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

Implementierungsleitfaden ISO/IEC 27001:2013

Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013

ISACA®
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Oberwallstraße 24
10117 Berlin

www.isaca.de
info@isaca.de

Autorenteam:
- 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: Mai 2016 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe Informationssicherheit)

Implementierungsleitfaden ISO/IEC 27001:2013

Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013

ISACA®
Trust in, and value from, information systems
Germany Chapter

Warum dieser Guide?

Informationssicherheit ist unverzichtbar. Sie muss als Bestandteil der Unternehmensführung allerdings darauf ausgerichtet sein, die Geschäftsziele optimal zu unterstützen. Auch oder vielleicht gerade in Zeiten sogenannter »Cyber-Bedrohungen« und des vielerorts aufkommenden Begriffs der »Cyber-Sicherheit« bietet ein gut strukturiertes Informationssicherheits-Managementsystem (ISMS) nach international anerkannten Standards die optimale Grundlage zur effizienten und effektiven Umsetzung einer ganzheitlichen Sicherheitsstrategie.

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. Unabhängig von der Namensgebung des gewählten Ansatzes ist in allen Fällen 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 vorliegende *Implementierungsleitfaden ISO/IEC 27001: 2013* (kurz: Implementierungsleitfaden) enthält praxisorientierte Empfehlungen und Hinweise für Organisationen, die entweder bereits ein ISMS nach der internationalen ISO/IEC-Norm 27001:2013, Information technology — Security techniques — 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: Gerhard Funk, Julia Hermann, Angelika Holl, Nikolai Jeliazkov, Oliver Knörle, Boban Krsic, Nico Müller, Jan Ötting, Jan Rozek, Andrea Rupprich, Dr. Tim Sattler, Michael Schmid und Holger Schrader.

Projektleitung und Redaktion: Oliver Knörle

Inhaltsverzeichnis

1. Einleitung

Das systematische Management der Informationssicherheit nach ISO/IEC 27001:2013 soll einen effektiven Schutz von Informationen und IT-Systemen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit gewährleisten.[1] Dieser Schutz ist kein Selbstzweck, sondern dient der Unterstützung von Geschäftsprozessen, der Erreichung von Unternehmenszielen und dem Erhalt von Unternehmenswerten 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 vs. Risiken
- **C – Compliance-Sicht**
  - Externe Vorgaben durch Gesetze, Regulatoren 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.

Technische und organisatorische Maßnahmen

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

ISO/IEC 27001:2013 und die darin systematisch und ganzheitlich dargelegten TOMs, die – in unterschiedlicher Ausprägung und Güte – zum Betrieb eines jeden ISMS gehören, unterstützen die Erreichung der eingangs aufgeführten Ziele aus allen drei Sichten:

- 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)*, eine effektive und zielgruppengerechte Kommunikationsstrategie (vgl. Kapitel *3.9 Communication*) sowie angemessene Regelwerke und Organisationsstrukturen (vgl. Kapitel *3.5 Roles, Responsibilities and Competencies*).
- 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 27001:2013. 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 empfohlenen Maßnahmen des 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 Monitoring & KPIs*) 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 Competence and Awareness*) sind für die Compliance-Sicht ebenfalls von wesentlicher Bedeutung.

1 Authentizität, Verbindlichkeit und Nicht-Abstreitbarkeit können als Teilziele der Integrität angesehen werden.

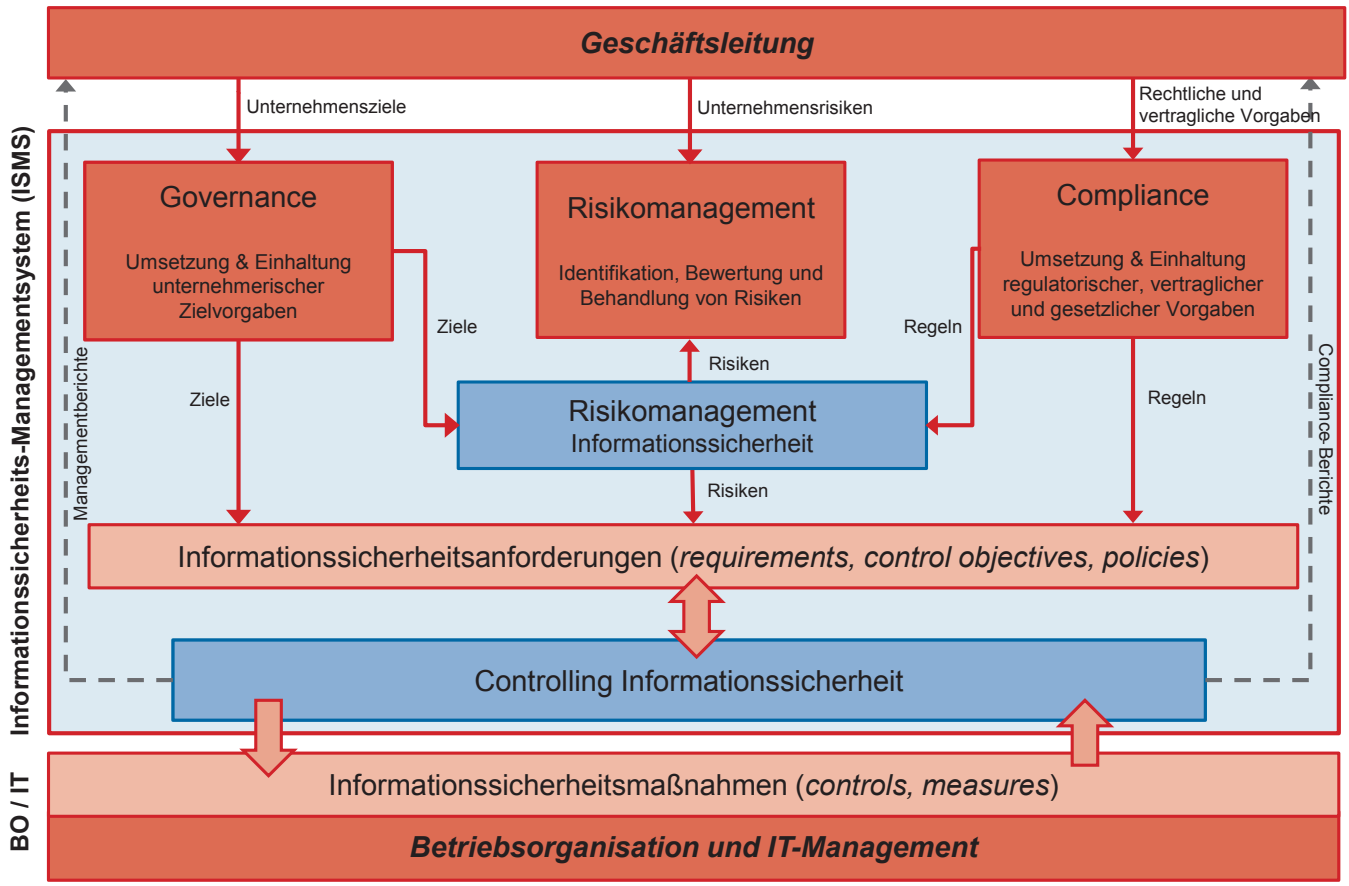


Abbildung 1: Einbindung des ISMS in die Unternehmenssteuerung[2]

2 Quelle: Carmao GmbH

2. Aufbau des Leitfadens

2.1 Themenbereiche

Der vorliegende Implementierungsleitfaden orientiert sich an den wesentlichen Themenbereichen der Norm ISO/IEC 27001:2013, allerdings ohne erneut die Abschnittsstruktur des Standards identisch wiederzugeben. Vielmehr werden die relevanten Themenbereiche eines ISMS nach ISO/IEC 27001:2013 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:

1. Context of the Organization
2. Leadership and Commitment
3. IS Objectives
4. IS Policy
5. Roles, Responsibilities and Competencies
6. Risk Management
7. Performance Monitoring & KPIs
8. Documentation
9. Communication
10. Compentence and Awareness
11. Supplier Relationships
12. Internal Audit
13. Incident Management
14. Continual Improvement

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

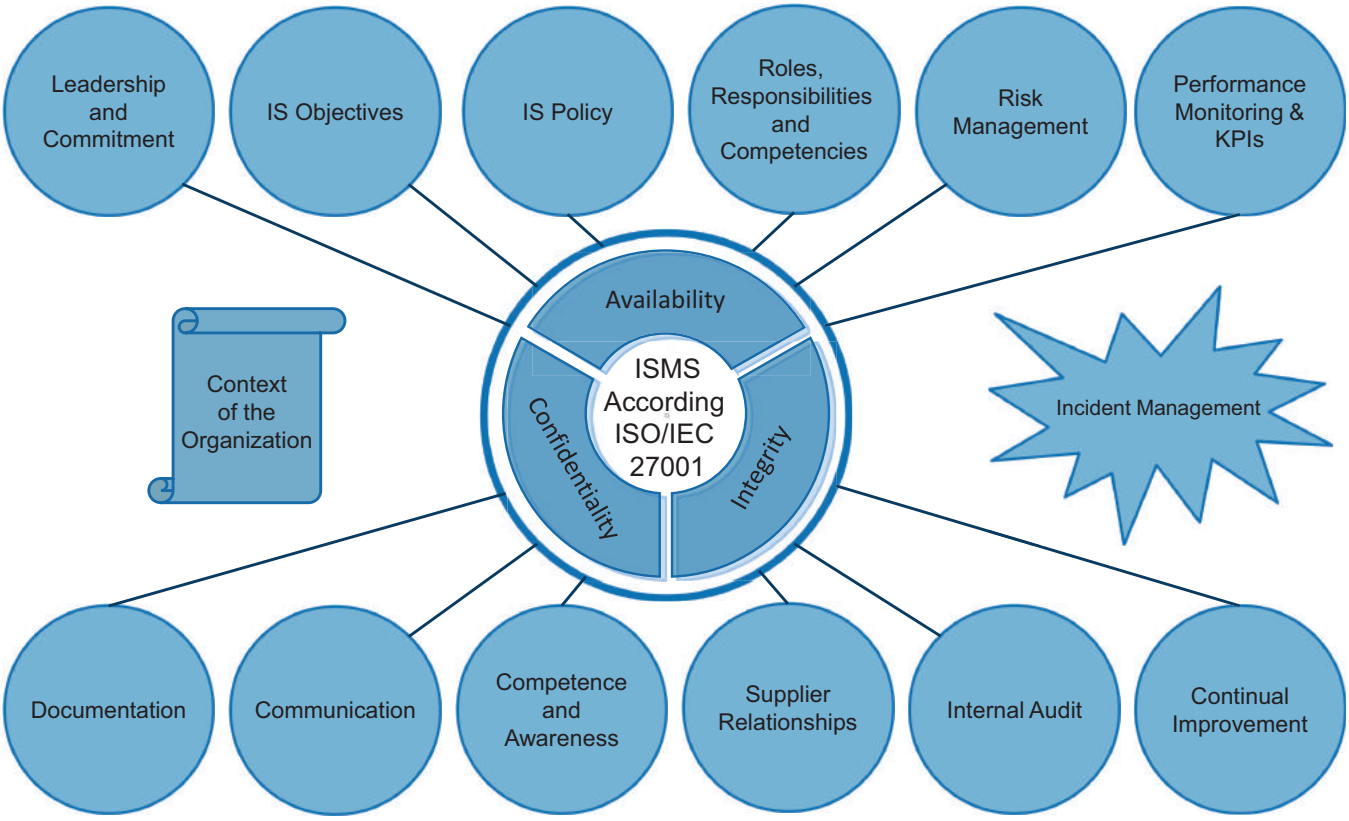


Abbildung 2: Bausteine eines ISMS nach ISO/IEC 27001:2013

ISO/IEC 27001:2013 (respektive ISO/IEC 27002:2013) 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 27001:2013
- **Anforderungen an die Dokumentation**
  Darstellung von Dokumentationsanforderungen, sowohl aus normativen Gesichtspunkten als auch aus Sicht der Praxis
- **Referenzen**
  Angabe der für den Themenbereich relevanten Kapitelnummern aus ISO/IEC 27001:2013 sowie weitere Quellenangaben, sofern erforderlich und sinnvoll

2.3 Konventionen

Sofern im weiteren Verlauf die Begriffe »*Norm*« oder »*Standard*« ohne weitere Konkretisierung verwendet werden, beziehen sich diese stets auf die Norm ISO/IEC 27001:2013.

