DIN EN ISO/IEC 27005

DIN

ICS 03.100.70; 35.030

Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022); Deutsche Fassung EN ISO/IEC 27005:2024

Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022); German version EN ISO/IEC 27005:2024

Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information (ISO/IEC 27005:2022); Version allemande EN ISO/IEC 27005:2024

Gesamtumfang 81 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

www.din.de
www.dinmedia.de

3563040

Nationales Vorwort

Der Text von ISO/IEC 27005:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27005:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 31000:2018	siehe	DIN ISO 31000:2018-10
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2022	siehe	DIN EN ISO/IEC 27001:2024-01
ISO/IEC 27017	siehe	DIN EN ISO/IEC 27017
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Es wird darauf hingewiesen, dass der Begriff „control“ (3.1.16), der in der Referenzquelle DIN ISO 31000 als „Steuerung“ festgelegt ist, im übrigen Text mit „Maßnahme“ übersetzt wurde, um dem etablierten Sprachgebrauch im Bereich der Informationssicherheitsmanagementsysteme zu entsprechen.

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001:2024-01, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023*

DIN EN ISO/IEC 27017, *Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste*

DIN EN ISO/IEC 27701, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

– Leerseite –

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27005

August 2024

ICS 35.030

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Datenschutz — Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022)

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

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information (ISO/IEC 27005:2022)

Diese Europäische Norm wurde vom CEN am 1. August 2024 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Ref. Nr. EN ISO/IEC 27005:2024 D

Inhalt

Bilder

Tabellen

Europäisches Vorwort

Der Text von ISO/IEC 27005:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27005:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2025, und etwaige entgegenstehende nationale Normen müssen bis Februar 2025 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27005:2022 wurde von CEN-CENELEC als EN ISO/IEC 27005:2024 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe http://patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection,* erarbeitet.

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO/IEC 27005:2018), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

— der gesamte Leitfaden wurde an ISO/IEC 27001:2022 und ISO 31000:2018 angepasst;

— die Terminologie wurde an die Terminologie in ISO 31000:2018 angepasst;

— die Gliederung der Abschnitte wurde an den Aufbau der ISO/IEC 27001:2022 angepasst;

— Konzepte für Risikoszenarien wurden eingeführt;

— der ereignisbasierte Ansatz wird dem auf Werten basierenden Ansatz zur Risikoidentifizierung gegenübergestellt;

— der Inhalt der Anhänge wurde überarbeitet und in einem einzigen Anhang zusammengefasst.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

Einleitung

Dieses Dokument bietet einen Leitfaden für:

— die Implementierung der in ISO/IEC 27001 festgelegten Anforderungen im Hinblick auf Informationssicherheitsrisiken;

— die wesentlichen Verweisungen innerhalb der von ISO/IEC JTC 1/SC 27 entwickelten Normen zur Unterstützung von Maßnahmen im Rahmen der Handhabung von Informationssicherheitsrisiken;

— Aktionen zur Bewältigung von Risiken im Zusammenhang mit der Informationssicherheit (siehe ISO/IEC 27001:2022, 6.1 und Abschnitt 8);

— die Implementierung eines Leitfadens zum Risikomanagement in ISO 31000 im Zusammenhang mit der Informationssicherheit.

Dieses Dokument enthält einen ausführlichen Leitfaden zum Risikomanagement und ergänzt die Leitlinien in ISO/IEC 27003.

Dieses Dokument richtet sich an:

— Organisationen, die beabsichtigen, ein Informationssicherheitsmanagementsystem (ISMS) in Übereinstimmung mit ISO/IEC 27001 einzuführen und umzusetzen;

— Personen, die das Informationssicherheitsrisikomanagement durchführen oder daran beteiligt sind (z. B. Fachkräfte für ISMS, Risikoeigentümer und andere interessierte Parteien);

— Organisation, die ihren Risikomanagementprozess im Bereich der Informationssicherheit verbessern wollen.

1 Anwendungsbereich

Dieses Dokument enthält einen Leitfaden, der Organisationen dabei hilft,

— die Anforderungen der ISO/IEC 27001 in Bezug auf Aktionen zur Bewältigung von Informationssicherheitsrisiken zu erfüllen;

— Maßnahmen zur Handhabung von Informationssicherheitsrisiken, insbesondere zur Risikobeurteilung und -behandlung im Bereich der Informationssicherheit, durchzuführen.

Dieses Dokument gilt für alle Organisationen, unabhängig von ihrer Art, Größe oder Branche.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

3.1 Begriffe im Zusammenhang mit Informationssicherheitsrisiken

3.1.1
externer Kontext
externes Umfeld, in dem die Organisation versucht, ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der externe Kontext kann Folgendes beinhalten:

— soziale, kulturelle, politische, rechtliche, behördliche, finanzielle, technologische, wirtschaftliche, geologische Umgebung, seien sie internationaler, nationaler, regionaler oder lokaler Art;

— Schlüsselfaktoren und Trends, die die Ziele der Organisation beeinflussen;

— die Beziehungen, Wahrnehmungen, Werte, Erfordernisse und Erwartungen externer interessierter Parteien;

— vertragliche Beziehungen und Verpflichtungen;

— die Komplexität der Netzwerke und Abhängigkeiten.

[QUELLE: ISO Guide 73:2009, 3.3.1.1, modifiziert — Anmerkung 1 zum Begriff wurde modifiziert.]

3.1.2
interner Kontext
interne Umgebung, innerhalb derer die Organisation versucht, ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der interne Kontext kann Folgendes beinhalten:

— Vision, Mission und Werte;

— Leitung, Organisationsstruktur, Rollen und Rechenschaftspflichten;

— Strategie, Ziele und Richtlinien;

— die Organisationskultur;

— von der Organisation übernommene Normen, Leitlinien und Modelle;

— Fähigkeiten im Sinne von Ressourcen und Wissen (z. B. Kapital, Zeit, Menschen, Prozesse, Systeme und Technologien);

— Daten, Informationssysteme und Informationsflüsse;

— Beziehungen zu internen interessierten Parteien unter Berücksichtigung ihrer Wahrnehmungen und Werte;

— vertragliche Beziehungen und Verpflichtungen;

— interne gegenseitige Abhängigkeiten und Verbindungen.

[QUELLE: ISO Guide 73:2009, 3.3.1.2, modifiziert — Anmerkung 1 zum Begriff wurde modifiziert.]

3.1.3
Risiko
Auswirkung von Unsicherheit auf Ziele

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ziele können verschiedene Aspekte und Kategorien umfassen und auf verschiedenen Ebenen angewendet werden.

Anmerkung 3 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Information im Hinblick auf das Verständnis oder Wissen über ein *Ereignis* (3.1.11), seine *Auswirkungen* (3.1.14) oder seine *Wahrscheinlichkeit* (3.1.13).

Anmerkung 4 zum Begriff: Das Risiko wird üblicherweise anhand der *Risikoquellen/Risikoursachen* (3.1.6), der potentiellen Ereignisse, ihrer Auswirkungen und ihrer Wahrscheinlichkeit dargestellt.

Anmerkung 5 zum Begriff: Im Kontext von Informationssicherheitsmanagementsystemen können Informationssicherheitsrisiken als Auswirkung von Ungewissheit auf Informationssicherheitsziele beschrieben werden.

Anmerkung 6 zum Begriff: Informationssicherheitsrisiken sind üblicherweise mit einer negativen Auswirkung von Ungewissheit auf Informationssicherheitsziele verbunden.

Anmerkung 7 zum Begriff: Informationssicherheitsrisiken können mit der Möglichkeit verbunden sein, dass *Bedrohungen* (3.1.9) *Schwachstellen* (3.1.10) eines Informationswerts oder einer Gruppe solcher Werte ausnutzen und damit einer Organisation Schaden zufügen.

[QUELLE: ISO 31000:2018, 3.1, modifiziert — die Formulierung: „Sie kann positiv, negativ oder beides sein und Möglichkeiten und Bedrohungen ansprechen, schaffen oder zu ihnen führen“ wurde durch „in positiver oder negativer Hinsicht“ in Anmerkung 1 zum Begriff ersetzt; die ursprüngliche Anmerkung 3 zum Begriff wurde in Anmerkung 4 zum Begriff umnummeriert und Anmerkung 3, Anmerkung 5, Anmerkung 6 und Anmerkung 7 zum Begriff wurden hinzugefügt.]

3.1.4
Risikoszenario
Abfolge oder Kombination von *Ereignissen* (3.1.11), die von der ursprünglichen Ursache zur unerwünschten *Folge* (3.1.14) führen

[QUELLE: ISO 17666:2016, 3.1.13, modifiziert — Anmerkung 1 zum Begriff wurde gestrichen.]

3.1.5
Risikoeigentümer
Person oder Entität, die Verantwortung und Berechtigung hat, ein *Risiko* (3.1.3) zu handhaben

[QUELLE: ISO Guide 73:2009, 3.5.1.5]

3.1.6
Risikoquelle
Risikoursache
Element, das allein oder gemeinsam mit anderen Faktoren potentiell zu *Risiken* (3.1.3) führt

Anmerkung 1 zum Begriff: Eine Risikoquelle kann eine dieser drei Arten sein:

— menschlich;

— umweltbedingt;

— technisch.

Anmerkung 2 zum Begriff: Die Art einer menschlichen Risikoquelle kann absichtlich oder unabsichtlich sein.

[QUELLE: ISO 31000:2018, 3.4, modifiziert — Anmerkung 1 und Anmerkung 2 zum Begriff wurden hinzugefügt.]

3.1.7
Risikokriterien
Festlegungen, um die Signifikanz eines *Risikos* (3.1.3) zu bewerten

Anmerkung 1 zum Begriff: Risikokriterien basieren auf Zielen der Organisation sowie dem *externen Kontext* (3.1.1) und dem *internen Kontext* (3.1.2).

Anmerkung 2 zum Begriff: Risikokriterien können aus Normen, Gesetzen, Richtlinien und anderen Anforderungen abgeleitet werden.

[QUELLE: ISO Guide 73:2009, 3.3.1.3]

3.1.8
Risikobereitschaft
Größe und Art des *Risikos* (3.1.3), das eine Organisation willens ist, einzugehen oder beizubehalten

[QUELLE: ISO Guide 73:2009, 3.7.1.2]

3.1.9
Bedrohung
mögliche Ursache eines *Informationssicherheitsvorfalls* (3.1.12), der zu Schaden für ein System oder eine Organisation führen kann

3.1.10
Schwachstelle
Schwäche eines Wertes oder einer *Maßnahme* (3.1.16), die so ausgenutzt werden kann, dass ein *Ereignis* (3.1.11) mit einer negativen *Folge* (3.1.14) eintritt

3.1.11
Ereignis
Eintritt oder Veränderung einer bestimmten Kombination von Umständen

Anmerkung 1 zum Begriff: Ein Ereignis kann einmal oder mehrmals eintreten und mehrere Ursachen und mehrere *Auswirkungen* (3.1.14) haben.

Anmerkung 2 zum Begriff: Ein Ereignis kann auch etwas sein, das erwartet wird und nicht eintritt oder etwas, das unerwartet eintritt.

[QUELLE: ISO 31000:2018, 3.5, modifiziert — Anmerkung 3 zum Begriff wurde entfernt.]

3.1.12
Informationssicherheitsvorfall
einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, den Geschäftsbetrieb zu gefährden und die Informationssicherheit zu bedrohen

3.1.13
Wahrscheinlichkeit
Möglichkeit, dass etwas geschieht

Anmerkung 1 zum Begriff: In der Terminologie des Risikomanagements bezeichnet der Begriff „Wahrscheinlichkeit" die Möglichkeit, dass etwas geschieht, gleichgültig ob diese Möglichkeit objektiv oder subjektiv, qualitativ oder quantitativ definiert, gemessen oder bestimmt und mit allgemeinen Begriffen oder mathematisch (z. B. durch die statistische Wahrscheinlichkeit oder die Häufigkeit in einer bestimmten Zeitspanne) beschrieben wird.

Anmerkung 2 zum Begriff: Der englische Begriff „likelihood" hat in einigen Sprachen keine direkte Entsprechung, stattdessen wird oftmals die Entsprechung des Begriffs „probability" verwendet. Allerdings wird im Englischen „probability" oftmals sehr eng als mathematischer Begriff interpretiert. Deshalb wird in der englischen Terminologie des Risikomanagements der Begriff „likelihood" mit der Absicht verwendet, dass er dieselbe weit gefasste Bedeutung haben sollte wie der Begriff „Wahrscheinlichkeit" in vielen anderen Sprachen.

[QUELLE: ISO 31000:2018, 3.7]

3.1.14
Auswirkung
Ergebnis eines *Ereignisses* (3.1.11), welches die Ziele betrifft

Anmerkung 1 zum Begriff: Eine Auswirkung kann gewiss oder ungewiss sein und sich direkt oder indirekt bzw. positiv oder negativ auf Ziele auswirken.

Anmerkung 2 zum Begriff: Auswirkungen können qualitativ oder quantitativ beschrieben werden.

Anmerkung 3 zum Begriff: Jede Auswirkung kann durch kaskadierende und kumulative Effekte eskalieren.

[QUELLE: ISO 31000:2018, 3.6]

3.1.15
Risikoniveau
Signifikanz eines *Risikos* (3.1.3), das mittels einer Kombination von *Auswirkungen* (3.1.14) und deren *Wahrscheinlichkeit* (3.1.13) ausgedrückt wird

[QUELLE: ISO Guide 73:2009, 3.6.1.8, modifiziert — die Formulierung: „Größe eines Risikos oder einer Kombination von Risiken" wurde durch „Signifikanz eines Risikos" ersetzt.]

3.1.16
Steuerung
Maßnahme, die das *Risiko* (3.1.3) beibehält und/oder verändert

Anmerkung 1 zum Begriff: Steuerungen umfassen unter anderem alle Prozesse, Grundsätze, Instrumente, Verfahren oder andere Bedingungen und/oder Aktionen, welche Risiken beibehalten oder verändern.

Anmerkung 2 zum Begriff: Steuerungen können nicht immer die beabsichtigte oder angenommene verändernde Wirkung ausüben.

[QUELLE: ISO 31000:2018, 3.8]

3.1.17
Restrisiko
Risiko (3.1.3), das nach einer *Risikobehandlung* (3.2.7) verbleibt

Anmerkung 1 zum Begriff: Das Restrisiko kann nicht identifizierte Risiken beinhalten.

Anmerkung 2 zum Begriff: Restrisiken können auch ein beibehaltenes Risiko beinhalten.

[QUELLE: ISO Guide 73:2009, 3.8.1.6, modifiziert — Anmerkung 2 zum Begriff wurde modifiziert.]

3.2 Begriffe im Zusammenhang mit der Handhabung von Informationssicherheitsrisiken

3.2.1
Risikomanagementprozess
systematische Anwendung von Managementrichtlinien, -verfahren und -praktiken auf die Tätigkeiten des Kommunizierens, Abstimmens und Festlegens des Kontextes sowie Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von *Risiken* (3.1.3)

[QUELLE: ISO Guide 73:2009, 3.1]

3.2.2
Risikokommunikation und -konsultation
Satz fortlaufender und iterativer Prozesse, den eine Organisation durchführt, um Informationen zu liefern, zu teilen oder zu erhalten und den Dialog mit interessierten Parteien in Bezug auf die Handhabung von *Risiken* (3.1.3) zu suchen

Anmerkung 1 zum Begriff: Die Information kann sich auf die Existenz, die Beschaffenheit, die Gestalt, die *Wahrscheinlichkeit* (3.1.13), die Signifikanz, die Bewertung, die Akzeptanz und die Behandlung von Risiken beziehen.

Anmerkung 2 zum Begriff: Bei Konsultationen handelt es sich um einen bidirektionalen Prozess von fundierter Kommunikation zwischen einer Organisation und ihren interessierten Parteien zu einer Angelegenheit, bevor eine Entscheidung getroffen oder eine Zielrichtung für diese Angelegenheit bestimmt wird. Eine Konsultation ist:

— ein Prozess, der sich auf eine Entscheidung eher durch Beeinflussung als durch Machtbefugnis auswirkt;

— eine Eingabe für das Treffen von Entscheidungen, nicht aber das gemeinsame Treffen von Entscheidungen.

3.2.3
Risikobeurteilung
übergreifender Prozess, der aus *Risikoidentifizierung* (3.2.4), *Risikoanalyse* (3.2.5) und *Risikobewertung* (3.2.6) besteht

[QUELLE: ISO Guide 73:2009, 3.4.1]

3.2.4
Risikoidentifizierung
Prozess des Findens, Erkennens und Beschreibens von *Risiken* (3.1.3)

Anmerkung 1 zum Begriff: Die Risikoidentifizierung beinhaltet die Identifizierung der *Risikoquellen* (3.1.6), der *Ereignisse* (3.1.11), ihrer Ursachen und möglichen *Auswirkungen* (3.1.14).

Anmerkung 2 zum Begriff: Die Risikoidentifizierung kann historische Daten, theoretische Analysen, fundierte Meinungen und Expertenmeinungen sowie Erfordernisse von interessierten Parteien umfassen.

[QUELLE: ISO Guide 73:2009, 3.5.1, modifiziert — in Anmerkung 2 zum Begriff wurde „Stakeholder" durch „interessierte Partei" ersetzt.]

3.2.5
Risikoanalyse
Prozess, um die Beschaffenheit des *Risikos* (3.1.3) zu verstehen und das *Risikoniveau* (3.1.15) zu bestimmen

Anmerkung 1 zum Begriff: Die Risikoanalyse liefert die Grundlage für die *Risikobewertung* (3.2.6) und die Entscheidungen im Zuge der *Risikobehandlung* (3.2.7).

Anmerkung 2 zum Begriff: Die Risikoanalyse beinhaltet die Risikoabschätzung.

[QUELLE: ISO Guide 73:2009, 3.6.1]

3.2.6
Risikobewertung
Prozess, bei dem die Ergebnisse der *Risikoanalyse* (3.2.5) mit den *Risikokriterien* (3.1.7) verglichen werden, um zu bestimmen, ob das *Risiko* (3.1.3) und/oder seine Signifikanz akzeptabel oder tragbar sind

Anmerkung 1 zum Begriff: Die Risikobewertung unterstützt bei der Entscheidung über die *Risikobehandlung* (3.2.7).

[QUELLE: ISO Guide 73:2009, 3.7.1, modifiziert — „Größe" wurde durch „Signifikanz" ersetzt.]

3.2.7
Risikobehandlung
Prozess zur Veränderung eines *Risikos* (3.1.3)

Anmerkung 1 zum Begriff: Die Risikobehandlung kann Folgendes umfassen:

— Vermeiden des Risikos, indem entschieden wird, die Aufgabe, aus der sich ein Risiko ergibt, nicht zu beginnen oder fortzuführen;

— Eingehen oder Vergrößern des Risikos mit dem Ziel, eine Chance wahrzunehmen;

— Beseitigen der *Risikoursache* (3.1.6);

— Verändern der *Wahrscheinlichkeit* (3.1.13);

— Verändern der *Auswirkungen* (3.1.14);

— Teilen des Risikos mit einer anderen Partei oder anderen Parteien (einschließlich Verträgen und Risikofinanzierung) und

— Beibehalten des Risikos auf Grundlage einer informierten Entscheidung.

Anmerkung 2 zum Begriff: Die Behandlung von Risiken im Bereich der Informationssicherheit beinhaltet nicht das „Eingehen oder Vergrößern des Risikos mit dem Ziel, eine Chance wahrzunehmen", aber die Organisation kann diese Option für das allgemeine Risikomanagement nutzen.

Anmerkung 3 zum Begriff: Risikobehandlungen, die sich mit negativen Auswirkungen beschäftigen, werden manchmal auch als „Risikominderung", „Risikoeliminierung", „Risikovorsorge" und „Risikoreduzierung" bezeichnet.

Anmerkung 4 zum Begriff: Die Risikobehandlung kann zu neuen Risiken führen oder vorhandene Risiken verändern.

[QUELLE: ISO Guide 73:2009, 3.8.1 modifiziert — Anmerkung 1 zum Begriff wurde hinzugefügt und die ursprüngliche Anmerkung 1 und Anmerkung 2 zum Begriff wurden in Anmerkung 2 und Anmerkung 3 zum Begriff umnummeriert.]

3.2.8
Risikoakzeptanz
informierte Entscheidung, ein bestimmtes *Risiko* (3.1.3) zu tragen

Anmerkung 1 zum Begriff: Risikoakzeptanz kann ohne *Risikobehandlung* (3.2.7) oder während des Risikobehandlungsprozesses erfolgen.

Anmerkung 2 zum Begriff: Akzeptierte Risiken werden einer Überwachung und Überprüfung unterzogen.

[QUELLE: ISO Guide 73:2009, 3.7.1.6]

3.2.9
Risikoteilung
Form der *Risikobehandlung* (3.2.7), welche die mit anderen Parteien vereinbarte Verteilung des *Risikos* (3.1.3) beinhaltet

Anmerkung 1 zum Begriff: Rechtliche oder behördliche Anforderungen können die Risikoteilung einschränken, verbieten oder anordnen.

Anmerkung 2 zum Begriff: Die Risikoteilung kann durch Versicherungen oder andere Vertragsformen vollzogen werden.

Anmerkung 3 zum Begriff: Wie weit das Risiko verteilt wird, kann von der Zuverlässigkeit und Klarheit der Teilungsvereinbarungen abhängen.

Anmerkung 4 zum Begriff: Die Risikoübertragung ist eine Form der Risikoteilung.

[QUELLE: ISO Guide 73:2009, 3.8.1.3]

3.2.10
Risikobeibehaltung
zeitweilige Akzeptanz des potentiellen Nutzens eines Gewinns oder der Belastung durch einen Verlust aufgrund eines bestimmten *Risikos* (3.1.3)

Anmerkung 1 zum Begriff: Die Beibehaltung kann auf eine bestimmte Zeitspanne beschränkt sein.

Anmerkung 2 zum Begriff: Das beibehaltene *Risikoniveau* (3.1.15) kann von *Risikokriterien* (3.1.7) abhängen.

[QUELLE: ISO Guide 73:2009, 3.8.1.5, modifiziert — das Wort „zeitweilig" wurde am Anfang der Definition hinzugefügt und die Formulierung „Die Risikobeibehaltung schließt die Akzeptanz von Restrisiken ein" wurde durch „Die Beibehaltung kann auf eine bestimmte Zeitspanne beschränkt werden" in Anmerkung 1 zum Begriff ersetzt.]

4 Aufbau dieses Dokuments

Dieses Dokument ist wie folgt strukturiert:

— Abschnitt 5: Handhabung von Informationssicherheitsrisiken;

— Abschnitt 6: Kontextfestlegung;

— Abschnitt 7: Prozess der Risikobeurteilung der Informationssicherheit;

— Abschnitt 8: Prozess der Risikobehandlung der Informationssicherheit;

— Abschnitt 9: Betrieb;

— Abschnitt 10: Unterstützung verbundener ISMS-Prozesse.

Abgesehen von den Beschreibungen in den allgemeinen Unterabschnitten sind alle Risikomanagementaufgaben, wie sie in Abschnitt 7 bis Abschnitt 10 dargestellt sind, wie folgt strukturiert:

Eingabe: Identifizierung aller Informationen, die zur Durchführung der Aufgabe erforderlich sind.

Aktion: Beschreibung der Aufgabe.

Auslöser: Bereitstellung eines Leitfadens für den Beginn der Aufgabe, z. B. aufgrund einer Änderung innerhalb der Organisation oder nach einem Plan oder einer Änderung im externen Kontext der Organisation.

Ausgabe: Identifizierung aller Informationen, die nach der Durchführung der Aufgabe abgeleitet werden, sowie aller Kriterien, die diese Ausgabe erfüllen sollte.

Leitfaden: Bereitstellung eines Leitfadens zur Durchführung der Aufgabe, eines Schlüsselworts und eines Schlüsselkonzepts.

5 Handhabung von Informationssicherheitsrisiken

5.1 Prozess zur Handhabung von Informationssicherheitsrisiken

Der Prozess zur Handhabung von Informationssicherheitsrisiken wird in Bild 1 dargestellt.

ANMERKUNG Dieser Prozess beruht auf dem allgemeinen Risikomanagementprozess nach ISO 31000.

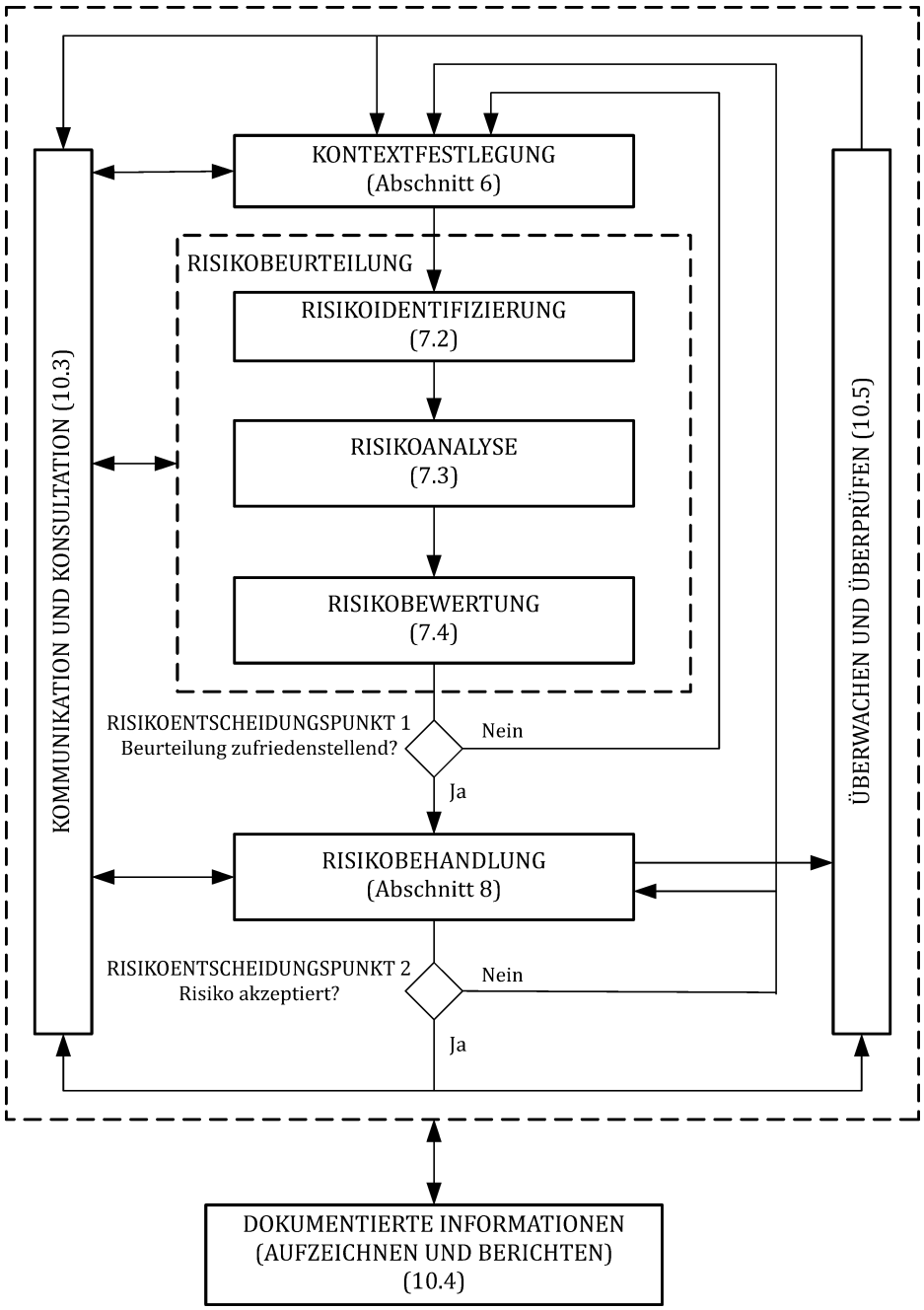


Bild 1 — Prozess zur Handhabung von Informationssicherheitsrisiken

Wie in Bild 1 veranschaulicht, kann der Prozess zur Handhabung der Informationssicherheitsrisiken für Aufgaben zur Risikobeurteilung und/oder Risikobehandlung iterativ sein. Ein iterativer Ansatz bei der Durchführung von Risikobeurteilungen kann die Tiefe und den Detaillierungsgrad der Beurteilung bei jeder Iteration erhöhen. Der iterative Ansatz bietet ein gutes Gleichgewicht zwischen der Minimierung des Zeit- und Arbeitsaufwands für die Festlegung von Maßnahmen und der gleichzeitigen Sicherstellung einer angemessenen Risikobeurteilung.

