5.18

→

A.9	Access Control (Fortsetzung)	
A.9.3.1	Use Of Secret Authentication Information	5.17
A.9.4.1	Information Access Restriction	8.3
A.9.4.2	Secure Log-On Procedures	8.5
A.9.4.3	Password Management System	5.17
A.9.4.4	Use Of Privileged Utility Programs	8.18
A.9.4.5	Access Control To Program Source Code	8.4
A.10	**Cryptography**	
A.10.1.1	Policy On The Use Of Cryptographic Controls	8.24
A.10.1.2	Key Management	8.24
A.11	**Physical And Environmental Security**	
A.11.1.1	Physical Security Perimeter	7.1
A.11.1.2	Physical Entry Controls	7.2
A.11.1.3	Securing Offices, Rooms And Facilities	7.3
A.11.1.4	Protecting Against External And Environmental Threats	7.5
A.11.1.5	Working In Secure Areas	7.6
A.11.1.6	Delivery And Loading Areas	7.2
A.11.2.1	Equipment Siting And Protection	7.8
A.11.2.2	Supporting Utilities	7.11
A.11.2.3	Cabling security	7.12
A.11.2.4	Equipment Maintenance	7.13
A.11.2.5	Removal Of Assets	7.10
A.11.2.6	Security Of Equipment And Assets Off-Premises	7.9
A.11.2.7	Secure Disposal Or Re-Use Of Equipment	7.14
A.11.2.8	Unattended User Equipment	8.1
A.11.2.9	Clear Desk And Clear Screen Policy	7.7
A.12	**Operations Security**	
A.12.1.1	Documented operating procedures	5.37
A.12.1.2	Change management	8.32
A.12.1.3	Capacity management	8.6
A.12.1.4	Separation of development, testing and operational environments	8.31
A.12.2.1	Controls against malware	8.7
A.12.3.1	Information backup	8.13
A.12.4.1	Event logging	8.15
A.12.4.2	Protection of log information	8.15
A.12.4.3	Administrator and operator logs	8.15
A.12.4.4	Clock synchronization	8.17
A.12.5.1	Installation of software on operational systems	8.19
A.12.6.1	Management of technical vulnerabilities	8.8
A.12.6.2	Restrictions on software installation	8.19
A.12.7.1	Information systems audit controls	8.34

→

A.13	**Communications Security**	
A.13.1.1	Network controls	8.20
A.13.1.2	Security of network services	8.21
A.13.1.3	Segregation in networks	8.22
A.13.2.1	Information transfer policies and procedures	5.14
A.13.2.2	Agreements on information transfer	5.14
A.13.2.3	Electronic messaging	5.14
A.13.2.4	Confidentiality or non-disclosure agreements	6.6
A.14	**System Acquisition, Development And Maintenance**	
A.14.1.1	Information Security Requirements Analysis And Specification	5.8
A.14.1.2	Securing Application Services On Public Networks	8.26
A.14.1.3	Protecting Application Services Transactions	8.26
A.14.2.1	Secure Development Policy	8.25
A.14.2.2	System Change Control Procedures	8.32
A.14.2.3	Technical Review Of Applications After Operating Platform Changes	8.32
A.14.2.4	Restrictions On Changes To Software Packages	8.32
A.14.2.5	Secure System Engineering Principles	8.27
A.14.2.6	Secure Development Environment	8.31
A.14.2.7	Outsourced Development	8.30
A.14.2.8	System Security Testing	8.29
A.14.2.9	System Acceptance Tests	8.29
A.14.3.1	Protection Of Test Data	8.33
A.15	**Supplier relationships**	
A.15.1.1	Information security policy for supplier relationships	5.19
A.15.1.2	Addressing security within supplier agreements	5.20
A.15.1.3	Information and communication technology supply chain	5.21
A.15.2.1	Monitoring and review of supplier services	5.22
A.15.2.2	Managing changes to supplier services	5.22
A.16	**Information Security Incident Management**	
A.16.1.1	Responsibilities And Procedures	5.24
A.16.1.2	Reporting Information Security Events	6.8
A.16.1.3	Reporting Information Security Weaknesses	6.8
A.16.1.4	Assessment Of And Decision On Information Security Events	5.25
A.16.1.5	Response To Information Security Incidents	5.26
A.16.1.6	Learning From Information Security Incidents	5.27
A.16.1.7	Collection Of Evidence	5.28
A.17	**Information Security Aspects Of Business Continuity Management**	
A.17.1.1	Planning Information Security Continuity	5.29
A.17.1.2	Implementing Information Security Continuity	5.29
A.17.1.3	Verify, Review And Evaluate Information Security Continuity	5.29
A.17.2.1	Availability Of Information Processing Facilities	8.14