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.

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

3. Bausteine eines ISMS nach ISO/IEC 27001:2013

3.1 Context of the Organization

Eine der ersten Aufgaben bei der Implementierung eines ISMS ist die Festlegung des konkreten Geltungsbereichs (engl.: scope) des Managementsystems sowie die Durchführung einer Anforderungs- und Umfeldanalyse im Hinblick auf die Organisation und deren Stakeholder.

Festlegung des Geltungsbereichs

Der Geltungsbereich muss laut Norm dokumentiert vorliegen und sollte neben den vom ISMS einbezogenen Prozessen und Geschäftsbereichen auch die Ergebnisse der durchgeführten Anforderungs- und Umfeldanalyse umfassen.

- 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-27001:2013-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) des Annex A dokumentiert, d. h., ob die jeweilige Maßnahme innerhalb des ISMS zur Anwendung kommt oder nicht inklusive der jeweiligen Begründung für Anwendung oder 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, wie bereits erwähnt, 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 22301:2012 etc.), Schnittstellen zu anderen wichtigen Abteilungen wie Risikomanagement, Personalabteilung, Datenschutz, 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. BDSG, 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 31000:2009, Abschnitt 5.3.2 *»Establishing the external context«* und Abschnitt 5.3.3 *»Establishing the internal 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 durchaus 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, Regulierungsbehörden bzw. Gesetzgeber, Kunden, Klienten, Lieferanten bzw. Zulieferer, Dienstleister, Angestellte etc.

- Als Basis der Erhebung relevanter 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 27001:2013 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 (A.18.1)

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

- Übersicht aller für den konkreten Geltungsbereich des ISMS relevanten Interessengruppen (Stakeholder)

Referenzen

ISO/IEC 27001:2013 – Abschnitte 4.3 und 6.1.3
ISO/IEC TR 27023:2015
ISO 22301:2012
ISO 31000:2009
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 die Zustimmung und die Unterstützung durch die Leitungsebene unumgänglich, da die eingeführten Prozesse des Managementsystems sonst keinen verbindlichen Charakter und somit u.U. keine Akzeptanz finden würden.

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 Informationssicherheitsleitlinie (vgl. *Information Security Policy* in Kapitel *3.4 IS Policy*).

- 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[1,2].

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.

1 Joint Committee Report on Risks and Vulnerabilities in the EU Financial System, Kapitel 7 (*http://www.esma.europa.eu/system/files/jc-2014-18_report_on_risks_and_vulnerabilities_in_the_eu_financial_system_march_2014.pdf*).

2 Erläuterung zu den MaRisk in der Fassung vom 14.12.2012, AT 4.2, AT 7.2 *(https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1210_erlaeuterungen_ba.pdf?__blob=publicationFile&v=3)*.

- Bei großen Unternehmen ist das »Topmanagement«[3] 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 27001:2013 fordert vom Topmanagement eine klare Vorbildfunktion hinsichtlich der Informationssicherheit. In der Praxis gehören hierzu neben einem sichtbaren Engagement und einem klaren Bekenntnis 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

3 Siehe Kapitel *3.1 Context of the Organization* und ISO/IEC 27000:2014, Clause 2.84.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 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:

- Ein Dokument, das die Ableitung und Bewertung von Risiken aus festgestellten Abweichungen zwischen strategischen IS-Zielen und Zielerreichungsgrad schriftlich festhält, idealerweise als Risikobehandlungsplan.
- Dokumente, die als Nachweise zur Berichterstattung an das Topmanagement vorgehalten werden, z. B. in Form von Präsentationen, Protokollen oder Reports.

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 allerdings die für sie passende Dokumentationsform und -häufigkeit finden.

Referenzen

ISO/IEC 27001:2013 – Abschnitte 5.1, 9.1 und 9.3

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 Unternehmensziele und die daraus abgeleiteten IT-Ziele dienen als Grundlage für die Ausgestaltung bzw. Festlegung der Ziele für die Informationssicherheit 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 IS-Leitlinie stehen.
- 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 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 in die Planung von Projekten, Produkten und Systemen integriert werden.
- Bei der Formulierung von IS-Zielen ist darauf zu achten, dass echte und langfristig orientierte Ziele/Zielvorgaben beschrieben werden und nicht die für die Zielerreichung notwendigen operativen technischen/organisatorischen Maßnahmenziele oder Maßnahmen.
- Wie bei jeder Zielformulierung empfiehlt es sich, auch bei der Festlegung von IS-Zielen »smarte«[4] 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 COBIT 5, konkret COBIT 5 for Information Security oder The Definitive Guide to IT Service Metrics[5] (siehe auch Kapitel *3.7 Performance Monitoring & KPIss*).
- 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, in einem ersten Schritt wenige, aber für die jeweilige Organisation 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).

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 bestehen folgende Mindestanforderungen an die Dokumentation:

- Eine Dokumentation der IS-Ziele muss vorgehalten werden.

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

- Die Ausgestaltung der Dokumentation der IS-Ziele sollte inklusive eines Umsetzungsplans bzw. Referenzen auf konkrete Projekte erfolgen. Üblicherweise wird bereits in der IS-Leitlinie auf die (Dokumentation der) IS-Ziele verwiesen. Die IS-Ziele können auch als Teil der IS-Strategie formuliert werden.

Referenzen

ISO/IEC 27001:2013 – Abschnitt 6.2
COBIT 5 for Information Security
McWhirter, Kurt; Gaughan, Ted: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

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 eines effektiven ISMS sowie 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

4 SMART: spezifisch, messbar, akzeptiert, realistisch, terminiert.
5 McWhirter, K.; Gaughan, T.: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

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 seiner 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 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 and Awareness*).
- 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 weitergehenden 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.
- 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 durchaus 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 allerdings, dass sich die Leitlinie sichtbar an den vorhandenen Unternehmens- und IT-Zielen orientiert und die Kernaussagen beim Leser einen Wiedererkennungseffekt zur betroffenen Organisation hervorrufen.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 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 A.5.1)
- Begleitende Dokumente und Organigramme, beispielsweise zur Verdeutlichung der Aufbauorganisation im Kontext Informationssicherheit (sofern nicht in der Leitlinie enthalten)

Referenzen

ISO/IEC 27001:2013 – Abschnitt 5.2

3.5 Roles, Responsibilities and Competencies

Gemäß Abschnitt 5.3 der Norm ISO/IEC 27001:2013 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 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[6]- oder SoD[7]-Matrix).

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

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

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 Vermögenswerteigentümers (engl.: asset owner) zu definieren und zu etablieren.[8]

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.
- Interessenkonflikte, die in der Praxis auf jeden Fall vermieden werden sollten:
  - Informationssicherheitsbeauftragter (ISB bzw. CISO[9]) und IT-Leiter/CIO[10]
  - 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 er 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 Interessenkonflikt münden und sollte deshalb ausführlich analysiert und abgewogen werden.
- Je nach Größe und Geschäftsaktivitäten der Organisation/des Unternehmens 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 TOMs). 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 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 27001:2013 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 Verbindung zum Thema Informationssicherheit mitbringen bzw. über ausreichend intrinsische Motivation verfügen. Neben den erforderlichen Fachkenntnissen sind Sozialkompetenzen ein weiteres Muss, da ohne gutes Kommunikationsverhalten, integres Auftreten, sachliche Überzeugungsfähigkeit und Konfliktmanagement viele der Aufgaben, die sich im Zusammenhang mit der Umsetzung der Informationssicherheitsstrategie und (manchmal auch unangenehmer oder unbeliebter) Maßnahmen ergeben, sich nicht oder nicht zufriedenstellend lösen lassen.
- Beispiele für die organisatorischen Strukturen hinsichtlich Informationssicherheit finden sich u. a. in »COBIT 5 for Information Security« (Appendix C) und dem BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise. Hierin sind u. a. die Rollen und Verantwortlichkeiten des CISO, des Steuerungskomitees, des Informationssicherheitsmanagers, die Rollen im Risikomanagementprozess sowie der fachlichen Dateneigentümer beschrieben.

8 Siehe Abschnitt 6.1.2 c und Control A.8.1.2 »Ownership of assets«.
9 CISO: Chief Information Security Officer.
10 CIO: Chief Information Officer.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 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/Stellenprofile
- Ausgestaltung der strategischen und operativen Zusammenarbeit zwischen DSB und CISO

Referenzen

ISO/IEC 27001:2013 – Abschnitte 5.3, 7.1 und 7.2
COBIT 5 for Information Security
BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise

3.6 Risk Management[11]

Ganz allgemein gesprochen ermöglicht Risikomanagement zu analysieren, was alles passieren kann und was die möglichen Folgen sein können, *bevor* entschieden wird, was getan werden sollte und wann dies getan werden sollte, um potenziellen Schäden angemessen vorzubeugen. Ziel ist es, die identifizierten Risiken auf ein akzeptables Niveau zu reduzieren, wobei darüber, was als *akzeptabel* angesehen wird, die jeweiligen Verantwortungsträger im jeweiligen Kontext, manchmal auch in der jeweiligen Situation, entscheiden müssen. Hinzu kommt die Entscheidung darüber, wie mit den identifizierten und bewerteten Risiken umzugehen ist.

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.

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[12]

Erfolgsfaktoren aus der Praxis

Wie entstehen Risiken?

Risiken im Kontext der Informationssicherheit ergeben sich u. a. inhärent aus dem Einsatz von IT-Systemen und (neuer) IT-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.

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

12 Beispielsweise durch Anpassung der Sicherheitsstrategie oder Umsetzung angemessener Sicherheitsmaßnahmen.

Wie werden Risiken entdeckt und bewertet?

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).[13]

Der Risikobeurteilungsprozess beinhaltet u. a. Folgendes:

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

Methoden zur Risikoidentifikation

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: [14]

- 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 müssen. 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 §9 BDSG Anlage 1. Der Informationssicherheitsbeauftragte wiederum erkennt die Reichweite des Projekts (Auswirkung bei Verfügbarkeitseinschränkungen oder Datenabfluss) und fordert daher einen Penetrationstest vor dem Live-Gang.

- 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

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 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 neuer Technologien oder geänderte Gefährdungssituationen)[15]. Oder anders formuliert: »Beim Risikomanagement hängt der Erfolg von den Vorbereitungen ab.«[16]

Risikoakzeptanzkriterien

Die Festlegung von Risikoakzeptanzkriterien ist eine zentrale Aufgabe im Risikomanagementprozess, denn nur dadurch

13 In der ISO 31000 sind diese Aktivitäten im Abschnitt *5.3 »Establishing the context«* beschrieben.

14 Siehe auch IEC 31010:2009 – Annex B – Risk Assessment Techniques.

15 Beispielsweise durch APTs oder Zero-Day-Schwachstellen.

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

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).
- Risikoakzeptanzkriterien können mehrere Schwellwerte umfassen. Jede Schwellwertstufe kann an eine bestimmtes 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[17] 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 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, ist in der Praxis ebenso wenig umsetzbar, wie es möglich oder sinnvoll ist, alle IT-Systeme auf ein und demselben Sicherheitsniveau zu betreiben. Ein »angemessen hohes« Sicherheitsniveau für bestimmte Komponenten und Prozesse bedeutet gleichzeitig auch ein »angemessen niedriges« Sicherheitsniveau für andere Komponenten und Prozesse. Die Kunst besteht darin, mit ausreichend Erfahrung und mithilfe ausgewählter Methoden und Bewertungskriterien diese Unterscheidung treffen zu können.

17 Je größer der Risikoappetit ist, desto mehr Handlungsspielraum und Geschäftspotenzial ist in der Regel vorhanden.

Nach Festlegung der Risikobeurteilungsmethode folgen die jeweils iterativ durchzuführenden Schritte des Risikomanagementprozesses:

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

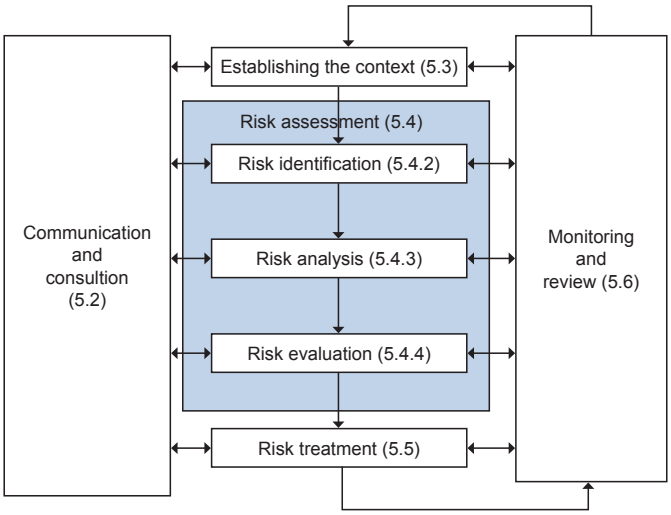


Abbildung 3: Risikomanagementprozess nach ISO 31000[18]

Schritt 1: Risikoidentifikation

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

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

- 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.).
- Risikoanalysen
  - Für geschäftskritische Prozesse, Anwendungen und Systeme werden ggf. bewusst 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.