Die Kontextfestlegung bedeutet die Zusammenstellung des internen und externen Kontexts für die Handhabung von Informationssicherheitsrisiken oder eine Risikobeurteilung der Informationssicherheit.

Wenn die Risikobeurteilung genügend Informationen liefert, um die erforderlichen Aktionen zur Änderung der Risiken auf ein akzeptables Niveau zu bestimmen, ist die Aufgabe abgeschlossen und es folgt die Risikobehand-

lung. Sind die Informationen unzureichend, sollte eine weitere Iteration der Risikobeurteilung durchgeführt werden. Dies kann eine Änderung des Kontexts der Risikobeurteilung (z. B. eine Überarbeitung des Anwendungsbereichs), die Einbindung von Fachwissen aus dem betreffenden Bereich oder andere Möglichkeiten zur Erhebung von Daten beinhalten, die eine Änderung des Risikos auf ein akzeptables Niveau ermöglichen (siehe „Risikoentscheidungspunkt 1“ in Bild 1).

Die Risikobehandlung erfolgt in einem iterativen Prozess durch:

— Formulieren und Auswählen der Risikobehandlungsoptionen;

— Planen und Implementieren der Risikobehandlung;

— Beurteilen der Wirksamkeit dieser Behandlung;

— Entscheiden, ob das verbleibende Risiko akzeptabel ist;

— Fortsetzen der Behandlung, falls nicht akzeptabel.

Es ist möglich, dass die Risikobehandlung nicht sofort zu einem akzeptablen Niveau der Restrisiken führt. In dieser Situation kann ein weiterer Versuch unternommen werden, eine zusätzliche Risikobehandlung zu finden, oder es kann eine weitere Iteration der Risikobeurteilung erfolgen, entweder als Ganzes oder teilweise. Dies kann eine Änderung des Kontexts der Risikobeurteilung (z. B. durch eine Überarbeitung des Anwendungsbereichs) und die Einbindung von Fachwissen aus dem betreffenden Bereich beinhalten. Das Wissen über maßgebliche Bedrohungen oder Schwachstellen kann zu besseren Entscheidungen über geeignete Risikobehandlungsmaßnahmen in der nächsten Iteration der Risikobeurteilung führen (siehe „Risikoentscheidungspunkt 2“ in Bild 1).

Die Kontextfestlegung wird in Abschnitt 6, die Maßnahmen zur Risikobeurteilung in Abschnitt 7 und die Maßnahmen zur Risikobehandlung in Abschnitt 8 eingehend behandelt.

Weitere Maßnahmen, die für die Handhabung von Informationssicherheitsrisiken erforderlich sind, werden in Abschnitt 10 behandelt.

5.2 Zyklen des Informationssicherheitsrisikomanagements

Die Risikobeurteilung und die Risikobehandlung sollten regelmäßig und bei Änderungen aktualisiert werden. Dies sollte für die gesamte Risikobeurteilung gelten, und die Aktualisierungen können in zwei Risikomanagementzyklen unterteilt werden:

— strategischer Zyklus, in dem sich Geschäftswerte, Risikoquellen und Bedrohungen, Zielvorgaben oder Auswirkungen von Informationssicherheitsereignissen aufgrund von Veränderungen im Gesamtkontext der Organisation weiterentwickeln. Dies kann als Eingabe für eine allgemeine Aktualisierung der Risikobeurteilung bzw. Risikobeurteilungen und der Risikobehandlungen dienen. Es kann auch als Eingabe für die Identifizierung neuer Risiken dienen und völlig neue Risikobeurteilungen anstoßen;

— operativer Zyklus, bei dem die oben genannten Elemente als Eingabeinformationen oder geänderte Kriterien dienen, die sich auf eine Risikobeurteilung oder Beurteilung auswirken, bei der die Szenarien überprüft und aktualisiert werden sollten. Die Überprüfung sollte gegebenenfalls eine Aktualisierung der entsprechenden Risikobehandlung beinhalten.

Der strategische Zyklus sollte über eine längere Zeitspanne oder bei größeren Veränderungen durchgeführt werden, während der operative Zyklus kürzer sein sollte, je nach den im Einzelnen ermittelten und beurteilten Risiken und der entsprechenden Risikobehandlung.

Der strategische Zyklus gilt für das Umfeld, in dem die Organisation ihre Ziele zu erreichen sucht, während der operative Zyklus für alle Risikobeurteilungen gilt, die den Kontext des Risikomanagementprozesses

berücksichtigen. In beiden Zyklen kann es viele Risikobeurteilungen mit unterschiedlichem Kontext und Anwendungsbereich bei jeder Beurteilung geben.

6 Kontextfestlegung

6.1 Organisatorische Aspekte

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 4.1.

Eine Organisation wird definiert als Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen. Eine Organisation ist nicht notwendigerweise ein Unternehmen, eine andere Körperschaft oder eine juristische Person, sie kann auch eine Teilmenge einer juristischen Person sein (z. B. die IT-Abteilung eines Unternehmens) und kann als „Organisation" im Rahmen von ISMS betrachtet werden.

Es ist wichtig zu verstehen, dass die Risikobereitschaft, d. h. der Umfang der Risiken, die eine Organisation bereit ist, einzugehen oder zu akzeptieren, von Organisation zu Organisation sehr unterschiedlich sein kann. Zu den Faktoren, die sich auf die Risikobereitschaft einer Organisation auswirken, gehören beispielsweise Größe, Komplexität und Branche. Die Risikobereitschaft sollte von der obersten Führungsebene festgelegt und regelmäßig überprüft werden.

Die Organisation sollte sicherstellen, dass die Rolle des Risikoeigentümers in Bezug auf die Managementaufgaben für die identifizierten Risiken festgelegt wird. Risikoeigentümer sollten angemessen rechenschaftspflichtig und befugt sein, die identifizierten Risiken zu handhaben.

6.2 Identifizierung grundlegender Anforderungen von interessierten Parteien

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 4.2.

Die grundlegenden Anforderungen der interessierten Parteien sollten identifiziert werden, ebenso wie der Compliance-Status mit diesen Anforderungen. Dazu gehört die Identifizierung aller Referenzdokumente, die Sicherheitsregeln und -maßnahmen definieren und die im Rahmen der Risikobeurteilung zur Informationssicherheit gelten.

Diese Referenzdokumente können unter anderem Folgendes umfassen:

a) ISO/IEC 27001:2022, Anhang A;

b) zusätzliche Normen, die ISMS abdecken;

c) zusätzliche Normen, die für einen bestimmten Sektor anwendbar sind (z. B. Finanzwesen, Gesundheitswesen);

d) spezifische internationale und/oder nationale Vorschriften;

e) die internen Sicherheitsregeln der Organisation;

f) Sicherheitsregeln und -maßnahmen aus Verträgen und Vereinbarungen;

g) Sicherheitsmaßnahmen, die auf der Grundlage früherer Tätigkeiten zur Risikobehandlung umgesetzt wurden.

Sämtliche Nichteinhaltungen der grundlegenden Anforderungen sollten erklärt und begründet werden. Diese grundlegenden Anforderungen und deren Compliance sollten als Eingabe für die Wahrscheinlichkeitsbeurteilung und für die Risikobehandlung dienen.

6.3 Anwendung der Risikobeurteilung

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 4.3.

Organisationen können Risikobeurteilungen eingebettet in viele verschiedene Prozesse durchführen, z. B. Projektmanagement, Schwachstellenmanagement, Vorfallsmanagement, Problemmanagement oder sogar spontan für ein bestimmtes identifiziertes, spezifisches Thema. Unabhängig davon, wie die Risikobeurteilungen durchgeführt werden, sollten sie zusammen alle für die Organisation maßgeblichen Aspekte im Anwendungsbereich eines ISMS abdecken.

Die Risikobeurteilung sollte der Organisation helfen, Entscheidungen über die Handhabung von Risiken zu treffen, die das Erreichen ihrer Ziele beeinträchtigen. Sie sollte daher auf diejenigen Risiken und Maßnahmen ausgerichtet sein, die bei erfolgreicher Handhabung die Wahrscheinlichkeit erhöhen, dass die Organisation ihre Ziele erreicht.

Weitere Informationen über den Kontext eines ISMS und die durch die Risikobeurteilung zu erfassenden Aspekte sind in ISO/IEC 27003 enthalten.

6.4 Festlegung und Aufrechterhaltung der Informationssicherheitsrisikokriterien

6.4.1 Allgemeines

ISO/IEC 27001:2022, 6.1.2 a), legt die Anforderungen an Organisationen fest, ihre Risikokriterien zu definieren, d. h. die Festlegungen, anhand derer sie die Signifikanz der von ihnen identifizierten Risiken bewerten und Entscheidungen über Risiken treffen.

ISO/IEC 27001 legt die Anforderungen für eine Organisation fest, die Risikokriterien für die Informationssicherheit aufstellen und aufrechterhalten muss, die Folgendes beinhalten:

a) die Risikoakzeptanzkriterien;

b) Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen.

Im Allgemeinen sollte Folgendes bei der Festlegung der Risikokriterien berücksichtigt werden:

— die Natur und Art der Ungewissheiten, die die Ergebnisse und Ziele (sowohl materiell als auch immateriell) beeinflussen können;

— wie die Auswirkung und die Wahrscheinlichkeit festgelegt, vorhergesagt und gemessen werden;

— zeitliche Faktoren;

— Konsistenz bei der Anwendung der Messungen;

— Art und Weise, wie das Risikoniveau bestimmt wird;

— wie Kombinationen und Abfolgen mehrerer Risiken berücksichtigt werden;

— die Fähigkeiten der Organisation.

Weitere Erwägungen zu Risikokriterien sind in Anhang A aufgeführt.

6.4.2 Risikoakzeptanzkriterien

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 a) 1).

Bei der Risikobewertung sollten Risikoakzeptanzkriterien verwendet werden, um festzustellen, ob ein Risiko akzeptabel ist oder nicht.

Bei der Risikobehandlung können Risikoakzeptanzkriterien verwendet werden, um festzustellen, ob die vorgeschlagene Risikobehandlung ausreicht, um ein akzeptables Risikoniveau zu erreichen, oder ob eine weitere Risikobehandlung erforderlich ist.

Eine Organisation sollte Niveaus für die Risikoakzeptanz festlegen. Die folgenden Punkte sollten bei der Entwicklung beachtet werden:

a) Konsistenz zwischen den Akzeptanzkriterien für Informationssicherheitsrisiken und den allgemeinen Risikoakzeptanzkriterien der Organisation;

b) die Führungsebene, die befugt ist, Entscheidungen über die Akzeptanz von Risiken zu treffen, ist identifiziert;

c) die Kriterien für die Risikoakzeptanz können mehrere Schwellenwerte umfassen, und die Befugnis zum Akzeptieren kann verschiedenen Führungsebenen zugewiesen werden;

d) Risikoakzeptanzkriterien können allein auf Wahrscheinlichkeit und Auswirkung beruhen oder so erweitert werden, dass auch das Kosten-Nutzen-Verhältnis zwischen voraussichtlichen Verlusten und den Kosten der Maßnahmen berücksichtigt wird;

e) für verschiedene Risikoklassen können unterschiedliche Kriterien für die Risikoakzeptanz gelten (z. B. werden Risiken, die zu einem Verstoß gegen Vorschriften oder Gesetze führen können, nicht immer beibehalten, während die Akzeptanz von Risiken zulässig sein kann, wenn die Akzeptanz auf eine vertragliche Anforderung zurückzuführen ist);

f) Risikoakzeptanzkriterien können Anforderungen für eine künftige zusätzliche Behandlung enthalten (z. B. kann ein Risiko kurzfristig beibehalten werden, selbst wenn das Risikoniveau die Risikoakzeptanzkriterien übersteigt, wenn eine Genehmigung vorliegt und die Verpflichtung besteht, Maßnahmen zu ergreifen, um eine ausgewählte Reihe von Maßnahmen durchzuführen, um innerhalb einer bestimmten Zeitspanne ein akzeptables Niveau zu erreichen);

g) Risikoakzeptanzkriterien sollten auf der Grundlage der Risikobereitschaft definiert werden, die angibt, welche Art von Risiko die Organisation bereit ist, einzugehen oder beizubehalten;

h) Risikoakzeptanzkriterien können je nach Kontext absolut oder bedingt sein.

Risikoakzeptanzkriterien sollten unter Berücksichtigung der folgenden Einflussfaktoren festgelegt werden:

— Organisationsziele;

— organisatorische Möglichkeiten;

— rechtliche und behördliche Aspekte;

— betriebliche Maßnahmen;

— technologische Beschränkungen;

— finanzielle Beschränkungen;

— Prozesse;

— Lieferantenbeziehungen;

— menschliche Faktoren (z. B. im Zusammenhang mit dem Datenschutz).

Die Aufzählung von Einflussfaktoren erhebt keinen Anspruch auf Vollständigkeit. Die Organisation sollte die Einflussfaktoren auf der Grundlage des Kontexts berücksichtigen.

Ein einfaches Akzeptanzkriterium (ja/nein) reicht in der Praxis nicht immer aus.

In vielen Fällen kann die Entscheidung, ein Risiko zu akzeptieren, auf bestimmten Risikoniveaus getroffen werden (bestimmte Kombinationen von Wahrscheinlichkeit und Auswirkungen). Es kann jedoch Umstände geben, unter denen es notwendig ist, Schwellenwerte für die Akzeptanz extremer Auswirkungen unabhängig von ihrer Wahrscheinlichkeit oder extrem hoher Wahrscheinlichkeiten ungeachtet der Auswirkungen festzulegen, wobei der Effekt auf die Organisation in erster Linie aus dem einen oder dem anderen hervorgehen.

Beispielsweise sollte die Akzeptanz eines seltenen Ereignisses, das den Aktienwert eines Unternehmens vernichtet, oder eines ständigen Ressourcenverbrauchs, der sich aus der Erfordernis ergibt, häufige geringfügige Verstöße gegen eine Richtlinie zu kontrollieren, in erster Linie danach beurteilt werden, welcher der beiden Faktoren die vorherrschenden Auswirkungen auf die Organisation hat.

Daher sollten die Risikoakzeptanzkriterien idealerweise die Wahrscheinlichkeit und die Auswirkungen unabhängig voneinander sowie die Kosten für die Handhabung berücksichtigen und nicht nur die Höhe des Risikos als eine Kombination aus Wahrscheinlichkeit und Auswirkungen.

Eine Organisation mit einer hohen Risikobereitschaft kann eine höhere Akzeptanzschwelle festlegen und damit mehr Risiken akzeptieren als eine Organisation mit einer geringeren Risikobereitschaft. Dies schützt die Organisation vor einer Übersteuerung, d. h. vor so vielen Informationssicherheitsmaßnahmen, dass sie die Organisation daran hindern, ihre Ziele zu erreichen.

Die Risikoakzeptanzkriterien können unterschiedlich sein, je nachdem, wie lange die Risiken voraussichtlich bestehen werden (z. B. können die Risiken mit einer vorübergehenden oder kurzfristigen Aktivität verbunden sein).

Die Risikokriterien sollten laufend überprüft und bei Bedarf aktualisiert werden, wenn sich Änderungen im Zusammenhang mit dem Informationssicherheitsrisikomanagement ergeben.

BEISPIEL Ein kleines Unternehmen kann anfangs eine große Risikobereitschaft haben, aber wenn es wächst, kann es seine Risikobereitschaft herabsetzen.

Die Risikoakzeptanzkriterien sollten von der zuständigen Führungsebene genehmigt werden.

6.4.3 Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen

6.4.3.1 Allgemeines

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 a) 2).

Die Kriterien für die Risikobeurteilung legen fest, wie die Signifikanz eines Risikos in Bezug auf die Auswirkungen, die Wahrscheinlichkeit und das Risikoniveau bestimmt wird.

Die Kriterien für die Beurteilung der Informationssicherheitsrisiken sollten die Angemessenheit der Risikomanagementmaßnahmen berücksichtigen.

Zu den Überlegungen für das Erreichen dieses Ziels gehören:

a) der Klassifizierungsgrad von Informationen;

b) die Menge und die Konzentration der Informationen;

c) der strategische Wert der Geschäftsprozesse, bei denen die Informationen genutzt werden;

d) die Kritikalität der Informationen und der mit den Informationen verbundenen Werte;

e) die betriebliche und geschäftliche Bedeutung von Verfügbarkeit, Vertraulichkeit und Integrität;

f) die Erwartungen und Wahrnehmungen der interessierten Parteien (z. B. der obersten Führungsebene);

g) negative Auswirkungen wie der Verlust des Firmenwerts und des guten Rufs;

h) Konsistenz in Bezug auf die organisatorischen Risikokriterien.

Die Kriterien für die Risikobeurteilung oder eine formale Grundlage für deren Festlegung sollten für alle Arten der Risikobeurteilung in der gesamten Organisation standardisiert werden, da dies die Kommunikation, den Vergleich und die Zusammenfassung von Risiken, die mit mehreren Geschäftsbereichen verbunden sind, erleichtern kann.

Zu den Kriterien für die Risikobeurteilung der Informationssicherheit gehören in der Regel:

— die Auswirkungen;

— die Wahrscheinlichkeit;

— das Risikoniveau.

6.4.3.2 Folgekriterien

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 a) 2).

Die ISO/IEC 27001 befasst sich mit den Auswirkungen, die direkt oder indirekt durch die Wahrung oder den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Anwendungsbereich des ISMS betroffen sind. Es sollten Folgekriterien entwickelt und festgelegt werden, die sich auf das Ausmaß des Schadens oder Verlusts oder den Schaden für eine Organisation oder eine Person beziehen, der durch den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen entsteht. Bei der Festlegung von Folgekriterien sollten insbesondere die folgenden Punkte berücksichtigt werden:

a) Verlust von Menschenleben oder Schaden für Einzelpersonen oder Gruppen;

b) Verlust der Freiheit, der Würde oder des Rechts auf Privatsphäre;

c) Verlust von Personal und intellektuellem Kapital (Fertigkeiten und Fachwissen);

d) eingeschränkter Eigen- oder Fremdbetrieb (z. B. Schädigung einer Geschäftsfunktion oder eines Prozesses);

e) Auswirkungen auf Pläne und Termine;

f) Verlust von Geschäfts- und Finanzwerten;

g) Verlust von Geschäftsvorteilen oder Marktanteilen;

h) Schädigung des öffentlichen Vertrauens oder Rufs;

i) Verstöße gegen rechtliche, behördliche oder gesetzliche Anforderungen;

j) Verstöße gegen Verträge oder die Dienstgüte;

k) nachteilige Auswirkungen auf interessierte Parteien;

l) negative Auswirkungen auf die Umwelt, Verschmutzung.

Folgekriterien legen fest, wie eine Organisation die Signifikanz potentieller Informationssicherheitsereignisse für die Organisation einstuft. Es ist wichtig zu bestimmen, wie viele Kategorien von Auswirkungen verwendet werden, wie sie definiert werden und welche Auswirkungen mit jeder Kategorie verbunden sind. Üblicherweise sind die Folgekriterien für verschiedene Organisationen unterschiedlich, je nach dem internen und externen Kontext der Organisation.

BEISPIEL 1 Der Höchstbetrag, den die Organisation in einem Geschäftsjahr abzuschreiben bereit ist, und der Mindestbetrag in derselben Zeitspanne, der sie in die Liquidation zwingen würde, können eine realistische Ober- und Untergrenze für die in Geld ausgedrückte Tragweite von Auswirkungen für eine Organisation bilden.

Dieser kontextabhängige Bereich kann dann in mehrere Folgekategorien unterteilt werden, deren Anzahl und Verteilung von der Risikowahrnehmung und der Risikobereitschaft der Organisation abhängen sollte. Monetäre Folgeskalen werden üblicherweise in einer logarithmischen Skala ausgedrückt, z. B. in Dekaden oder Potenzen von 10 (z. B. 100 bis 1 000; 1 bis 10 000 usw.), aber es können auch alternative Quantisierungsschemata verwendet werden, wenn sie besser in den Kontext der Organisation passen.

Da Auswirkungen in verschiedenen Domänen oder Abteilungen einer Organisation zunächst auf unterschiedliche Weise statt konkret in Geld ausgedrückt werden können, ist es nützlich, wenn diese verschiedenen Ausdrücke mit einer gemeinsamen Verankerungsskala in Beziehung gesetzt werden können, um sicherzustellen, dass annähernd gleiche Niveaus der Auswirkung in den verschiedenen Domänen korrekt miteinander verglichen werden. Dies sollte eine domänenübergreifende Aggregation der Risiken ermöglichen.

BEISPIEL 2 Eine Datenschutzverletzung kann nicht nur die Privatsphäre eines Einzelnen beeinträchtigen, sondern auch zum Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen führen, die in den Anwendungsbereich des ISMS fallen. Dies kann auch zu einem Compliance-Verstoß gegen das geltende Datenschutzgesetz führen. Die möglichen Auswirkungen reichen von Informationsverlusten, dem Verlust von informationsbezogenen Werten und Informationsprozessen bis hin zum Verlust von operativen Geschäftszielen und Geschäftsprognosen.

6.4.3.3 Wahrscheinlichkeitskriterien

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 a) 2).

Die Bestimmung der Wahrscheinlichkeitskriterien hängt u. a. von folgenden Aspekten ab:

a) zufälligen oder naturbedingten Ereignissen;

b) dem Grad der Gefährdung maßgeblicher Informationen oder der mit den Informationen verbundenen Werte durch die Bedrohung;

c) dem Ausmaß, in dem eine Schwachstelle der Organisation ausgenutzt wird;

d) technischem Versagen;

e) menschlichen Handlungen oder Unterlassungen.

Die Wahrscheinlichkeit kann in wahrscheinlichkeitsbasierten Begriffen ausgedrückt werden (die Wahrscheinlichkeit, dass ein Ereignis in einem bestimmten Zeitrahmen eintritt) oder in frequentistischen Begriffen (die fiktive durchschnittliche Anzahl von Ereignissen in einem bestimmten Zeitrahmen). Die Wahrscheinlichkeit, ausgedrückt in Begriffen, die sich auf die Häufigkeit beziehen, wird oft verwendet, wenn sie kommuniziert wird, obwohl nur die Wahrscheinlichkeit, ausgedrückt in wahrscheinlichkeitsbasierten Begriffen, verwendet werden kann, wenn eine Aggregation von Wahrscheinlichkeiten durchgeführt wird.

Die Wahrscheinlichkeitskriterien sollten den vorhersehbaren, handhabbaren Bereich erwarteter Ereigniswahrscheinlichkeiten abdecken. Jenseits der Grenzen der praktischen Handhabbarkeit ist es in der Regel nur noch notwendig, die Überschreitung der einen oder anderen Grenze zu erkennen, um eine angemessene Risikomanagemententscheidung zu treffen (Bezeichnung als Extremfall). Sind die endlichen Skalen zu breit,

führt dies in der Regel zu einer übermäßig groben Quantisierung und kann zu Fehlern bei der Beurteilung führen. Dies ist insbesondere dann der Fall, wenn die Wahrscheinlichkeiten in den oberen Bereich der exponentiell dargestellten Skalen fallen, da die Abstufungen in den oberen Bereichen von Natur aus sehr groß sind.

Obwohl fast alles „möglich" ist, sollte den Risikoquellen, die für den Kontext der Organisation und den Anwendungsbereich ihres ISMS am wichtigsten sind, die größte Aufmerksamkeit geschenkt werden.

6.4.3.4 Kriterien zur Bestimmung des Risikoniveaus

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 a) 2).

Zweck der Skalen für das Risikoniveau ist es, den Risikoeigentümern bei der Entscheidung über die Beibehaltung oder anderweitige Behandlung von Risiken zu helfen und ihnen bei der Risikobehandlung Vorrang einzuräumen. Das beurteilte Niveau eines bestimmten Risikos sollte der Organisation helfen, die Dringlichkeit zu bestimmen, mit der dieses Risiko angegangen werden muss.

Je nach Situation empfiehlt es sich, das inhärente Risikoniveau (ohne Einbeziehung irgendwelcher Maßnahmen) oder das aktuelle Risikoniveau (unter Berücksichtigung der Wirksamkeit bereits durchgeführter Maßnahmen) zu berücksichtigen. Die Organisation sollte eine Risikoeinstufung unter Berücksichtigung der folgenden Punkte vornehmen:

a) die Folgekriterien und Wahrscheinlichkeitskriterien;

b) die Auswirkungen, die Informationssicherheitsereignisse auf strategischer, taktischer und operativer Ebene haben können (dies kann als ungünstigster Fall oder mit anderen Worten definiert werden, sofern dieselbe Grundlage konsistent verwendet wird);

c) rechtliche und behördliche Anforderungen sowie vertragliche Verpflichtungen;

d) Risiken, die über die Grenzen des Tätigkeitsbereichs der Organisation, einschließlich unvorhergesehener Auswirkungen auf Dritte, hinausgehen.

Für die Bewertung analysierter Risiken sind Kriterien für das Risikoniveau erforderlich.

Die Kriterien für das Risikoniveau können qualitativ (z. B. sehr hoch, hoch, mittel, niedrig) oder quantitativ (z. B. ausgedrückt als Erwartungswert des monetären Verlusts, des Verlusts von Menschenleben oder des Marktanteils über eine bestimmte Zeitspanne) sein.

BEISPIEL Risiken können als jährliche Verlusterwartung quantifiziert werden, d. h. als durchschnittlicher Geldwert der Auswirkungen je Jahr, die im nächsten Jahr eintreten.

Unabhängig davon, ob quantitative oder qualitative Kriterien verwendet werden, sollten Bewertungsskalen letztlich in einer Referenzskala verankert sein, die von allen interessierten Parteien verstanden wird, und sowohl die Risikoanalyse als auch die Risikobewertung sollten zumindest eine regelmäßige formale Kalibrierung anhand der Referenzskala umfassen, um die Gültigkeit, Konsistenz und Vergleichbarkeit der Ergebnisse sicherzustellen.

Wenn ein qualitativer Ansatz verwendet wird, sollten die Niveaus einer jeden qualitativen Skala eindeutig sein, ihre Abstufungen sollten klar definiert sein, die qualitativen Beschreibungen für jedes Niveau sollten in einer objektiven Sprache ausgedrückt werden und die Niveaus sollten sich nicht überschneiden. Wenn unterschiedliche Skalen verwendet werden (z. B. zur Erfassung von Risiken in verschiedenen Geschäftsbereichen), sollte eine Äquivalenz bestehen, um vergleichbare Ergebnisse zu ermöglichen.

6.5 Wahl eines angemessenen Verfahrens

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 b).

Im Allgemeinen sollten der Ansatz und die Verfahren für das Risikomanagement der Informationssicherheit auf den Ansatz und die Verfahren für die Handhabung der sonstigen Risiken der Organisation abgestimmt werden.

Der gewählte Ansatz sollte dokumentiert werden.

Nach ISO/IEC 27001:2022, 6.1.2 b), muss die Organisation im Rahmen des ISMS sicherstellen, dass wiederholte Risikobeurteilungen der Informationssicherheit zu konsistenten, gültigen und vergleichbaren Ergebnissen führen. Das bedeutet, dass das gewählte Verfahren die folgenden Eigenschaften der Ergebnisse sicherstellen sollte:

— Konsistenz: Beurteilungen derselben Risiken, die von verschiedenen Personen oder von denselben Personen bei verschiedenen Gelegenheiten und im selben Kontext durchgeführt werden, sollten zu ähnlichen Ergebnissen führen;

— Vergleichbarkeit: Es sollten Kriterien für die Risikobeurteilung festgelegt werden, um sicherzustellen, dass für unterschiedliche Risiken durchgeführte Beurteilungen vergleichbare Ergebnisse liefern, wenn sie gleichwertige Risikoniveaus darstellen;

— Gültigkeit: Die Beurteilungen sollten zu Ergebnissen führen, die so weit wie möglich mit der Realität übereinstimmen.

Verfahren des operativen Risikomanagements werden in der Regel für das Risikomanagement der Informationssicherheit eingesetzt. Das gewählte Verfahren kann jeden geeigneten Ansatz in Bezug auf die Berücksichtigung des Restrisikos verwenden. Bei den gebräuchlichsten Ansätzen zur Handhabung von Informationssicherheitsrisiken wird das aktuelle Risiko verwendet, um die Wahrscheinlichkeit und die Auswirkungen von Risiken zu beurteilen.

7 Prozess zur Beurteilung von Informationssicherheitsrisiken

7.1 Allgemeines

Die Organisation sollte den organisatorischen Risikobeurteilungsprozess (falls vorhanden) nutzen, um Risiken für Informationen zu beurteilen oder einen Risikobeurteilungsprozess für die Informationssicherheit zu definieren.