→

A.18	Compliance	
A.18.1.1	Identification of applicable legislation and contractual requirements	5.31
A.18.1.2	Intellectual Property Rights	5.32
A.18.1.3	Protection Of Records	5.33
A.18.1.4	Privacy And Protection Of Personally Identifiable Information	5.34
A.18.1.5	Regulation Of Cryptographic Controls	5.31
A.18.2.1	Independent Review Of Information Security	5.35
A.18.2.2	Compliance With Security Policies And Standards	5.36
A.18.2.3	Technical Compliance Review	5.36, 8.8

8.2 Versionsvergleich ISO/IEC 27001/2:2022 vs. ISO/IEC 27001/2:2013

Nachfolgend finden Sie eine kurze Darstellung der wesentlichen inhaltlichen Änderungen der ISO/IEC 27001:2022 sowie der ISO/IEC 27002:2022 gegenüber den Vorgängerversionen aus dem Jahr 2013.

ISO/IEC 27001:2022 vs. ISO/IEC 27001:2013

Im Oktober 2022 wurde die dritte Edition der ISO/IEC 27001 veröffentlicht. Wie andere ISO/IEC-Standards, die Anforderungen an ein Managementsystem beschreiben (z. B. ISO 9001, ISO 14001, ISO 22301), folgt auch die ISO/IEC 27001 einem einheitlichen Aufbau, der sogenannten »*Harmonized Structure*« aus Annex SL der ISO/IEC Directives, Part 1. Da sich diese Struktur 2021 geändert hat, wurden die Hauptkapitel der ISO/IEC 27001:2022 entsprechend angepasst. Folgende Änderungen haben sich dadurch in den Hauptkapiteln[1] ergeben:

- Die Organisation (Kapitel 4 »*Context of the organization*«) hat nun zusätzlich zur Festlegung relevanter Anforderungen von interessierten Parteien auch zu definieren, welche dieser Anforderungen im Rahmen des ISMS adressiert werden (Abschnitt 4.2 c).
- Management von Änderungen (Kapitel 6 »*Planning*«) wurde in Abschnitt 6.2 »*Information security objectives and planning to achieve them*« um den Aspekt ergänzt, dass zusätzlich zu den Anforderungen an die Festlegung und Umsetzung von Informationssicherheitszielen diese auch überwacht werden müssen. Das Kapitel wurde ferner mit Abschnitt 6.3 »*Planning of changes*« zur Durchführung von geplanten Änderungen am ISMS erweitert. Die Umstände, die eine Änderung des ISMS erforderlich machen, können geplant oder ungeplant sein (wie in Abschnitt 6.1 »*Actions to address risks and opportunities*« beschrieben), aber die Änderungen selbst müssen geplant durchgeführt werden.
- In Kapitel 8 »*Operation*« wird in der neuen Fassung ergänzt, dass explizit Kriterien zur Umsetzung der Prozesse aus Kapitel 6 »*Planning*« zu etablieren sind und die Umsetzung gemäß diesen Kriterien zu erfolgen hat.
- In Kapitel 9 »*Performance evaluation*« wurden die Abschnitte 9.2 »*Internal Audit*« und 9.3 »*Management Review*« in weitere Unterabschnitte aufgeteilt, bleiben dabei aber inhaltlich identisch.
- Der Abschnitt 9.3 »*Management Review*« wurde in drei Unterabschnitte unterteilt. Hier wurde ergänzt, dass Managementreviews nun auch die Änderungen an Bedürfnissen und Erwartungen interessierter Parteien, die für das ISMS relevant sind, zu erfassen haben (Abschnitt 9.3.2 »*Management review inputs*«, *c)*.
- Kontinuierliche Verbesserung: Kapitel 10 wurde neu geordnet, sodass die Aussage, die Eignung, Angemessenheit und Wirksamkeit des ISMS kontinuierlich zu verbessern, vor dem Abschnitt über die Nichtkonformität steht, mit dem Ziel, Verbesserungen statt Korrekturmaßnahmen zu fördern.
- Die neue Version der ISO/IEC 27001:2022 enthält im Wesentlichen einen vollständigen Ersatz von Annex A, der die Controls der ISO/IEC 27002:2022 widerspiegelt. Der einzige Unterschied zwischen den Angaben im Annex der ISO/IEC 27001 und den Controls aus der ISO/IEC 27002 liegt in der Formulierung der Anforderungen: Im Annex der ISO/IEC 27001:2022 wird das Wort »shall« verwendet, die Controls sind hier somit obligatorisch formuliert, während die ISO/IEC 27002 das Wort »should« verwendet, die Anforderungen sind also hier als Empfehlung zu verstehen.
- Die im Annex aufgeführten Controls erheben nach wie vor keinen Anspruch auf Vollständigkeit und es können zusätzliche Maßnahmen erforderlich sein. Es steht Unternehmen außerdem wie bisher frei, die Maßnahmen aus anderen Quellen (z. B. NIST Cybersecurity Framework, BSI IT-Grundschutz, ISF Standard of Good Practice etc.) zu verwenden, um ihre Informationssicherheitsrisiken zu mindern. In diesem Fall ist lediglich eine Erklärung zur Anwendbarkeit zu erstellen, die ein Mapping von den gewählten Maßnahmen zu den Controls aus dem Annex der ISO/IEC 27001:2022 sowie die erforderlichen Gründe zur Auswahl enthält. Dadurch wird bestätigt, dass keine Anforderungen vernachlässigt wurden, die tatsächlich anwendbar und notwendig sind, um vorliegende Risiken zu mindern (vgl. ISO/IEC 27001:2022, Abschnitt 6.1.3 »*Information security risk treatment*«, (b) sowie Anmerkung 2 von Abschnitt 6.1.3; (c) wurde leicht geändert, um diesen Aspekt noch klarer herauszustellen).