18 Siehe ISO 31000.

  - Innerhalb des Projektmanagements sollten Risikoanalysen (mit jeweils angepasstem Umfang) als ein Pflichtelement aufgenommen werden.
- 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 sozusagen 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 im Allgemeinen 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, Gruppenleiter, Bereichsleiter oder Abteilungsleiter). 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.[19]

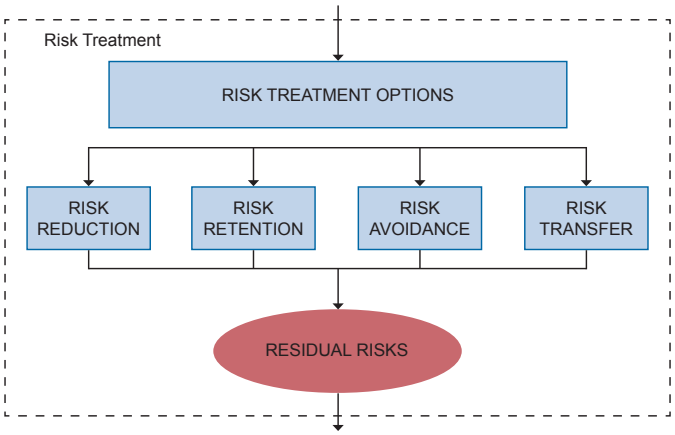


Abbildung 4: Risikobehandlungsoptionen nach ISO/IEC 27005[20]

- 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 [21] IT-

19 Siehe u. a. Abschnitt 9 der ISO/IEC 27005:2009 – »Information security risk treatment«.

20 Siehe ISO/IEC 27005.

21 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.

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.

Wie werden Risiken dokumentiert?

- 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, Auswertemöglichkeiten 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.

Allgemeine Empfehlungen

- 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).

- Das Risikomanagement sollte nach Möglichkeit prozessorientiert sein, anstatt die einzelnen Vermögensgüter (Assets) in den Vordergrund zu stellen. Damit wird zum einen gewährleistet, dass Risiken und Gefährdungen optimalerweise (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 bewerten. Eine 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 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz liefert Ansatzpunkte, wie mithilfe der in den IT-Grundschutz-Katalogen 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, Basis-Sicherheitscheck, 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 TOMs 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 27001:2013 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 27001:2013 – Abschnitte 6.1, 8.2, 8.3
ISO/IEC 27005
ISO 31000
COBIT 5 for Information Security
BSI-Standards 100-2 und 100-3

3.7 Performance Monitoring & KPIs[22]

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.

Leistungsindikatoren/Key-Performance-Indikatoren

Um die Effektivität und Effizienz der ISMS-Prozesse und der etablierten Maßnahmen kontinuierlich zu überprüfen, werden in der Praxis konkrete Indikatoren verwendet. 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 gegebenenfalls steuernd einzugreifen. Diese Leistungsindikatoren werden in Bezug auf die zu erreichenden Unternehmensziele, gesetzliche Vorgaben und Schutzbedürfnisse zusammengefasst. Die aggregierten Leistungs- oder Performance-Indikatoren werden Key-Performance-Indikatoren (KPI) genannt.

Der Nutzen und die Bedeutung von KPIs liegen in der Möglichkeit, grundlegende Aussagen über das Schutzsystem treffen zu können. Sie dienen dem Management als nachvollziehbare und verständliche Grundlage für fundierte Entscheidungen zur Steuerung der Informationssicherheit. Durch KPIs können 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

Leistungsindikatoren sind nur dann sinnvoll zur Darstellung der Istsituation und Steuerung einsetzbar, wenn sie bestimmte Voraussetzungen erfüllen. Die Fachliteratur liefert zahlreiche Qualitätskriterien für Leistungsindikatoren: Einen guten Startpunkt bietet der Report »Information Security Metrics – State of the art«[23], der im Rahmen des Forschungsprojekts Controlled Information Security (COINS) der Swedish Civil Contingencies Agency (in Schwedisch: MSB) entstanden ist.

- Jeder Leistungsindikator 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 KPIs 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 muss erfasst werden.
- Leistungsindikatoren können auch zur Bewertung und Steuerung von Dienstleisterverhältnissen genutzt werden und beispielsweise als Vertragsbestandteil oder in ein (Security-)SLA aufgenommen werden.

22 KPI: Key-Performance-Indikator.

23 Barabanov, R.: Information Security Metrics – State of the Art. DSV Report series No 11 – 007, 2011.

Relevante KPIs für das ISMS

Es gibt viele Quellen für Leistungsindikatoren der Informationssicherheit, die eine riesige Auswahl bieten, so etwa COBIT 5 for Information Security[24], The CIS Security Metrics[25] oder Performance Measurement Guide for Information Security[26], um nur einige davon zu nennen. Die konkrete Auswahl von KPIs soll auf den Gegebenheiten der jeweiligen Organisation basieren, die bereits beschriebenen Qualitätskriterien erfüllen und kontinuierlich optimiert werden.

Im Folgenden finden sich einige allgemein gehaltene Beispiele für solche Leistungsindikatoren:

- **Integration von Informationssicherheit/IT-Sicherheit in Projekten**
  - Anteil der Projekte mit berücksichtigten Anforderungen an IT-Sicherheit im Verhältnis zu der Gesamtzahl der Projekte
  - Verhältnis der Projekte mit IT-Sicherheitsdefiziten bei der Produktivsetzung mit und ohne formale Risikobetrachtung in der Projektphase zu der Gesamtzahl der Projekte
- **Abweichungen von IT-Sicherheits- und Architekturstandards**
  - Anzahl und Entwicklung der genehmigten Abweichungen zu hauseigenen Vorgaben im Zeitablauf
  - Entwicklung der detektierten nicht genehmigten Abweichungen zum Vorgabenstandard im Zeitablauf
  - Verhältnis der detektierten Abweichungen, die behoben wurden, zu den nachträglich genehmigten Abweichungen
- **Incident Response/Problem Management**
  - Verhältnis der nicht zu schließenden Sicherheitsschwachstellen (Abweichungen zum Standard) zur Gesamtanzahl von gefundenen Abweichungen
  - Anteil der Sicherheitsschwachstellen, die im vorgegebenen Zeitraum erfolgreich behoben werden konnten, von der Gesamtzahl der bekannten Schwachstellen
- **Asset Ownership**
  - Anteil der Informationsgüter, die einem Eigentümer zugeordnet sind, an der Gesamtzahl der Informationsgüter in Prozent

Metriken nutzen

Ein Indikator ist fest mit einer Schutzmaßnahme verbunden (technisch oder organisatorisch), um an festgelegten Parametern ihre Effektivität zu messen. Ein Indikator hat einen definierten Normbereich für den Regelbetrieb mit einem (oder mehreren) Toleranzbereich(en) sowie Schwellwerte zur Alarmierung. Damit die steuernde Person dennoch nicht mit Einzelwerten behelligt wird, kann jeder Indikator einen Regelkreislauf haben, der eine vordefinierte Gegenmaßnahme enthält. Verlässt der Messwert den ordnungsgemäßen Normbereich und kommt in den Toleranzbereich, wird die Gegenmaßnahme eingeleitet. Wirkt diese nicht und der Schwellwert wird überschritten oder kommt es regelmäßig zu Schwankungen im Toleranzbereich, so wird eine Alarmierung ausgelöst.

Beispiel:

In Analogie zu einem Auto wird dem Fahrer nicht jede einzelne Abweichung eines Sensorwerts am Motor aus dem Normbereich angezeigt, es sei denn, die Leistungsziele oder der Erhalt der Motorintegrität sind gefährdet. In einem solchen Fall geht eine Warnleuchte an. Daraus kann der Fahrer Rückschlüsse ziehen und eine risikobasierte Entscheidung über die weitere Fahrzeugnutzung treffen.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 bestehen folgende Mindestanforderungen an die Dokumentation:

- **Dokumentation der Messstruktur für alle KPIs. Das beantwortet die folgenden Fragen:**
  - Wie sind die Metriken im Einzelnen definiert?
  - 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 geeignet sind, die Wirksamkeitsüberwachung zu belegen.**

Referenzen

ISO/IEC 27001:2013 – Abschnitt 9.1
ISO/IEC 27004:2009 – Abschnitte 5, 6, 7, 8, 9, 10 und Annex A
COBIT 5 for Information Security

3.8 Documentation

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

- Die Erstellung und Aktualisierung sowie die Genehmigung und ggf. Veröffentlichung von Dokumenten müssen nach einem definierten Verfahren (Workflow) erfolgen.

24 ISACA: COBIT 5 for Information Security, 2012.
25 The Center for Internet Security: The CIS Security Metrics, 2010.
26 Chew, E.; Swanson, M.; Stine, K.; Bartol, N.; Brown, A.; Robinson, W.: Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1, 2008.

- 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 sinnvoller 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 27001:2013 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 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 27001:2013 bestehen immer 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, Abschnitt 6.2)
- Kompetenznachweise
  (Evidence of competence, Abschnitt 7.2 d)
- Nachweise zur korrekten Ausführung der ISMS-Prozesse[27]
  (Operational planing and control, Abschnitt 8.1)
- 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)

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

- 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).

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

Referenzen

ISO/IEC 27001:2013

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 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:

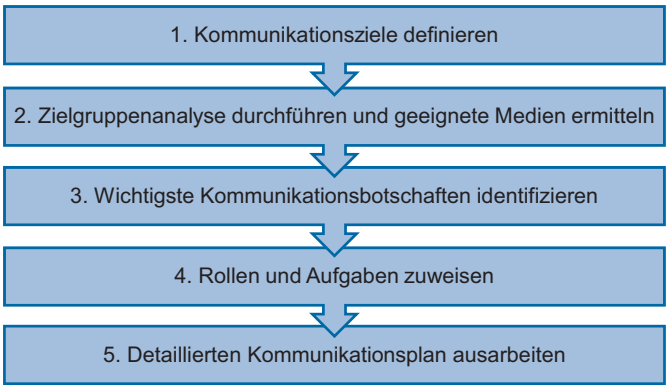


Abbildung 5: Ausarbeitung eines Kommunikationsplans

- 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 folgt 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
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

- 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 27001:2013 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 27001:2013 – Abschnitt 7.4

3.10 Competence and Awareness

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

Natürlich ist die Sensibilisierung der Mitarbeiter und Führungskräfte kein Allheilmittel, wenn es um die Vermeidung von Sicherheitsvorfällen geht. Es gibt auch keine empirischen Nachweise, dass die Anzahl an Sicherheitsvorfällen mit oder nach der Durchführung von Sensibilisierungskampagnen sinkt. Für berichtete Sicherheitsvorfälle ist meist sogar das Gegenteil der Fall, da die Mitarbeiter aufgrund der gestiegenen Sensibilität für das Thema vermehrt Vorfälle melden (unabhängig davon, ob darunter auch Fehlmeldungen sind). Das heißt im Umkehrschluss, dass viele gemeldete Ereignisse nicht schlecht sein müssen. Eines ist allerdings klar: Je weniger sich ein Mitarbeiter oder eine Führungskraft der konkreten Risiken bewusst ist, mit denen er oder sie tagtäglich konfrontiert ist, und je weniger die geltenden Sicherheitsvorgaben und -prozesse bei den jeweils Betroffenen bekannt sind, desto schwieriger wird es, das angestrebte Sicherheitsniveau im Unternehmen zu erfüllen und transparent zu machen.