Die Risikobeurteilung ermöglicht es Risikoeigentümern, die Risiken im Einklang mit der Behandlungsperspektive zu priorisieren, und zwar in erster Linie auf der Grundlage ihrer Auswirkungen und der Wahrscheinlichkeit oder anderer festgelegter Kriterien.

Der Kontext der Risikobeurteilung sollte festgelegt werden, einschließlich einer Beschreibung des Anwendungsbereichs und des Zwecks sowie der internen und externen Aspekte, die die Risikobeurteilung beeinflussen.

Die Risikobeurteilung besteht aus den folgenden Aufgaben:

a) Risikoidentifizierung, d. h. ein Prozess zum Auffinden, Erkennen und Beschreiben von Risiken (weitere Einzelheiten zur Risikoidentifizierung sind in 7.2 enthalten);

b) Risikoanalyse, d. h. ein Prozess zum Verstehen der Risikoarten und Bestimmen des Risikoniveaus. Bei der Risikoanalyse werden die Ursachen und Quellen des Risikos, die Wahrscheinlichkeit, dass ein bestimmtes Ereignis eintritt, die Wahrscheinlichkeit, dass dieses Ereignis Auswirkungen hat, und der Schweregrad dieser Auswirkungen berücksichtigt (weitere Einzelheiten zur Risikoanalyse sind in 7.3 zu finden);

c) Risikobewertung, d. h. ein Prozess, bei dem die Ergebnisse der Risikoanalyse mit Risikokriterien verglichen werden, um festzustellen, ob das Risiko und/oder seine Signifikanz akzeptabel ist, und um die analysierten

Risiken für die Risikobehandlung zu priorisieren. Auf der Grundlage dieses Vergleichs kann die Notwendigkeit einer Behandlung erwogen werden (weitere Einzelheiten zur Risikobewertung sind in 7.4 enthalten).

Der Prozess der Risikobeurteilung sollte sich auf Verfahren (siehe 6.5) und Instrumente stützen, die hinreichend detailliert konzipiert sind, um so weit wie möglich, konsistente, gültige und reproduzierbare Ergebnisse sicherzustellen. Außerdem sollten die Ergebnisse vergleichbar sein, z. B. um festzustellen, ob das Risiko gestiegen oder gesunken ist.

Die Organisation sollte sicherstellen, dass ihr Ansatz für das Informationssicherheitsrisikomanagement auf den Ansatz für das organisatorische Risikomanagement abgestimmt ist, so dass alle Informationssicherheitsrisiken mit anderen organisatorischen Risiken verglichen werden können und nicht nur isoliert betrachtet werden.

In ISO/IEC 27001 wird kein bestimmter Ansatz vorgeschrieben, der zur Erfüllung der Anforderungen in ISO/IEC 27001:2022, 6.1.2 zu verwenden ist. Dennoch gibt es zwei Hauptansätze für die Beurteilung: einen ereignisbasierten Ansatz und einen auf Werten basierenden Ansatz. Sie werden in 7.2.1 näher erläutert.

7.2 Identifizierung von Informationssicherheitsrisiken

7.2.1 Identifizierung und Beschreibung von Informationssicherheitsrisiken

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 c) 1).

Eingabe: Ereignisse, die das Erreichen der Informationssicherheitsziele in der Organisation oder in anderen Organisationen negativ beeinflussen können.

Aktion: Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sollten identifiziert werden.

Auslöser: Risikoeigentümer, interessierte Parteien und/oder Experten erkennen neue oder veränderte Ereignisse bzw. Situationen, die sich auf das Erreichen der Informationssicherheitsziele auswirken können, oder haben das Bedürfnis, danach zu suchen.

Ausgabe: Eine Liste der identifizierten Risiken.

Anleitung zur Umsetzung:

Unter Risikoidentifizierung wird der Prozess zum Finden, Erkennen und Beschreiben von Risiken verstanden. Dazu gehört die Identifizierung von Risikoquellen und Ereignissen.

Ziel der Risikoidentifizierung ist es, eine Liste von Risiken zu erzeugen, die sich auf Ereignisse stützt, die das Erreichen der Informationssicherheitsziele verhindern, beeinträchtigen oder verzögern können.

Die identifizierten Risiken sollten diejenigen sein, die, wenn sie eintreten, Auswirkungen auf das Erreichen der Ziele haben können.

ISO/IEC 27001:2022, 6.1.2 c), verlangt, dass die Organisation einen Prozess zur Beurteilung der Informationssicherheitsrisiken definiert und anwendet, der die Informationssicherheitsrisiken identifiziert. Für die Risikoidentifizierung gibt es zwei gängige Ansätze.

a) Ereignisbasierter Ansatz: Identifizierung strategischer Szenarien durch Betrachtung der Risikoquellen und der Art und Weise, wie sie interessierte Parteien nutzen oder beeinflussen, um das gewünschte Ziel dieser Risiken zu erreichen.

b) Wertbasierter Ansatz: Identifizierung von Betriebsszenarien, die in Bezug auf Werte, Bedrohungen und Schwachstellen detailliert sind.

Einem ereignisbasierten Ansatz liegt das Konzept zugrunde, dass Risiken durch eine Bewertung von Ereignissen und Auswirkungen identifiziert und beurteilt werden können. Ereignisse und Auswirkungen lassen sich häufig durch Feststellung der Bedenken der obersten Führungsebene, der Risikoeigentümer und der Anforderungen, die bei der Bestimmung des Kontexts der Organisation identifiziert wurden, ermitteln (ISO/IEC 27001:2022, Abschnitt 4). Gespräche mit der obersten Führungsebene und den Personen in der Organisation, die für einen Geschäftsprozess verantwortlich sind, können dabei helfen, nicht nur die maßgeblichen Ereignisse und Auswirkungen, sondern auch die Risikoeigentümer zu identifizieren.

Bei einem ereignisbasierten Ansatz können übergeordnete oder strategische Szenarien erstellt werden, ohne dass ein erheblicher Zeitaufwand für die detaillierte Identifizierung von Werten erforderlich ist. Auf diese Weise kann die Organisation ihre Bemühungen zur Risikobehandlung auf die kritischen Risiken konzentrieren. Bei der Bewertung von Ereignissen nach diesem Ansatz kann auf historische Daten zurückgegriffen werden, bei denen die Risiken über lange Zeitspannen unverändert bleiben, und es somit den interessierten Parteien ermöglicht, ihre Ziele zu erreichen. Bei Risiken, für die keine historischen Daten zur Verfügung stehen oder die nicht zuverlässig sind, können jedoch Ratschläge, die auf dem Wissen und der Erfahrung von Experten oder der Untersuchung von Risikoquellen beruhen, die Bewertung unterstützen.

Einem auf Werten basierenden Ansatz liegt das Konzept zugrunde, dass Risiken durch eine Prüfung von Werten, Bedrohungen und Schwachstellen identifiziert und beurteilt werden können. Ein Wert ist alles, was eine Bedeutung für die Organisation hat und daher geschützt werden muss. Bei der Identifizierung von Werten ist zu berücksichtigen, dass ein Informationssystem aus Aufgaben, Prozessen und zu schützenden Informationen besteht. Die Werte können je nach Art und Priorität als primäre und unterstützende Werte identifiziert werden, wobei ihre Abhängigkeiten sowie ihre Wechselwirkungen mit ihren Risikoquellen und den interessierten Parteien der Organisation hervorgehoben werden. Eine Bedrohung nutzt eine Schwachstelle eines Werts aus, um die Vertraulichkeit, Integrität und/oder Verfügbarkeit der entsprechenden Informationen zu gefährden. Wenn alle gültigen Kombinationen von Werten, Bedrohungen und Schwachstellen im Rahmen des ISMS aufgezählt werden können, wären theoretisch alle Risiken identifiziert. Für die weiteren Schritte der Risikobeurteilung sollte eine Liste von Werten erstellt werden, die mit Informationen und informationsverarbeitenden Einrichtungen verbunden sind.

Mit dem auf Vermögenswerten basierenden Ansatz können wertspezifische Bedrohungen und Schwachstellen identifiziert werden, und die Organisation kann eine detaillierte spezifische Risikobehandlung festlegen.

Weitere Informationen zu beiden Ansätzen sind in Anhang A enthalten.

Im Prinzip unterscheiden sich die beiden Ansätze nur in der Ebene, auf der die Identifizierung eingeleitet wird. Beide Ansätze können dasselbe Risikoszenario beschreiben, z. B. wenn ein Informationswert auf der Detailebene und eine Geschäftsexposition auf der allgemeinen Ebene liegt. Die Identifizierung der beitragenden Risikoquellen mit Hilfe einer ereignisbasierten Beurteilung erfordert in der Regel ein Herunterbrechen von der allgemeinen Ebene des Szenarios auf die Detailebene, während bei einer auf Werten basierenden Beurteilung in der Regel eine Aufwärtssuche vom Wert bis zum Szenario erfolgt, um einen Überblick darüber zu erhalten, wie sich die Auswirkungen kumulieren.

Die Risikoidentifizierung ist von entscheidender Bedeutung, da ein Informationssicherheitsrisiko, das in dieser Phase nicht identifiziert wird, nicht in die weitere Analyse einbezogen wird.

Bei der Risikoidentifizierung sollten Risiken unabhängig davon berücksichtigt werden, ob ihre Quelle unter der Kontrolle der Organisation steht, auch wenn keine spezifischen Risikoquellen offensichtlich sind. Insbesondere bei der Beurteilung komplexer Risikoszenarien sollte eine iterative Risikobeurteilung durchgeführt werden. Die erste Runde sollte sich auf hochqualifizierte Beobachtungen konzentrieren, und in den folgenden Runden sollten weitere Detailstufen behandelt werden, bis die eigentlichen Ursachen der Risiken ermittelt werden können.

Jeder andere Ansatz zur Risikoidentifizierung kann verwendet werden, solange mit ihm die Erzielung konsistenter, gültiger und vergleichbarer Ergebnisse sichergestellt ist und die Anforderung von ISO/IEC 27001:2022, 6.1.2 b) erfüllt werden.

Die Handhabung von Informationssicherheitsrisiken sollte nicht durch willkürliche oder restriktive Ansichten darüber eingeschränkt werden, wie Risiken strukturiert, gruppiert, kumuliert, aufgeteilt oder beschrieben werden sollten. Risiken können sich scheinbar überschneiden oder Teilmengen bzw. konkrete Ausprägungen anderer Risiken sein. Allerdings sollten Maßnahmen für einzelne Risiken getrennt von umfassenderen Risiken oder aggregierten Risiken für die Zwecke der Risikobehandlung betrachtet und identifiziert werden.

BEISPIEL 1 Beispiel für zwei sich überschneidende Risiken: (1) Es besteht die Gefahr eines Brands im Stammhaus; (2) es besteht die Gefahr eines Brands, der den Betrieb der Buchhaltung beeinträchtigt, wenn sich die Buchhaltung im Stammhaus, aber auch in mehreren anderen Gebäuden befindet.

Beispiele für konkrete Ausprägungen eines Risikos: (1) Es liegt ein Datenverlust vor; (2) es liegt ein Datenverlust von personenbezogenen Daten vor.

Das zweite Risiko ist eine konkrete Ausprägung des ersten Risikos, aber es hat wahrscheinlich andere Eigenschaften und ist mit anderen Maßnahmen verbunden als das erste Risiko, und es kann wichtig sein, es getrennt von dem viel umfassenderen ersten Risiko zu handhaben.

Eine Aggregation von Risiken sollte nur dann vorgenommen werden, wenn sie auf der Ebene, auf der der Kontext der Organisation betrachtet wird, maßgeblich sind. Bei der Planung von Behandlungsoptionen kann es notwendig sein, Risiken, die für die Zwecke der Budgetierung des Gesamtrisikomanagements zusammengefasst werden, getrennt zu betrachten, da zu ihrer Handhabung unterschiedliche Maßnahmen erforderlich sein können.

BEISPIEL 2 Ein Rechenzentrum kann mehreren unabhängigen Gefährdungen ausgesetzt sein: Überschwemmung, Feuer, Stromspitzen und Vandalismus.

Um das Gesamtrisiko des Unternehmens abzuschätzen, können die einzelnen Risiken dieser Ereignisse zu einem Gesamtrisiko zusammengefasst werden. Da jedoch jedes dieser Ereignisse unterschiedliche Maßnahmen zur Handhabung des Risikos erfordert, sollten sie für die Zwecke der Risikobehandlung getrennt betrachtet und identifiziert werden. Risiken (Kombinationen von Wahrscheinlichkeiten und Auswirkungen) können nicht immer unmittelbar aggregiert werden.

7.2.2 Identifizierung von Risikoeigentümern

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 c) 2).

Eingabe: Liste der identifizierten Risiken.

Aktion: Die Risiken sollten den Risikoeigentümern zugeordnet werden.

Auslöser: Die Identifizierung von Risikoeigentümern wird notwendig, wenn:

— sie bisher noch nicht erfolgt ist;

— ein Personalwechsel in dem betreffenden Geschäftsbereich, in dem die Risiken angesiedelt sind, stattfindet.

Ausgabe: Liste der Risikoeigentümer mit den zugehörigen Risiken.

Anleitung zur Umsetzung:

Die oberste Führungsebene, der Sicherheitsausschuss, die Prozessverantwortlichen, die Funktionsverantwortlichen, die Abteilungsleiter und die Eigentümer von Werten können die Risikoeigentümer sein.

Eine Organisation sollte den organisatorischen Risikobeurteilungsprozess (falls vorhanden) nutzen, um die Risikoeigentümer zu identifizieren; andernfalls sollte sie Kriterien für die Identifizierung der Risikoeigentümer definieren. Solche Kriterien sollten berücksichtigen, dass Risikoeigentümer:

— rechenschaftspflichtig sind und die Befugnis haben, die Risiken, deren Eigentümer sie sind, zu handhaben, d. h. sie sollten eine Position in der Organisation haben, die es ihnen erlaubt, diese Befugnis tatsächlich auszuüben;

— den jeweiligen Sachverhalt verstehen und in der Lage sind, informierte Entscheidungen zu treffen (z. B. über die Behandlung der Risiken).

Das Risikoniveau und die Frage, für welchen Wert das Risiko gelten sollte, können als Grundlage für die Identifizierung von Risikoeigentümern dienen.

Die Zuweisung sollte im Rahmen des Risikobeurteilungsprozesses erfolgen.

7.3 Analyse von Informationssicherheitsrisiken

7.3.1 Allgemeines

Ziel der Risikoanalyse ist es, das Risikoniveau zu bestimmen.

Auf die Norm ISO 31000 wird in ISO/IEC 27001 als allgemeines Modell verwiesen. In ISO/IEC 27001:2022, 6.1.2, wird vorgeschrieben, dass die Risikoanalyse für jedes identifizierte Risiko auf der Beurteilung der sich aus dem Risiko ergebenden Auswirkungen und der Beurteilung der Wahrscheinlichkeit des Risikos beruht, um ein Risikoniveau zu bestimmen.

Techniken zur Risikoanalyse auf der Grundlage von Auswirkungen und Wahrscheinlichkeit können u. a. sein:

a) qualitativ, unter Verwendung einer Skala von qualifizierenden Attributen (z. B. hoch, mittel, niedrig); oder

b) quantitativ, unter Verwendung einer Skala mit numerischen Werten (z. B. monetäre Kosten, Häufigkeit oder Wahrscheinlichkeit des Auftretens); oder

c) semiquantitativ, unter Verwendung qualitativer Skalen mit zugewiesenen Werten.

Risikoanalysen sollten auf diejenigen Risiken und Maßnahmen ausgerichtet sein, die bei erfolgreicher Handhabung die Wahrscheinlichkeit erhöhen, dass die Organisation ihre Ziele erreicht. Es ist leicht, einen erheblichen Teil der Zeit auf eine Risikobeurteilung zu verwenden, insbesondere auf die Beurteilung von Wahrscheinlichkeiten und Auswirkungen. Um eine effiziente Entscheidungsfindung beim Risikomanagement zu ermöglichen, kann es ausreichen, erste und grobe Schätzungen der Wahrscheinlichkeit und der Auswirkungen vorzunehmen.

7.3.2 Beurteilung potentieller Auswirkungen

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 d) 1).

Eingabe: Eine Liste der identifizierten maßgeblichen Ereignis- oder Risikoszenarien einschließlich der Identifizierung von Risikoquellen, Geschäftsprozessen, Geschäftszielen und Folgekriterien. Außerdem Listen aller bestehenden Maßnahmen inklusive Angaben zu ihrer Wirksamkeit, ihrer Implementierung und ihrem Verwendungsstatus.

Aktion: Die Auswirkungen, die sich aus der unzureichenden Wahrung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen ergeben, sollten identifiziert und beurteilt werden.

Auslöser: Die Beurteilung der Auswirkungen wird notwendig, wenn:

— sie bisher noch nicht erfolgt ist;

— die durch die „Risikoidentifizierung“ erstellte Liste Änderungen erfährt;

— Risikoeigentümer oder interessierte Parteien die Einheiten geändert haben, in denen sie die Auswirkungen festlegen wollen, oder

— Änderungen des Anwendungsbereichs oder des Kontexts festgestellt werden, die sich auf die Auswirkungen auswirken.

Ausgabe: Eine Liste potentieller Auswirkungen im Zusammenhang mit Risikoszenarien mit ihren Auswirkungen für Werte oder Ereignisse, je nach angewandtem Ansatz.

Anleitung zur Umsetzung:

Wird die Sicherheit von Informationen nicht angemessen gewahrt, kann dies zum Verlust ihrer Vertraulichkeit, Integrität oder Verfügbarkeit führen. Der Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit kann weitere Auswirkungen für die Organisation und deren Ziele haben. Die Auswirkungsanalyse kann ausgehend von den Auswirkungen für die Informationssicherheit durchgeführt werden, indem überlegt wird, was bei einem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit der betreffenden Informationen geschehen kann. In der Regel kann der Risikoeigentümer die Auswirkungen abschätzen, wenn das Ereignis eintritt. Folgende Elemente sollten beachtet werden:

— Einschätzung (oder Maß auf der Grundlage von Erfahrungswerten) der Verluste (Uhrzeit oder Datum) aufgrund des Ereignisses als Folge der Unterbrechung oder Störung des Betriebs;

— Einschätzung/Wahrnehmung des Schweregrads der Folge (z. B. ausgedrückt in Geld);

— Wiederherstellungskosten, je nachdem, ob die Wiederherstellung intern erfolgen kann (durch das Team des Risikoeigentümers) oder ob eine externe Entität hinzugezogen werden muss.

7.3.3 Beurteilung der Wahrscheinlichkeit

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 d) 2).

Eingabe: Eine Liste der identifizierten maßgeblichen Ereignis- oder Risikoszenarien einschließlich der Identifizierung von Risikoquellen, Geschäftsprozessen, Geschäftszielen und Wahrscheinlichkeitskriterien. Außerdem Listen aller bestehenden Maßnahmen mit Angaben zu ihrer Wirksamkeit, ihrer Implementierung und ihrem Verwendungsstatus.

Aktion: Die Wahrscheinlichkeit des Eintretens möglicher oder tatsächlicher Szenarien sollte anhand festgelegter Wahrscheinlichkeitskriterien beurteilt und ausgedrückt werden.

Auslöser: Neben den Auswirkungen ist die Beurteilung der Wahrscheinlichkeit ein Schwerpunkt des Risikobeurteilungsprozesses, wenn es darum geht, das Risikoniveau zu bestimmen.

Die Beurteilung der Wahrscheinlichkeit wird notwendig, wenn:

— sie bisher noch nicht erfolgt ist;

— Änderungen des Anwendungsbereichs oder des Kontexts festgestellt werden, die sich auf die Wahrscheinlichkeit auswirken können;

— Schwachstellen in umgesetzten Maßnahmen entdeckt werden;

— Prüfungen/Audits der Wirksamkeit der Maßnahmen zu unerwarteten Ergebnissen führen;

— Änderungen in der Bedrohungsumgebung entdeckt werden (z. B. neue Bedrohungsakteure/Quellen).

Ausgabe: Eine Liste von Ereignissen oder Risikoszenarien, ergänzt durch Wahrscheinlichkeiten dafür, dass diese eintreten.

Anleitung zur Umsetzung:

Nach der Identifizierung der Risikoszenarien muss die Wahrscheinlichkeit des Eintretens der einzelnen Szenarien und Auswirkungen mit Hilfe qualitativer oder quantitativer Analysetechniken analysiert werden. Die Beurteilung der Wahrscheinlichkeit ist nicht immer einfach und sollte auf unterschiedliche Weise ausgedrückt werden. Dabei sollte berücksichtigt werden, wie häufig die Risikoquellen vorliegen oder wie leicht einige von ihnen (z. B. Schwachstellen) ausgenutzt werden können. In diesem Zusammenhang sollten die folgenden Punkte beachtet werden:

— Erfahrung und anwendbare Statistiken für die Wahrscheinlichkeit von Risikoquellen;

— für vorsätzliche Risikoquellen: der Grad der Motivation [z. B. die Rentabilität (Kosten/Nutzen) des Angriffs] und die Fähigkeiten (z. B. das Niveau der Fertigkeiten möglicher Angreifer), die sich im Laufe der Zeit ändern, außerdem die den möglichen Angreifern zur Verfügung stehenden Ressourcen und die Einflüsse auf mögliche Angreifer, wie z. B. Schwerkriminalität, terroristische Organisationen oder ausländische Nachrichtendienste, sowie die Wahrnehmung der Attraktivität und Verletzlichkeit von Informationen für einen möglichen Angreifer;

— für zufällige Risikoquellen: geografische Faktoren (z. B. die Nähe zu gefährlichen Einrichtungen oder Aktivitäten), die Möglichkeit von Naturkatastrophen wie extreme Wetterverhältnisse, vulkanische Aktivitäten, Erdbeben, Überschwemmungen, Tsunamis und Faktoren, die menschliche Fehler und Fehlfunktionen von Geräten beeinflussen können;

— bekannte Schwachstellen und etwaige ausgleichende Maßnahmen, sowohl einzeln als auch in ihrer Gesamtheit;

— bestehende Maßnahmen und wie wirksam sie bekannten Schwachstellen entgegenwirken.

Die Einschätzung der Wahrscheinlichkeit ist von Natur aus unsicher, nicht nur, weil sie Dinge berücksichtigt, die noch nicht geschehen sind und daher nicht vollständig bekannt sind, sondern auch, weil die Wahrscheinlichkeit ein statistisches Maß und nicht direkt repräsentativ für einzelne Ereignisse ist. Die drei grundlegenden Quellen der Beurteilungsungewissheit sind:

— persönliche Ungewissheit, die auf das Urteil des Beurteilers zurückzuführen ist und die sich aus der Variabilität der mentalen Heuristiken der Entscheidungsfindung ergibt;

— die methodische Ungewissheit, die sich aus der Verwendung von Instrumenten ergibt, die Ereignisse zwangsläufig vereinfachen;

— systemische Ungewissheit über das zu erwartende Ereignis selbst, die sich aus unzureichendem Wissen ergibt (insbesondere, wenn die Nachweise begrenzt sind oder sich eine Risikoquelle mit der Zeit verändert).

Um die Verlässlichkeit der Wahrscheinlichkeitseinschätzung zu erhöhen, sollten Organisationen die Verwendung eines solchen Verfahrens die folgenden Punkte in Betracht ziehen:

a) Teambeurteilungen anstelle von Einzelbeurteilungen;

b) externe Quellen, z. B. Berichte über Verstöße gegen die Informationssicherheit;

c) Skalen mit einer dem Ansatz der Organisation angemessenen Reichweite und Auflösung;

d) eindeutige Kategorien, wie „einmal im Jahr“, statt „selten“.

Bei der Beurteilung der Wahrscheinlichkeit von Ereignissen ist es wichtig, den Unterschied zwischen unabhängigen und abhängigen Ereignissen zu erkennen. Die Wahrscheinlichkeit von Ereignissen, die voneinander abhängen, ist durch die Beziehung zwischen ihnen bedingt (z. B. kann ein zweites Ereignis unvermeidlich

sein, wenn ein erstes Ereignis eintritt), so dass eine getrennte Beurteilung der beiden Wahrscheinlichkeiten nicht notwendig ist. Die Wahrscheinlichkeiten maßgeblicher unabhängiger Ereignisse sind allesamt wesentliche Beitragskriterien für die Wahrscheinlichkeit einer Folge, zu der sie beitragen.

BEISPIEL Die Wahrscheinlichkeit eines Denial-of-Service-Angriffs auf einen Server hängt von der aktuellen Bedrohungslage sowie der Anfälligkeit und Zugänglichkeit des Servers ab. Die Wahrscheinlichkeit bösartiger Pakete kann jedoch 100 % betragen, sobald der Angriff begonnen hat, und ihre Beurteilung hilft nicht bei der Beurteilung der Wahrscheinlichkeit eines Denial-of-Service-Angriffs.

Um eine unnötige Komplexität der Beurteilung zu vermeiden, ist es wichtig, alle Abhängigkeiten zwischen den zu einem Risikoszenario beitragenden Ereignissen zu identifizieren und in erster Linie die Wahrscheinlichkeiten dieser voneinander unabhängigen Ereignisse zu beurteilen.

Die Gesamtwahrscheinlichkeit der geschäftlichen Auswirkungen eines Informationssicherheitsereignisses hängt in der Regel von der Wahrscheinlichkeit potentiell mehrerer untergeordneter Ereignisse und deren Auswirkungen ab. Anstatt zu versuchen, die Wahrscheinlichkeit geschäftlicher Auswirkungen in einer einzigen übergeordneten Beurteilung abzuschätzen, kann es sinnvoller sein, zunächst die Wahrscheinlichkeiten der einzeln beurteilten untergeordneten Ereignisse, die dazu beitragen, zusammenzufassen.

7.3.4 Bestimmung der Risikoniveaus

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 d) 3).

Eingabe: Eine Liste der Risikoszenarien mit ihren Auswirkungen für Werte oder Ereignisse und deren Wahrscheinlichkeit (quantitativ oder qualitativ).

Aktion: Das Risikoniveau sollte als eine Kombination aus der beurteilten Wahrscheinlichkeit und den beurteilten Auswirkungen für alle maßgeblichen Risikoszenarien bestimmt werden.

Auslöser: Die Bestimmung der Risikoniveaus ist notwendig, wenn die Risiken der Informationssicherheit bewertet werden sollen.

Ausgabe: Eine Liste von Risiken mit zugewiesenen Niveauwerten.

Anleitung zur Umsetzung:

Das Risikoniveau kann auf vielerlei Weise bestimmt werden. Es wird in der Regel als eine Kombination aus der beurteilten Wahrscheinlichkeit und den beurteilten Auswirkungen für alle maßgeblichen Risikoszenarien bestimmt. Alternative Berechnungen können sowohl einen Wert als auch die Wahrscheinlichkeit und die Folge umfassen. Außerdem ist die Berechnung nicht notwendigerweise linear, z. B. kann die Wahrscheinlichkeit im Quadrat mit der Folge kombiniert werden. In jedem Fall sollte das Risikoniveau anhand der in 6.4.3.4 beschriebenen Kriterien bestimmt werden.

7.4 Bewertung der Informationssicherheitsrisiken

7.4.1 Vergleich der Ergebnisse der Risikoanalyse mit den Risikokriterien

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 e) 1).

Eingabe: Eine Liste von Risikokriterien und Risiken mit zugewiesenen Niveauwerten.

Aktion: Risikoniveaus sollten mit Risikobewertungskriterien, insbesondere Risikoakzeptanzkriterien, verglichen werden.

Auslöser: Der Vergleich der Ergebnisse einer Risikoanalyse mit den Risikokriterien wird erforderlich, wenn die Informationssicherheitsrisiken für die Behandlung priorisiert werden sollen.

Ausgabe: Eine Liste von Vorschlägen für Entscheidungen über zusätzliche Aktionen im Zusammenhang mit dem Risikomanagement.

Anleitung zur Umsetzung:

Nach der Identifizierung der Risiken und der Zuweisung von Werten für die Wahrscheinlichkeit und den Schweregrad der Auswirkungen sollten die Organisationen ihre Risikoakzeptanzkriterien anwenden, um festzustellen, ob die Risiken akzeptiert werden können oder nicht. Wenn sie nicht akzeptiert werden können, sollten sie vorrangig behandelt werden.

Um Risiken zu bewerten, sollten Organisationen die beurteilten Risiken mit den Risikokriterien vergleichen, die bei der Erstellung des Kontexts festgelegt wurden.

Entscheidungen zur Risikobewertung sollten auf dem Vergleich des beurteilten Risikos mit den festgelegten Akzeptanzkriterien beruhen, wobei idealerweise der Grad des Vertrauens in die Beurteilung berücksichtigt wird. In einigen Fällen, z. B. beim häufigen Auftreten von Ereignissen mit relativ geringen Auswirkungen, kann es hilfreich sein, deren kumulative Wirkung über eine bestimmte Zeitspanne zu betrachten, anstatt das Risiko jedes einzelnen Ereignisses zu berücksichtigen, da dies eine realistischere Darstellung der Gesamtrisiken liefern kann.