ISO/IEC 27002:2022 vs. ISO/IEC 27002:2013

In der neuen Version der ISO/IEC 27002:2022 fällt bereits die Änderung des **Titels** von »Information technology – Security techniques – Code of practice for information security controls« zu »Information security, cybersecurity and privacy protection – Information security controls« auf. Der Begriff »Code of Practice« wurde entfernt, um seinen Zweck als tonangebendes Referenzwerk für Maßnahmen der Informationssicherheit besser widerzuspiegeln. Neben dem Wort »Information Security« werden die Begriffe »Cyber Security« und »Privacy Protection« hervorgehoben. Infolgedessen werden in der neuen Fassung Cyber-Security-Maßnahmen als Teilmenge von Informationssicherheits-Maßnahmen und Datenschutz-Maßnahmen explizit adressiert.

1 Im Folgenden wird der Begriff »Kapitel« auch für die ISO/IEC 27001:2013 verwendet.

Die ISO/IEC 27002:2013 wurde inhaltlich wesentlich erweitert: Die 2013er-Norm besteht aus insgesamt 80 Seiten (zuzüglich 10 Seiten Inhaltsverzeichnis und Vorwort), wohingegen die aktualisierte Version 131 Seiten (zuzüglich 10 Seiten Inhaltsverzeichnis und Vorwort sowie 17 Seiten Annex) umfasst. Die Norm aus 2013 enthält Verweise auf 27 andere ISO-Normen, in der neuen Fassung sind mehr als doppelt so viele zu finden. Insgesamt wird auf 56 andere Quellen verwiesen.

Neu hinzugekommen ist auch ein Kapitel/Glossar für Begriffe, Definitionen und Abkürzungen, anstelle eines ausschließlichen Verweises auf die ISO/IEC 27000, wie es in der alten Fassung gehandhabt wurde.

Die Struktur der neuen ISO/IEC 27002:2022 wurde vollständig überarbeitet. Als thematische Gliederung enthält die neue Fassung statt 14 Kapitel/Domains (»Security Control Clauses«) nun 4 Themen (siehe unten ausführlicher). Dem direkt nachgelagert sind die 93 Maßnahmen (»Controls«). Damit fällt die ursprüngliche Eingliederung in »Control objectives« zunächst weg. Diese wird zukünftig für jede Maßnahme als Zweck (»Purpose«) dargestellt. Insgesamt umfassen Maßnahmen in der neuen Version die folgenden Inhalte:

- eine kurze Bezeichnung der Maßnahme (»*Control title*«),
- zusätzliche Attribute (»*Attribute table*«),
- eine Beschreibung der Control,
- eine Beschreibung des Zwecks der Control (»*Purpose*«),
- eine Implementierungsanleitung für die Control (»*Guidance*«) sowie
- erläuternden Text oder Verweise auf andere zugehörige Dokumente (»*Other Information*«).