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 der relevanten Informationssicherheitsrichtlinien aufseiten der Vorgabenempfänger (Mitarbeiter, Führungskräfte, externe Partner) muss sichergestellt werden.
- Der Beitrag eines jeden Mitarbeiters innerhalb des ISMS-Geltungsbereichs zur Wirksamkeit der Informationssicherheitsrichtlinien sollte aus den Materialien, die im Rahmen einer Awareness-Maßnahme verwendet werden, hervorgehen und kann optional durch Tests nachgewiesen werden.
- Auswirkungen und ggf. Sanktionen bei Nichteinhaltung von Sicherheitsbestimmungen sollten aus den Materialien, die im Rahmen einer Awareness-Maßnahme verwendet werden, hervorgehen.

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:

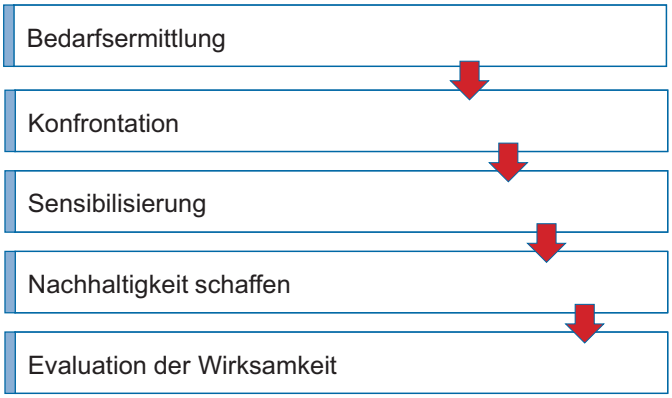


Abbildung 6: Phasenmodell für Security-Awareness-Kampagnen

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 Mitarbeiter, 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.

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 aufgenommen.

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 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-Materialen 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-Materialen durch die eigenen Mitarbeiter im Rahmen der IS-Kampagne. Eine zusätzliche Motivation zur Mitarbeit kann über ein Incentive-System[28] erreicht werden.

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:

- Aktuelle News veröffentlichen (z. B. über das Intranet, Mitarbeiterzeitung)
- Einbindung eines Onlinequiz zum Thema IS im Intranet (evtl. mit Incentivierung)
- Nutzung eines Bildschirmschoners mit ansprechenden Sicherheitsbotschaften

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
- Ergebnisse eines Quiz oder Tests zum Thema Informationssicherheit

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 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-/Schulungsplan**
  - 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 27001:2013 – Abschnitte 7.2 und 7.3

3.11 Supplier Relationships

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

Der Begriff »Dienstleister« bzw. »Lieferant«

Im Selbstverständnis der Norm ISO/IEC 27001:2013 umfasst der Begriff »Supplier« eine große Bandbreite von Geschäftsbeziehungen zu externen Firmen und Partnern und kann beispielsweise Beziehungen aus den Bereichen Logistik, Versorgungseinrichtungen, IT-(Outsourcing-)Dienstleister, Facility Management, Reinigungsdienstleister, aber auch viele andere beinhalten.

Die Anforderungen von ISO/IEC 27001:2013 fokussieren auf verschiedene Schutzmaßnahmen, beispielsweise die Erstellung von Richtlinien (Abschnitt 15.1.1) und Vereinbarung vertraglicher Regelungen mit dem Lieferanten (Abschnitt 15.1.2), wobei auch die Risiken aus dessen ITK-Infrastruktur, Lieferketten und sonstigen Weiterverlagerungen zu berücksichtigen sind (Abschnitt 15.1.3). Regelungen zur Überwachung (Abschnitt 15.2.1) und zum Change-Management (Abschnitt 15.2.2) sind ebenfalls erforderlich.

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 notwendigen Aktivitäten. Eine Zertifizierung nach diesem Standard ist nicht möglich, jedoch wird eine gemeinsame Terminologie geschaffen, die u. a. viele konkrete Hilfestellungen zur Umsetzung gibt.

28 Incentive = Anreiz, Leistungsanreiz.

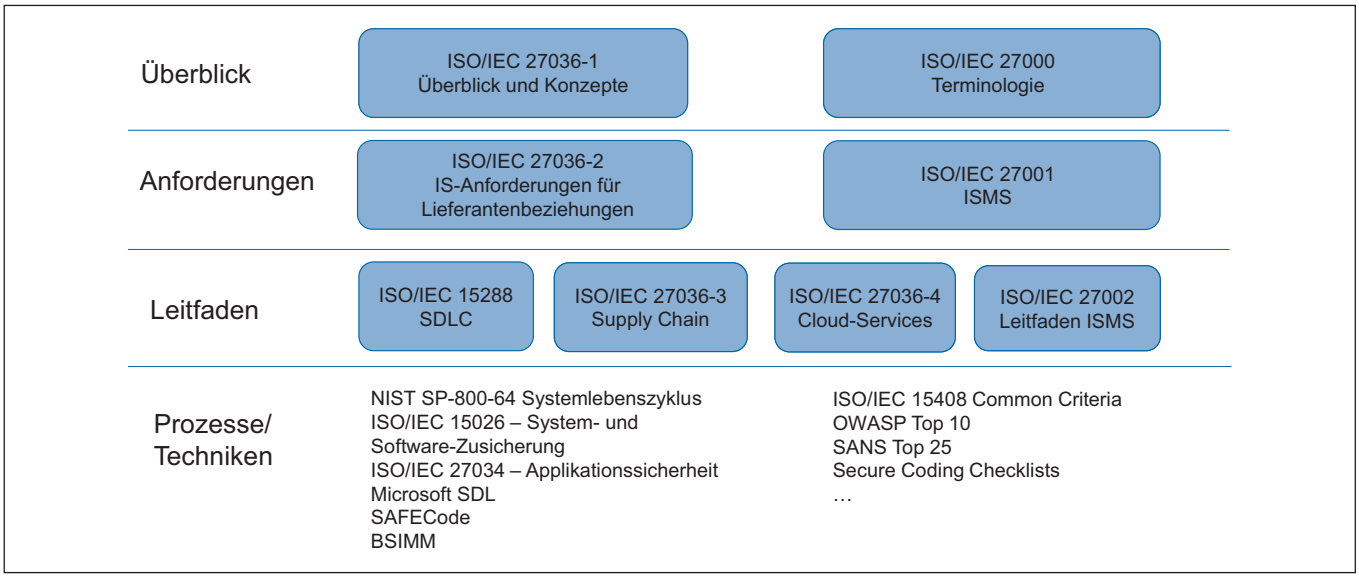


Abbildung 7: IS-Normenübersicht zu Lieferantenbeziehungen

Abbildung 7 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.

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

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 Zurverfügungstellung von Zertifikaten inklusive der jeweiligen Geltungsbereiche.

Zertifizierungen

Das Verlangen nach Informationssicherheit bei Kunden wird zunehmend durch Zertifizierungen beantwortet. Hierfür geeignet sind ISO/IEC 27001, ISO/IEC 27018 für die Verarbeitung personenbezogener Daten in einer Cloud oder – in Teilen – der internationale Standard ISAE 3402 »Assurance Reports on Controls at a Service Organization«.

- 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. 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[29] agieren, sehr kritisch zu prüfen.
- In diesen Kontext fällt ebenfalls das Thema Auftragsdatenverarbeitung nach § 11 BDSG[30] (ADV) unabhängig davon, wo der Dienstleister angesiedelt ist.

Kennzahlen

Folgende Kennzahlen[31] können beispielsweise zur Auswertung der Informationssicherheit in Bezug auf Dienstleister genutzt werden:

29 EWR: europäischer Wirtschaftsraum.
30 BDSG: Bundesdatenschutzgesetz.
31 Auszug aus McWhirter, Kurt; Gaughan, Ted: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

- Anzahl der Dienstleisterbeziehungen, die den definierten IS-Lieferantenprozess durchlaufen haben, im Verhältnis zu allen Dienstleisterbeziehungen
- Anzahl der Dienstleister, die IS-Maßnahmen vertraglich zusichern, im Verhältnis zu allen Dienstleistern
- Anzahl der Audits bei Dienstleistern in einem Jahr im Verhältnis zu allen Dienstleistern
- Anzahl der gemessenen Richtlinienverstöße durch Lieferanten
- Anzahl der Sicherheitsvorfälle bei Dienstleistern im vergangenen Berichtszeitraum

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 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:

- Es ist nach A.15.1.1 erforderlich, eine Richtlinie für Dienstleisterbeziehungen zu erstellen. In diesem Dokument sollten die Vorgaben, die sich aus der Beschaffungsstrategie und jeglicher Dienstleisterbeziehung ergeben, definiert werden.

Referenzen

ISO/IEC 27001:2013 – Abschnitte 4.3 und 8.1
ISO/IEC 27036-1:2014

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 27001:2013 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 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 Revision gemeint. 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 – Audits plant und verwaltet.

Erfolgsfaktoren aus der Praxis

Bei der Umsetzung interner Audits können zwei Bereiche unterschieden werden:

1. Das »Auditprogramm« bzw. »Auditrahmenwerk«, das als ein organisatorischer Überbau zur Steuerung und Überwachung aller Aktivitäten im Kontext interner Audits dient und die Schnittstelle zu anderen Prozessen im ISMS bildet.
2. 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 ist 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 für den Ressourceneinsatz im Auditbereich.

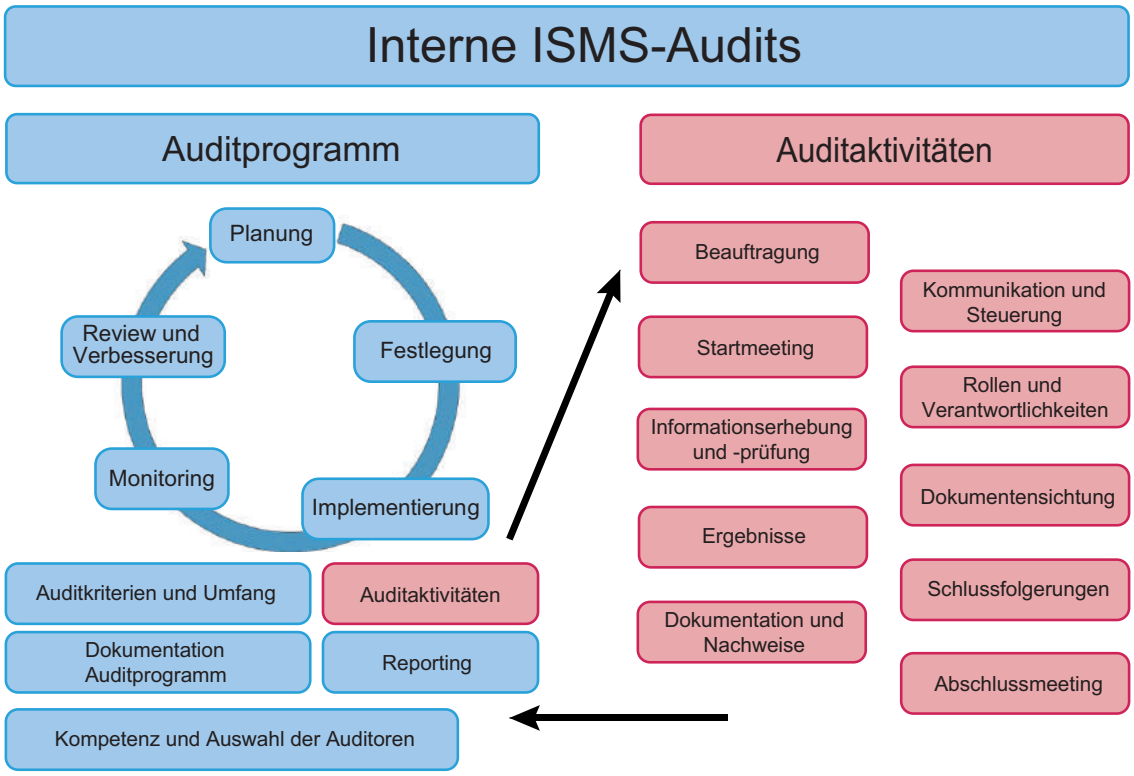


Abbildung 8: Struktur für interne ISMS-Audits (Auditprogramm vs. Auditaktivitäten)