Bei der Abgrenzung zwischen behandlungsbedürftigen und nicht behandlungsbedürftigen Risiken kann es zu Ungewissheiten kommen. Unter bestimmten Umständen ist die Verwendung eines einzigen Niveaus als akzeptables Risikoniveau, das die zu behandelnden von den nicht zu behandelnden Risiken trennt, nicht immer angemessen. In einigen Fällen kann es effektiver sein, ein Element der Flexibilität in die Kriterien aufzunehmen, indem zusätzliche Parameter wie Kosten und Wirksamkeit möglicher Maßnahmen einbezogen werden.

Die Risikoniveaus können auf der Grundlage eines Konsenses zwischen Risikoeigentümern einerseits und Fachleuten in den Bereichen Betriebswirtschaft und Technik andererseits validiert werden. Es ist wichtig, dass die Risikoeigentümer gute Kenntnisse der Risiken haben, für die sie verantwortlich sind, und dass sich diese Kenntnisse in den Ergebnissen einer objektiven Beurteilung widerspiegeln. Folglich sollte jede Diskrepanz zwischen den beurteilten Risikoniveaus und den von den Risikoeigentümern wahrgenommenen Risikoniveaus untersucht werden, um festzustellen, was der Realität besser entspricht.

7.4.2 Priorisierung der analysierten Risiken für die Risikobehandlung

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.2 e) 2).

Eingabe: Eine Liste der Ergebnisse des Vergleichs der Risiken mit den Risikokriterien.

Aktion: Die Risiken auf der Liste sollten unter Berücksichtigung der beurteilten Risikoniveaus für die Risikobehandlung nach Prioritäten geordnet werden.

Auslöser: Die Priorisierung der analysierten Risiken für die Risikobehandlung wird notwendig, wenn die Informationssicherheitsrisiken behandelt werden sollen.

Ausgabe: Eine Liste der priorisierten Risiken mit Risikoszenarien, die zu diesen Risiken führen.

Anleitung zur Umsetzung:

Die Risikobewertung nutzt das durch die Risikoanalyse gewonnene Risikoverständnis, um Vorschläge für die Entscheidung über die nächsten Schritte zu machen. Diese sollten die folgenden Punkte berücksichtigen:

— ob eine Risikobehandlung erforderlich ist;

— Prioritäten für die Risikobehandlung unter Beachtung der beurteilten Risikoniveaus.

Die für die Priorisierung der Risiken verwendeten Risikokriterien sollten die Ziele der Organisation, die vertraglichen, rechtlichen und behördlichen Anforderungen und die Ansichten der maßgeblichen interessierten Parteien berücksichtigen. Die Prioritäten, wie sie bei der Risikobewertung gesetzt werden, beruhen hauptsächlich auf den Akzeptanzkriterien.

8 Prozess zur Informationssicherheitsrisikobehandlung

8.1 Allgemeines

Die Eingabe für die Behandlung von Informationssicherheitsrisiken beruht auf den Ergebnissen des Risikobeurteilungsprozesses in Form einer nach Risikokriterien geordneten Menge von zu behandelnden Risiken.

Das Ergebnis dieses Prozesses ist eine Reihe von notwendigen Maßnahmen zur Informationssicherheit [siehe ISO/IEC 27001:2022, 6.1.3 b)], die in Übereinstimmung mit dem Risikobehandlungsplan [siehe ISO/IEC 27001:2022, 6.1.3 e)] eingesetzt oder verbessert werden müssen. Auf diese Weise eingesetzt, besteht die Wirksamkeit des Risikobehandlungsplans darin, das Informationssicherheitsrisiko, dem die Organisation gegenübersteht, so zu verändern, dass es die Akzeptanzkriterien der Organisation erfüllt.

8.2 Auswahl geeigneter Optionen zur Behandlung von Informationssicherheitsrisiken

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 a).

Eingabe: Eine Liste der priorisierten Risiken mit Ereignis- oder Risikoszenarien, die zu diesen Risiken führen.

Aktion: Optionen der Risikobehandlung sollten gewählt werden.

Auslöser: Die Auswahl geeigneter Optionen zur Behandlung von Informationssicherheitsrisiken wird notwendig, wenn kein Risikobehandlungsplan vorliegt oder der Plan unvollständig ist.

Ausgabe: Eine Liste der priorisierten Risiken mit den ausgewählten Risikobehandlungsoptionen.

Anleitung zur Umsetzung:

Zu den Optionen für die Risikobehandlung zählen:

— die Risikovermeidung, indem entschieden wird, die Ausführung der Aufgabe, aus der sich ein Risiko ergibt, nicht zu beginnen oder fortzuführen;

— die Risikoänderung, indem die Wahrscheinlichkeit des Auftretens eines Ereignisses oder einer Folge oder der Schweregrad der Folge verändert wird;

— die Risikobeibehaltung im Rahmen einer fundierten Wahl;

— die Risikoteilung, indem die Verantwortung mit anderen Parteien entweder intern oder extern (z. B. Teilung der Auswirkungen über eine Versicherung) aufgeteilt wird.

BEISPIEL 1 Ein Beispiel für Risikovermeidung ist ein Bürostandort in einem Überschwemmungsgebiet, bei dem die Gefahr einer Überschwemmung und daraus resultierender Schäden am Büro sowie Einschränkungen der Verfügbarkeit des Büros und/oder des Zugangs zum Büro bestehen. Die entsprechenden physischen Maßnahmen können sich als unzureichend erweisen, um dieses Risiko zu verringern; in diesem Fall kann die beste verfügbare Option die Risikovermeidung sein. Dies kann die Schließung oder die Einstellung des Betriebs dieses Büros bedeuten.

BEISPIEL 2 Ein weiteres Beispiel für Risikovermeidung ist die Entscheidung, bestimmte Informationen von Einzelpersonen nicht zu erheben, so dass es für die Organisation nicht notwendig ist, die Informationen in ihren Informationssystemen zu verwalten, zu speichern und zu übertragen.

Bei der Risikoteilung ist mindestens eine Maßnahme erforderlich, um die Wahrscheinlichkeit oder die Folge zu ändern, aber die Organisation überträgt die Verantwortung für die Durchführung der Maßnahme an eine andere Partei.

Die Optionen für die Risikobehandlung sollten auf der Grundlage der Ergebnisse der Risikobeurteilung, der voraussichtlichen Kosten für die Umsetzung dieser Optionen und des erwarteten Nutzens dieser Optionen, sowohl einzeln als auch im Zusammenhang mit anderen Maßnahmen, ausgewählt werden. Die Risikobehandlung sollte nach definierten Risikoniveaus, zeitlichen Beschränkungen und der notwendigen Abfolge der Umsetzungen sowie den in 7.4 festgelegten Ergebnissen der Risikobewertung priorisiert werden. Bei der Wahl der Option kann berücksichtigt werden, wie ein bestimmtes Risiko von den betroffenen Parteien wahrgenommen wird und welche Art der Risikokommunikation für diese Parteien am besten geeignet ist.

8.3 Festlegung aller Maßnahmen, die zur Umsetzung der gewählten Optionen für die Informationssicherheitsrisikobehandlung erforderlich sind

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 b).

Eingabe: Eine Liste der priorisierten Risiken mit den ausgewählten Risikobehandlungsoptionen.

Aktion: Bestimmung aller Maßnahmen aus den aus einer geeigneten Quelle ausgewählten Maßnahmenpaketen, die zur Behandlung der Risiken auf der Grundlage der gewählten Risikobehandlungsoptionen erforderlich sind, z. B. Änderung, Beibehaltung, Vermeidung oder Teilung der Risiken.

Auslöser: ISMS-Konformität; Handhabung von Informationssicherheitsrisiken.

Ausgabe: Alle notwendigen Maßnahmen.

Anleitung zur Umsetzung:

Besonderes Augenmerk sollte auf die Bestimmung der notwendigen Maßnahmen gelegt werden. Bei jeder Maßnahme sollte überprüft werden, ob sie notwendig ist, indem nachfragt wird,

— welche Auswirkungen diese Maßnahme auf die Wahrscheinlichkeit oder die Folge dieses Risikos hat;

— auf welche Weise die Maßnahme das Risikoniveau aufrechterhält.

Nur Maßnahmen, die mehr als nur eine vernachlässigbare Auswirkung auf das Risiko haben, sollten als „notwendig“ bezeichnet werden. Für jedes Risiko, das als behandlungsbedürftig eingestuft wird, sollten eine oder mehrere Maßnahmen ergriffen werden.

Es gibt viele Quellen für Maßnahmenpakete. Sie können in ISO/IEC 27001:2022, Anhang A, in branchenspezifischen Verhaltenskodizes (z. B. ISO/IEC 27017) und anderen nationalen, regionalen und industriellen Maßnahmenpaketen gefunden werden. Eine Organisation kann auch eine oder mehrere benutzerdefinierte Maßnahmen festlegen (siehe ISO/IEC 27003).

Wenn eine benutzerdefinierte Maßnahme definiert ist, sollte der Wortlaut der Maßnahme genau und angemessen beschreiben, um was es sich bei der Maßnahme handelt und wie sie funktioniert. Soweit zutreffend und angemessen, kann diese Formulierung sinnvollerweise folgende Aspekte umfassen:

— ob es sich um eine dokumentierte Maßnahme handelt;

— wer für die Maßnahme verantwortlich ist;

— wie sie überwacht wird;

— wie sie nachgewiesen werden kann;

— etwaige Ausnahmen;

— Häufigkeit der Durchführung der Maßnahme;

— die Toleranzgrenzen für die Maßnahme;

— wenn es nicht offensichtlich ist, der Grund, warum die Maßnahme besteht.

Liegt die Maßnahme außerhalb der Toleranzgrenzen, ist sie nicht wirksam genug, um das festgestellte Risiko zu bewältigen.

BEISPIEL 1 „Es gibt einen dokumentierten Prozess zur Handhabung von Malware, für den der IT-Sicherheitsmanager verantwortlich ist. Dies schließt Macs aus und wird über die Anbieterkonsole überwacht, wobei wöchentlich Berichte über die Leistung an den CIO gesendet werden."

Ein solch detaillierter Ansatz für die Formulierung von Maßnahmen kann sinnvoll sein, wenn die benutzerdefinierten Maßnahmen auch dazu dienen sollen, die Organisation bei der Berichterstattung über die Vertrauenswürdigkeit der Maßnahmen zu unterstützen. Wichtiger ist jedoch, dass der Wortlaut der Maßnahmen für die Mitarbeiter der Organisation verständlich ist und ihnen hilft, Entscheidungen über die Handhabung dieser Maßnahmen und der damit verbundenen Risiken zu treffen.

Die Bestimmung der Maßnahmen kann neue, noch nicht umgesetzte Maßnahmen einschließen, aber auch die Verwendung bereits vorhandener Maßnahmen in der Organisation. Eine bereits laufende Maßnahme sollte jedoch nicht automatisch in die Risikobeurteilung einbezogen werden, denn:

— die Maßnahme ist nicht erforderlich, um ein oder mehrere Informationssicherheitsrisiken zu handhaben;

— es kann sich um eine Maßnahme handeln, die in gewisser Weise zur Handhabung eines oder mehrerer Informationssicherheitsrisiken beiträgt, aber nicht wirksam genug ist, um in die Risikobeurteilung einbezogen oder durch das ISMS verwaltet zu werden oder;

— sie kann derzeit aus Gründen umgesetzt werden, die nicht mit der Informationssicherheit zusammenhängen (z. B. Qualität, Effizienz, Effektivität oder Compliance) oder;

— sie wird derzeit umgesetzt, kann aber aus Sicht der Informationssicherheit gestrichen werden, da ihre Wirkung nicht ausreicht, um ihren weiteren Status als wesentliche Maßnahme zu rechtfertigen.

Wird eine Maßnahme zu anderen Zwecken als der ausschließlichen Handhabung von Informationssicherheitsrisiken eingesetzt, sollte darauf geachtet werden, dass die Maßnahme so verwaltet wird, dass sowohl die Ziele der Informationssicherheit als auch die nicht für die Informationssicherheit maßgeblichen Ziele erreicht werden.

BEISPIEL 2 Interne Videoüberwachung zur Kontrolle der Qualität des Produktionsprozesses sowie aus Gründen der Informationssicherheit (zum Schutz vor Betrug).

Bei der Festlegung von Maßnahmen aus einem bestehenden Maßnahmenkatalog (z. B. ISO/IEC 27001:2022, Anhang A, oder einer branchenspezifischen Maßnahmenliste) sollte der Wortlaut der Maßnahme dem entsprechen, was zur Handhabung des Risikos erforderlich ist, und genau wiedergeben, was die Maßnahme ist oder sein sollte. Wenn der Gesamtansatz darin besteht, einen bestehenden Maßnahmenkatalog zu verwenden (z. B. ISO/IEC 27001:2022, Anhang A, oder eine branchenspezifische Maßnahmenliste) und der Maßnahmenkatalog keine Maßnahme enthält, die die erforderliche Maßnahme genau beschreibt, dann sollte die Definition einer benutzerdefinierten Maßnahme in Betracht gezogen werden, die die Maßnahme genau beschreibt.

Maßnahmen können als präventiv, detektierend und korrektiv eingestuft werden:

a) Präventive Maßnahme: eine Maßnahme, die das Eintreten eines Informationssicherheitsereignisses verhindern soll, das zu einer oder mehreren Auswirkungen führen kann;

b) detektierende Maßnahme: eine Maßnahme, die dazu dient, das Auftreten eines Informationssicherheitsereignisses zu erkennen;

c) korrektive Maßnahme: eine Maßnahme, die die Auswirkungen eines Informationssicherheitsereignisses begrenzen soll.

Die Maßnahmenart beschreibt, ob eine Maßnahme zur Verhinderung oder Erkennung eines Ereignisses oder zur Reaktion auf dessen Folge(n) durchgeführt wird oder durchgeführt werden soll.

BEISPIEL 3 Eine Informationssicherheitsrichtlinie ist eine Maßnahme, die das Risiko aufrechterhält, aber die Einhaltung der Richtlinie soll die Wahrscheinlichkeit des Auftretens eines Risikos verringern und kann daher als präventiv eingestuft werden.

Der Nutzen der Kategorisierung von Maßnahmen in präventive, detektierende und korrektive Maßnahmen liegt in ihrer Anwendung, um sicherzustellen, dass der Aufbau von Risikobehandlungsplänen gegenüber dem Versagen von Maßnahmen resilient ist. Vorausgesetzt, es gibt eine angemessene Mischung aus präventiven, detektierenden und korrektiven Maßnahmen:

— detektierende Maßnahmen sollten das Risiko mindern, wenn die präventiven Maßnahmen versagen;

— korrektive Maßnahmen sollten das Risiko mindern, wenn die detektierenden Maßnahmen versagen;

— präventive Maßnahmen sollten die Wahrscheinlichkeit verringern, dass die korrektiven Maßnahmen jemals eingesetzt werden müssen.

Beim Einsatz von Maßnahmen sollten Organisationen zunächst entscheiden, ob es möglich ist, das Eintreten eines Ereignisses zu erkennen. Ist das nicht der Fall, sollten detektierende Maßnahmen umgesetzt werden. Wenn es nicht möglich ist, ein Ereignis zu erkennen, können detektierende Maßnahmen unwirksam sein, und es gibt keine Möglichkeit festzustellen, ob eine präventive Maßnahme funktioniert.

BEISPIEL 4 Wenn nicht klar ist, ob ein Computer Teil eines „Botnetzes“ geworden ist, kann nicht festgestellt werden, ob die Maßnahmen, die verhindern sollen, dass er Teil eines Botnetzes wird, wie vorgesehen funktionieren.

Detektive Maßnahmen können zwar angemessen, aber dennoch unwirksam sein.

BEISPIEL 5 Die Implementierung von Angriffserkennungs-/Präventionssystemen kann ein wirksames Mittel sein, um zu verhindern, dass Schadsoftware in das Netz eindringt, aber sie nützen nichts, wenn die Systeme nicht überwacht werden und keine Warnungen mit Aufforderung zum Handeln ausgegeben werden, falls ein Ausbruch nicht eingedämmt wird.

Im Allgemeinen sind detektierende Maßnahmen letztendlich in den Fällen unwirksam, in denen sie umgangen werden können oder in denen ihre Meldung nicht zu geeigneten Aktionen führt. Als Nächstes sollten korrektive Maßnahmen geprüft werden. Wenn die detektierenden Maßnahmen fehlschlagen, hat das wahrscheinlich eine oder mehrere unerwünschte Auswirkungen. Die Implementierung der korrektiven Maßnahmen kann dazu beitragen, diese Auswirkungen zu begrenzen. Obwohl korrektive Maßnahmen erst nach dem Eintreten der Auswirkungen wirksam werden, ist es oft notwendig, sie lange vor dem Eintreten eines Ereignisses einzusetzen.

BEISPIEL 6 Die Festplattenverschlüsselung verhindert nicht, dass ein Laptop gestohlen wird oder dass später versucht wird, die Daten zu extrahieren. Sie mindert jedoch den Schweregrad der mit einer Offenlegung verbundenen Auswirkungen. Die Maßnahme muss natürlich durchgeführt werden, bevor der Laptop gestohlen wird.

Die Kategorisierung von Maßnahmen ist nicht absolut und hängt von dem Kontext ab, in dem die Verwendung einer Maßnahme beschrieben wird.

BEISPIEL 7 Die Datensicherung verhindert nicht das Eintreten eines Ereignisses, das andernfalls zu einem Datenverlust führen würde (z. B. ein Festplattencrash oder der Verlust eines Laptops), aber sie hilft, die Auswirkungen zu verringern. Manche Organisationen betrachten dies daher möglicherweise eher als korrektive Maßnahme denn als präventive Maßnahme. Ebenso verhindert die Verschlüsselung nicht den Verlust von Informationen, aber wenn das Ereignis als „personenbezogene Daten, die einem Angreifer offengelegt wurden“, beschrieben wird, dann ist die Verschlüsselung eher eine präventive als eine korrektive Maßnahme.

Die Reihenfolge, in der die Maßnahmen zur Behandlung der Risiken durchgeführt werden, hängt von verschiedenen Faktoren ab. Viele Techniken können verwendet werden. Es liegt in der Verantwortung der jeweiligen Risikoeigentümer, ein Gleichgewicht zwischen den Kosten für die Investition in Maßnahmen und den Auswirkungen im Falle des Eintretens der Risiken zu finden.

Bei der Identifizierung vorhandener Maßnahmen kann festgestellt werden, dass diese Maßnahmen den derzeitigen Bedarf übersteigen. Vor der Aufhebung redundanter oder unnötiger Maßnahmen sollte eine Kosten-Nutzen-Analyse durchgeführt werden (insbesondere wenn die Maßnahmen hohe Wartungskosten verursachen). Da sich Maßnahmen gegenseitig beeinflussen können, kann die Aufhebung redundanter Maßnahmen die Gesamtsicherheit verringern. Maßnahmen sollten nur dann in die Risikobehandlung einbezogen werden, wenn sie für die Handhabung eines oder mehrerer der identifizierten Informationssicherheitsrisiken erforderlich sind. Eine Maßnahme sollte eine Auswirkung auf die Auswirkungen oder die Wahrscheinlichkeit der identifizierten Informationssicherheitsrisiken haben. Maßnahmen sollten nicht in die Risikobehandlung einbezogen werden, wenn sie aus Gründen, die nicht mit der Informationssicherheit zusammenhängen, durchgeführt werden.

Es sollten auch Maßnahmen in Betracht gezogen werden, die zwar umgesetzt wurden, aber bekanntermaßen Schwachstellen aufweisen. Wenn die Beurteilung aller Risiken, die eine Maßnahme mit Schwachstellen handhabt, innerhalb der Akzeptanzkriterien liegt, ist es nicht notwendig, die Maßnahme zu verbessern. Auch wenn die Maßnahme nicht vollständig wirksam ist, ist es nicht immer notwendig, sie zu verbessern, um sie vollständig wirksam zu machen. Es sollte nicht davon ausgegangen werden, dass alle Maßnahmen in vollem Umfang funktionieren müssen, damit die Organisation ihre Risiken erfolgreich handhaben kann. Für jede einzelne Maßnahme kann eine Toleranzgrenze für ein Versagen festgelegt werden, bei deren Unterschreitung davon ausgegangen werden kann, dass die Maßnahme nicht wirksam genug ist, um die identifizierten Risiken zu handhaben. Solange die Maßnahme innerhalb der Toleranzgrenzen funktioniert, ist keine Verbesserung erforderlich.

8.4 Vergleich der festgelegten Maßnahmen mit denen in ISO/IEC 27001:2022, Anhang A

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 c).

Eingabe: Alle notwendigen Maßnahmen (siehe 8.3).

Aktion: Vergleich aller notwendigen Maßnahmen mit denen in ISO/IEC 27001:2022, Anhang A.

Auslöser: Die Identifizierung fehlender Maßnahmen wird erforderlich, wenn Pläne zur Risikobehandlung erstellt werden.

Ausgabe: Alle für die Risikobehandlung geltenden Maßnahmen.

Anleitung zur Umsetzung:

ISO/IEC 27001:2022, 6.1.3 c), verlangt von einer Organisation, dass sie die Maßnahmen, die sie zur Umsetzung der von ihr gewählten Risikobehandlungsoptionen für notwendig erachtet, mit den in ISO/IEC 27001:2022, Anhang A, aufgeführten Maßnahmen vergleicht. Dieser Schritt dient als Sicherheitsüberprüfung, um zu verifizieren, dass keine notwendigen Maßnahmen bei der Risikobeurteilung ausgelassen wurden. Diese Sicherheitsüberprüfung dient nicht dazu, in der Risikobeurteilung fehlende Maßnahmen nach ISO/IEC 27001:2022, Anhang A, zu identifizieren. Die Sicherheitsüberprüfung dient dazu, fehlende notwendige Maßnahmen aus beliebigen Quellen zu identifizieren, indem die Maßnahmen mit anderen Normen und Listen von Maßnahmen verglichen werden. Die bei dieser Überprüfung identifizierten unterlassenen Maßnahmen können branchenspezifische oder benutzerdefinierte Maßnahmen sein oder aus ISO/IEC 27001:2022, Anhang A, stammen. Die Leitlinien für die Festlegung von Maßnahmen in 8.3 sollten bei der Überlegung, ob fehlende Maßnahmen der Risikobeurteilung hinzugefügt werden sollten, beachtet werden.

BEISPIEL Es ist wichtig, dass eine bereits in der Organisation funktionierende Maßnahme nicht automatisch und ohne weitere Überlegung in die Risikobeurteilung aufgenommen wird.

Es ist wichtig, daran zu denken, dass dieser Vergleich der Maßnahmen anhand der Risikobeurteilung und nicht anhand der Erklärung zur Anwendbarkeit vorgenommen wird. Das Prinzip besteht darin, jedes Risiko der

Reihe nach zu betrachten und die für das jeweilige Risiko als notwendig erachteten Maßnahmen mit den Maßnahmen in ISO/IEC 27001:2022, Anhang A, zu vergleichen, um herauszufinden, ob notwendige Maßnahmen für die einzelnen Risiken fehlen.

8.5 Erstellung einer Erklärung zur Anwendbarkeit

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 d).

Eingabe: Alle für die Risikobehandlung geltenden Maßnahmen (siehe 8.4).

Aktion: Eine Erklärung zur Anwendbarkeit wird erstellt.

Auslöser: Dokumentation aller notwendigen Maßnahmen, ihrer Begründung und ihres Umsetzungsstatus.

Ausgabe: Erklärung zur Anwendbarkeit.

Anleitung zur Umsetzung:

In Übereinstimmung mit ISO/IEC 27001:2022, 6.1.3 d) sollte die Erklärung zur Anwendbarkeit (SOA, en: Statement of Applicability) mindestens Folgendes enthalten:

a) die notwendigen Maßnahmen;

b) Begründung für deren Aufnahme;

c) Angabe dazu, ob sie umgesetzt sind oder nicht;

d) Begründung für den Ausschluss von Maßnahmen aus ISO/IEC 27001:2022, Anhang A.

Die SOA kann leicht erstellt werden durch eine Untersuchung der Risikobeurteilung, um notwendige Maßnahmen zu identifizieren, und durch eine Untersuchung des Risikobehandlungsplans zur Identifikation der Maßnahmen, deren Umsetzung geplant ist. Nur die in der Risikobeurteilung identifizierten Maßnahmen können in die SOA aufgenommen werden. Unabhängig von der Risikobeurteilung können der SOA keine Maßnahmen hinzugefügt werden. Es sollte Konsistenz zwischen den Maßnahmen, die zur Realisierung ausgewählter Risikobehandlungsoptionen notwendig sind, und der SOA bestehen. In der SOA kann angegeben werden, dass die Begründung für die Aufnahme einer Maßnahme für alle Maßnahmen gleich ist und dass sie in der Risikobeurteilung als notwendig erachtet wurden, um ein oder mehrere Risiken so zu behandeln, dass sie ein akzeptables Niveau aufweisen. Eine weitere Begründung für die Aufnahme einer Maßnahme ist für keine der Maßnahmen erforderlich. Der Umsetzungsstatus aller in der SOA enthaltenen Maßnahmen kann als „umgesetzt“, „teilweise umgesetzt“ oder „nicht umgesetzt“ angegeben werden. Dies kann entweder für jede einzelne Maßnahme oder als Gesamterklärung geschehen.

BEISPIEL Die SOA enthält die Erklärung: „Alle Maßnahme wurden umgesetzt.“ Zur Vervollständigung der SOA sind keine zusätzlichen Analysen oder Informationen erforderlich.

8.6 Behandlungsplan für Informationssicherheitsrisiken

8.6.1 Ausarbeitung des Risikobehandlungsplans

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 e).

Eingabe: Ergebnisse aus Risikobeurteilungen.

Aktion: Ein Risikobehandlungsplan wird erstellt.

Auslöser: Die Erfordernis der Organisation, Risiken zu behandeln.

Ausgabe: Risikobehandlungsplan.

Anleitung zur Umsetzung:

Der Zweck dieser Aufgabe ist die Erstellung eines Plans bzw. von Plänen für die Behandlung spezifischer Risikogruppen, die auf der Liste der prioritären Risiken stehen (siehe Abschnitt 7). Ein Risikobehandlungsplan dient dazu, Risiken so zu verändern, dass sie den Risikoakzeptanzkriterien einer Organisation entsprechen (siehe 6.4.2). Es gibt zwei mögliche Auslegungen des Begriffs „Plan" im Zusammenhang mit der Risikobehandlung. Bei der ersten handelt es sich um einen Projektplan, d. h. ein Plan zur Umsetzung der notwendigen Maßnahmen in der Organisation. Bei der zweiten handelt es sich um einen Gestaltungsplan, d. h. der Plan, der nicht nur die notwendigen Maßnahmen identifiziert, sondern auch beschreibt, wie die Maßnahmen mit ihrer Umgebung und untereinander interagieren, um Risiken zu verändern. In der Praxis können beide verwendet werden.

Sobald die Maßnahmen umgesetzt sind, hat der Projektplan keinen Wert mehr, außer als Aufzeichnung des Verlaufs, während der Gestaltungsplan weiterhin nützlich ist.

Jedes Risiko, das einer Behandlung bedarf, sollte in einem der Risikobehandlungspläne behandelt werden. Eine Organisation kann sich für mehrere Risikobehandlungspläne entscheiden, die zusammen alle erforderlichen Aspekte der Risikobehandlung umsetzen. Diese können auf der Grundlage des Orts, an dem sich die Informationen befinden (z. B. ein Plan für das Rechenzentrum, ein anderer für die mobile Datenverarbeitung usw.), nach Werten (z. B. verschiedene Pläne für verschiedene Klassifizierungen von Werten) oder nach Ereignissen (wie bei der Risikobeurteilung nach dem ereignisbasierten Verfahren) organisiert werden.

Bei der Erstellung des Risikobehandlungsplans sollten Organisationen Folgendes berücksichtigen:

— Prioritäten im Verhältnis zum Risikoniveau und zur Dringlichkeit der Behandlung;

— ob verschiedene Arten von Maßnahmen (präventiv, detektiv, korrektiv) oder deren Zusammensetzung anwendbar sind;

— ob es notwendig ist, die Abwicklung einer Maßnahme abzuwarten, bevor mit der Umsetzung einer neuen Maßnahme für denselben Wert begonnen wird;

— ob es eine Verzögerung gibt zwischen dem Zeitpunkt, an dem die Maßnahme umgesetzt wird, und dem Zeitpunkt, an dem sie voll wirksam ist und funktioniert.