Wie oben bereits erwähnt, gliedern sich Maßnahmen in der neuen Fassung in 4 Themen:

- »***People controls***«, Kapitel 6, für Maßnahmen, bei denen Personen im Vordergrund stehen, wie z. B. »Screening« oder »Remote working«;
- »***Physical controls***«, Kapitel 7, wenn physische Gegenstände betroffen sind, wie z. B. Zutrittskontrolle;
- »***Technological controls***«, Kapitel 8, wenn die Technik betroffen ist; und
- alle sonstigen Maßnahmen werden den »***Organizational controls***«, Kapitel 5, zugeordnet.

Eine hilfreiche Ergänzung in der neuen Fassung sind die Attribute (»*Attribute table*«), die fünf verschiedenen Kategorien zugeordnet werden können:

- »Control types« (mögliche Werte: preventive, detective, corrective),
- »Information security properties« (mögliche Werte: confidentiality, integrity, availability),
- »Cybersecurity concepts« (mögliche Werte: identify, protect, detect, respond, recover),
- »Operational capabilities« (mögliche Werte: z. B. physical security, governance) sowie
- »Security domains« (mögliche Werte: z. B. protection, defence).

Mithilfe dieser neuen Attribute kann der Fokus auf bestimmte Aspekte deutlich besser gesetzt werden, so können z. B. verschiedene Ansichten für verschiedene Zielgruppen erstellt werden, Anforderungen kategorisiert werden sowie die Maßnahmen einfach gefiltert werden.

Die Umstrukturierung auf Maßnahmen-Ebene wirkt sich wie folgt aus: In der neuen Fassung wurden 11 neue Controls hinzugefügt, eine Control wurde aufgeteilt, 57 Controls wurden in 24 Controls zusammengefasst und 58 Controls wurden umformuliert.

Die neue Fassung beinhaltet damit 93 Maßnahmen/Controls in 4 Themen im Vergleich zu 114 Maßnahmen/Controls in 14 Security Control Clauses der alten Fassung.

Neue Maßnahmen

Wie bereits erwähnt, befinden sich 11 neue Maßnahmen in der neuen Norm:

- »*Threat intelligence*« (Abschnitt 5.7) ist in dieser Form definitiv neu. Es geht hierbei u. a. um die Sammlung und Auswertung von Informationen zum konkreten Bedrohungsumfeld der Organisation, um geeignete reaktive Maßnahmen ergreifen zu können: Dabei wird zwischen strategischer, taktischer und operativer Threat intelligence unterschieden.
- »*Information security for use of cloud services*« (Abschnitt 5.23), diese Maßnahme war in der 2013er-Version implizit bei Supplier Relationships verankert. Die Maßnahme umfasst die Informationssicherheit von Cloud-Services aus der Sicht des Kunden. So wird etwa eine Richtlinie zum Thema Cloud Computing im Unternehmen gefordert.
- »*ICT readiness for business continuity*« (Abschnitt 5.30); ICT steht hier für »Information and Communications Technologies« und die Maßnahme geht über die alten Informationssicherheitsaspekte beim Business Continuity Management (alte Fassung, Clause 17) hinaus: es wird etwa als Basis das Durchführen von Business-Impact-Analysen (BIA) beschrieben.

- »*Data masking*« (Abschnitt 8.11) beschäftigt sich nicht nur mit dem Thema Maskierung von (personenbezogenen) Daten, sondern geht u. a. auch auf Eigenschaften der Pseudonymisierung und Anonymisierung von Daten ein, rechtliche Aspekte werden ebenfalls adressiert.
- »*Data leakage prevention*« (Abschnitt 8.12) erweitert die ursprüngliche Forderung nach Informationsklassifizierung und bietet ein vielfältiges Spektrum an Maßnahmen zum Schutz vor Datenabfluss, unter anderem werden die Aspekte Monitoring und deren technische Umsetzung behandelt.