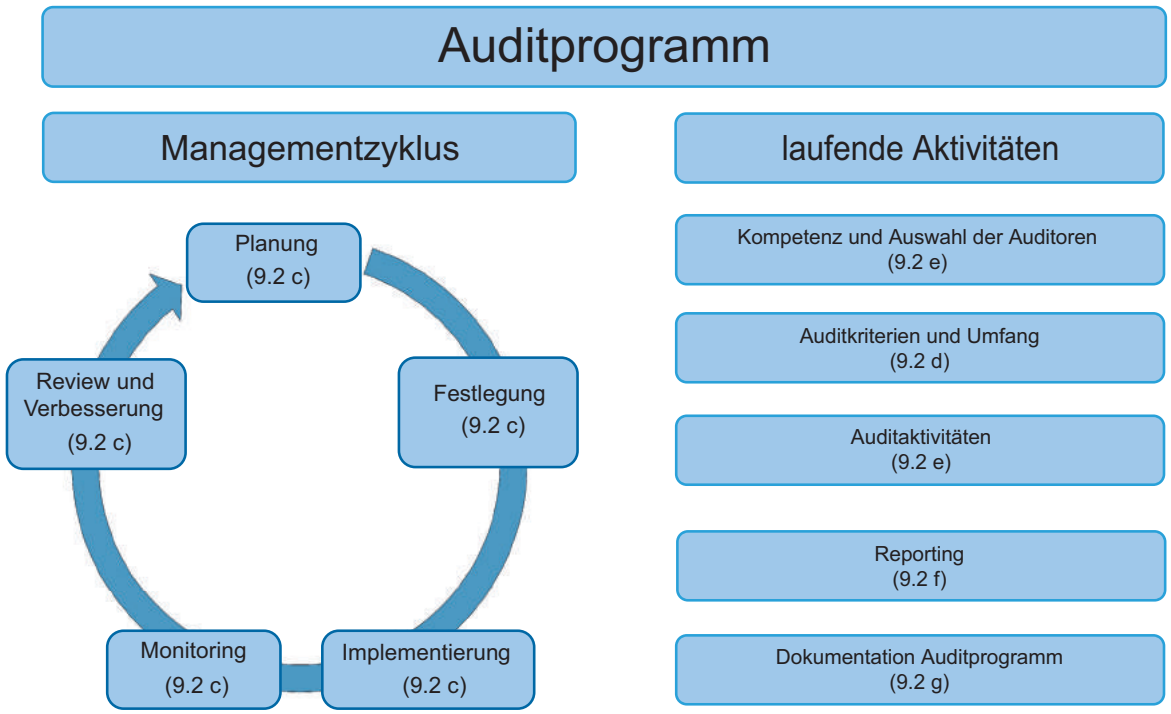


Abbildung 9: Anforderungen an das Auditprogramm[32]

32 Verweise in Klammern beziehen sich auf den Abschnitt 9.2 der Norm ISO/IEC 27001:2013.

Das Auditprogramm

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

- 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 dokumentierten 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.

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
- 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,
- 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 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.[32]

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 ist.
- 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, 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 Dateneigentümern 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.[33]
- 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 wird 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.
- 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 19011:2011 und ISO/IEC 27007:2011 erfüllt werden, wobei zu beachten ist, dass die normativen Anforderungen nach ISO/IEC 27001:2013 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 je-

32 Siehe auch Abschnitte 7.4, 7.5 und 7.6 der ISO/IEC 19011.

33 Siehe auch »Communication – The Missing Piece«, ISACA Journal 3/2012 *(http://www.isaca.org/Journal/Past-Issues/2012/Volume-3/Documents/12v3-Communication.pdf).*

doch sinngemäß auch für die internen ISMS-Audits angewendet werden.[34]

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 27006:2011 Requirements for bodies providing audit and certification of information security management systems« und »ISO/IEC TS 17021-2:2012 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 27001:2013 bestehen folgende Mindestanforderungen an die Dokumentation:

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

Referenzen

ISO/IEC 27001:2013 – Abschnitt 9.2
ISO/IEC 19011:2011
ISO/IEC 27007:2011
ISO/IEC 27006:2011
ISO/IEC TS 17021-2:2012

3.13 Incident Management

Obwohl dies 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-)Lösungen umsetzt, der erhält langfristig auch den bestmöglichen Nutzen eines innerhalb »unvorhersehbarer« Rahmenbedingungen (= Risiken) agierenden 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.

34 Siehe *www.isaca.de*.

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 Cyber-Angriffs.

- In diesem Kapitel wird »nur« das Thema »Informationssicherheitsvorfälle« adressiert. Für die Erarbeitung eines ganzheitlichen Notfallvorsorgesystems wird auf die ISO 22301:2012 »Societal security – 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 27002:2013). Dieser kann selbstverständlich nicht jede Eventualität abdecken und dient daher 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 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 nochmal 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.
- Der Prozess zur Sicherheitsvorfallbehandlung und dessen Detaillierungsgrad sollte dem Risikoappetit der Organisation und den Rahmenbedingungen des ISMS Rechnung tragen.

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.

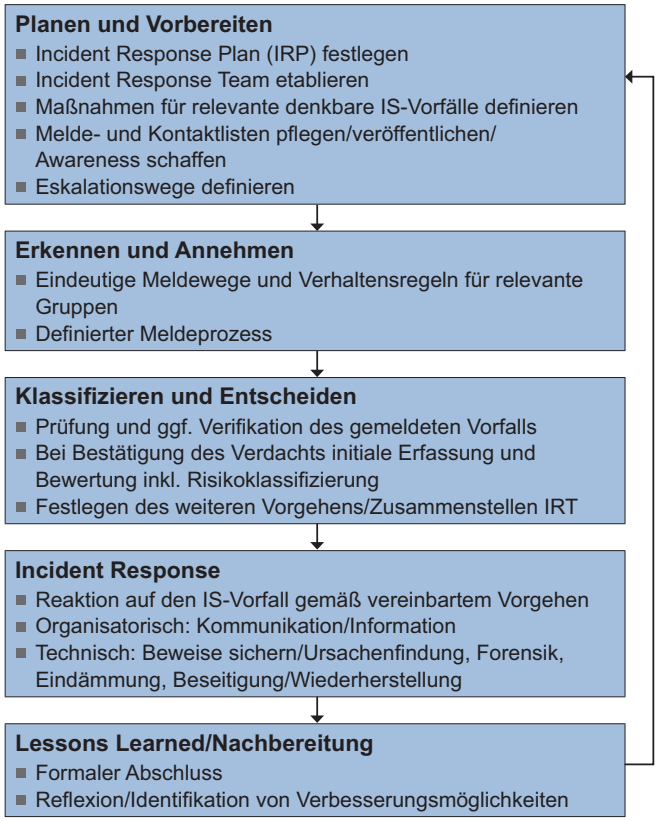


Abbildung 10: Incident Response Management – Phasenmodell angelehnt an ISO/IEC 27035

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 Zweifelfall 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) des/der betroffenen Personen und Informationen/IT-Systeme
  - Beschreibung des Security Incident (Wie ist der Angreifer vorgegangen, welche Schwachstellen wurden ausgenutzt? Bisher entstandener Schaden)

- 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. ISO, 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 A.16.1.7).

   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 der gewünschten Zielkonfiguration: 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 weitergehende 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 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.
- Die Bearbeitung von Sicherheitsvorfällen muss zum Abschluss immer zu einem Bericht führen, wie derartige Vorfälle in Zukunft zu vermeiden bzw. in ihrer Auswirkung zu minimieren sind. Daraus können ggf. weitere technische und organisatorische Maßnahmen abgeleitet werden, die in den Regelbetrieb zu überführen sind.

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 bestehen keine Mindestanforderungen an die Dokumentation.

Darüber hinaus 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 27001:2013 – A.16 (Annex A)
ISO/IEC 27035:2011
ISO 22301:2012

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 Maßnahmenzielen und Verantwortlichkeiten für deren Erreichung
  - Etablierung der Sicherheitsmaßnahmen zur Erreichung der Maßnahmenziele und der operativen Prozessverantwortlichen für diese Maßnahmen
  - Definition der Leistungsindikatoren, die eine Leistungsmessung gegen die Maßnahmenziele erlauben
  - 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 Maßnahmenzielerreichung mit Lieferung an das Security Controlling innerhalb des ISMS
  - Einleitung von Korrekturen bei festgestellten Mängeln oder Nichtkonformitäten
- **Check**
  - Überwachen der einzelnen Sicherheitsmaßnahmenindikatoren und Vergleichen der einzelnen Leistungsfähigkeiten mit den Maßnahmenzielen
  - Aufsicht über die eingeleiteten Gegenmaßnahmen und deren Verantwortliche, wenn eine Sicherheitsmaßnahme den Normbereich der Effektivität verlassen hat.
  - Erstellen von Sicherheitsberichten mit Key-Performance-Indikatoren für das Management, basierend auf den Maßnahmenzielen und Sicherheitszielen. Diese Berichte sollten Handlungsoptionen für notwendige Managemententscheidungen enthalten, die Sicherheitsmaßnahmen stärken, die regelmäßig in den Toleranzbereich laufen oder den Schwellwert zur Ineffektivität überschreiten.
- **Act**
  - Treffen von notwendigen Managemententscheidungen, um die Effektivität von Sicherheitsmaßnahmen oder ganzen Maßnahmenzielen 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
- Prüfung durch die Leitung (Managementbewertung)
- Betriebliches Vorschlagswesen (Verbesserungsvorschlag)
- Regelmäßig durchzuführende Risikoanalysen

- Maßnahmen aus dem KVP sollten in den übergreifenden Umsetzungs- bzw. Risikobehandlungsplan (der in der Regel aus der Informationssicherheitsrisikoeinschätzung resultiert) mit 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 Risikoanalysen stellen einen wesentlichen Bestandteil der Verbesserung des ISMS dar, da hierbei risikominimierende Maßnahmen identifiziert und in Risikobehandlungspläne zur Umsetzung aufgenommen werden. Außerdem wird über die Risikobehandlung die Umsetzung dieser Maßnahmen überwacht und deren Wirksamkeit bewertet.
- Korrektur vs. Korrekturmaßnahme: Bei Feststellung von Mängeln und Nichtkonformitäten muss die Organisation reagieren und diese korrigieren bzw. abstellen (siehe

Abschnitt 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 Abschnitt 10.1 c bis g).

Anforderungen an die Dokumentation

Gemäß ISO/IEC 27001:2013 bestehen folgende Mindestanforderungen an die Dokumentation:

- Nachweise über die Art von Nichtkonformitäten sowie über sämtliche umgesetzte reaktive Maßnahmen (Abschnitt 10.1 f)
- 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

Referenzen

ISO/IEC 27001:2013 – Abschnitt 10
ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2015 – Annex SL

4. Glossar

ADV Auftragsdatenverarbeitung – die Verarbeitung von personenbezogenen Daten durch Dienstleister (extern oder intern durch rechtlich eigenständige Einheiten einer Unternehmensgruppe) gemäß § 11 BDSG.

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 27005:2011 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.

BDSG Bundesdatenschutzgesetz

BIA Business Impact Analysis

BO Betriebsorganisation

BSI Bundesamt für Sicherheit in der Informationstechnik

BSIMM Building Security in Maturity Model

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.

DSB Datenschutzbeauftragter

EU Europäische Union

EWR Europäischer Wirtschaftsraum

GoBS Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

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

IKS Internes Kontrollsystem

IS Informationssicherheit, Information Security

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

KPI Key-Performance-Indikator – ein Leistungsindikator

KVP Kontinuierlicher Verbesserungsprozess

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

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

QS Qualitätssicherung

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

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 31000:2009)

Scope Geltungsbereich

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.

TMG Telemediengesetz

TOMs Technische und organisatorische Maßnahmen

UWG Gesetz gegen den unlauteren Wettbewerb

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.