Für jedes behandelte Risiko sollte der Behandlungsplan die folgenden Angaben enthalten:

— Gründe für die Auswahl der Behandlungsoptionen einschließlich des erwarteten Nutzens;

— für die Genehmigung und Implementierung des Plans rechenschaftspflichtige und verantwortliche Kreise;

— vorgeschlagene Aktionen;

— erforderliche Ressourcen, einschließlich jener für Eventualitäten;

— Leistungskennzahlen;

— Beschränkungen;

— erforderliche Berichte und Überwachungen;

— wann Aktionen voraussichtlich ausgeführt und abgeschlossen werden;

— Umsetzungsstatus.

Die Maßnahmen des Risikobehandlungsplans sollten entsprechend dem Risikoniveau und der Dringlichkeit der Behandlung nach Priorität geordnet werden. Je höher das Risiko und in manchen Fällen auch die Häufigkeit des Auftretens des Risikos, desto eher muss die Maßnahme umgesetzt werden.

Für jedes im Risikobehandlungsplan aufgeführte Risiko sollten detaillierte Umsetzungsinformationen erfasst werden, die unter anderem Folgendes umfassen können:

— Namen der Risikoeigentümer und der für die Umsetzung verantwortlichen Personen;

— Termine oder Fristen für die Umsetzung;

— geplante Maßnahmen zur Überprüfung des Umsetzungsergebnisses;

— Umsetzungsstatus;

— Kostenniveau (Investition, Betrieb).

8.6.2 Zustimmung durch die Risikoeigentümer

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 f).

Eingabe: Risikobehandlungsplan/-pläne.

Aktion: Zustimmung der Risikoeigentümer zum Risikobehandlungsplan (bzw. den Risikobehandlungsplänen).

Auslöser: Das Erfordernis, einen oder mehrere Risikobehandlungspläne zu genehmigen.

Ausgabe: Genehmigte(r) Risikobehandlungsplan/-pläne.

Anleitung zur Umsetzung:

Der Behandlungsplan für Informationssicherheitsrisiken sollte von den Risikoeigentümern genehmigt werden, sobald er ausgearbeitet ist. Die Risikoeigentümer sollten auch über die Akzeptanz von Restrisiken der Informationssicherheit entscheiden. Diese Entscheidung sollte auf der Grundlage definierter Risikoakzeptanzkriterien getroffen werden.

Die Ergebnisse der Risikobeurteilung, der Risikobehandlungsplan und die verbleibenden Risiken sollten für die Risikoeigentümer verständlich sein, damit sie ihrer Verantwortung gerecht werden können.

8.6.3 Akzeptanz der Restrisiken für die Informationssicherheit

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 6.1.3 f).

Eingabe: Genehmigte(r) Risikobehandlungsplan/-pläne und Risikoakzeptanzkriterien.

Aktion: Es wird bestimmt, ob die Restrisiken akzeptabel sind.

Auslöser: Das Erfordernis für die Organisation, über die Beibehaltung von Restrisiken zu entscheiden.

Ausgabe: Akzeptierte Restrisiken.

Anleitung zur Umsetzung:

Um die Restrisiken zu bestimmen, sollten die Risikobehandlungspläne in die anschließende Beurteilung der Restwahrscheinlichkeit und der Auswirkungen einfließen. Die in den Risikobehandlungsplänen vorgeschlagenen Maßnahmen und ihre Wirksamkeit sollten unter dem Gesichtspunkt betrachtet werden, ob sie die Wahrscheinlichkeit oder die Auswirkungen oder beides verringern und ob das Niveau der Restrisiken den Risiken zugeordnet ist. Das Niveau der Restrisiken wird dann vom Risikoeigentümer geprüft, um festzustellen, ob die Restrisiken akzeptabel sind.

In den Risikobehandlungsplänen sollte beschrieben werden, wie die beurteilten Risiken behandelt werden sollen, um die Risikoakzeptanzkriterien zu erfüllen.

In einigen Fällen entspricht das Niveau des Restrisikos nicht immer den Kriterien für die Risikoakzeptanz, da die angewandten Kriterien nicht die aktuellen Umstände berücksichtigen.

BEISPIEL Es kann argumentiert werden, dass es notwendig ist, Risiken beizubehalten, weil der mit den Risiken verbundene Nutzen eine wichtige Geschäftsmöglichkeit darstellt oder weil die Kosten für eine Risikoveränderung zu hoch sind.

Es ist jedoch nicht immer möglich, die Risikoakzeptanzkriterien rechtzeitig zu überarbeiten. In solchen Fällen können die Risikoeigentümer Risiken beibehalten, die die üblichen Akzeptanzkriterien nicht erfüllen. Wenn dies notwendig ist, sollte der Risikoeigentümer ausdrücklich zu den Risiken Stellung nehmen und eine Begründung für die Entscheidung liefern, die üblichen Risikoakzeptanzkriterien außer Kraft zu setzen.

Die Risikoakzeptanz kann einen Prozess beinhalten, mit dem sich vor der endgültigen Entscheidung über die Risikoakzeptanz die Befürwortung von Behandlungen erreichen lässt. Es ist wichtig, dass die Risikoeigentümer die vorgeschlagenen Risikobehandlungspläne und die sich daraus ergebenden Restrisiken überprüfen und genehmigen und alle mit einer solchen Genehmigung verbundenen Bedingungen notieren. Je nach Risikobeurteilungsprozess und Risikoakzeptanzkriterien kann dies erfordern, dass eine Führungskraft mit mehr Befugnis als der Risikoeigentümer der Risikoakzeptanz zustimmt.

Es kann einige Zeit dauern, bis ein Plan zur Behandlung beurteilter Risiken umgesetzt ist. Risikokriterien können zulassen, dass das Risikoniveau einen gewünschten Schwellenwert bis zu einem bestimmten Grad überschreitet, wenn ein Plan zur Verringerung des Risikos innerhalb einer akzeptablen Zeitspanne vorhanden ist. Bei Entscheidungen über die Risikoakzeptanz können die in den Risikobehandlungsplänen vorgesehenen Fristen und die Frage berücksichtigt werden, ob der Fortschritt bei der Umsetzung der Risikobehandlung den Planungen entspricht oder nicht.

Manche Risiken können sich im Lauf der Zeit verändern (unabhängig davon, ob diese Veränderung auf die Umsetzung eines Risikobehandlungsplans zurückzuführen ist). Risikoakzeptanzkriterien können dies berücksichtigen und Risikoakzeptanzschwellen aufweisen, die von der Zeitdauer abhängen, während der eine Organisation einem beurteilten Risiko ausgesetzt sein kann.

9 Betrieb

9.1 Durchführung des Prozesses zur Risikobeurteilung der Informationssicherheit

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 8.2.

Eingabe: Dokumente über den Prozess zur Risikobeurteilung der Informationssicherheit einschließlich der Risikobeurteilung und der Risikoakzeptanzkriterien.

Aktion: Der Prozess zur Risikobeurteilung sollte in Übereinstimmung mit Abschnitt 7 durchgeführt werden.

Auslöser: Das Erfordernis der Organisation, Risiken in geplanten Intervallen oder aufgrund von Ereignissen zu beurteilen.

Ausgabe: Bewertete Risiken.

Anleitung zur Umsetzung:

Der in ISO/IEC 27001:2022, 6.1 definierte und angewendete Prozess zur Informationssicherheitsrisikobeurteilung sollte in die Betriebsabläufe der Organisation integriert werden und in geplanten Zeitabständen bzw. dann durchgeführt werden, wenn wesentliche Änderungen vorgesehen sind oder eintreten. Beim Prozess der Risikobeurteilung der Informationssicherheit sollten die in ISO/IEC 27001:2022, 6.1.2 a) festgelegten Kriterien berücksichtigt werden. Die Zeitabstände, in denen die Risikobeurteilung durchgeführt wird, sollten für das ISMS geeignet sein. Wenn eine wesentliche Änderung des ISMS (oder seines Kontexts) bzw. eine Änderung in der Bedrohungslandschaft (z. B. eine neue Art von Informationssicherheitsangriff) eingetreten ist, sollte die Organisation bestimmen, ob diese Änderung eine zusätzliche Beurteilung des Informationssicherheitsrisikos erfordert.

Bei der Planung von routinemäßigen Risikobeurteilungen sollten Organisationen alle Zeitpläne berücksichtigen, die für ihre allgemeinen Geschäftsprozesse und die damit verbundenen Budgetzyklen gelten.

BEISPIEL Wenn es einen jährlichen Budgetzyklus gibt, kann von der Organisation verlangt werden, dass sie zu einem bestimmten Zeitpunkt des Jahres Finanzierungsanträge stellt. Die Mittel werden dann später gewährt (gekürzt oder verweigert).

Wenn die Beschaffungsprozesse betroffen sind, kann es einen weiteren Budgetzyklus geben, bevor Empfehlungen zur Risikobehandlung umgesetzt und ihre Wirksamkeit vor der nächsten routinemäßigen Risikobeurteilung beurteilt werden können. In solchen Fällen sollten Risikobeurteilungen eingeplant werden:

a) um ihre Empfehlungen zur Risikobehandlung rechtzeitig für die Beantragung der Mittel abzugeben;

b) um nach den Ergebnissen der Budgetzuweisungen neu beurteilt zu werden;

c) um die nächste routinemäßige Beurteilung nach jeder Beschaffungsmaßnahme durchzuführen, sobald die Empfehlungen umgesetzt wurden.

9.2 Durchführung des Prozesses zur Risikobehandlung der Informationssicherheit

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 8.3.

Eingabe: Bewertetes Risiko bzw. bewertete Risiken.

Aktion: Der Prozess der Risikobehandlung sollte in Übereinstimmung mit Abschnitt 8 durchgeführt werden.

Auslöser: Das Erfordernis der Organisation, Risiken in geplanten Intervallen oder aufgrund von Ereignissen zu behandeln.

Ausgabe: Beibehaltene oder akzeptierte Restrisiken.

Anleitung zur Umsetzung:

ISO/IEC 27001:2022, 8.3 legt die Anforderungen an Organisationen zur Umsetzung ihrer Risikobehandlungspläne fest. Die in 8.6 enthaltenen Überlegungen sind auch für diesen Unterabschnitt maßgeblich.

10 Unterstützung verbundener ISMS-Prozesse

10.1 Kontext der Organisation

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, Abschnitt 4.

Eingabe: Informationen über die Organisation, ihren internen und externen Kontext.

Aktion: Alle maßgeblichen Daten sollten berücksichtigt werden, um interne und externe Aspekte zu identifizieren und zu beschreiben, die das Risikomanagement der Informationssicherheit und die Anforderungen der interessierten Parteien beeinflussen.

Auslöser: ISO/IEC 27001:2022 legt die Anforderungen an solche Informationen fest, um Informationssicherheitsziele festlegen zu können.

Ausgabe: Risikobezogene interne und externe Aspekte, die das Risikomanagement der Informationssicherheit beeinflussen.

Anleitung zur Umsetzung:

Die Organisation sollte ein übergeordnetes (z. B. strategisches) Verständnis der wichtigen Themen haben, die das ISMS positiv oder negativ beeinflussen können. Darüber hinaus sollte sie den internen und externen Kontext kennen, der für ihren Zweck maßgeblich ist und der ihre Fähigkeit beeinflusst, die beabsichtigten Ergebnisse ihres ISMS zu erreichen. Mit den angestrebten Ergebnissen sollten die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sichergestellt sein unter Anwendung des Risikomanagementprozesses und der Kenntnis darüber, welche Risiken angemessen gehandhabt werden.

Um Risiken zuverlässig identifizieren zu können, sollte die Organisation die Umstände, unter denen sie tätig ist, in ausreichendem Maß verstehen. Das bedeutet, dass die Organisation Informationen über den internen und externen Kontext der Organisation, ihre interessierten Parteien und deren Anforderungen sammeln sollte (siehe ISO/IEC 27001:2022, 4.1 und 4.2). Das Sammeln dieser Informationen sollte erfolgen, bevor die Organisation versucht, ihre Informationssicherheitsrisiken oder andere Risiken, die das beabsichtigte Ergebnis des ISMS beeinflussen können, zu beurteilen (siehe ISO/IEC 27001:2022, 6.1.1).

Die Organisation sollte alle internen und externen Risikoquellen berücksichtigen. Das Verständnis der Organisation für interessierte Parteien, die der Organisation entgegenstehen, und deren Interessen, ist von großer Bedeutung.

BEISPIEL 1 Ein Beispiel für eine interessierte Partei mit Interessen, die den Zielen der Organisation entgegenstehen, ist der Angreifer. Der Angreifer wünscht sich eine Organisation mit schwacher Sicherheitsstufe. Die Organisation trägt dem Interesse dieser Partei Rechnung, indem sie das Gegenteil (eine starke Sicherheitsstufe) hat, d. h. die Organisation berücksichtigt mögliche Konflikte mit den Zielen des ISMS. Die Organisation stellt durch wirksame Maßnahmen der Informationssicherheit sicher, dass diese Interessen nicht erfüllt werden.

Schnittstellen zu Diensten oder Aufgaben, die nicht vollständig in den Anwendungsbereich des ISMS fallen, sollten bei der Risikobeurteilung der Organisation zur Informationssicherheit berücksichtigt werden.

BEISPIEL 2 Ein Beispiel für eine solche Situation ist das gemeinsame Nutzen von Werten (z. B. Anlagen, IT-Systemen und Datenbanken) mit anderen Organisationen oder die Ausgliederung einer Geschäftsfunktion.

Wie andere maßgebliche Faktoren, die sich auf die Informationssicherheit auswirken, berücksichtigt werden, hängt von der Wahl der Risikoidentifizierung und der Analyseverfahren durch die Organisation ab.

Die Informationssicherheitsziele der Organisation (siehe ISO/IEC 27001:2022, 6.2) können die Kriterien für die Risikoakzeptanz einschränken (z. B. kann das akzeptable Risikoniveau von den potentiellen Belohnungen abhängen, die mit verschiedenen Geschäftsaktivitäten verbunden sind). Darüber hinaus kann die Informationssicherheitspolitik die Risikobehandlung einschränken (z. B. können bestimmte Risikobehandlungsoptionen durch diese Politik ausgeschlossen werden).

10.2 Führung und Verpflichtung

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 5.1.

Eingabe: Informationen über Ergebnisse der Risikobeurteilung zur Informationssicherheit oder Ergebnisse der Risikobehandlung zur Informationssicherheit, die eine Genehmigung oder eine Bestätigung erfordern.

Aktion: Die Ergebnisse in Bezug auf die Informationssicherheitsrisiken sollten von der zuständigen Managementebene geprüft werden, um über weitere Maßnahmen zu entscheiden oder diese zu unterstützen.

Auslöser: ISO/IEC 27001 verlangt, dass eine zuständige Managementebene in alle Aktivitäten im Zusammenhang mit Informationssicherheitsrisiken einbezogen wird.

Ausgabe: Entscheidungen oder Befürwortung im Zusammenhang mit Informationssicherheitsrisiken.

Anleitung zur Umsetzung:

Die oberste Führungsebene ist für das Risikomanagement verantwortlich und sollte die Risikobeurteilungen leiten und vorantreiben. Dazu gehören die folgenden Aufgaben:

— Sicherstellen, dass für das Umgehen mit Risiken die erforderlichen Ressourcen bereitgestellt werden;

— Zuweisen von Befugnis, Verantwortlichkeit und Rechenschaftspflicht auf geeigneten Ebenen in der Organisation in Bezug auf das Risikomanagement;

— Kommunizieren mit den entsprechenden interessierten Parteien.

10.3 Kommunikation und Konsultation

ANMERKUNG 1 Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 7.4.

ANMERKUNG 2 ISO/IEC 27001 bezieht sich direkt auf den Kommunikationsteil dieser Tätigkeit.

Eingabe: Informationen über die im Rahmen des Risikomanagementprozesses identifizierten Risiken, ihre Ursachen, Auswirkungen und ihre Eintrittswahrscheinlichkeit.

Aktion: Informationen über Risiken, ihre Ursachen, Auswirkungen, ihre Wahrscheinlichkeit und die zu ihrer Behandlung ergriffenen Maßnahmen sollten den externen und internen interessierten Parteien mitgeteilt bzw. von diesen eingeholt werden.

Auslöser: ISO/IEC 27001 verlangt eine solche Kommunikation.

Ausgabe: Die Wahrnehmung und das kontinuierliche Verständnis der maßgeblichen interessierten Parteien für den Prozess und die Ergebnisse des Informationssicherheitsrisikomanagements der Organisation.

Anleitung zur Umsetzung:

Die Kommunikations- und Konsultationstätigkeit zielt darauf ab, eine Einigung über das Risikomanagement zu erzielen, indem Informationen über Risiken mit den Risikoeigentümern und anderen maßgeblichen interessierten Parteien ausgetauscht und/oder geteilt werden. Die Informationen umfassen unter anderem die Existenz, die Beschaffenheit, die Gestalt, die Wahrscheinlichkeit, die Auswirkungen, die Bedeutung, die Behandlung und die Akzeptanz von Risiken.

ISO/IEC 27001:2022, 6.1.2 c) 2) verlangt, dass Eigentümer der Informationssicherheitsrisiken identifiziert werden. Die Risikoeigentümerschaft kann absichtlich verwechselt oder verheimlicht werden. Selbst wenn Risikoeigentümer identifiziert werden können, zögern sie mitunter, ihre Verantwortung für die Risiken anzuerkennen, und es kann schwierig sein, sie zur Teilnahme am Risikomanagementprozess zu bewegen. Es sollte ein festgelegtes Kommunikationsverfahren geben, um die Betroffenen über die Risikoeigentümerschaft zu informieren.

ISO/IEC 27001:2022, 6.1.3 f), verlangt, dass die Risikoeigentümer den Risikobehandlungsplan bzw. die Risikobehandlungspläne genehmigen und über die Akzeptanz von Restrisiken entscheiden. Die Kommunikation zwischen den Risikoeigentümern und den für die Umsetzung des ISMS zuständigen Mitarbeitern ist eine wichtige Aufgabe. Es sollte eine Einigung darüber erzielt werden, wie Informationen über Risiken mit den Risikoeigentümern und ggf. anderen interessierten Parteien und Entscheidungsträgern ausgetauscht und/oder geteilt werden. Die Informationen umfassen unter anderem die Existenz, die Beschaffenheit, die Gestalt, die Wahrscheinlichkeit, die Bedeutung, die Behandlung und die Akzeptanz von Risiken. Die Kommunikation sollte bidirektional sein.

Je nach Beschaffenheit und Sensibilität des Risikos bzw. der Risiken kann es erforderlich sein, bestimmte Informationen über Risiken, ihre Beurteilung und Behandlung nach dem Grundsatz „Kenntnis nur, wenn nötig“ auf diejenigen zu beschränken, die für die Identifizierung, Beurteilung und Behandlung der Risiken verantwortlich

sind. Die Risikokommunikation sollte in Absprache mit den Risikoeigentümern oder potentiellen Risikoeigentümern nach dem Grundsatz „Kenntnis nur, wenn nötig“ gesteuert werden, wobei der von den verschiedenen interessierten Parteien geforderte Detaillierungsgrad zu berücksichtigen ist, mit dem Ziel, die Veröffentlichung der sensibleren Risiken und der damit verbundenen bekannten Schwachstellen zu vermeiden.

Die Risikowahrnehmung kann aufgrund unterschiedlicher Annahmen, Konzepte, Erfordernisse, Probleme und Bedenken der jeweiligen interessierten Parteien in Bezug auf das Risiko oder die zur Diskussion stehenden Themen variieren. Interessierte Parteien werden wahrscheinlich auf der Grundlage ihrer Risikowahrnehmung über die Akzeptanz von Risiken entscheiden. Dies ist besonders wichtig, damit sichergestellt werden kann, dass die Risikowahrnehmung der interessierten Parteien ebenso wie ihre Nutzenwahrnehmung identifiziert und dokumentiert werden können und die zugrunde liegenden Gründe klar verstanden und angesprochen werden.

Kommunikation und Konsultation in Bezug auf Risiken können dazu führen, dass sich interessierte Parteien besser in das Geschehen einbringen und sich Entscheidungen und Ergebnisse zu eigen machen. Die Kommunikation mit interessierten Parteien und deren Konsultation bei der Entwicklung von Kriterien und der Auswahl von Verfahren für die Risikobeurteilung kann auch dazu beitragen, dass sich die interessierten Parteien die Ergebnisse besser zu eigen machen. Es ist weniger wahrscheinlich, dass interessierte Parteien die Ergebnisse von Prozessen in Frage stellen, die sie mitgestaltet haben. Infolgedessen ist die Wahrscheinlichkeit, dass sie Ergebnisse akzeptieren und Aktionspläne unterstützen, oft größer. Handelt es sich bei den interessierten Parteien um Führungskräfte, kann dies das Engagement für das Erreichen der Risikomanagementziele und die Bereitstellung der erforderlichen Ressourcen fördern.

Die Risikokommunikation sollte durchgeführt werden, um:

— die Vertrauenswürdigkeit im Hinblick auf das Ergebnis des Risikomanagement der Organisation herzustellen;

— Risikoinformationen zu sammeln;

— die Ergebnisse der Risikobeurteilung auszutauschen und den Risikobehandlungsplan vorzulegen;

— sowohl das Auftreten als auch die Auswirkungen von Verstößen gegen die Informationssicherheit infolge eines Mangels an gegenseitigem Verständnis zwischen den Risikoeigentümern und interessierten Parteien zu vermeiden oder deren Häufigkeit zu verringern;

— die Risikoeigentümer zu unterstützen;

— sich neues Wissen über die Informationssicherheit anzueignen;

— sich mit anderen Parteien zu koordinieren und Reaktionen zu planen, um die Auswirkungen eines Vorfalls zu verringern;

— den Risikoeigentümern und anderen Parteien, die ein berechtigtes Interesse am Risiko haben, ein Gefühl der Verantwortung zu vermitteln;

— das Bewusstsein zu verbessern.

Eine Organisation sollte Pläne zur Risikokommunikation sowohl für den Normalbetrieb als auch für Notfälle entwickeln. Die Risikokommunikation und -beratung sollten kontinuierlich erfolgen.

Die Koordinierung zwischen den Hauptrisikoeigentümern und den maßgeblichen interessierten Parteien kann durch die Bildung eines Ausschusses erreicht werden, in dem die Diskussion über Risiken, ihre Priorisierung und angemessene Behandlung sowie ihre Akzeptanz stattfinden kann.

Risikomitteilungen können freiwillig an externe Dritte weitergeleitet werden, um ein besseres Risikomanagement oder eine bessere Koordinierung von Reaktionen oder eine bessere Sensibilisierung zu ermöglichen und können unter bestimmten Umständen auch von Aufsichtsbehörden oder Geschäftspartnern verlangt werden.

Es ist wichtig, mit der zuständigen Abteilung für Öffentlichkeitsarbeit oder Kommunikation innerhalb der Organisation zusammenzuarbeiten, um alle Aufgaben im Zusammenhang mit der Risikokommunikation zu koordinieren. Dies ist von entscheidender Bedeutung, wenn die Krisenkommunikation aktiviert wird, z. B. als Reaktion auf bestimmte Vorfälle.

10.4 Dokumentierte Informationen

10.4.1 Allgemeines

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 7.5.

ISO/IEC 27001 legt fest, dass Organisationen dokumentierte Informationen über den Prozess der Risikobeurteilung (siehe ISO/IEC 27001:2022, 6.1.2) und die Ergebnisse (siehe ISO/IEC 27001:2022, 8.2) sowie den Prozess der Risikobehandlung (ISO/IEC 27001:2022, 6.1.3) und die Ergebnisse (ISO/IEC 27001:2022, 8.3) aufbewahren müssen.

10.4.2 Dokumentierte Informationen über Prozesse

Eingabe: Wissen über die Prozesse zur Beurteilung und Behandlung von Informationssicherheitsrisiken in Übereinstimmung mit Abschnitt 7 und Abschnitt 8, die von der Organisation festgelegt wurden.

Aktion: Informationen über die Risikobeurteilung für die Informationssicherheit und die Behandlungsprozesse sollten dokumentiert und aufbewahrt werden.

Auslöser: ISO/IEC 27001 verlangt dokumentierte Informationen über die Prozesse zur Beurteilung und Behandlung von Informationssicherheitsrisiken.

Ausgabe: Dokumentierte Informationen, die von interessierten Parteien (z. B. Zertifizierungsstelle) verlangt werden oder von der Organisation als notwendig für die Effektivität des Prozesses zur Beurteilung von Informationssicherheitsrisiken oder des Prozesses zur Behandlung von Informationssicherheitsrisiken erachtet werden.

Anleitung zur Umsetzung:

Dokumentierte Informationen über den Prozess der Risikobeurteilung zur Informationssicherheit sollten Folgendes enthalten:

a) eine Definition der Risikokriterien (einschließlich der Risikoakzeptanzkriterien und der Kriterien für die Durchführung von Risikobeurteilungen zur Informationssicherheit);

b) eine Begründung für die Konsistenz, Gültigkeit und Vergleichbarkeit von Ergebnissen;

c) eine Beschreibung des Risikoidentifizierungsverfahrens (einschließlich der Identifizierung von Risikoeigentümern);

d) eine Beschreibung des Verfahrens zur Analyse der Informationssicherheitsrisiken (einschließlich der Beurteilung möglicher Auswirkungen, der realistischen Wahrscheinlichkeit und des resultierenden Risikoniveaus);

e) eine Beschreibung des Verfahrens zum Vergleichen der Ergebnisse mit den Risikokriterien und der Priorisierung von Risiken zur Risikobehandlung.

Dokumentierte Informationen über den Prozess der Risikobehandlung zur Informationssicherheit sollten folgende Beschreibungen enthalten:

— das Verfahren zur Auswahl geeigneter Optionen zur Informationssicherheitsrisikobehandlung;

— das Verfahren zur Festlegung notwendiger Maßnahmen;

— die Art und Weise, in der ISO/IEC 27001:2022, Anhang A, verwendet wird, um festzustellen, dass notwendige Maßnahmen nicht versehentlich übersehen wurden;

— die Art und Weise, wie Risikobehandlungspläne erstellt werden;

— die Art und Weise, in der die Genehmigung der Risikoeigentümer eingeholt wird.

10.4.3 Dokumentierte Informationen über Ergebnisse

Eingabe: Die Ergebnisse der Risikobeurteilung und -behandlung für die Informationssicherheit.

Aktion: Informationen über die Risikobeurteilung für die Informationssicherheit und die Behandlungsergebnisse sollten dokumentiert und aufbewahrt werden.

Auslöser: ISO/IEC 27001 verlangt dokumentierte Informationen über die Ergebnisse der Beurteilung und Behandlung von Informationssicherheitsrisiken.

Ausgabe: Dokumentierte Informationen über die Ergebnisse der Risikobeurteilung und -behandlung zur Informationssicherheit.

Anleitung zur Umsetzung:

Da Organisationen Risikobeurteilungen in geplanten Intervallen durchführen müssen oder immer dann, wenn erhebliche Änderungen vorgeschlagen werden oder auftreten, sollte zumindest ein Zeitplan vorhanden sein, und die Risikobeurteilungen sollten in Übereinstimmung mit diesem Zeitplan durchgeführt werden. Wenn eine Änderung vorgeschlagen wird oder eingetreten ist, sollte ein Nachweis über die Durchführung einer zugehörigen Risikobeurteilung erbracht werden. Andernfalls sollte die Organisation erklären, warum die Änderung erheblich ist oder nicht.

Dokumentierte Informationen über die Ergebnisse der Risikobeurteilung zur Informationssicherheit sollten Folgendes enthalten:

a) die identifizierten Risiken, ihre Auswirkungen und die Wahrscheinlichkeit dafür, dass sie eintreten;

b) die Identität des Risikoeigentümers/der Risikoeigentümer;

c) die Ergebnisse der Anwendung der Risikoakzeptanzkriterien;

d) die Priorität bei der Risikobehandlung.

Es wird auch empfohlen, die Begründung für Risikoentscheidungen zu notieren, um aus Fehlern im Einzelfall zu lernen und kontinuierliche Verbesserungen zu ermöglichen.

Dokumentierte Informationen über die Ergebnisse der Risikobehandlung für die Informationssicherheit sollten Folgendes enthalten:

— Identifizierung der notwendigen Maßnahmen;

— sofern angemessen und verfügbar den Nachweis, dass diese notwendigen Maßnahmen Risiken so verändern, dass die Risikoakzeptanzkriterien der Organisation erfüllt sind.

10.5 Überwachen und Überprüfen

10.5.1 Allgemeines

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 9.1.