Die weiteren neuen Maßnahmen sind:

- »*Physical security monitoring*« (Abschnitt 7.4)
- »*Configuration management*« (Abschnitt 8.9)
- »*Information deletion*« (Abschnitt 8.10)
- »*Monitoring activities*« (Abschnitt 8.16)
- »*Web filtering*« (Abschnitt 8.23)
- »*Secure coding*« (Abschnitt 8.28)

Aufgeteilte Maßnahme

Eine Maßnahme wurde in der neuen Norm in zwei eigenständige Maßnahmen aufgeteilt:

Die Maßnahme »*Technical compliance review*« (alte Fassung, Security Control Clause 18.2.3) wird inhaltlich aufgeteilt, zum einen in den organisatorischen Teil »*Compliance with policies and standards for information security*« (Abschnitt 5.36), mit Ausführungen zum Prüfen der Einhaltung der Richtlinien, zum anderen in den technischen Teil »*Management of technical vulnerabilities*« (Abschnitt 8.8), der stark erweitert wurde und ausführlich dargestellt wird. So wird umfangreich auf die Identifizierung und Evaluierung von technischen Schwachstellen eingegangen, es wird z. B. die Durchführung von Pentests explizit empfohlen.

Zusammengefasste Maßnahmen

Insgesamt wurden 57 Maßnahmen in 24 Maßnahmen zusammengefasst, was eine deutliche Komprimierung bedeutet. An dieser Stelle beschränken wir uns auf zwei ausgewählte Beispiele:

- »*Information security in project management*« (Abschnitt 5.8) wurde aus 2 ursprünglichen Domänen/Security Control Clauses zusammengeführt. Zum einen aus der gleichbenannten Maßnahme »*Information security in project management*« (alte Fassung, Security Control Clause 6.1.5), zum anderen wurde auch der Inhalt aus »*Information security requirements analysis and specification*« (alte Fassung, Security Control Clause 14.1.1) mit hineingenommen.
- »*User endpoint devices*« (Abschnitt 8.1) wurde auch aus 2 ursprünglichen Domänen/Security Control Clauses zusammengeführt. Zum einen aus der Maßnahme »*Mobile device policy*« (alte Fassung, Security Control Clause 6.2.1), zum anderen wurde auch der Inhalt aus »*Unattended user equipment*« (alte Fassung, Security Control Clause 11.2.8) eingepflegt. Damit werden alle Aspekte, die im Rahmen des Schutzes von Endgeräten für Benutzer zu berücksichtigen sind, zusammengeführt.

Bewertung

Mit der neuen Version ist eine deutliche Weiterentwicklung sowie eine Aktualisierung in Bezug auf anerkannte Maßnahmen der Informationssicherheit erkennbar, so wie es der Standard auch in der Einführung verspricht. Wichtige Best Practices und Trends der Informationssicherheitsbranche sind in der neuen Fassung berücksichtigt worden, wobei mit 11 neuen Maßnahmen keine massiven thematischen Erweiterungen vorgenommen wurden.

Die Aufteilung in organisatorische, personenbezogene, physische sowie technische Maßnahmen bietet aus Sicht der Autoren eine deutliche Verbesserung in der Struktur. Es werden im Vergleich zur 2013er-Version umfangreiche zusätzliche Informationen aufgeführt sowie ausführlichere Hilfestellungen geboten. Texte und Definitionen sind geschärft worden und die Attribute sorgen für Einheitlichkeit in der Auslegung. Die Attribute der Kategorie *»Cybersecurity concepts«* etwa entsprechen den Funktionen des NIST Cybersecurity Framework, womit ein direkter Bezug zu einem weiteren Management-Framework geschaffen wird.

Mit diesen und weiteren formalen Ergänzungen lassen sich vielfältige Sichten auf unterschiedliche Teilaspekte erstellen. Diese Möglichkeiten sowie der höhere Detailgrad können die Erstellung von unternehmensbezogenen Richtlinien vereinfachen.

Ausblick

Die Aktualisierung weiterer bestehender Normen und Standards der ISO/IEC-27000er-Reihe, die die Struktur der ISO/IEC 27002:2013 übernommen haben, wird folgen und voraussichtlich bis 2024 abgeschlossen sein.

Organisationen haben bereits die Möglichkeit, die neuen Maßnahmen aus Annex A als Maßnahmen zu verwenden. Mit den vorliegenden Mapping-Tabellen lassen sich auch für zertifizierte Unternehmen Erklärungen zur Anwendbarkeit erstellen, die bei Bedarf noch der bisherigen 2013er-Version entsprechen. Mit Veröffentlichung der Version ISO/IEC 27001:2022 sollte dieser Schritt für die Erlangung der Zertifizierung nur dann nötig sein, wenn die Zertifizierung noch explizit nach der 2013er-Version erfolgen soll. Dies könnte z. B. notwendig sein, wenn die Zertifizierungsstelle noch keine Akkreditierung für die Zertifizierung nach der 2022er-Version

hat. Das Dokument »Transition Requirements for ISO/IEC 27001:2022« des International Accreditation Forum[2] regelt den Übergang von Version 2013 auf Version 2022. Bestehende Maßnahmen eines zertifizierten ISMS können damit im Rahmen einer dreijährigen Übergangsfrist an die neue ISO/IEC 27002:2022 und damit an den neuen Annex angepasst werden (bis spätestens 31.10.2025). Durch die mitgelieferten Mappings sollte sich der Aufwand für eine solche Anpassung im Wesentlichen auf die neuen Maßnahmen sowie auf Verbesserungen bestehender Maßnahmen des Standards fokussieren können.