5. Referenzen

Normen und Standards

ISO 9001:2015 Quality management systems — Requirements

ISO 19011:2011 Guidelines for auditing management systems

ISO 22301:2012 Societal security — Business continuity management systems — Requirements

ISO 31000:2009 Risk management — Principles and guidelines

IEC 31010:2009 Risk management — Risk assessment techniques

ISO Guide 73:2009 Risk management — Vocabulary

ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance

ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management

ISO/IEC 27006:2011 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing

ISO/IEC 27018:2014 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 27035:2011 Information technology — Security techniques — Information security incident management

ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for 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 — Procedures specific to ISO, 2015

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

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

ISO/IEC TS 17021-2:2012 Conformity assessment — Requirements for bodies providing audit and certification of management systems

ONR 49000:2008 Risikomanagement für Organisationen und Systeme

Weitere Quellen

COBIT 5 for Information Security, ISACA, 2012

BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, 2008

BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5, 2008

IT-Grundschutz-Kataloge des BSI, 14. Ergänzungslieferung, 2014

Leitfaden Cyber-Sicherheits-Check, BSI/ISACA, 2014

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

6. Abbildungsverzeichnis

7. Anlage 1: Mapping ISO/IEC 27001:2013 vs. ISO/IEC 27001:2005

Legende: ● = vollständige Abdeckung der Inhalte ○ = teilweise Abdeckung der Inhalte

Norm-Abschnitte (4 – 6)

ISO/IEC 27001:2013	ISO/IEC 27001:2005																
4 Context of the organization	**4 Information security management system**																
4.1 Understanding the organization and its context	4.1 General requirements					●											
4.2 Understanding the needs and expectations of interested parties	4.2 Establishing and managing the ISMS																
4.3 Determining the scope of the information security management system	4.2.1 Establish the ISMS				●			○	●				●	●	●		
4.4 Information security management system	4.2.2 Implement and operate the ISMS														○		
5 Leadership	4.2.3 Monitor and review the ISMS													○			○
5.1 Leadership and commitment	4.2.4 Maintain and improve the ISMS																
5.2 Policy	4.3 Documentation requirements																
5.3 Organizational roles, responsibilities and authorities	4.3.1 General				○				○				○	○	○	○	
6 Planning	4.3.2 Control of documents								○								
6.1 Actions to address risks and opportunities	4.3.3 Control of records								○	○							
6.1.1 General	**5 Management responsibility**																
6.1.2 Information security risk assessment	5.1 Management commitment							●	●	●				○			●
6.1.3 Information security risk treatment	5.2 Resource management																
6.2 Information security objectives and planning to achieve them	5.2.1 Provision of resources			○		○											
	5.2.2 Training, awareness and competence																
	6 Internal ISMS audits									○							
	7 Management review of the ISMS																
	7.1 General																
	7.2 Review input														○		
	7.3 Review output			●													
	8 ISMS improvement																
	8.1 Continual improvement																
	8.2 Corrective action																
	8.3 Preventive action		●												○		

ISO/IEC 27001:2013	ISO/IEC 27001:2005																					
Norm-Abschnitte (7 – 10)	4.1 General requirements	4.2 Establishing and managing the ISMS	4.2.1 Establish the ISMS	4.2.2 Implement and operate the ISMS	4.2.3 Monitor and review the ISMS	4.2.4 Maintain and improve the ISMS	4.3 Documentation requirements	4.3.1 General	4.3.2 Control of documents	4.3.3 Control of records	5.1 Management commitment	5.2 Resource management	5.2.1 Provision of resources	5.2.2 Training, awareness and competence	6 Internal ISMS audits	7 Management review of the ISMS	7.1 General	7.2 Review input	7.3 Review output	8 ISMS improvement	8.1 Continual improvement	8.2 Corrective action	8.3 Preventive action
4 Information security management system																						
7 Support																						
7.1 Resources				○									●									
7.2 Competence														●								
7.3 Awareness				○										●								
7.4 Communication						○					○											
7.5 Documented information																						
7.5.1 General								●														
7.5.2 Creating and updating								○	●													
7.5.3 Control of documented information									●	●												
8 Operation																						
8.1 Operational planning and control				●						○												○
8.2 Information security risk assessment					●			○														
8.3 Information security risk treatment					●					○												
9 Performance evaluation																						
9.1 Monitoring, measurement, analysis and evaluation					○	●		○								○						
9.2 Internal audit					○			○		○					●							
9.3 Management review					○			○									●	●	●			
10 Improvement																						
10.1 Nonconformity and corrective action						○															●	●
10.2 Continual improvement						○							○							●		

ISO/IEC 27001:2013	ISO/IEC 27001:2005																			
Annex A (A.5 – A.9)	A.10.10 Monitoring																			
	A.10.9 Electronic commerce services																			
	A.10.8 Exchange of information														○					
	A.10.7 Media handling													○	●					
	A.10.6 Network security management																			
	A.10.5 Back-up																			
	A.10.4 Protection against malicious and mobile code																			
	A.10.3 System planning and acceptance																			
	A.10.2 Third party service delivery management																			
	A.10.1 Operational procedures and responsibilities				○															
	A.10 Communications and operations management																			
	A.9.2 Equipment security																			
	A.9.1 Secure areas																			
	A.9 Physical and environmental security																			
	A.8.3 Termination or change of employment									●			○					○		
	A.8.2 During employment								●											
	A.8.1 Prior to employment				○			●												
	A.8 Human resources security																			
	A.7.2 Information classification													●						
	A.7.1 Responsibility for assets												●							
	A.7 Asset management																			
	A.6.2 External parties																			
	A.6.1 Internal organization				●															
	A.6 Organization of information security																			
	A.5.1 Information security policy		●																	
	A.5 Security policy																			
	A.5 Information security policies																			
	A.5.1 Management direction for information security																			
	A.6 Organisation of information security																			
	A.6.1 Internal organisation																			
	A.6.2 Mobile devices and teleworking																			
	A.7 Human resource security																			
	A.7.1 Prior to employment																			
	A.7.2 During employment																			
	A.7.3 Termination and change of employment																			
	A.8 Asset management																			
	A.8.1 Responsibility of assets																			
	A.8.2 Information classification																			
	A.8.3 Media handling																			
	A.9 Access control																			
	A.9.1 Business requirements for access control																			
	A.9.2 User access management																			
	A.9.3 User responsibilities																			

ISO/IEC 27001:2013	ISO/IEC 27001:2005																	
Annex A (A.10 – A.13)	A.5.1 Information security policy	**A.5 Security policy**	**A.6 Organization of information security**	A.6.1 Internal organization	A.6.2 External parties	**A.7 Asset management**	A.7.1 Responsibility for assets	A.7.2 Information classification	**A.8 Human resources security**	A.8.1 Prior to employment	A.8.2 During employment	A.8.3 Termination or change of employment	**A.9 Physical and environmental security**	A.9.1 Secure areas	A.9.2 Equipment security	**A.10 Communications and operations management**	A.10.1 Operational procedures and responsibilities	A.10.2 Third party service delivery management
A.9.4 System and application access control																		
A.10 Cryptography																		
A.10.1 Cryptographic controls																		
A.11 Physical and environmental security																		
A.11.1 Secure areas														●				
A.11.2 Equipment															●			
A.12 Operations security																		
A.12.1 Operational procedures and responsibilities																	●	
A.12.2 Protection from malware																		●
A.12.3 Backup																		
A.12.4 Logging and monitoring																		
A.12.5 Control of operational software																		
A.12.6 Technical vulnerability management																		
A.12.7 Information systems audit considerations																		
A.13 Communications strategy																		
A.13.1 Network security management																		
A.13.2 Information transfer				○														

ISO/IEC 27001:2005																		
A.10.10 Monitoring											●							
A.10.9 Electronic commerce services																		
A.10.8 Exchange of information																		●
A.10.7 Media handling																		
A.10.6 Network security management																	●	
A.10.5 Back-up										●								
A.10.4 Protection against malicious and mobile code									●									
A.10.3 System planning and acceptance								○										
A.10.2 Third party service delivery management																		
A.10.1 Operational procedures and responsibilities								●										
A.10 Communications and operations management																		
A.9.2 Equipment security							●											
A.9.1 Secure areas						●												
A.9 Physical and environmental security																		
A.8.3 Termination or change of employment																		
A.8.2 During employment																		
A.8.1 Prior to employment																		
A.8 Human resources security																		
A.7.2 Information classification																		
A.7.1 Responsibility for assets																		
A.7 Asset management																		
A.6.2 External parties																		
A.6.1 Internal organization																		○
A.6 Organization of information security																		
A.5.1 Information security policy																		
A.5 Security policy																		

ISO/IEC 27001:2013	ISO/IEC 27001:2005																	
Annex A (A.14 – A.18)	A.10.10 Monitoring																	
	A.10.9 Electronic commerce services																	
	A.10.8 Exchange of information																	
	A.10.7 Media handling																	
	A.10.6 Network security management																	
	A.10.5 Back-up																	
	A.10.4 Protection against malicious and mobile code																	
	A.10.3 System planning and acceptance			○				○						○				
	A.10.2 Third party service delivery management						●	●										
	A.10.1 Operational procedures and responsibilities																	
	A.10 Communications and operations management																	
	A.9.2 Equipment security																	
	A.9.1 Secure areas																	
	A.9 Physical and environmental security																	
	A.8.3 Termination or change of employment																	
	A.8.2 During employment																	
	A.8.1 Prior to employment																	
	A.8 Human resources security																	
	A.7.2 Information classification																	
	A.7.1 Responsibility for assets																	
	A.7 Asset management																	
	A.6.2 External parties						●											
	A.6.1 Internal organization																	○
	A.6 Organization of information security																	
	A.5.1 Information security policy																	
	A.5 Security policy																	
	A.14 System acquisition, development and maintenance																	
	A.14.1 Security requirements for Information systems																	
	A.14.2 Security in development and support processes																	
	A.14.3 Test data																	
	A.15 Supplier relationships																	
	A.15.1 Information security in supplier relationships																	
	A.15.2 Supplier service delivery management																	
	A.16 Information security incident management																	
	A.16.1 Management of information security incidents and management																	
	A.17 Information security aspects of business continuity management																	
	A.17.1 Information security continuity																	
	A.17.2 Redundancies																	
	A.18 Compliance																	
	A.18.1 Compliance with legal requirements																	
	A.18.2 Information security reviews																	

ISO/IEC 27001:2013	ISO/IEC 27001:2005								
Annex A (A.5 – A.7) cont.	A.15.3 Information systems audit considerations								
	A.15.2 Compliance with security policies and standards, and technical compliance								
	A.15.1 Compliance with legal requirements								
	A.15 Compliance								
	A.14.1 Information security aspects of business continuity management								
	A.14 Business continuity management								
	A.13.2 Management of information security incidents and improvements								
	A.13.1 Reporting information security events and weaknesses								
	A.13 Information security incident management								
	A.12.6 Technical vulnerability management								
	A.12.5 Security in development and support processes								
	A.12.4 Security of system files								
	A.12.3 Cryptographic controls								
	A.12.2 Correct processing in applications								
	A.12.1 Security requirements of information systems								
	A.12 Information systems acquisition, development and maintenance								
	A.11.7 Mobile computing and teleworking					●			
	A.11.6 Application and information access control								
	A.11.5 Operating system access control								
	A.11.4 Network access control								
	A.11.3 User responsibilities								
	A.11.2 User access management								
	A.11.1 Business requirement for access control								
	A.11 Access control								
A.5 Information security policies									
A.5.1 Management direction for information security									
A.6 Organisation of information security									
A.6.1 Internal organisation									
A.6.2 Mobile devices and teleworking									
A.7 Human resource security									
A.7.1 Prior to employment									
A.7.2 During employment									
A.7.3 Termination and change of employment									

ISO/IEC 27001:2013	ISO/IEC 27001:2005									
Annex A (A.8 – A.9) cont.	A.15.3 Information systems audit considerations									
	A.15.2 Compliance with security policies and standards, and technical compliance									
	A.15.1 Compliance with legal requirements									
	A.15 Compliance									
	A.14.1 Information security aspects of business continuity management									
	A.14 Business continuity management									
	A.13.2 Management of information security incidents and improvements									
	A.13.1 Reporting information security events and weaknesses									
	A.13 Information security incident management									
	A.12.6 Technical vulnerability management									
	A.12.5 Security in development and support processes				○					
	A.12.4 Security of system files									○
	A.12.3 Cryptographic controls									
	A.12.2 Correct processing in applications									
	A.12.1 Security requirements of information systems									
	A.12 Information systems acquisition, development and maintenance									
	A.11.7 Mobile computing and teleworking									
	A.11.6 Application and information access control									●
	A.11.5 Operating system access control									●
	A.11.4 Network access control						○			
	A.11.3 User responsibilities								●	
	A.11.2 User access management							●		
	A.11.1 Business requirement for access control						●			
	A.11 Access control									
	A.8 Asset management	A.8.1 Responsibility of assets	A.8.2 Information classification	A.8.3 Media handling	**A.9 Access control**	A.9.1 Business requirements for access control	A.9.2 User access management	A.9.3 User responsibilities	A.9.4 System and application access control	