Der Überwachungsprozess der Organisation (siehe ISO/IEC 27001:2022, 9.1) sollte alle Aspekte des Prozesses der Risikobeurteilung und Risikobehandlung zu folgenden Zwecken umfassen:

a) Sicherstellung, dass die Risikobehandlungen sowohl in der Gestaltung als auch im Betrieb wirksam, effizient und wirtschaftlich sind;

b) Beschaffung von Informationen zur Verbesserung künftiger Risikobeurteilungen;

c) Analyse von Vorfällen (einschließlich Beinaheunfällen), Veränderungen, Trends, Erfolgen und Fällen von Versagen und daraus gezogene Lehren;

d) Erkennung von Veränderungen im internen und externen Kontext einschließlich Änderungen der Risikokriterien und der Risiken selbst, die eine Überarbeitung der Risikobehandlungen und der Prioritäten erfordern können;

e) Identifizierung aufkommender Risiken.

Die aus dem Risikomanagement stammenden beibehaltenen Risikoszenarien können in Überwachungsszenarien umgewandelt werden, um einen wirksamen Überwachungsprozess sicherzustellen. Weitere Einzelheiten zu den Überwachungsszenarien sind in A.2.7 angegeben.

10.5.2 Überwachung und Überprüfung der die Risiken beeinflussenden Faktoren

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 9.1.

Eingabe: Alle im Rahmen des Risikomanagements erlangten Risikoinformationen.

Aktion: Die Risiken und ihre Faktoren (d. h. Wert der Werte, Auswirkungen, Bedrohungen, Schwachstellen, Eintrittswahrscheinlichkeit) sollten überwacht und überprüft werden, um etwaige Veränderungen im Kontext der Organisation frühzeitig zu identifizieren und den Überblick über das Gesamtbild der Risiken zu behalten.

Auslöser: Überprüfung der Organisationsrichtlinien und Erkennung von Änderungen in der aktuellen Betriebs- oder Bedrohungsumgebung.

Ausgabe: Kontinuierliche Ausrichtung des Risikomanagements an den Geschäftszielen der Organisation und an den Risikoakzeptanzkriterien.

Anleitung zur Umsetzung:

ISO/IEC 27001:2022, 9.1, verlangt von Organisationen, dass sie die Leistungsfähigkeit ihrer Informationssicherheit (und die Wirksamkeit des ISMS) bewerten. In Übereinstimmung mit dieser Anforderung sollten die Organisationen ihren Risikobehandlungsplan (bzw. ihre Risikobehandlungspläne) als Gegenstand der Bewertungen ihrer Leistungsfähigkeit verwenden. Zu diesem Zweck sollte eine Organisation zunächst ein oder mehrere Informationserfordernisse definieren, z. B., um zu beschreiben, was die oberste Führungsebene über die Fähigkeit der Organisation, sich gegen Bedrohungen zu verteidigen, wissen möchte. Anhand dieser Spezifikation auf oberster Ebene sollte eine Organisation dann die Messungen bestimmen, die sie durchführen muss, und wie diese Messungen kombiniert werden sollten, um den Informationsbedarf zu decken.

Risiken sind nicht statisch. Ereignisszenarien, Beträge von Werten, Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen können sich abrupt und ohne Anzeichen ändern. Um diese Veränderungen zu erkennen, sollte eine ständige Überwachung durchgeführt werden. Dies kann durch externe Dienste unter-

stützt werden, die Informationen über neue Bedrohungen oder Schwachstellen liefern. Die Organisationen sollten die kontinuierliche Überwachung maßgeblicher Faktoren sicherstellen, z. B.:

a) neue Risikoquellen einschließlich neu gemeldeter Schwachstellen in der IT;

b) neue Werte, die in den Anwendungsbereich des Risikomanagements aufgenommen wurden;

c) notwendige Änderung der Beträge von Werten (z. B. aufgrund geänderter Geschäftsanforderungen);

d) identifizierte Schwachstellen, um diejenigen zu ermitteln, die neuen oder wiederauftauchenden Bedrohungen ausgesetzt sind;

e) Veränderungen in den Nutzungsmustern bestehender oder neuer Technologien, die neue Angriffsmöglichkeiten eröffnen können;

f) Änderungen von Gesetzen und Vorschriften;

g) Veränderungen in der Risikobereitschaft und in der Wahrnehmung dessen, was jetzt akzeptabel ist und was nicht mehr akzeptabel ist;

h) Vorfälle im Bereich der Informationssicherheit, sowohl innerhalb als auch außerhalb der Organisation.

Neue Risikoquellen oder veränderte Wahrscheinlichkeiten bzw. Auswirkungen können zuvor beurteilte Risiken erhöhen. Bei der Überprüfung von geringen und beibehaltenen Risiken sollte jedes Risiko einzeln und sollten alle diese Risiken zusammen untersucht werden, um ihre potentiellen kumulierten Auswirkungen zu beurteilen. Wenn Risiken nicht mehr in die Kategorie „geringes oder akzeptables Risiko“ fallen, sollten sie mit einer oder mehreren der unter 8.2 genannten Optionen behandelt werden.

Faktoren, die die Wahrscheinlichkeit des Auftretens von Ereignissen und die entsprechenden Auswirkungen beeinflussen, können sich ebenso ändern wie Faktoren, die die Eignung oder die Kosten der verschiedenen Behandlungsmöglichkeiten beeinflussen. Größere Veränderungen, die sich auf die Organisation auswirken, sollten ein Grund für eine genauere Überprüfung sein. Die Risikoüberwachung sollte regelmäßig wiederholt werden, und die ausgewählten Optionen für die Risikobehandlung sollten in regelmäßigen Abständen überprüft werden.

Neue Bedrohungen, Schwachstellen oder veränderte Wahrscheinlichkeiten bzw. Auswirkungen können zuvor als gering beurteilte Risiken erhöhen. Bei der Überprüfung von geringen und beibehaltenen Risiken sollte jedes Risiko einzeln und sollten alle diese Risiken zusammen betrachtet werden, um ihre potentiellen kumulierten Auswirkungen zu beurteilen. Wenn Risiken nicht in die Kategorie „geringes oder akzeptables Risiko“ fallen, sollten sie mit einer oder mehreren der in Abschnitt 8 genannten Optionen behandelt werden.

Faktoren, die die Wahrscheinlichkeit des Auftretens von Bedrohungen und die entsprechenden Auswirkungen beeinflussen, können sich ebenso ändern wie Faktoren, die die Eignung oder die Kosten der verschiedenen Behandlungsmöglichkeiten beeinflussen. Größere Veränderungen, die sich auf die Organisation auswirken, sollten Anlass für eine genauere Überprüfung sein. Die Risikoüberwachung sollte regelmäßig wiederholt werden, und die ausgewählten Optionen für die Risikobehandlung sollten in regelmäßigen Abständen überprüft werden.

Die Ergebnisse der Risikoüberwachung können in andere Risikoüberprüfungen einbezogen werden. Die Organisation sollte alle Risiken regelmäßig und, wenn größere Änderungen vorgeschlagen werden oder eintreten, nach ISO/IEC 27001:2022, Abschnitt 8, überprüfen.

10.6 Managementbewertung

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 9.3.

Eingabe: Ergebnisse der Beurteilung(en) von Informationssicherheitsrisiken, Status des Plans zur Behandlung von Informationssicherheitsrisiken.

Aktion: Die Ergebnisse der Beurteilung von Informationssicherheitsrisiken und der Status des Plans zur Behandlung von Informationssicherheitsrisiken sollten überprüft werden, um zu bestätigen, dass die Restrisiken die Kriterien für die Risikoakzeptanz erfüllen und dass der Plan zur Risikobehandlung alle maßgeblichen Risiken und ihre Behandlungsoptionen berücksichtigt.

Auslöser: Ein Teil des Zeitplans für die Überprüfungsmaßnahmen.

Ausgabe: Änderungen der Risikoakzeptanzkriterien und der Kriterien für die Durchführung von Risikobeurteilungen für die Informationssicherheit, aktualisierter Plan zur Behandlung von Informationssicherheitsrisiken oder SOA.

10.7 Korrekturmaßnahme

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 10.1.

Eingabe: Der Risikobehandlungsplan erweist sich als unwirksam, d. h. das Restrisiko bleibt auch nach Abschluss des Behandlungsplans auf einem inakzeptablen Niveau.

Aktion: Der Risikobehandlungsplan wird überarbeitet und umgesetzt, um das Restrisiko auf ein akzeptables Niveau zu reduzieren.

Auslöser: Die Entscheidung über die Überarbeitung des Risikobehandlungsplans.

Ausgabe: Ein überarbeiteter Risikobehandlungsplan und dessen Umsetzung.

Anleitung zur Umsetzung:

Nichtkonformitäten in Bezug auf die Wirksamkeit des Risikobehandlungsplans können durch ein internes oder externes Audit oder durch Überwachung und anhand von Anzeichen festgestellt werden. Der Behandlungsplan sollte unter Berücksichtigung der folgenden Punkte überarbeitet werden:

— Ergebnisse des Prozesses zur Informationssicherheitsrisikobehandlung;

— schrittweise Umsetzung des Plans (z. B. eine Maßnahme wird „im Planungszustand“, „im Gestaltungszustand“, „im Bereitstellungszustand“ umgesetzt);

— identifizierte Schwierigkeiten bei der Umsetzung von Maßnahmen (z. B. technische oder finanzielle Probleme, Inkonsistenzen mit internen oder externen Faktoren wie dem Datenschutz).

Es gibt auch Fälle, in denen die Benutzer, selbst wenn die Restrisiken nach Abschluss des Behandlungsplans akzeptabel sind, dessen Anwendung ablehnen oder versuchen, ihn zu umgehen, weil diese Maßnahmen von den Benutzern im Hinblick auf die Benutzerfreundlichkeit nicht akzeptiert werden (z. B. nicht ergonomisch, zu kompliziert oder zu lang).

Die Organisation sollte die Wirksamkeit des überarbeiteten Behandlungsplans überprüfen.

10.8 Fortlaufende Verbesserung

ANMERKUNG Dieser Unterabschnitt bezieht sich auf ISO/IEC 27001:2022, 10.2

Eingabe: Alle im Rahmen des Risikomanagements erlangten Risikoinformationen.

Aktion: Der Prozess des Informationssicherheitsrisikomanagements sollte kontinuierlich überwacht, überprüft und bei Bedarf verbessert werden.

Auslöser: Die Organisation ist bestrebt, die aus dem Risikomanagementprozess für die Informationssicherheit gezogenen Lehren in entsprechende Verbesserungen und Optimierungen zu überführen.

Ausgabe: Kontinuierliche Relevanz des Risikomanagementprozesses für die Informationssicherheit in Bezug auf die Geschäftsziele der Organisation oder eine Aktualisierung des Prozesses.

Anleitung zur Umsetzung:

Um sicherzustellen, dass der Prozess des Risikomanagements im Bereich der Informationssicherheit korrekt ist, muss laufend überwacht und überprüft werden, dass der Kontext, das Ergebnis der Risikobeurteilung und die Risikobehandlung sowie die Managementpläne maßgeblich und den Umständen angemessen bleiben.

Die Organisation sollte sicherstellen, dass der Prozess des Risikomanagements für die Informationssicherheit und die damit zusammenhängenden Aufgaben unter den gegebenen Umständen angemessen bleiben und befolgt werden. Alle vereinbarten Verbesserungen des Prozesses oder Aktionen, die notwendig sind, um die Einhaltung des Prozesses zu verbessern, sollten den zuständigen Führungskräften mitgeteilt werden. Diese Führungskräfte sollten die Zusicherung erhalten, dass kein Risiko oder Risikoelement übersehen oder unterschätzt wird und dass die notwendigen Aktionen durchgeführt und Entscheidungen getroffen werden, um ein realistisches Risikoverständnis und die Fähigkeit zur Reaktion sicherzustellen.

Es sollte angemerkt werden, dass während des Änderungsmanagementprozesses eine kontinuierliche Rückmeldung an den Risikomanagementprozess gegeben werden sollte, um sicherzustellen, dass Änderungen an Informationssystemen, welche Änderungen von Risiken nach sich ziehen können, umgehend berücksichtigt werden, und sogar die Maßnahmen zur Risikobeurteilung geändert werden, um sie angemessen zu bewerten.

Darüber hinaus sollte die Organisation regelmäßig die Kriterien verifizieren, die zur Messung des Risikos verwendet werden. Durch diese Verifizierung sollte sichergestellt werden, dass alle Elemente nach wie vor gültig sind und mit den Geschäftszielen, -strategien und -richtlinien übereinstimmen und dass Änderungen des Geschäftskontexts im Rahmen des Risikomanagementprozesses für die Informationssicherheit angemessen berücksichtigt werden. Diese Überwachungs- und Überprüfungsaufgaben sollten sich auf folgende Punkte beziehen (aber nicht darauf beschränkt sein):

— rechtlicher und ökologischer Kontext;

— Wettbewerbskontext;

— Ansatz der Risikobeurteilung;

— Beträge und Kategorie von Werten;

— Folgekriterien;

— Wahrscheinlichkeitskriterien;

— Risikobewertungskriterien;

— Risikoakzeptanzkriterien;

— Gesamtbetriebskosten;

— notwendige Ressourcen.

Die Organisation sollte sicherstellen, dass ständig Ressourcen für die Risikobeurteilung und die Risikobehandlung zur Verfügung stehen, um Risiken zu überprüfen, neue oder veränderte Bedrohungen oder Schwachstellen anzugehen und das Management entsprechend zu beraten.

Die Überwachung des Risikomanagements kann dazu führen, dass der Ansatz, die Methodik oder die verwendeten Instrumente abhängig von den folgenden Faktoren geändert oder ergänzt werden:

— die Risikoreife der Organisation;

— identifizierte Änderungen;

— Iteration der Risikobeurteilung;

— das Ziel des Risikomanagementprozesses für die Informationssicherheit (z. B. Aufrechterhaltung der Betriebsfähigkeit, Resilienz bei Zwischenfällen, Compliance);

— der Gegenstand des Prozesses des Informationssicherheitsrisikomanagements (z. B. Organisation, Geschäftseinheit, Informationsprozess, seine technische Umsetzung, Anwendung, Verbindung zum Internet).

Die Zyklen des Risikomanagements in Bezug auf den Anwendungsbereich der Risikobeurteilung und der Risikobehandlung sind in 5.2 dargestellt.

Anhang A
(informativ)

Beispiele für Techniken zur Unterstützung des Risikobeurteilungsprozesses

A.1 Risikokriterien für die Informationssicherheit

A.1.1 Kriterien im Zusammenhang mit der Risikobeurteilung

A.1.1.1 Allgemeine Überlegungen zur Risikobeurteilung

Im Allgemeinen dominiert bei der Beurteilung von Informationsrisiken die persönliche Ungewissheit, und verschiedene Analysten neigen bei der Interpretation der Punkte auf den Wahrscheinlichkeits- und Auswirkungsskalen zu unterschiedlicher Ungewissheit. Die Referenzskalen sollten An-, Wahrscheinlichkeits- und Risikokategorien auf gemeinsame, eindeutig festgelegte objektive Werte beziehen, die möglicherweise in Begriffen wie finanziellem Verlust in Geldeinheiten und fiktiver Häufigkeit des Auftretens in einer endlichen Zeitspanne ausgedrückt werden, die für den quantitativen Ansatz spezifisch sind.

Insbesondere bei einem qualitativen Ansatz sollten die Risikoanalysten geschult werden und regelmäßig anhand einer verankerten Referenzskala üben, um die Ausgewogenheit ihres Urteils zu wahren.

A.1.1.2 Qualitativer Ansatz

A.1.1.2.1 Auswirkungsskala

Tabelle A.1 enthält ein Beispiel für eine Auswirkungsskala.

Tabelle A.1 — Beispiel einer Auswirkungsskala

Auswirkungen	Beschreibung
5 – Katastrophal	**Branchenspezifische oder behördliche Auswirkungen außerhalb der Organisation** Erhebliche Auswirkungen auf das/die branchenspezifische(n) Ökosystem(e) mit Auswirkungen, die lang anhaltend sein können. Und/oder: Schwierigkeiten für den Staat oder sogar Unvermögen, eine behördliche Funktion oder eine seiner Aufgaben von existenzieller Bedeutung sicherzustellen. Und/oder: kritische Auswirkungen für die Sicherheit von Personen und Sachen (Gesundheitskrise, erhebliche Umweltverschmutzung, Zerstörung wichtiger Infrastrukturen usw.).
4 – Kritisch	**Verheerende Auswirkungen für die Organisation** Unvermögen der Organisation, ihre Tätigkeit ganz oder teilweise sicherzustellen, mit möglicherweise schwerwiegenden Auswirkungen für die Sicherheit von Personen und Sachen. Die Organisation wird die Situation höchstwahrscheinlich nicht überstehen (ihr Überleben ist bedroht), die Tätigkeitsbereiche oder staatlichen Sektoren, in denen sie tätig ist, werden wahrscheinlich nur geringfügig betroffen sein, ohne dass dies dauerhafte Auswirkungen hat.
3 – Schwerwiegend	**Erhebliche Auswirkungen für die Organisation** Starke Beeinträchtigung bei der Durchführung der Tätigkeit, möglicherweise mit signifikanten Auswirkungen für die Sicherheit von Personen und Sachen. Die Organisation wird die Situation nur unter großen Schwierigkeiten überstehen (Betrieb in einem stark eingeschränkten Modus), ohne dass dies Auswirkungen auf die Branche oder den Staat hat.

Tabelle A.1 (*fortgesetzt*)

Auswirkungen	Beschreibung
2 – Signifikant	**Signifikante, aber begrenzte Auswirkungen für die Organisation** Beeinträchtigung bei der Durchführung der Tätigkeit ohne signifikante Auswirkungen für die Sicherheit von Personen und Sachen. Die Organisation wird die Situation trotz einiger Schwierigkeiten überstehen (Betrieb in degradiertem Modus).
1 – Geringfügig	**Vernachlässigbare Auswirkungen für die Organisation** Keine Auswirkungen für den Betrieb oder die Durchführung der Tätigkeit bzw. für die Sicherheit von Personen und Sachen. Die Organisation wird die Situation ohne große Schwierigkeiten überstehen (die Margen werden aufgezehrt).

A.1.1.2.2 Wahrscheinlichkeitsskala

Tabelle A.2 und Tabelle A.4 enthalten Beispiele für alternative Darstellungsformen von Wahrscheinlichkeitsskalen. Die Wahrscheinlichkeit kann entweder in wahrscheinlichkeitsbasierten Begriffen wie in Tabelle A.2 oder in frequentistischen Begriffen wie in Tabelle A.4 ausgedrückt werden. Die wahrscheinlichkeitsbasierte Darstellung gibt die durchschnittliche Wahrscheinlichkeit an, mit der ein Risikoereignis in einer bestimmten Zeitspanne eintritt, während die frequentistische Darstellung angibt, wie oft das Risikoereignis in einer bestimmten Zeitspanne im Durchschnitt zu erwarten ist. Da die beiden Ansätze lediglich denselben Sachverhalt aus zwei verschiedenen Perspektiven ausdrücken, kann jede der beiden Darstellungen verwendet werden, je nachdem, was die Organisation für eine bestimmte Risikokategorie als am geeignetsten betrachtet.

Wenn jedoch beide Ansätze als Alternativen innerhalb derselben Organisation verwendet werden, ist es wichtig, dass jeder begrifflich gleichwertige Rang auf beiden Skalen die gleiche tatsächliche Wahrscheinlichkeit darstellt. Andernfalls hängen die Ergebnisse der Beurteilung davon ab, welche Skala verwendet wird, und nicht von der tatsächlichen Wahrscheinlichkeit der zu beurteilenden Risikoquelle. Wenn beide Ansätze verwendet werden, sollte das wahrscheinlichkeitsbasierte Niveau für jeden fiktiven Rang mathematisch aus dem frequentistischen Wert des gleichwertigen Rangs berechnet werden oder umgekehrt, je nachdem, welcher Ansatz zum Definieren der Primärskala verwendet wird.

Wenn nur einer der beiden Ansätze verwendet wird, müssen die Abstufungen der Skala nicht so eng definiert werden, da eine Priorisierung der Wahrscheinlichkeiten unabhängig von den verwendeten absoluten Werten erreicht werden kann. Obwohl in Tabelle A.2 und Tabelle A.4 je nach Kontext der Organisation und der zu beurteilenden Risikokategorie völlig unterschiedliche Abstufungen und Wahrscheinlichkeitsbereiche verwendet werden, können beide für die Analyse gleichermaßen effektiv sein, wenn sie ausschließlich verwendet werden. Sie wären jedoch nicht sicher als Alternativen im gleichen Kontext verwendbar, da die Werte, die mit gleichwertigen Einstufungen verbunden sind, nicht korrelieren.

Die in Tabelle A.2 und Tabelle A.4 verwendeten Kategorien und Werte sind nur Beispiele. Welcher Wert für die einzelnen Wahrscheinlichkeitsstufen am besten geeignet ist, hängt vom Risikoprofil und der Risikobereitschaft der Organisation ab.

Tabelle A.2 — Beispiel einer Wahrscheinlichkeitsskala

Wahrscheinlichkeit	Beschreibung
5 – Fast sicher	Die Risikoquelle wird ihr Ziel höchstwahrscheinlich mit einer der in Betracht gezogenen Angriffsmethoden erreichen. Die Wahrscheinlichkeit des Risikoszenarios ist sehr hoch.
4 – Sehr wahrscheinlich	Die Risikoquelle wird ihr Ziel wahrscheinlich mit einer der in Betracht gezogenen Angriffsmethoden erreichen. Die Wahrscheinlichkeit des Risikoszenarios ist hoch.

Tabelle A.2 (*fortgesetzt*)

Wahrscheinlichkeit	Beschreibung
3 – Wahrscheinlich	Die Risikoquelle kann ihr Ziel mit einer der in Betracht gezogenen Angriffsmethoden erreichen. Die Wahrscheinlichkeit des Risikoszenarios ist signifikant.
2 – Eher unwahrscheinlich	Die Risikoquelle hat relativ geringe Chancen, ihr Ziel mit einer der in Betracht gezogenen Angriffsmethoden zu erreichen. Die Wahrscheinlichkeit des Risikoszenarios ist niedrig.
1 – Unwahrscheinlich	Die Risikoquelle hat eine sehr geringe Chance, ihr Ziel mit einer der in Betracht gezogenen Angriffsmethoden zu erreichen. Die Wahrscheinlichkeit des Risikoszenarios ist sehr niedrig.

Bezeichnungen wie „niedrig“, „mittel“ und „hoch“ können bei beiden Ansätzen der Wahrscheinlichkeitsbeurteilung an die Einstufungen angehängt werden. Diese können nützlich sein, wenn mit interessierten Parteien, die keine Risikospezialisten sind, die Wahrscheinlichkeitsstufen erörtert werden. Sie sind jedoch subjektiv und daher zwangsläufig mehrdeutig. Daher sollten sie nicht als primäre Deskriptoren bei der Durchführung oder Meldung von Beurteilungen verwendet werden.

A.1.1.2.3 Risikoniveau

Der Nutzen qualitativer Skalen und die Konsistenz der daraus abgeleiteten Risikobeurteilungen hängen vollständig von der Konsistenz ab, mit der die Kategorienbezeichnungen von allen interessierten Parteien interpretiert werden. Die Niveaus einer jeden qualitativen Skala sollten eindeutig sein, ihre Abstufungen sollten klar definiert sein, die qualitativen Beschreibungen für jedes Niveau sollten in einer objektiven Sprache ausgedrückt werden und die Kategorien sollten sich nicht überschneiden.

Folglich sollten bei der Verwendung von verbalen Deskriptoren der Wahrscheinlichkeit, der Auswirkungen oder des Risikos diese formell auf eindeutige Skalen bezogen werden, die in numerischen (wie in Tabelle A.4) oder ratiometrischen (wie in Tabelle A.2) Bezugspunkten verankert sind. Alle interessierten Parteien sollten über die Referenzskalen informiert werden, um sicherzustellen, dass die Interpretation der qualitativen Beurteilungsdaten und -ergebnisse einheitlich ist.

Tabelle A.3 enthält ein Beispiel für einen qualitativen Ansatz.

Tabelle A.3 — Beispiel für einen qualitativen Ansatz bei den Risikokriterien

Wahrscheinlichkeit	Folge				
	Katastrophal	Kritisch	Schwerwiegend	Signifikant	Geringfügig
Fast sicher	sehr hoch	sehr hoch	hoch	hoch	mittel
Sehr wahrscheinlich	sehr hoch	hoch	hoch	mittel	niedrig
Wahrscheinlich	hoch	hoch	mittel	niedrig	niedrig
Eher unwahrscheinlich	mittel	mittel	niedrig	niedrig	sehr niedrig
Unwahrscheinlich	niedrig	niedrig	niedrig	sehr niedrig	sehr niedrig

Die Gestaltung einer qualitativen Risikomatrix sollte sich an den Risikoakzeptanzkriterien der Organisation orientieren (siehe 6.4.2 und A.1.2).

BEISPIEL Eine Organisation macht sich manchmal mehr Gedanken über extreme Auswirkungen, obwohl deren Auftreten unwahrscheinlich ist, oder sie macht sich vor allem Gedanken über häufige Ereignisse mit geringeren Auswirkungen.

Bei der Gestaltung einer qualitativen oder quantitativen Risikomatrix ist das Risikoprofil einer Organisation üblicherweise asymmetrisch. Bagatellereignisse sind im Allgemeinen am häufigsten, und die erwartete Häufigkeit nimmt in der Regel ab, wenn die Auswirkungen signifikanter werden, bis hin zu sehr geringen Wahrscheinlichkeiten extremer Auswirkungen. Es ist auch unüblich, dass das Geschäftsrisiko eines Ereignisses mit hoher Wahrscheinlichkeit und wenig signifikanten Auswirkungen dem eines Ereignisses mit geringer Wahrscheinlichkeit und sehr signifikanten Auswirkungen entspricht. Obwohl eine Risikomatrix, die symmetrisch um die Diagonale niedrig/niedrig bis hoch/hoch ist, leicht zu erstellen und naiv akzeptabel zu sein scheint, ist es unwahrscheinlich, dass sie das tatsächliche Risikoprofil einer Organisation genau wiedergibt und daher ungültige Ergebnisse liefern kann. Um sicherzustellen, dass eine Risikomatrix realistisch ist und die Anforderung der kontinuierlichen Verbesserung erfüllen kann (siehe ISO/IEC 27001:2022, 10.2), sollten bei der Festlegung oder Änderung der Skalen und der Matrix die Gründe für die Zuordnung jeder Kategorie zu den Wahrscheinlichkeits- und Folgeskalen und der Risikomatrix sowie für die Übereinstimmung der Kategorien mit dem Risikoprofil der Organisation dokumentiert werden. Zumindest sollten die Ungewissheiten, die mit der Verwendung inkrementeller Skalenmatrizen verbunden sind, mit der gebotenen Vorsicht für die Benutzer beschrieben werden.

Der Nutzen qualitativer Skalen und die Konsistenz der daraus abgeleiteten Risikobeurteilungen hängen vollständig von der Konsistenz ab, mit der die Kategorienbezeichnungen von allen interessierten Parteien interpretiert werden. Die Niveaus einer jeden qualitativen Skala sollten eindeutig sein, ihre Abstufungen sollten klar definiert sein, die qualitativen Beschreibungen für jedes Niveau sollten in einer objektiven Sprache ausgedrückt werden und die Kategorien sollten sich nicht überschneiden.

A.1.1.3 Quantitativer Ansatz

A.1.1.3.1 Endliche Skalen

Das Risikoniveau kann nach jedem beliebigen Verfahren und unter Berücksichtigung aller maßgeblichen Faktoren berechnet werden, wird aber in der Regel durch Multiplikation der Wahrscheinlichkeit mit der Folge angegeben.

Die Wahrscheinlichkeit gibt die Wahrscheinlichkeit oder Häufigkeit an, mit der ein Ereignis innerhalb eines bestimmten Zeitrahmens eintritt. Dieser Zeitrahmen ist in der Regel jährlich (je Jahr), kann aber so groß (z. B. je Jahrhundert) oder klein (z. B. je Sekunde) sein, wie es die Organisation wünscht.

Wahrscheinlichkeitsskalen sollten unter Verwendung praxisnaher Begriffe definiert werden, die den Kontext der Organisation widerspiegeln, so dass sie ihr beim Risikomanagement helfen und für alle interessierten Parteien leicht verständlich sind. Das bedeutet in erster Linie, dass der Bandbreite der dargestellten Wahrscheinlichkeiten realistische Grenzen gesetzt werden. Wenn die Höchst- und Mindestgrenzen der Skala zu weit auseinander liegen, umfasst jede Kategorie innerhalb der Skala eine zu große Bandbreite an Wahrscheinlichkeiten, was die Beurteilung unsicher macht.