Zertifizierungsstellen müssen spätestens ab 31.10.2023 mit Zertifizierungen nach der neuen Norm beginnen.

8.3 Ganzheitliche Absicherung der Wertschöpfungskette

Einer der zentralen Aspekte bei der Einführung bzw. Anpassung der ISMS/Cyber-Security-Strategie sollte die Einführung eines Prozesses zur Absicherung der Wertschöpfungskette der vom ISMS zu schützenden Organisation darstellen. Mit dieser Maßnahme kann der Grundstein für ein durchgängiges Sicherheitsmanagement gelegt werden, das einen Basisschutz im gesamten Unternehmen gewährleistet und die weiteren Aktivitäten risikobasiert ermittelt.

In der Praxis hat sich hierfür eine »Scorecard zur Geschäftskritikalität (Business Criticality Scorecard, BCS)« etabliert, mittels deren Basis z. B. szenarienbasiert eine Einstufung des grundsätzlichen Risiko-Levels des Prozesses bzw. der darin genutzten Applikationen dokumentiert wird.

Für einen durchgängigen Schutz ist es dienlich, dass die Organisation auf Basis einer Richtlinie mindestens für jeden Hauptprozess sowie für jede für den Prozess betriebene Applikation vom jeweiligen Prozesseigner in einer solchen Scorecard, die Kritikalität des Prozesses sowie den Schutzbedarf der darin verarbeiteten Informationen bewertet.

Darüber hinaus ist es wichtig, dass die Projektmethodik einer Organisation sicherstellt, dass für neue Vorhaben (analog zur Datenschutz- und/oder Betriebsrat-Meldung) eine solche Scorecard erstellt wird, sodass frühzeitig Informationssicherheitsanforderungen abgestimmt werden können.

Szenarienbasierte Priorisierung der zu schützenden Geschäftsprozesse

Die Scorecard zur Geschäftskritikalität dient der Durchführung einer High-Level-Identifizierung der aus dem Prozess bzw. der Anwendungen resultierenden Informationssicherheitsrisiken, um den notwendigen Aufwand in die Absicherung des betrachteten Assets festzulegen. Hier bietet sich die Identifizierung auf Basis von organisationsspezifischen Grundsatzfragen und Szenarien im Kontext der Informationssicherheitsziele an, die nachfolgend exemplarisch abgebildet sind (siehe Abbildung 12).

Szenario: Stellen Sie sich vor, ein Hacker (und/oder ein Mitbewerber) hätte Zugriff auf die Daten/Informationen des Prozesses? **[Vertraulichkeit]**	Wie schätzen Sie das Risiko für UNSERE ORGANISATION ein? W: Wählen Sie ein Element aus. S: Wählen Sie ein Element aus. Risikohöhe: Wählen Sie ein Element aus. Beschreiben Sie den konkreten Schaden, welcher für UNSERE ORGANISATION denkbar wäre.
Szenario: Stellen Sie sich vor, ein Hacker (und/oder ein Mitbewerber) könnte die Daten/Informationen des Service verfälschen (»Integritätsverlust«). **[Integrität]**	Wie schätzen Sie das Risiko für UNSERE ORGANISATION ein? W: Wählen Sie ein Element aus. S: Wählen Sie ein Element aus. Risikohöhe: Wählen Sie ein Element aus. Beschreiben Sie den konkreten Schaden, welcher für UNSERE ORGANISATION denkbar wäre.
Szenario: Stellen Sie sich vor, der Service bzw. die Daten wären für mehr als einen Tag nicht verfügbar. **[Verfügbarkeit]**	Wie schätzen Sie das Risiko für UNSERE ORGANISATION ein? W: Wählen Sie ein Element aus. S: Wählen Sie ein Element aus. Risikohöhe: Wählen Sie ein Element aus. Gäbe es einen Workaround, um die Geschäftsanforderungen zu erfüllen (z.B. manueller Prozess)? Ab welchem Zeitraum wäre ein Ausfall für UNSERE ORGANISATION kritisch? Wählen Sie ein Element aus.