ISO/IEC 27001:2013	ISO/IEC 27001:2005									
Annex A (A.10 – A.12) cont.	A.15.3 Information systems audit considerations									
	A.15.2 Compliance with security policies and standards, and technical compliance									
	A.15.1 Compliance with legal requirements									
	A.15 Compliance									
	A.14.1 Information security aspects of business continuity management									
	A.14 Business continuity management									
	A.13.2 Management of information security incidents and improvements									
	A.13.1 Reporting information security events and weaknesses									
	A.13 Information security incident management									
	A.12.6 Technical vulnerability management									
	A.12.5 Security in development and support processes					○				
	A.12.4 Security of system files									
	A.12.3 Cryptographic controls		●							
	A.12.2 Correct processing in applications									
	A.12.1 Security requirements of information systems									
	A.12 Information systems acquisition, development and maintenance									
	A.11.7 Mobile computing and teleworking									
	A.11.6 Application and information access control									
	A.11.5 Operating system access control									
	A.11.4 Network access control									
	A.11.3 User responsibilities					○				
	A.11.2 User access management									
	A.11.1 Business requirement for access control									
	A.11 Access control									
	A.10 Cryptography									
	A.10.1 Cryptographic controls									
	A.11 Physical and environmental security									
	A.11.1 Secure areas									
	A.11.2 Equipment									
	A.12 Operations security									
	A.12.1 Operational procedures and responsibilities									
	A.12.2 Protection from malware									
	A.12.3 Backup									

ISO/IEC 27001:2013	ISO/IEC 27001:2005							
Annex A (A.12 – A.13) cont.	A.15.3 Information systems audit considerations				●			
	A.15.2 Compliance with security policies and standards, and technical compliance							
	A.15.1 Compliance with legal requirements							
	A.15 Compliance							
	A.14.1 Information security aspects of business continuity management							
	A.14 Business continuity management							
	A.13.2 Management of information security incidents and improvements							
	A.13.1 Reporting information security events and weaknesses							
	A.13 Information security incident management							
	A.12.6 Technical vulnerability management			●				
	A.12.5 Security in development and support processes			○				
	A.12.4 Security of system files		●	○				
	A.12.3 Cryptographic controls							
	A.12.2 Correct processing in applications							
	A.12.1 Security requirements of information systems							
	A.12 Information systems acquisition, development and maintenance							
	A.11.7 Mobile computing and teleworking							
	A.11.6 Application and information access control							
	A.11.5 Operating system access control							
	A.11.4 Network access control						○	
	A.11.3 User responsibilities							
	A.11.2 User access management							
	A.11.1 Business requirement for access control							
	A.11 Access control							
A.12.4 Logging and monitoring								
A.12.5 Control of operational software								
A.12.6 Technical vulnerability management								
A.12.7 Information systems audit considerations								
A.13 Communications strategy								
A.13.1 Network security management								
A.13.2 Information transfer								

ISO/IEC 27001:2013	ISO/IEC 27001:2005							
Annex A (A.14 – A.15) cont.	A.15.3 Information systems audit considerations							
	A.15.2 Compliance with security policies and standards, and technical compliance							
	A.15.1 Compliance with legal requirements							
	A.15 Compliance							
	A.14.1 Information security aspects of business continuity management							
	A.14 Business continuity management							
	A.13.2 Management of information security incidents and improvements							
	A.13.1 Reporting information security events and weaknesses							
	A.13 Information security incident management							
	A.12.6 Technical vulnerability management							
	A.12.5 Security in development and support processes			●				
	A.12.4 Security of system files				●			
	A.12.3 Cryptographic controls							
	A.12.2 Correct processing in applications		○	○				
	A.12.1 Security requirements of information systems		●					
	A.12 Information systems acquisition, development and maintenance							
	A.11.7 Mobile computing and teleworking							
	A.11.6 Application and information access control							
	A.11.5 Operating system access control							
	A.11.4 Network access control							
	A.11.3 User responsibilities							
	A.11.2 User access management							
	A.11.1 Business requirement for access control							
	A.11 Access control							
	A.14 System acquisition, development and maintenance							
	A.14.1 Security requirements for Information systems							
	A.14.2 Security in development and support processes							
	A.14.3 Test data							
	A.15 Supplier relationships							
	A.15.1 Information security in supplier relationships							
	A.15.2 Supplier service delivery management							

ISO/IEC 27001:2013	ISO/IEC 27001:2005								
Annex A (A.16 – A.18) cont.	A.15.3 Information systems audit considerations								
	A.15.2 Compliance with security policies and standards, and technical compliance								●
	A.15.1 Compliance with legal requirements							●	
	A.15 Compliance								
	A.14.1 Information security aspects of business continuity management				●				
	A.14 Business continuity management								
	A.13.2 Management of information security incidents and improvements		●						
	A.13.1 Reporting information security events and weaknesses		●						
	A.13 Information security incident management								
	A.12.6 Technical vulnerability management								
	A.12.5 Security in development and support processes								
	A.12.4 Security of system files								
	A.12.3 Cryptographic controls								
	A.12.2 Correct processing in applications								
	A.12.1 Security requirements of information systems								
	A.12 Information systems acquisition, development and maintenance								
	A.11.7 Mobile computing and teleworking								
	A.11.6 Application and information access control								
	A.11.5 Operating system access control								
	A.11.4 Network access control								
	A.11.3 User responsibilities								
	A.11.2 User access management								
	A.11.1 Business requirement for access control								
	A.11 Access control								
	A.16 Information security incident management								
	A.16.1 Management of information security incidents and management								
	A.17 Information security aspects of business continuity management								
	A.17.1 Information security continuity								
	A.17.2 Redundancies								
	A.18 Compliance								
	A.18.1 Compliance with legal requirements								
	A.18.2 Information security reviews								

8. Anlage 2: Versionsvergleich ISO/IEC 27001:2013 vs. ISO/IEC 27001:2005

Nachfolgend finden Sie eine kurze Darstellung der wesentlichen inhaltlichen Änderungen der ISO/IEC 27001:2013 gegenüber der Vorgängerversion aus dem Jahr 2005.

Die wesentliche Änderung in Bezug auf die **Leitungsebene** ist die Entfernung der 2005er-Maßnahme A.6.1.1 »*Management commitment to information security*« und die stärkere Integration der Anforderungen an die Unternehmensleitung in die Grundlagen des Informationssicherheitsmanagements im normativen Abschnitt 5.1 der Version 2013. Zudem wird nun nicht mehr von »Management«, sondern primär von »Topmanagement« gesprochen (siehe Abschnitte 5 und 9.3). Durch diese Änderung wird die grundlegende Bedeutung des Engagements (engl. *commitment*) der höchsten Leitungsebene noch stärker in den Vordergrund gerückt. Des Weiteren wird in der neuen Version die nachvollziehbare Konsistenz der Informationssicherheitsziele mit den Geschäftszielen explizit gefordert und ist durch das Topmanagement sicherzustellen.

Die **Integration des Themas Informationssicherheit** in andere Geschäftsprozesse und allgemein in alle Projekte wird in der aktuellen Version als eine explizite Anforderung hervorgehoben (siehe Maßnahme A.6.1.5 »*Information security in project management*«).

Die Version 2005 forderte im Kontext der **Informationssicherheitsleitlinie**, dass geschäftliche, gesetzliche oder amtliche Anforderungen und vertragliche Sicherheitsverpflichtungen beschrieben sind. Dies wird man gemäß der Version 2013 nun eher im Scope-Dokument erwarten (siehe Abschnitt 4). Darüber hinaus müssen in der Informationssicherheitsleitlinie nicht mehr zwingend (alle) Kriterien für das Risikomanagement im Kontext Informationssicherheit definiert sein. Das wird man nun in entsprechend detailliert ausgearbeiteten Methodenbeschreibungen bzw. in einer separat ausgearbeiteten Risikostrategie zur Informationssicherheit erwarten (siehe Abschnitt 6.1).

Der außerordentliche Stellenwert des **Risikomanagements** im Rahmen eines ISMS wird in der 2013er-Version noch deutlicher hervorgehoben als zuvor (siehe Abschnitt 0.1). Zudem wird dem Themengebiet eine klarere Strukturierung gegeben als in der Vorgängerversion. Dort waren Anforderungen an das Risikomanagement verteilt in verschiedenen Abschnitten enthalten, beispielsweise als Unterpunkte des Abschnitts 4.2.1 »*Establish the ISMS*«. Nun werden dem Thema drei eigene Abschnitte gewidmet (siehe Abschnitte 6.1, 8.2, 8.3). Die Forderung nach einem Risikobehandlungsplan ist nach wie vor als ein zentrales Element enthalten (vgl. Abschnitt 8.3 der ISO/IEC 27001:2013 vs. Abschnitte 4.2.2 und 7.3 der ISO/IEC 27001:2005).

Die Anforderungen bzgl. der im Kontext eines ISMS notwendigen **Rollen und Verantwortlichkeiten** finden sich in der ISO/IEC 27001:2013 zwar in anderen Abschnitten wieder, waren aber im Kern bereits in der Version 2005 vorhanden (vgl. Abschnitte 5.3, 7.1 und 7.2 der ISO/IEC 27001:2013 vs. Abschnitte 5.2.1 und 5.2.2 der ISO/IEC 27001:2005).

In der Version 2005 waren das Monitoring und die **Effektivitätsmessung von Sicherheitsmaßnahmen** ein Unterpunkt des Abschnitts »*Management Review*« (siehe Abschnitte 4.2.2 d und 4.2.3). Dort wurden einige allgemeine Anforderungen hinsichtlich der Überwachung und Überprüfung des ISMS aufgeführt. Die Hinweise der ISO/IEC 27004:2009 wurden nicht explizit erwähnt und galten daher höchstens als Empfehlung. In der 2013er-Version wird dem Thema nun größere Aufmerksamkeit und sogar ein eigener Abschnitt gewidmet. Dokumentationsanforderungen zum Performance Monitoring sind nun verpflichtender Bestandteil für eine etwaige Zertifizierung (siehe Abschnitt 9.1).

Bei den Anforderungen bzgl. **interner Audits** ist es zu keinen fundamentalen Änderungen gekommen (vgl. Abschnitt 9.2 der ISO/IEC 27001:2013 vs. Abschnitte 4.2.3 e und 6 der ISO/IEC 27001:2005). Interne Audits sind nach wie vor durchzuführen, allerdings ohne dass eine Prozessdokumentation zur Beschreibung des Vorgehens erstellt werden muss. Für größere Institutionen ist es jedoch noch immer empfehlenswert, diesen Prozess formal zu dokumentieren, um damit beispielsweise mehrere für interne Audits zuständige Organisationseinheiten einen identischen Prozess nutzen zu lassen bzw. die Abgrenzungen und Verantwortlichkeiten dieser Auditabteilungen klar herauszustellen (ISMS-Audits, Interne Revision, Datenschutz, technische IT-Sicherheitsaudits etc.). Die Erstellung und Umsetzung eines ausreichend detaillierten Auditprogramms ist hingegen explizit gefordert (siehe Abschnitt 9.2 c). Abschnitt 9.2 a, Satz 2 könnte zu der Annahme verleiten, dass die Anforderungen nun weniger restriktiv sind als in Abschnitt 6 der Version 2005. Dies ist jedoch nicht der Fall. Es muss bei internen Audits obligatorisch auf *alle* An-

forderungen aus der Norm geachtet werden. Somit ist auch auf die Einhaltung relevanter Gesetzgebung und Regularien und die vorhandenen Anforderungen der Interessengruppen zu achten (siehe Abschnitte 4.2 und 4.3).

Bezüglich der Anforderungen an die **Dokumentation** ist ein wichtiger Unterschied zur Version aus 2005, dass in Abschnitt 7.5 der Version 2013 keine explizite Aufzählung der zu erstellenden Dokumente mehr erfolgt. Konkrete Informationen und Dokumente ergeben sich nunmehr ausschließlich aus den Anforderungen der jeweiligen Einzelabschnitte und, je nach Geltungsbereich, des Annex A.

Die wichtigsten Änderungen im Kontext der **Kommunikation** betreffen die Aufnahme des Themas in einen eigenen Abschnitt (siehe Abschnitt 7.4) und die expliziten Anforderungen an interne **und** externe Kommunikation. Die Anforderungen sind nun wesentlich spezifischer als in der Vorgängerversion, folgen aber weitestgehend der gängigen Praxis.

In der alten Norm wurde das Thema **Awareness** nur in einem einzigen Satz explizit behandelt (siehe Abschnitt 5.2.2). Die neue Norm weist hingegen einen eigenen Abschnitt auf und verdeutlicht so die Wichtigkeit von Awareness-Maßnahmen. Es werden auch drei konkrete Anforderungen definiert, die nachweislich zu erfüllen sind (siehe Abschnitt 7.3).