BEISPIEL 1 Der höchste Punkt auf der Skala für die endliche Wahrscheinlichkeit kann sinnvollerweise als die Zeit definiert werden, die die Organisation üblicherweise benötigt, um auf Ereignisse zu reagieren, und der niedrigste endliche Punkt als die Dauer der langfristigen strategischen Planung der Organisation.

Wahrscheinlichkeiten oberhalb und unterhalb der definierten Grenzen der Skala können sinnvollerweise als „größer als das Höchstmaß der Skala“ und „kleiner als das Mindestmaß der Skala“ ausgedrückt werden, wodurch klar zum Ausdruck kommt, dass Wahrscheinlichkeiten jenseits der Grenzen der definierten Skala Extremfälle sind, die ausnahmsweise zu berücksichtigen sind (möglicherweise unter Verwendung von besonderen Kriterien „außerhalb des zulässigen Bereichs“). Außerhalb dieser Grenzen ist die konkrete Wahrscheinlichkeit weniger wichtig als die Tatsache, dass es sich um eine Ausnahme in der gegebenen Richtung handelt.

In der Regel ist es hilfreich, die Auswirkungen anhand einer finanziellen Zahl zu messen, da dies eine Aggregation für die Risikoberichterstattung ermöglicht.

BEISPIEL 2 Monetäre Folgeskalen beruhen in der Regel auf Faktoren von 10 (100 bis 1 000; 1 000 bis 10 000 usw.).

Die Breiten der Kategorien einer Wahrscheinlichkeitsskala sollte unter Berücksichtigung der Breiten der gewählten Folgeskala ausgewählt werden, um zu vermeiden, dass eine übermäßige Bandbreite von Risiken in jede Kategorie fällt.

BEISPIEL 3 Wenn Wahrscheinlichkeit und Folge durch die Indizes einer Exponentialskala (d. h. die Logarithmen der Werte auf der Skala) dargestellt werden, sollten diese addiert werden.

Der Risikowert kann dann wie folgt berechnet werden: antilog [log (Wahrscheinlichkeitswert) + log (Folgewert)].

Tabelle A.4 — Beispiel einer logarithmischen Wahrscheinlichkeitsskala

Ungefähre Durchschnittshäufigkeit	Logarithmischer Ausdruck	Skalenwert
Jede Stunde	(ungefähr 10^5)	5
Alle 8 Stunden	(ungefähr 10^4)	4
Zweimal wöchentlich	(ungefähr 10^3)	3
Einmal monatlich	(ungefähr 10^3)	2
Einmal jährlich	(10^1)	1
Einmal im Jahrzehnt	(10^0)	0

BEISPIEL 4 In Tabelle A.4 ist ein Beispiel für ein häufig vorkommendes Ereignis ein computergestützter Passwortangriff oder ein verteilter Denial-of-Service-Angriff durch ein Botnetz. Die Angriffshäufigkeit kann tatsächlich viel höher sein.

BEISPIEL 5 In Tabelle A.4 ist ein Beispiel für ein Ereignis mit geringer Häufigkeit ein Vulkanausbruch. Selbst wenn ein Ereignis nur einmal im Jahrhundert vorhergesagt wird, bedeutet das nicht, dass es während der Lebensdauer eines ISMS nicht eintreten würde.

Tabelle A.5 zeigt ein Beispiel für eine logarithmische Auswirkungsskala. Ein Zweck bei der Berücksichtigung der Häufigkeit ist es, sicherzustellen, dass Schutzmaßnahmen stark genug sind, um häufig auftretenden Angriffssequenzen standzuhalten, selbst wenn die Wahrscheinlichkeit einer solchen Angriffssequenz gering ist.

Tabelle A.5 — Beispiel einer logarithmischen Auswirkungsskala

Folge (Verlust von)	Logarithmischer Ausdruck	Skalenwert
1 000 000 £	(10^6)	6
100 000 £	(10^5)	5
10 000 £	(10^4)	4
1 000 £	(10^3)	3
100 £	(10^2)	2
Weniger als 100 £	(10^1)	1

Wenn sowohl die Wahrscheinlichkeits- als auch die Auswirkungsskala einen Logarithmus zur Basis 10 für die Zuweisung von Niveaustufen verwenden, können Risikoanalysten am Ende zu viele Risiken auf demselben Risikoniveau vorfinden und nicht in der Lage sein, eine angemessene Priorisierung oder Sicherheitsinvestitionsentscheidung zu treffen. In diesem Fall kann es sinnvoll sein, die Basis zu verringern und die Anzahl der berücksichtigten Niveaustufen zu erhöhen. Es sollte erwähnt werden, dass bei Auswahl unterschiedlicher Grundlagen für die Wahrscheinlichkeit und die Auswirkungen keine sinnvolle Gleichung zur Summierung zweier Faktoren angewendet werden kann.

BEISPIEL 6 Wenn sich die Wahrscheinlichkeit beim Übergang von einem Risikoniveau zum nächsten verdoppelt, während die Auswirkungen um den Faktor 10 teurer sind, ergibt die Gleichung die Risiken a) und b), wobei das Risiko b) ein 10-mal teureres Auswirkungenniveau hat als das Risiko a), aber nur halb so wahrscheinlich ist wie das Risiko a), das auf demselben Risikoniveau landet. Dies ist wirtschaftlich gesehen falsch.

In Tabelle A.4 und Tabelle A.5 sind Wahrscheinlichkeits- und Auswirkungenbereiche aufgeführt, die die meisten Eventualitäten in sehr unterschiedlichen Organisationen abdecken. Es ist unwahrscheinlich, dass ein einzelnes Unternehmen mit dem Risikospektrum konfrontiert wird, das durch die Gesamtheit dieser Beispielskalen dargestellt wird. Der Kontext der Organisation und der Anwendungsbereich des ISMS sollten genutzt werden, um realistische Ober- und Untergrenzen sowohl für die Wahrscheinlichkeiten als auch für die Auswirkungen zu definieren, wobei zu berücksichtigen ist, dass die Quantifizierung von Risikobereichen, die über 1 000 zu 1 hinausgehen, wahrscheinlich nur von begrenztem praktischem Wert ist.

A.1.2 Risikoakzeptanzkriterien

Die Kriterien für die Risikoakzeptanz können einfach ein Wert sein, ab dem die Risiken als inakzeptabel gelten.

BEISPIEL 1 Wenn in Tabelle A.3 der Wert „mittel“ gewählt wird, würden alle Risiken mit einem Wert von „sehr niedrig“, „niedrig“ oder „mittel“ von der Organisation als akzeptabel und alle Risiken mit einem Wert von „hoch“ oder „sehr hoch“ als inakzeptabel angesehen werden.

Durch die Verwendung einer farbcodierten Risikomatrix, die die Skalen für Auswirkungen und Wahrscheinlichkeiten widerspiegelt, können Organisationen die Risikoverteilung aus einer oder mehreren Risikobeurteilungen grafisch darstellen. Eine solche Risikomatrix darf auch dazu verwendet werden, die Einstellung der Risikoorganisation zu den Risikowerten zu signalisieren und anzugeben, ob ein Risiko üblicherweise akzeptiert oder behandelt werden sollte.

BEISPIEL 2 Eine Risikomatrix mit drei Farben, z. B. rot, gelb und grün, kann verwendet werden, um drei Risikobewertungsstufen darzustellen, wie in Tabelle A.6 angegeben.

Es kann von Vorteil sein, andere Modelle mit Farben in einer Risikomatrix zu wählen.

BEISPIEL 3 Wenn eine Risikomatrix zum Vergleichen der Ergebnisse einer ursprünglich durchgeführten Risikobeurteilung mit den Ergebnissen einer Neubeurteilung für dieselben Risiken verwendet wird, kann die Risikominderung leichter dargestellt werden, wenn mehr Farben zum Darstellen der Risikoniveaus angewendet werden.

Es ist auch möglich, ein solches Modell um die Bestimmung zu ergänzen, welche Ebene der Geschäftsführung befugt ist, ein Risiko mit einem bestimmten Risikowert zu akzeptieren.

Tabelle A.6 enthält ein Beispiel für eine Bewertungsskala.

Tabelle A.6 — Beispiel für eine Bewertungsskala in Kombination mit einer Drei-Farben-Risikomatrix

Risikoniveau	Risikobewertung	Beschreibung
Niedrig (grün)	akzeptabel im Ist-Zustand	Das Risiko kann ohne weitere Aktionen akzeptiert werden.
Moderat (gelb)	unter Kontrolle tragbar	Es sollte eine Nachverfolgung in Bezug auf das Risikomanagement durchgeführt werden, und es sollten Aktionen im Rahmen einer kontinuierlichen Verbesserung mittel- und langfristig festgelegt werden.
Hoch (rot)	nicht akzeptabel	Kurzfristig sollten unbedingt Maßnahmen zur Verringerung des Risikos ergriffen werden. Andernfalls sollte die gesamte oder ein Teil der Tätigkeit abgelehnt werden.

A.2 Praktische Verfahren

A.2.1 Risikokomponenten für die Informationssicherheit

Bei der Identifizierung und Beurteilung von Informationssicherheitsrisiken sollten die folgenden Komponenten berücksichtigt werden:

— Auf die Vergangenheit bezogene Komponenten:

  — Sicherheitsereignisse und Vorfälle (sowohl innerhalb als auch außerhalb der Organisation);

  — Risikoquellen;

  — ausgenutzte Anfälligkeiten;

  — gemessene Auswirkungen;

— Komponenten bezogen auf die Zukunft:

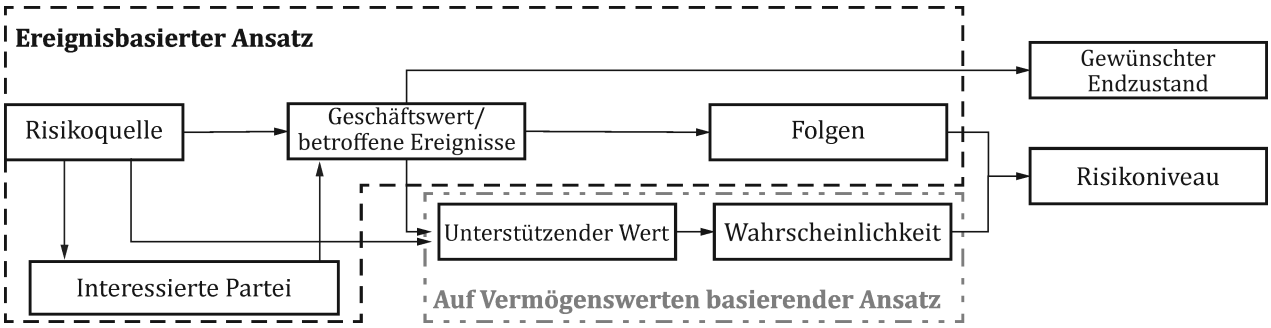
  — Bedrohungen;

  — Schwachstellen;

  — Auswirkungen;

  — Risikoszenarien.

Die Beziehungen zwischen den Risikokomponenten der Informationssicherheit werden in Bild A.1 dargestellt und in A.2.2 bis A.2.7 erläutert.



Legende

⟶ Bedrohung

Bild A.1 — Komponenten für die Risikobeurteilung der Informationssicherheit

Einzelheiten zum „Gewünschten Endzustand“ (DES, en: desired end state) können in A.2.3 b) nachgelesen werden.

A.2.2 Werte

Bei der Anwendung des auf Werten basierenden Ansatzes zur Risikoidentifizierung sollten die Werte identifiziert werden.

Im Rahmen des Risikobeurteilungsprozesses und der Entwicklung von Risikoszenarien sollte die Identifizierung von Ereignissen, Auswirkungen, Bedrohungen und Schwachstellen mit Werten verknüpft werden.

Im Rahmen des Risikobehandlungsprozesses ist jede Maßnahme auf eine Teilmenge der Werte anwendbar.

Die Werte können in zwei Kategorien unterteilt werden:

— Primär-/Geschäftsvermögen — Informationen oder Prozesse, die für eine Organisation von Wert sind;

— unterstützende Werte — Komponenten des Informationssystems, auf denen ein oder mehrere Geschäftsvermögen basieren.

Primär-/Geschäftsvermögen werden häufig im Rahmen des ereignisbasierten Ansatzes verwendet (Identifizierung von Ereignissen und deren Auswirkungen für das Geschäftsvermögen).

Die unterstützenden Werte werden häufig im Rahmen des auf Werten basierenden Ansatzes (Identifizierung und Analyse von Schwachstellen und Bedrohungen für diese Werte) und beim Prozess der Risikobehandlung (Festlegung des Werts bzw. der Werte, auf die die einzelnen Maßnahmen angewendet werden sollen) verwendet.

Geschäftsvermögen und unterstützendes Vermögen sind miteinander verbunden, daher können sich die für unterstützende Vermögen ermittelten Risikoquellen auf Geschäftsvermögen auswirken.

Aus diesem Grund ist es wichtig, die Beziehungen zwischen den Werten zu ermitteln und ihren Wert für die Organisation zu verstehen. Eine Fehleinschätzung des Werts kann zu einer Fehleinschätzung der mit dem Risiko verbundenen Auswirkungen führen, aber auch das Verständnis für die Wahrscheinlichkeit der betrachteten Bedrohungen beeinträchtigen.

BEISPIEL 1 Ein unterstützender Wert beherbergt ein Geschäftsvermögen (in diesem Fall Informationen).

Daten werden durch interne und externe Maßnahmen geschützt, um zu verhindern, dass eine Risikoquelle ihr Ziel in Bezug auf die Geschäftswerte erreicht, indem sie eine Schwachstelle des unterstützenden Werts ausnutzt. Bei der Unterscheidung zwischen verschiedenen Arten von Werten sollten die Abhängigkeiten zwischen den Werten dokumentiert und die Risikoausbreitung beurteilt werden, damit dokumentiert werden kann, dass ein und dasselbe Risiko nicht zweimal beurteilt wird, nämlich einmal, wenn es sich auf den unterstützenden Wert auswirkt, und einmal, wenn es den Primärwert betrifft. Vermögensabhängigkeitsdiagramme sind nützliche Instrumente, um solche Abhängigkeiten darzustellen und sicherzustellen, dass alle Abhängigkeiten berücksichtigt wurden.

BEISPIEL 2 Das Diagramm in Bild A.2 zeigt die abhängigen Werte für das Geschäftsvermögen „Auftrags- und Rechnungsbearbeitung anzeigen“ und kann wie folgt gelesen werden:

— „Administrator“ (Typ: Personal), der, wenn er nicht ordnungsgemäß geschult ist, ein Risiko für den Wert darstellt.

— „IT-Instandhaltung“ (Typ: Dienstleistung), die das Risiko auf den Wert überträgt.

— „Server“ (Typ: Hardware) oder für den Wert „Netzwerk“ (Typ Netzwerkkonnektivität). Der Server, wenn er nicht mehr funktioniert, oder wenn ein falsch konfiguriertes Netzwerk eine Minderung des Werts verursacht.

— „Webportal“ (Typ: Anwendung), den Betrieb einstellen oder nicht verfügbar sein.

Ohne „Webportal“ bietet der Geschäftsprozess „Auftrags- und Rechnungsabwicklung anzeigen“ den Kunden nicht den gewünschten Prozess.

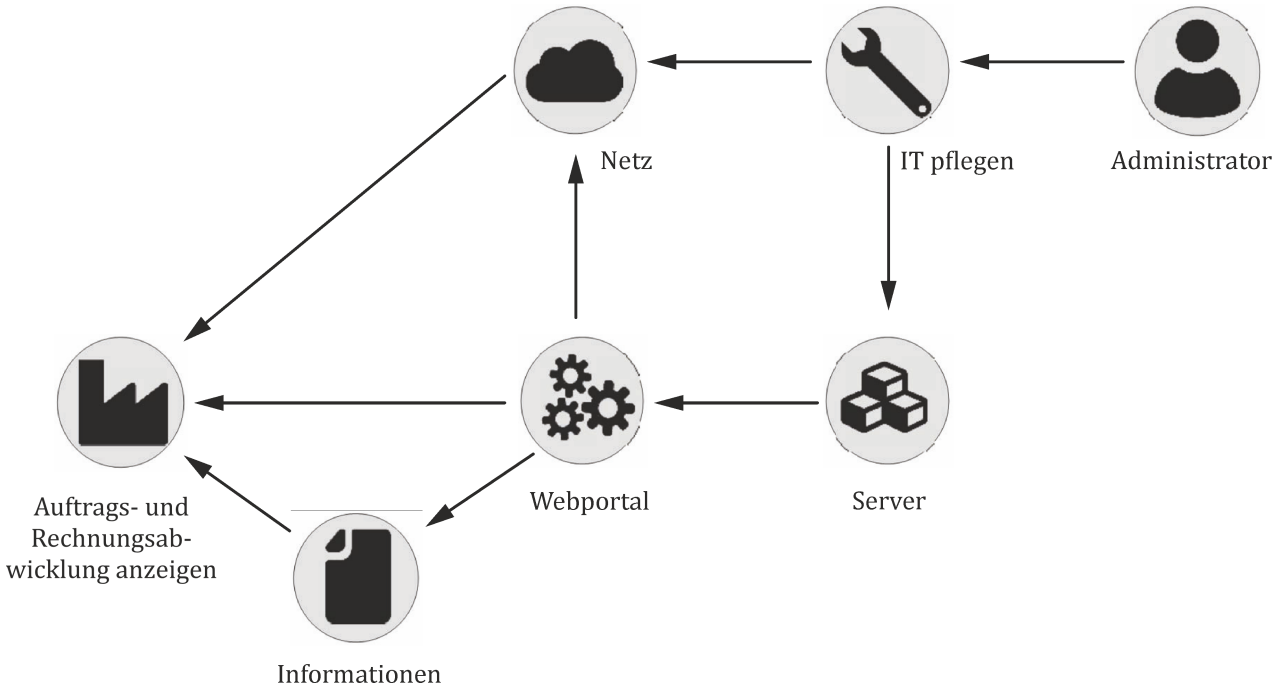


Bild A.2 — Beispiel eines Diagramms der Abhängigkeiten von Werten

A.2.3 Risikoquellen und gewünschter Endzustand

In diesem Absatz wird vorgeschlagen, diese Art von Risikoquellen zu charakterisieren. Zwei Hauptkriterien strukturieren diesen beschreibenden Ansatz:

— die Motivation;

— die Fähigkeit, zu handeln.

a) Risikoquellenidentifizierung

Tabelle A.7 enthält Beispiele und übliche Angriffsmethoden.

Tabelle A.7 — Beispiele und übliche Angriffsmethoden

Risikoquelle	Beispiele und übliche Angriffsmethoden
Staatliche Stellen	Staaten, Nachrichtendienste Methode: Angriffe, die im Allgemeinen von Fachleuten durchgeführt werden, die nach einem festgelegten Zeitplan und einer festgelegten Angriffsmethode arbeiten. Dieses Angreiferprofil zeichnet sich durch seine Fähigkeit aus, eine offensive Operation über eine lange Zeitspanne durchzuführen (stabile Ressourcen, Verfahren) und seine Instrumente und Methoden an die Topologie des Ziels anzupassen. Folglich verfügen diese Akteure auch über die Mittel, 0-Day-Schwachstellen zu erwerben oder zu entdecken, und einige sind in der Lage, isolierte Netze zu infiltrieren und sukzessive Angriffe durchzuführen, um ein oder mehrere Ziele zu erreichen (z. B. durch einen auf die Lieferkette gerichteten Angriff).
Organisierte Kriminalität	Cyberkriminelle Organisationen (Mafias, Banden, kriminelle Vereinigungen) Methode: Internetbetrug oder Betrug im persönlichen Gespräch, Lösegeldforderungen oder Angriffe über Erpressungstrojaner, Nutzung von Botnetzen usw. Insbesondere aufgrund der Verbreitung von Angriffssets, die online leicht erhältlich sind, führen Cyberkriminelle immer raffiniertere und besser organisierte Operationen zu lukrativen oder betrügerischen Zwecken durch. Einige haben die Mittel, 0-Day-Schwachstellen zu erwerben oder zu entdecken.

Tabelle A.7 (*fortgesetzt*)

Risikoquelle	Beispiele und übliche Angriffsmethoden
Terroristen	Cyber-Terroristen, Cyber-Milizen Methode: Angriffe, die in der Regel nicht sehr ausgeklügelt sind, aber zielstrebig mit dem Ziel einer Destabilisierung und Zerstörung durchgeführt werden: Denial-of-Service (z. B. um die Notdienste eines Krankenhauses unerreichbar zu machen oder ein industrielles Energieerzeugungssystem vorzeitig abzuschalten), Ausnutzung von Schwachstellen von Websites und Verunstaltung.
Ideologische Aktivisten	Cyber-Hacktivisten, Interessengruppen, Sekten Methode: Die Angriffsmethoden und die Raffinesse der Angriffe sind denen von Cyber-Terroristen relativ ähnlich, aber sie sind durch weniger zerstörerische Absichten motiviert. Einige Akteure führen diese Angriffe durch, um eine Ideologie, eine Botschaft zu vermitteln (z. B. massive Nutzung sozialer Netzwerke als Resonanzboden).
Spezialisierte Einrichtungen	„Cyber-Söldner"-Profil mit allgemein hohen technischen IT-Kapazitäten. Aus diesem Grund sollte es von den Scriptkiddies unterschieden werden, mit denen es jedoch den Geist der Herausforderung und der Suche nach Anerkennung teilt, jedoch mit einem lukrativen Ziel. Solche Gruppen können als spezialisierte Einrichtungen organisiert sein, die echte Hacking-Dienste anbieten. Methode: Diese Art von erfahrenen Hackern ist oft der Ursprung für die Entwicklung und Erstellung von Angriffspaketen und Instrumenten, die online erhältlich sind (möglicherweise gegen eine Gebühr) und dann von anderen Gruppen von Angreifern „schlüsselfertig" verwendet werden können. Es gibt keine besonderen Beweggründe außer dem finanziellen Gewinn.
Laie	Profil des Scriptkiddies-Hackers oder desjenigen, der über fundiertes IT-Wissen verfügt; motiviert durch das Streben nach sozialer Anerkennung, Spaß und Herausforderung. Methode: Grundlegende Angriffe, aber mit der Möglichkeit, die online erhältlichen Angriffspakete zu verwenden.
Rächer	Die Motivationen dieses Angreiferprofils sind von einem akuten Rachegefühl oder einem Gefühl der Ungerechtigkeit geleitet (z. B. wegen eines schweren Fehlers entlassener Angestellter, Dienstleister, der nach einem nicht verlängerten Vertrag unzufrieden ist usw.). Methode: Dieses Angreiferprofil zeichnet sich durch seine Entschlossenheit und sein internes Wissen über die Systeme und Organisationsprozesse aus. Dies kann ihn furchterregend machen und ihm erhebliche Macht verleihen, Schaden anzurichten.
Pathologischer Angreifer	Die Motivationen dieses Angreiferprofils sind pathologischer oder opportunistischer Natur und werden mitunter von einem Gewinnmotiv geleitet (z. B. unlauterer Konkurrent, unehrlicher Kunde, Betrüger und Schwindler). Methode: In diesem Fall verfügen die Angreifer entweder über Computerwissen, das sie dazu veranlasst, zu versuchen, die Transitsysteme ihres Ziels zu kompromittieren, oder sie verwenden die im Internet erhältlichen Angriffspakete bzw. sie beschließen, den IT-Angriff an ein spezialisiertes Unternehmen zu vergeben. In bestimmten Fällen können Angreifer ihre Aufmerksamkeit auf eine interne Quelle (einen unzufriedenen Mitarbeiter, einen skrupellosen Dienstleister) lenken und versuchen, ihn zu korrumpieren.

b) Modellierung der Motivation einer Risikoquelle — gewünschter Endzustand

Es gibt ein breites Spektrum von Motivationen; sie können politisch, finanziell, ideologisch, aber auch sozial sein oder sogar einen einmaligen oder pathologischen psychologischen Zustand darstellen.

Es ist zwar nicht möglich, eine Motivation direkt auszudrücken, aber sie kann durch die Absicht der Risikoquelle veranschaulicht und in Form eines gewünschten Endzustands (DES, en: desired end state) ausgedrückt werden: die Gesamtsituation, die die Risikoquelle nach der Konfrontation erreichen möchte. Eine systematische Klassifizierung von Situationen, die mit allgemeinen Aktionskategorien verbunden ist, kann die kontextbezogene Analyse leiten.

Tabelle A.8 enthält eine beispielhafte Klassifizierung von Motivationen, die den DES zum Ausdruck bringen.

Tabelle A.8 — Beispielhafte Klassifizierung von Motivationen, die den DES zum Ausdruck bringen

Erobern	Langfristige Aneignung von Ressourcen oder Wirtschaftsmärkten, Erlangung politischer Macht oder Durchsetzung von Werten
Erbeuten	Räuberischer Ansatz, entschieden offensiv, mit dem Ziel, sich Ressourcen oder Vorteile anzueignen
Verhindern	Offensiver Ansatz zur Begrenzung der Aktionen einer dritten Partei
Aufrecht-erhalten	Bemühungen um die Aufrechterhaltung einer ideologischen, politischen, wirtschaftlichen oder sozialen Situation
Verteidigen	Das Einnehmen einer strikt defensiven Ausweichhaltung oder einer explizit drohenden Haltung (z. B. Einschüchterung), um das aggressive Verhalten eines klar benannten Gegners zu verhindern oder dessen Aktion durch Verlangsamung zu unterbinden usw.
Überleben	Schutz einer Entität um jeden Preis, was zu extrem aggressiven Aktionen führen kann

c) Zielvorgaben

Um den DES zu erreichen, konzentriert sich die Risikoquelle auf ein oder mehrere Ziele, die sich auf die Geschäftswerte des Zielsystems auswirken. Dies sind die Zielvorgaben der Risikoquelle.

Tabelle A.9 enthält Beispiele für Zielvorgaben.

Tabelle A.9 — Beispiele für Zielvorgaben

Zielvorgabe	Beschreibung
Spionage	Nachrichtendienstlicher Betrieb (staatsbezogen, wirtschaftlich). In vielen Fällen zielt der Angreifer darauf ab, sich langfristig und völlig unbemerkt im Informationssystem einzunisten. Waffentechnik, Raumfahrt, Luftfahrt, Pharmazie, Energie und bestimmte staatliche Aktivitäten (Wirtschaft, Finanzen und Außenpolitik) sind bevorzugte Ziele.
Strategische Vorab-positionierung	Vorabpositionierung, die im Allgemeinen auf einen langfristigen Angriff abzielt, ohne dass das Endziel eindeutig feststeht (z. B. Kompromittierung der Netze von Telekommunikationsbetreibern, Infiltration von Masseninformations-Websites, um eine Operation zur politischen oder wirtschaftlichen Beeinflussung mit starkem Echo zu starten). Plötzliche und massive Kompromittierung von Computern zur Bildung eines Botnetzes kann dieser Kategorie zugeordnet werden.
Beeinflussung	Operationen, die darauf abzielen, falsche Informationen zu verbreiten oder Informationen zu verändern, Meinungsführer in den sozialen Netzwerken zu mobilisieren, den Ruf zu zerstören, vertrauliche Informationen offenzulegen, das Image einer Organisation oder eines Staates zu schädigen. Das Endziel besteht im Allgemeinen darin, die Wahrnehmung zu destabilisieren oder zu verändern.
Hindernis für die Funktions-fähigkeit	Sabotageakte, die beispielsweise darauf abzielen, eine Website unerreichbar zu machen, eine Informationssättigung herbeizuführen, die Nutzung einer digitalen Ressource zu verhindern oder eine physische Anlage unerreichbar zu machen. Industrielle Systeme können durch IT-Netze, mit denen sie verbunden sind, besonders gefährdet und angreifbar sein (z. B. durch das Senden von Befehlen, die zu einem Hardwareschaden oder einem Ausfall führen, der eine umfangreiche Wartung erfordert). Distributed-Denial-of-Service-Angriffe (DDoS) sind häufig verwendete Techniken zum Neutralisieren digitaler Ressourcen.
Einträglich	Operation, die entweder direkt oder indirekt auf einen finanziellen Gewinn abzielt. Im Zusammenhang mit der organisierten Kriminalität sind im Allgemeinen zu nennen: Betrug im Internet, Geldwäsche, Erpressung oder Veruntreuung, Finanzmarktmanipulation, Fälschung von Verwaltungsdokumenten, Identitätsdiebstahl usw. Bestimmte gewinnorientierte Operationen können sich einer Angriffsmethode bedienen, die zu den oben genannten Kategorien gehört (z. B. Spionage und Datendiebstahl, Ransomware, um eine Aktivität zu neutralisieren), aber der Endzweck bleibt finanziell.
Herausforderung, Spaß	Operation, die darauf abzielt, eine Leistung zum Zweck der sozialen Anerkennung, der Herausforderung oder einfach nur zum Spaß zu erbringen. Auch wenn das Ziel in erster Linie Spaß ist und keine besondere Absicht besteht, Schaden anzurichten, kann diese Art von Operation schwerwiegende Auswirkungen für das Opfer haben.