Abbildung 12: Szenarienbasierte Ermittlung des Risiko-Levels

2 International Accreditation Forum, Inc., Transition Requirements for ISO/IEC 27001:2022, Issue 1 (IAF MD 26:2022).

Neben der Kritikalitäts- und Risikobewertung können auch weitere Fakten, z. B. zum RTO/RPO oder zu betriebsrelevanten Prozessen, erhoben werden. Auf eine Scorecard gehört zumindest eine Beschreibung des jeweils betrachteten Hauptprozesses bzw. der dafür betriebenen Applikationen sowie eine eindeutige Identifikationsbezeichnung.

Basierend auf den erhobenen Informationen, z. B. Reifegrad-Umsetzung der Basisanforderungen und der Dokumentationsanforderungen, sowie insbesondere basierend auf der erhobenen Kritikalitäts- und Risikobewertung wird in der BCS vom Informationssicherheitsbeauftragten (ISB) entschieden, welcher Aufwand in die weitere Sicherheitsanalyse (des Prozesses) investiert werden muss, um ein für die Organisation adäquates Sicherheitsniveau zu erreichen.

Für weniger kritische Systeme kann dann z. B. eine zu definierende Standardabsicherung Anwendung finden und bei Prozessen mit höherem Risikopotenzial werden spezifische Sicherheitskonzepte oder technische Überprüfungen, wie z. B. die Durchführung eines Penetrationstests, eingefordert. Die möglichen Entscheidungsstufen könnten, wie in Tabelle 3 beispielhaft dargestellt, definiert sein.

Stufe	Aufwand Sicherheitsanalyse
0	Keine weitere Analyse notwendig
1	**Standardmaßnahmen** Durchführung einer GAP-Analyse auf die Standardmaßnahmen der Organisation oder alternativ, sofern durch die konzerneigene IT betrieben, eine Bestätigung der IT-Abteilung, dass die Maßnahmen umgesetzt sind.
2	**Erweiterte Sicherheitsanalyse** Durchführung einer spezifischen Schwachstellenanalyse mittels einer Bedrohungsmodellierung (z. B. STRIDE[3])
3	**Technische Sicherheitsanalyse** Durchführung eines Penetrationstests oder einer Quellcodeanalyse durch eine unabhängige dritte Partei

Tabelle 3: Aufwand Sicherheitsanalyse

Die BCS stellt somit eine Art »Vor-Filter« für das Risikomanagement dar, da ausgiebige Analysen nur dann durchgeführt werden müssen, wenn die initiale Bewertung der Kritikalität einen entsprechenden Bedarf identifiziert, aber über die Methodik dennoch gewährleistet ist, dass jeder Prozess zumindest einer High-Level-Analyse unterzogen wird und eine angemessene Basisabsicherung gewährleistet ist, was automatisch zu einer systematisch sichergestellten »weakest link«-Absicherung führt.

Weiterer Vorteil einer Scorecard-Lösung ist, dass man über diese auch weitere Aspekte – für die operativ zu steuernden Prozesse – abfragen kann, z. B. zu Compliance-Vorgaben, Überprüfung auf dokumentierte Betriebsprozesse, Verantwortlichkeiten für Patch- und Schwachstellenmanagement, Logauswertung, Datensicherung, Berechtigungskonzept und weitere. Dies kann Aspekte außerhalb der Informationssicherheit beinhalten, die aus anderen Managementsystemen heraus notwendig sind, z. B. aus dem Datenschutz-, Compliance- oder Qualitätsmanagement.