Die Version 2013 legt nachvollziehbar einen Schwerpunkt auf die beiden Themen **Outsourcing** und **Lieferantenbeziehungen** und widmet diesen sogar eine eigene Kontrolldomäne im Annex A (siehe A.15 »*Supplier relationships*«). Im Unterschied zur Vorgängerversion wird in der Norm nicht mehr (nur) von *Stakeholdern*, deren Anforderungen und Erwartungen initial zu ermitteln sind, gesprochen, sondern von dem weitreichenderen Begriff der *Interested Parties*. Lieferanten (*Supplier*) werden explizit aufgeführt (siehe auch Kapitel *3.1 Context of the Organization* in diesem Leitfaden). Allerdings hält sich die Norm zurück mit konkreten Vorgaben zur Umsetzung und überlässt die jeweilige Ausgestaltung der nicht zertifizierungsfähigen Norm ISO/IEC 27036.

Eine wesentliche Änderung in puncto **kontinuierliche Verbesserung** ist, dass der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) nicht mehr explizit erforderlich ist. Es kann vielmehr jede Organisationsform genutzt werden, die kontinuierliche Verbesserungen unterstützt. Allerdings ergibt sich aus dem Aufbau und den Inhalten der Norm (Abschnitte 4 bis 10) nun ein »im Hintergrund« wirkender PDCA-Zyklus:

- Plan: Kontext/Führungsaufgaben/Planung (Abschnitte 4, 5 und 6)
- Do: Rahmenbedingungen/Support/Umsetzung (Abschnitte 7 und 8)
- Check: Überprüfung (Abschnitt 9)
- Act: Reaktion/Verbesserung (Abschnitt 10)

Die explizite Anforderung zur Umsetzung von **Vorbeugungsmaßnahmen** ist nicht mehr enthalten. Diese ergibt sich aber implizit aus den Abschnitten 6.1.1 und 10.1. In Abschnitt 10.1 a ist gefordert, die Auswirkungen festgestellter Fehler zu behandeln. In der Praxis erfordert dies, nicht nur die unmittelbaren, sondern auch zukünftige Auswirkungen und deren Risikopotenzial zu betrachten. In Abschnitt 10.1 b wird dies nochmals deutlich hervorgehoben, indem gefordert wird, Maßnahmen zur Beseitigung der Fehler*ursachen* zu evaluieren, damit der Fehler nicht erneut oder nicht an anderer Stelle auftritt (Symptom- vs. Ursachenbehandlung). Dies bedeutet, dass sowohl die Fehlerursache(n) zu untersuchen ist (sind) als auch vorbeugende Maßnahmen wirksam implementiert werden müssen, damit der Fehler nicht erneut auftritt.

ISO/IEC 27001:2013 betrachtet Vorbeugungsmaßnahmen also nicht mehr als gesonderten Schritt, sondern als eine in alle Prozessschritte integrierte und notwendige Anforderung. Durch die Erkennung und Beseitigung von Fehlerursachen soll das erneute Auftreten der Fehler verhindert werden, was letztlich zur Verbesserung des ISMS insgesamt führt. ISO/IEC 27001:2013 nutzt nicht den Begriff »Fehler«, sondern spricht nur von Nichtkonformitäten (Abgrenzung: In ISO/IEC 27002:2013 wird der Begriff »*error*« allerdings weiterhin genutzt).

Zusammengefasst

Mit der 2013er-Version erfolgt keine fundamentale Neuausrichtung der Norm. Ein effizientes und angemessenes Risikomanagement bleibt nach wie vor einer der Kernpunkte der ISO/IEC 27001. Die unterstützenden Prozesse sind ebenfalls weiterhin notwendig. Sie werden nun präziser beschrieben und ihr Zusammenwirken innerhalb des gesamten Managementsystems kommt stärker zum Ausdruck als bislang. Insgesamt ist – auch mit den gleichzeitig durchgeführten Anpassungen der ISO/IEC 27002 – ein stabiles und übersichtliches Normenwerk entstanden, das den Verantwortungsträgern auch zukünftig eine wertvolle Hilfe beim Aufbau und Betrieb eines ISMS sein wird.

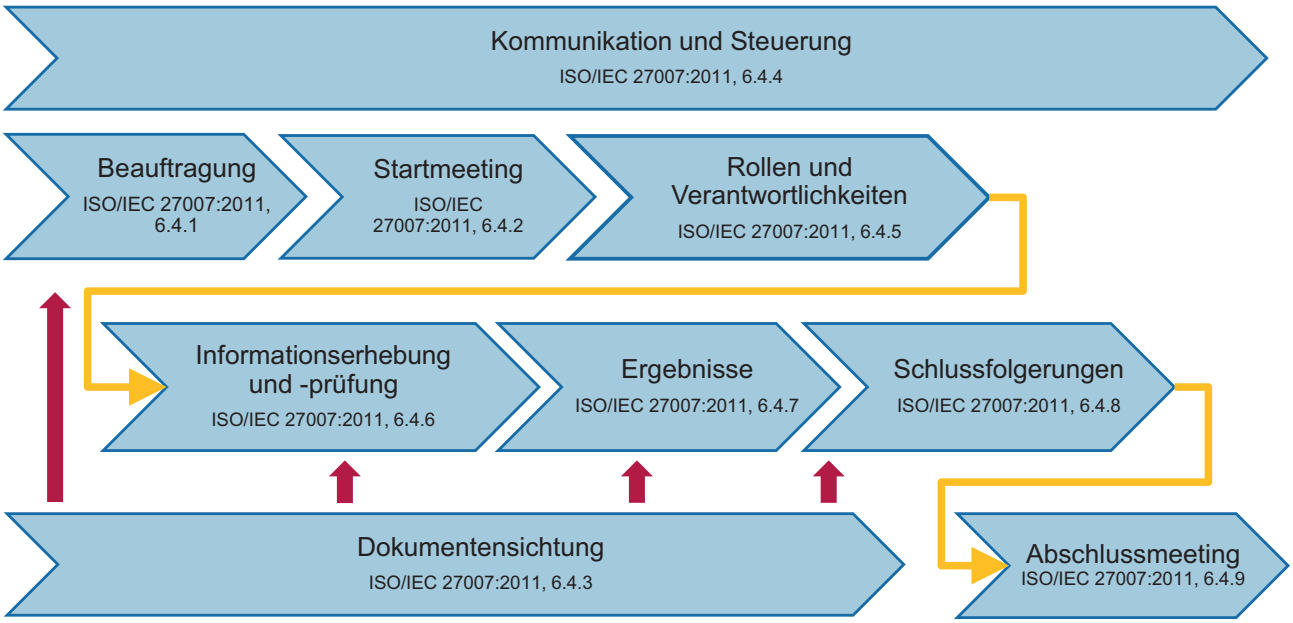
Weitere Managementstandards, die neu publiziert werden, folgen ebenfalls den ISO/IEC-Direktiven (Annex SL), so etwa auch die ISO 9001:2015 und ISO 22301:2012. Damit soll eine Harmonisierung der Managementsysteme ermöglicht und deren Zusammenspiel verbessert werden. Gleichzeitig werden dadurch Zertifizierungen nach mehreren Normen erleichtert und Unternehmen können somit wiederkehrende Anforderungen aus den unterschiedlichen Managementsystemen in einem einheitlichen Ansatz und »unter einem Dach« erfüllen.

9. Anlage 3: Interne ISMS-Audits – Mapping zur ISO/IEC 19011:2011 und ISO/IEC 27007:2011

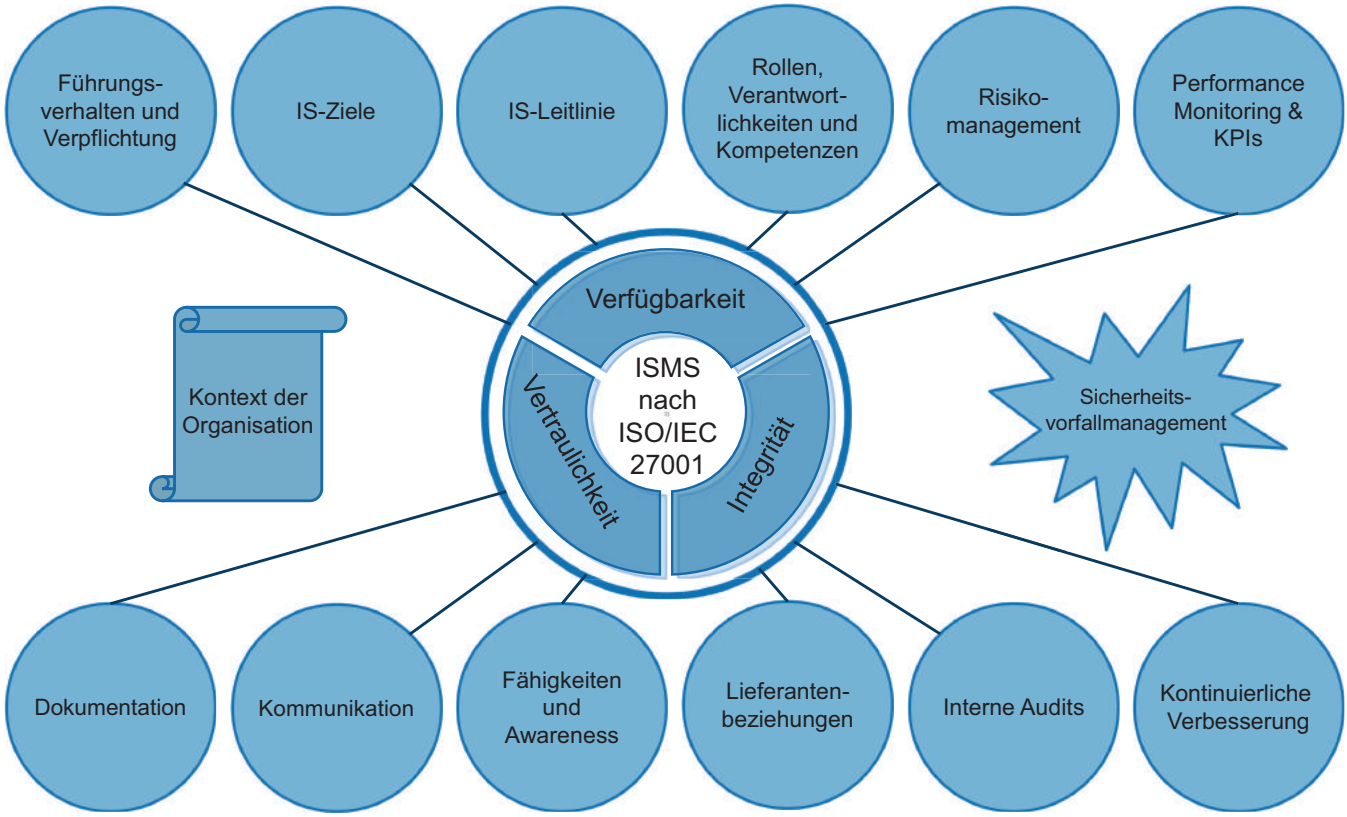
Anforderungen an interne ISMS-Audits aus ISO/IEC 27001:2013 vs. ISO/IEC 19011 & ISO/IEC 27007

Teilprozess/Aktivität	ISO/IEC 27001:2013	ISO/IEC 19011:2011 ISO/IEC 27007:2011
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	5.3 Establishing the audit programme
Implementierung des Auditprogramms	9.2 c	5.4 Implementing the audit programme
Monitoring des Auditprogramms	9.2 c	5.5 Monitoring the audit programme
Review und Verbesserung des Auditprogramms	9.2 c	5.6 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	5.4.7 Managing and maintaining audit programme records
Auditkriterien und Umfang je Audit festlegen	9.2 d	5.4.2 Defining the objectives, scope and criteria for an individual audit
Durchführung von ISMS-Audits	9.2 e	6 Performing an audit
Reporting der Auditergebnisse	9.2 f	5.4.6 Managing the audit programme outcome

10. Anlage 4: Durchführung interner ISMS-Audits (Prozessschaubild)



11. Anlage 5: Bausteine eines ISMS nach ISO/IEC 27001:2013 (deutsch)




CISA
Certified Information Systems Auditor
An ISACA Certification
CISM
Certified Information Security Manager
An ISACA Certification
CRISC
Certified in Risk and Information Systems Control
An ISACA Certification
CGEIT
Certified in the Governance of Enterprise IT
An ISACA Certification