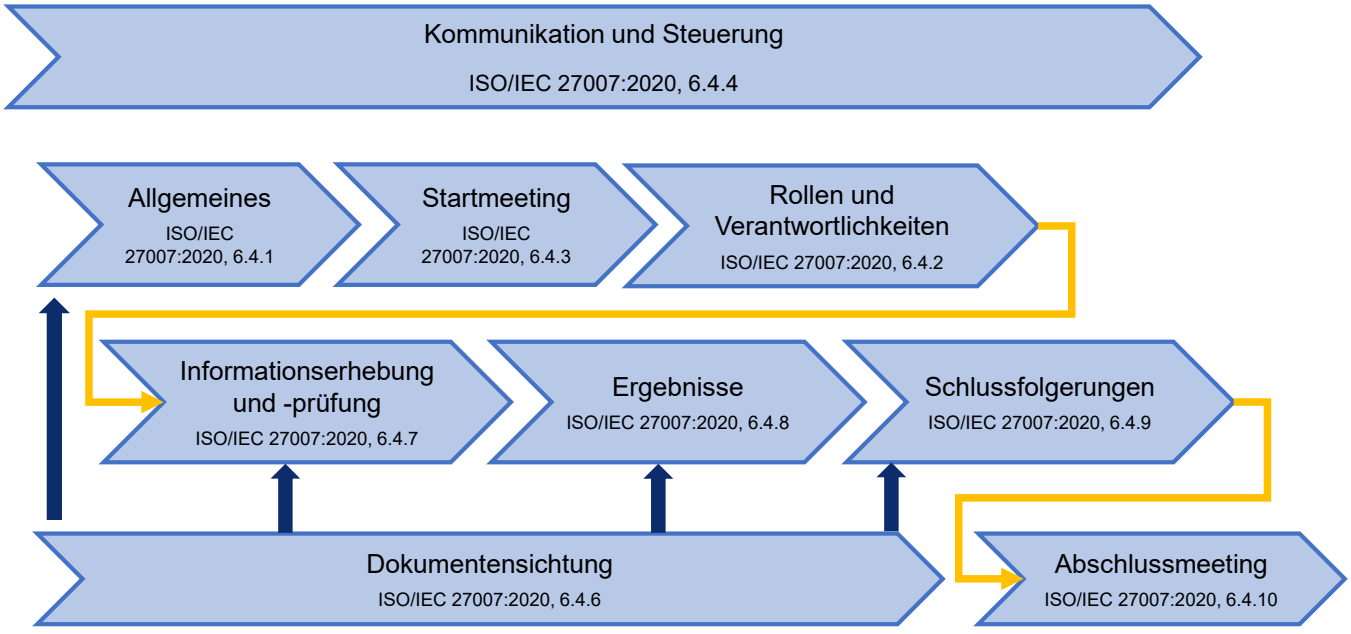
3 Siehe Abschnitt 3.6

8.4 Interne ISMS-Audits – Mapping zur ISO/IEC 19011 und ISO/IEC 27007

Anforderungen an interne ISMS-Audits aus ISO/IEC 27001:2022 vs. ISO/IEC 19011:2018 & ISO/IEC 27007:2020

Teilprozess/Aktivität	ISO/IEC 27001:2022	ISO/IEC 19011:2018 ISO/IEC 27007:2020
Planung des Auditprogramms	9.2 a 9.2 b 9.2 c	5.1 General 5.2 Establishing the audit programme objectives
Festlegung des Auditprogramms	9.2 c	A.5.4 Establishing the audit programme
Implementierung des Auditprogramms	9.2 c	A.5.5 Implementing the audit programme
Monitoring des Auditprogramms	9.2 c	A.5.6 Monitoring the audit programme
Review und Verbesserung des Auditprogramms	9.2 c	A.5.7 Reviewing and Improving the audit programme
Kompetenz und Auswahl der Auditoren	9.2 e	7 Competence and evaluation of auditors
Dokumentation und Nachweise	9.2 g	A.5.5.7 Managing and maintaining audit programme records
Auditkriterien und Umfang je Audit festlegen	9.2 d	A.5.5.2 Defining the objectives, scope and criteria for an individual audit
Durchführung von ISMS-Audits	9.2 e	6 Conducting an audit
Reporting der Auditergebnisse	9.2 f	A.5.5.6 Managing audit programme results

8.5 Durchführung interner ISMS-Audits (Prozessschaubild)



ISACA
Germany Chapter

Ihr Partner für Weiterbildung:
Der ISACA Germany Chapter e. V.

Der deutsche Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie IT-Governance-Experten fördert Ihre berufliche Weiterentwicklung durch Examensvorbereitungskurse auf die internationalen Berufszertifizierungen CISA, CISM, CRISC und CDPSE.

Unterstützend bieten wir Ihnen ein thematisch breit gefächertes Zertifikatsprogramm basierend auf dem Rahmenwerk COBIT 2019.

Unser komplettes Kursangebot können Sie auf unserer Webseite **www.isaca.de/seminare** einsehen. Neben Präsenzseminaren bieten wir alle Kurse auch als **Online-Seminare** an.
Für sämtliche Kurse erhalten Sie einen anerkannten Berufsfortbildungsnachweis (sog. CPE-Stunden).