Der Unterschied zwischen einem DES und einer Zielvorgabe lässt sich am Beispiel einer Risikoquelle verdeutlichen, deren Ziel es ist, einen Auftrag zu gewinnen (DES), und die versucht, vertrauliche Informationen über Verhandlungen von ihrem Konkurrenten zu stehlen (strategische Zielsetzung). Manchmal führt das betreffende Ziel (die gewünschte Information) nicht zu einem DES.

Es kann davon ausgegangen werden, dass der Wert des Ziels aus der Sicht der Risikoquelle auf seinem Beitrag zum DES beruht.

Ganz allgemein lassen sich die Zielvorgaben der Risikoquelle in zwei große Klassen einteilen:

— Ausbeutung von Zielressourcen zum eigenen Vorteil, z. B. Spionage, Diebstahl, Betrug, illegaler Handel;

— Behinderung des Ziels an der Nutzung seiner Ressourcen (Konfrontation ist immer relativ), z. B. Krieg, Terrorismus, Sabotage, Subversion, Destabilisierung.

A.2.4 Ereignisbasierter Ansatz

A.2.4.1 Ökosystem

Bei einem ereignisbasierten Ansatz sollten Szenarien durch die Analyse der verschiedenen Pfade erstellt werden, die für die Interaktionen zwischen der Organisation und den interessierten Parteien maßgeblich sind und die alle ein Ökosystem bilden, das von den Risikoquellen genutzt werden kann, um die Geschäftswerte und deren DES zu erreichen.

Immer mehr Angriffsmethoden nutzen die anfälligsten Glieder eines solchen Ökosystems, um ihre Ziele zu erreichen.

Die interessierten Parteien im Rahmen des ISMS, die bei der Analyse von Risikoszenarien berücksichtigt werden sollten, können zweierlei sein:

— externe Parteien einschließlich:

  — Kunden;

  — Partner, Vertragspartner;

  — Dienstleister (Unterauftragnehmer, Lieferanten).

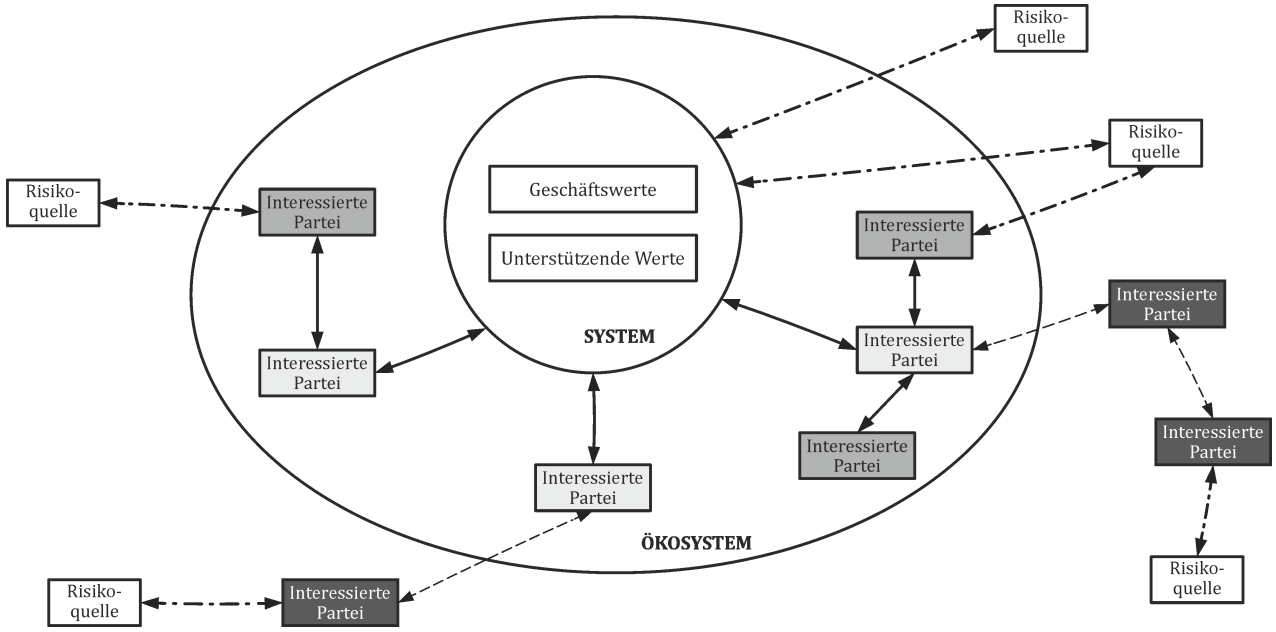
— interne Parteien einschließlich:

  — technikbezogene Dienstleister (z. B. vom IT-Management vorgeschlagene Support-Dienste);

  — Anbieter geschäftsbezogener Dienstleistungen (z. B. kommerzielle Entität, die Geschäftsdaten verwendet);

  — Tochtergesellschaften (vor allem in anderen Ländern).

Das Ziel bei der Identifizierung der interessierten Parteien ist es, einen klaren Überblick über das Ökosystem zu erhalten, um die am stärksten verwundbaren Parteien zu identifizieren. Die Sensibilisierung für das Ökosystem sollte in einer ersten Risikostudie angegangen werden. Bild A.3 zeigt die Identifizierung der interessierten Parteien des Ökosystems.



Legende

- Beziehung innerhalb des Ökosystems
- Beziehung, die die Grenze des Ökosystems überschreitet
- Beziehung innerhalb der Risikoquelle
- interne/externe interessierte Partei, die direkt mit dem System verbunden ist (erste Beziehungsebene)
- interessierte Partei, die mit einer anderen interessierten Partei verbunden ist (zweite Beziehungsebene)
- Entität außerhalb des Ökosystembereichs

Bild A.3 — Identifizierung der interessierten Parteien des Ökosystems

A.2.4.2 Strategische Szenarien

Auf der Grundlage der Informationen über Risikoquellen und betreffende Ereignisse können realistische Szenarien auf hoher Ebene (strategische Szenarien) erdacht werden, aus denen hervorgeht, auf welche Weise eine Risikoquelle ihren DES erreichen kann. Sie kann beispielsweise das Ökosystem durchdringen oder einige Geschäftsprozesse umleiten. Diese Szenarien werden ausgehend von den Risikoquellen und ihren DES durch Ableitung ermittelt: Für jedes dieser Szenarien können vom Standpunkt der Risikoquelle aus die folgenden Fragen gestellt werden:

— Welches sind die Geschäftswerte der Organisation, auf die die Risikoquellen abzielen müssen, um ihren DES zu erreichen?

— Werden sie, um ihren Angriff zu ermöglichen oder zu erleichtern, wahrscheinlich die kritische interessierte Partei des Ökosystems angreifen, die privilegierten Zugang zu den Geschäftswerten hat?

Sobald die am stärksten gefährdeten Elemente identifiziert sind, kann das strategische Szenario gezeichnet werden, indem die Abfolge der Ereignisse beschrieben wird, die von der Risikoquelle erzeugt werden, um ihren DES zu erreichen. Die Beeinträchtigung der Geschäftswerte entspricht den endgültigen Ereignissen, während die Ereignisse, die das Ökosystem betreffen, Zwischenereignisse sind. Das strategische Szenario spiegelt eine Auswirkungenabschätzung wider, die sich direkt aus den betreffenden Ereignissen ergibt.

Diese Szenarien können in Form von Angriffsgraphen oder direkt in der Ökosystemansicht der Abbildung des Informationssystems dargestellt werden, indem die Angriffspfade übereinandergelegt werden.

Strategische Szenarien erfordern zusätzliche Überlegungen über die Wahrscheinlichkeit der Ereignisse. Der auf Werten basierende Ansatz und die damit verbundenen Betriebsszenarien können verwendet werden, um die Wahrscheinlichkeit von Ereignissen zu definieren. Die in A.2.5.1 dargestellten Beispiele für Bedrohungen können verwendet werden, um die notwendigen Beurteilungen zu erhalten.

A.2.5 Auf Werten basierender Ansatz

A.2.5.1 Beispiele für Bedrohungen

Tabelle A.10 enthält Beispiele für typische Bedrohungen. Die Liste kann im Zuge der Bedrohungsbeurteilung verwendet werden. Bedrohungen, die als Risikoquellen betrachtet werden, können vorsätzlich, unabsichtlich oder umweltbedingt (natürlicher Art) sein und z. B. zur Beschädigung oder zum Verlust von wesentlichen Diensten führen. In der Liste ist für jeden Bedrohungstypen angegeben, ob D (vorsätzlich, en: deliberate), A (unabsichtlich, en: accidental) oder E (umweltbedingt, en: environmental) maßgeblich ist. D wird für alle vorsätzlichen Aktionen verwendet, die auf Informationen und informationsbezogene Werte abzielen, A wird für alle menschlichen Aktionen verwendet, die unabsichtlich Informationen und informationsbezogene Werte beschädigen können, und E wird für alle Vorfälle verwendet, die nicht auf menschlichen Aktionen beruhen. Die Gruppen von Bedrohungen sind nicht nach Priorität geordnet.

Maßnahmen können Bedrohungen abschwächen, indem sie diese Bedrohungen von ihrem Handeln abhalten oder ihr Eintreten verhindern. Die Auswahl von Maßnahmen zur Risikominderung erfordert auch die Berücksichtigung von detektierenden und responsiven Maßnahmen zur Identifizierung, Reaktion, Eindämmung und Wiederherstellung nach Ereignissen. Detektive und responsive Maßnahmen sind eher mit Auswirkungen als mit Bedrohungen verbunden.

BEISPIEL Die Protokollierung und Überwachung ermöglicht die Identifizierung von Sicherheitsereignissen und die Reaktion darauf.

Tabelle A.10 — Beispiele für typische Bedrohungen

Kategorie	Nr.	Beschreibung der Bedrohung	Art der Risikoquelle[a]
Physikalische Bedrohungen	TP01	Brand	A, D, E
	TP02	Wasser	A, D, E
	TP03	Verschmutzung, schädliche Strahlung	A, D, E
	TP04	Schwerer Unfall	A, D, E
	TP05	Explosion	A, D, E
	TP06	Staub, Korrosion, Frost	A, D, E
Natürliche Bedrohungen	TN01	Klimatische Erscheinung	E
	TN02	Seismische Erscheinung	E
	TN03	Vulkanische Erscheinung	E
	TN04	Meteorologische Erscheinung	E
	TN05	Überschwemmung	E
	TN06	Pandemische/epidemische Erscheinung	E

Tabelle A.10 (*fortgesetzt*)

Kategorie	Nr.	Beschreibung der Bedrohung	Art der Risikoquelle[a]
Infrastruktur-ausfälle	TI01	Ausfall eines Versorgungssystems	A, D
	TI02	Ausfall eines Kühl- oder Lüftungssystems	A, D
	TI03	Ausfall einer Stromversorgung	A, D, E
	TI04	Ausfall eines Telekommunikationsnetzes	A, D, E
	TI05	Störung von Telekommunikationseinrichtungen	A, D
	TI06	Elektromagnetische Strahlung	A, D, E
	TI07	Wärmestrahlung	A, D, E
	TI08	Elektromagnetische Impulse	A, D, E
Technische Ausfälle	TT01	Ausfall eines Geräts oder Systems	A
	TT02	Vollständige Auslastung des Informationssystems	A, D
	TT03	Verletzung der Pflegbarkeit eines Informationssystems	A, D
Menschliche Aktionen	TH01	Terror, Angriff, Sabotage	D
	TH02	Social Engineering	D
	TH03	Abfangen der Strahlung eines Geräts	D
	TH04	Fernspionage	D
	TH05	Lauschangriff	D
	TH06	Diebstahl von Datenträgern oder Dokumenten	D
	TH07	Diebstahl von Geräten	D
	TH08	Diebstahl einer digitalen Identität oder digitaler Zugangsdaten	D
	TH09	Wiederherstellung von recycelten oder ausrangierten Datenträgern	D
	TH10	Offenlegung von Informationen	A, D
	TH11	Dateneingabe aus nicht vertrauenswürdigen Quellen	A, D
	TH12	Manipulationen an Hardware	D
	TH13	Manipulationen an Software	A, D
	TH14	Drive-by-Exploits mit webbasierter Kommunikation	D
	TH15	Replay-Angriff, Man-in-the-Middle-Angriff	D
	TH16	Unbefugte Verarbeitung personenbezogener Daten	A, D
	TH17	Unbefugtes Betreten von Einrichtungen	D
	TH18	Unbefugte Nutzung von Geräten	D
	TH19	Unsachgemäße Nutzung von Geräten	A, D
	TH20	Beschädigung von Geräten oder Datenträgern	A, D
	TH21	Betrügerische Vervielfältigung von Software	D
	TH22	Nutzung gefälschter oder kopierter Software	A, D
	TH23	Beschädigung von Daten	D
	TH24	Rechtswidrige Datenverarbeitung	D
	TH25	Versenden oder Verbreiten von Schadsoftware	A, D, R
	TH26	Standortbestimmung	D

Tabelle A.10 (*fortgesetzt*)

Kategorie	Nr.	Beschreibung der Bedrohung	Art der Risikoquelle[a]
Beeinträchtigung von Funktionen oder Diensten	TC01	Nutzungsfehler	A
	TC02	Missbrauch von Rechten oder Berechtigungen	A, D
	TC03	Fälschung von Rechten oder Berechtigungen	D
	TC04	Verweigerung von Aktionen	D
Organisatorische Bedrohungen	TO01	Personalmangel	A, E
	TO02	Ressourcenmangel	A, E
	TO03	Versagen von Dienstleistern	A, E
	TO04	Verstoß gegen Gesetze oder Vorschriften	A, D
[a] D = vorsätzlich; A = unbeabsichtigt; E = umweltbedingt.			

A.2.5.2 Beispiele für Schwachstellen

Tabelle A.11 enthält Beispiele für Schwachstellen in verschiedenen Sicherheitsbereichen einschließlich Beispielen für Bedrohungen, die diese Schwachstellen ausnutzen können. Die Listen können bei der Beurteilung von Bedrohungen und Schwachstellen helfen, um maßgebliche Risikoszenarien zu ermitteln. In einigen Fällen können diese Schwachstellen auch von anderen Bedrohungen ausgenutzt werden.

Tabelle A.11 — Beispiele für typische Schwachstellen

Kategorie	Nr.	Beispiele für Schwachstellen
Hardware	VH01	Unzureichende Wartung/fehlerhafte Installation von Speichermedien
	VH02	Unzureichende regelmäßige Austauschprogramme für Geräte
	VH03	Anfälligkeit für Feuchtigkeit, Staub, Verschmutzung
	VH04	Empfindlichkeit gegenüber elektromagnetischer Strahlung
	VH05	Unzureichende Kontrolle von Konfigurationsänderungen
	VH06	Anfälligkeit für Spannungsschwankungen
	VH07	Anfälligkeit für Temperaturschwankungen
	VH08	Ungeschützte Speicherung
	VH09	Mangelnde Sorgfalt bei der Entsorgung
	VH10	Unkontrollierte Vervielfältigung
Software	VS01	Keine oder unzureichende Softwaretests
	VS02	Bekannte Mängel in der Software
	VS03	Keine Abmeldung beim Verlassen des Arbeitsplatzes
	VS04	Entsorgung oder Wiederverwendung von Speichermedien ohne ordnungsgemäße Löschung
	VS05	Unzureichende Konfiguration von Protokollen für Prüfpfade
	VS06	Falsche Zuteilung von Zugriffsrechten
	VS07	Weit verbreitete Software
	VS08	Anwendung von Anwendungsprogrammen auf die zeitlich falschen Daten
	VS09	Komplizierte Benutzerschnittstelle
	VS10	Unzureichende oder fehlende Dokumentation

Tabelle A.11 (*fortgesetzt*)

Kategorie	Nr.	Beispiele für Schwachstellen
	VS11	Falsche Parametereinstellung
	VS12	Falsche Daten
	VS13	Unzureichende Identifizierungs- und Authentifizierungsmechanismen (z. B. für die Benutzerauthentifizierung)
	VS14	Ungeschützte Passworttabellen
	VS15	Schlechtes Passwortmanagement
	VS16	Unnötige Dienste aktiviert
	VS17	Unausgereifte oder neue Software
	VS18	Unklare oder unvollständige Spezifikationen für Entwickler
	VS19	Unwirksame Änderungskontrolle
	VS20	Unkontrolliertes Herunterladen und Verwenden von Software
	VS21	Fehlende oder unvollständige Sicherungskopien
	VS22	Nichtvorlage von Managementberichten
Netz	VN01	Unzureichende Mechanismen für den Nachweis des Versands oder des Eingangs einer Nachricht
	VN02	Ungeschützte Kommunikationsleitungen
	VN03	Ungeschützter sensibler Datenverkehr
	VN04	Schlechte Verkabelung
	VN05	Einzelner Ausfallpunkt
	VN06	Unwirksame oder fehlende Mechanismen zur Identifizierung und Authentifizierung von Absender und Empfänger
	VN07	Unsichere Netzwerkarchitektur
	VN08	Übertragung von Passwörtern im Klartext
	VN09	Unzureichendes Netzmanagement (Ausfallsicherheit des Routings)
	VN10	Ungeschützte öffentliche Netzverbindungen
Personal	VP01	Fehlendes Personal
	VP02	Unzulängliche Einstellungsverfahren
	VP03	Unzureichende Sicherheitsschulung
	VP04	Unsachgemäße Nutzung von Software und Hardware
	VP05	Mangelndes Sicherheitsbewusstsein
	VP06	Unzureichende oder fehlende Überwachungsmechanismen
	VP07	Unbeaufsichtigte Arbeit durch Fremd- oder Reinigungspersonal
	VP08	Unwirksame oder fehlende Richtlinien für die korrekte Nutzung von Telekommunikationsmedien und -nachrichtenübermittlung
Standort	VS01	Unzureichende oder nachlässige Anwendung der physischen Zugangskontrolle zu Gebäuden und Räumen
	VS02	Standort in einem hochwassergefährdeten Gebiet
	VS03	Instabiles Stromnetz
	VS04	Unzureichender physischer Schutz des Gebäudes, der Türen und Fenster
	VO01	Kein formelles Verfahren für die Registrierung und Registrierungsaufhebung von Benutzern entwickelt oder ineffiziente Umsetzung

Tabelle A.11 (*fortgesetzt*)

Kategorie	Nr.	Beispiele für Schwachstellen
Organisation	VO02	Kein formelles Verfahren für die Überprüfung der Zugriffsrechte (Überwachung) entwickelt oder nicht wirksam umgesetzt
	VO03	Unzureichende Bestimmungen (bezüglich der Sicherheit) in Verträgen mit Kunden und/oder Dritten
	VO04	Verfahren zur Überwachung der Informationsverarbeitungseinrichtungen nicht entwickelt oder nicht wirksam umgesetzt
	VO05	Nicht regelmäßig durchgeführte Audits (Überwachung)
	VO06	Verfahren zur Risikoidentifizierung und -beurteilung wurden nicht entwickelt oder wurden nicht wirksam umgesetzt
	VO07	Unzureichende oder fehlende Fehlerberichte in Administrator- und Bedienerprotokollen
	VO08	Unzureichende Reaktion auf die Wartung
	VO09	Unzureichende oder fehlende Dienstgütevereinbarung
	VO10	Kein Verfahren für die Änderungskontrolle entwickelt oder Verfahren nicht wirksam umgesetzt
	VO11	Kein formelles Verfahren zum Kontrollieren der ISMS-Dokumentation entwickelt oder unwirksam umgesetzt
	VO12	Kein formelles Verfahren für die Überwachung der ISMS-Aufzeichnungen entwickelt oder unwirksam umgesetzt
	VO13	Formales Verfahren zur Autorisierung von öffentlich zugänglichen Informationen nicht entwickelt oder nicht wirksam umgesetzt
	VO14	Unsachgemäße Zuweisung von Verantwortlichkeiten für die Informationssicherheit
	VO15	Es gibt keine Kontinuitätspläne, sie sind unvollständig oder veraltet.
	VO16	Keine Nutzungsrichtlinie für E-Mails entwickelt oder deren Umsetzung ist unwirksam
	VO17	Verfahren für die Einführung von Software in operative Systeme wurden nicht entwickelt oder ihre Umsetzung ist unwirksam
	VO18	Verfahren für den Umgang mit Verschlusssachen wurden nicht entwickelt oder ihre Umsetzung ist unwirksam
	VO19	Zuständigkeiten für die Informationssicherheit sind in den Stellenbeschreibungen nicht enthalten
	VO20	Unzureichende oder fehlende Bestimmungen (zur Informationssicherheit) in Verträgen mit Arbeitnehmern
	VO21	Disziplinarverfahren bei Vorfällen im Bereich der Informationssicherheit nicht definiert oder nicht ordnungsgemäß funktionierend
	VO22	Keine formelle Richtlinie für die Nutzung tragbarer Computer entwickelt oder unwirksam umgesetzt
	VO23	Unzureichende Kontrolle außerbetrieblicher Werte
	VO34	Unzureichende oder fehlende Richtlinie für eine „aufgeräumte Arbeitsumgebung und Bildschirmsperren“
	VO25	Autorisierung von Informationsverarbeitungsanlagen nicht umgesetzt oder sie funktionieren nicht ordnungsgemäß
	VO26	Überwachungsmechanismen für Sicherheitsverletzungen nicht ordnungsgemäß umgesetzt
	VO27	Verfahren für die Meldung von Sicherheitsschwächen wurden nicht entwickelt oder ihre Umsetzung ist unwirksam
	VO28	Verfahren zur Einhaltung der Bestimmungen zum Schutz der Rechte an geistigem Eigentum wurden nicht entwickelt oder ihre Umsetzung ist unwirksam

A.2.5.3 Verfahren für die Beurteilung technischer Schwachstellen

Proaktive Verfahren wie das Prüfen von Informationssystemen können zur Identifizierung von Schwachstellen eingesetzt werden, abhängig von der Kritikalität des IKT-Systems und den verfügbaren Ressourcen (z. B. zugewiesene Mittel, verfügbare Technologie, Personen mit dem nötigen Fachwissen zur Durchführung der Prüfung). Zu den Prüfverfahren gehören:

— automatisiertes Schwachstellen-Scan-Tool;

— Sicherheitsprüfung und -bewertung;

— Penetrationstests;

— Code-Überprüfung.

Ein automatisiertes Schwachstellen-Scan-Tool wird verwendet, um eine Gruppe von Hosts oder ein Netzwerk auf bekannte verwundbare Dienste zu scannen [z. B. System erlaubt anonymes Dateiübertragungsprotokoll (FTP, en: File Transfer Protocol), Sendmail-Relaying]. Einige der potentiellen Schwachstellen, die von einem automatisierten Scan-Tool identifiziert werden, stellen jedoch nicht unbedingt reale Schwachstellen im Kontext der Systemumgebung dar (z. B. bewerten einige dieser Scan-Tools potentielle Schwachstellen, ohne die Umgebung und die Anforderungen der Website zu berücksichtigen). Einige der Schwachstellen, die von der automatisierten Scansoftware angezeigt werden, können für eine bestimmte Website tatsächlich nicht anfällig sein, können aber so konfiguriert werden, weil ihre Umgebung dies erfordert. Dieses Prüfverfahren kann daher zu falsch-positiven Ergebnissen führen.

Die Sicherheitsprüfung und -bewertung (STE, en: Security Testing and Evaluation) ist eine weitere Technik, die bei der Identifizierung von Schwachstellen in IKT-Systemen während des Risikobeurteilungsprozesses eingesetzt werden kann. Sie umfasst die Entwicklung und Durchführung eines Prüfplans (z. B. Prüfskript, Prüfverfahren und erwartete Prüfergebnisse). Der Zweck von Sicherheitsprüfungen besteht darin, die Wirksamkeit der Sicherheitsmaßnahmen eines IKT-Systems zu prüfen, so wie sie in einer Betriebsumgebung angewendet wurden. Ziel ist es, sicherzustellen, dass die angewandten Maßnahmen den genehmigten Sicherheitsspezifikationen für die Software und Hardware entsprechen und, dass durch sie die Sicherheitsrichtlinien der Organisation umgesetzt oder den Industrienormen entsprochen wird.

Penetrationstests können die Überprüfung von Sicherheitsmaßnahmen ergänzen und sicherstellen, dass die verschiedenen Aspekte des IKT-Systems gesichert sind. Penetrationstests können, wenn sie im Rahmen der Risikobeurteilung eingesetzt werden, dazu dienen, die Fähigkeit eines IKT-Systems zu beurteilen, vorsätzlichen Versuchen zur Umgehung der Systemsicherheit standzuhalten. Ziel ist es, das IKT-System aus der Sicht einer Bedrohungsquelle zu prüfen und mögliche Schwachstellen in den Schutzsystemen des IKT-Systems zu identifizieren.

Die Codeüberprüfung ist das gründlichste (aber auch teuerste) Verfahren der Schwachstellenbeurteilung.

Die Ergebnisse dieser Art von Sicherheitsprüfung helfen, die Schwachstellen eines Systems zu identifizieren.

Penetrationstools und -techniken können falsche Ergebnisse liefern, wenn die Schwachstelle nicht erfolgreich ausgenutzt wird. Um bestimmte Schwachstellen ausnutzen zu können, ist es notwendig das genaue System/die Anwendung/die Patches zu kennen, die auf dem geprüften System installiert sind. Wenn diese Daten zum Zeitpunkt der Prüfung nicht bekannt sind, ist es nicht unbedingt möglich, eine bestimmte Schwachstelle erfolgreich auszunutzen (z. B. eine entfernte Reverse-Shell zu erhalten). Es ist jedoch immer noch möglich, einen geprüften Prozess oder ein System zum Absturz zu bringen oder neu zu starten. In einem solchen Fall sollte das geprüfte Objekt ebenfalls als verwundbar angesehen werden.

Zu den Verfahren können die folgenden Aufgaben gehören:

— Befragung von Personen und Nutzern;

— Fragebögen;

— physische Prüfung;

— Dokumentenanalyse.

A.2.5.4 Betriebsszenarien

Bei einem auf Werten basierenden Ansatz können Betriebsszenarien erstellt werden, indem die verschiedenen Pfade innerhalb der unterstützenden Werte analysiert werden, die Risikoquellen nutzen können, um die Geschäftswerte und deren DES zu erreichen.

Die Analyse dieser Szenarien kann helfen, den ereignisbasierten Ansatz zu vertiefen.

Ein erfolgreicher Angriff ist oft das Ergebnis der Ausnutzung mehrerer Schwachstellen. Vorsätzliche Angriffe basieren in der Regel auf einem Ansatz aufeinanderfolgender Aktionen. Letzterer nutzt auf koordinierte Weise mehrere Schwachstellen IT-technischer, organisatorischer oder physischer Natur aus. Ein solcher Ansatz, der auf der gleichzeitigen Ausnutzung einzelner Schwachstellen beruht, kann schwerwiegende Auswirkungen haben, auch wenn die ausgenutzten Schwachstellen für sich betrachtet unbedeutend sein können.

Die analysierten Szenarien können nach einem typischen Angriffsablauf strukturiert werden. Es gibt mehrere Modelle, die verwendet werden können (z. B. das Cyber-Kill-Chain-Modell[1]). Der Ansatz sollte es ermöglichen, die kritischen unterstützenden Werte zu identifizieren, die als Vektoren für das Eindringen oder die Ausnutzung bzw. als Ausbreitungsrelais für den modellierten Angriff verwendet werden können.

Diese Szenarien können in Form von Graphen oder Angriffsdiagrammen dargestellt werden, die für die Darstellung der Angriffsmethoden des Angreifers nützlich sind.

A.2.6 Beispiele für Szenarien, die in beiden Ansätzen anwendbar sind

Risikoszenarien können entweder mit einem ereignisbasierten Ansatz, einem auf Werten basierenden Ansatz oder mit beiden erstellt werden.

Bild A.4 zeigt die Risikobeurteilung anhand von Risikoszenarien.

1 Das Cyber-Kill-Chain-Modell ist der Handelsname eines von Lockheed Martin angebotenen Produkts. Diese Angabe dient nur zur Unterrichtung der Benutzer dieses Dokuments und bedeutet keine Anerkennung dieses genannten Produkts durch ISO. Gleichwertige Produkte dürfen verwendet werden, wenn nachgewiesen werden kann, dass sie zu denselben Ergebnissen führen.

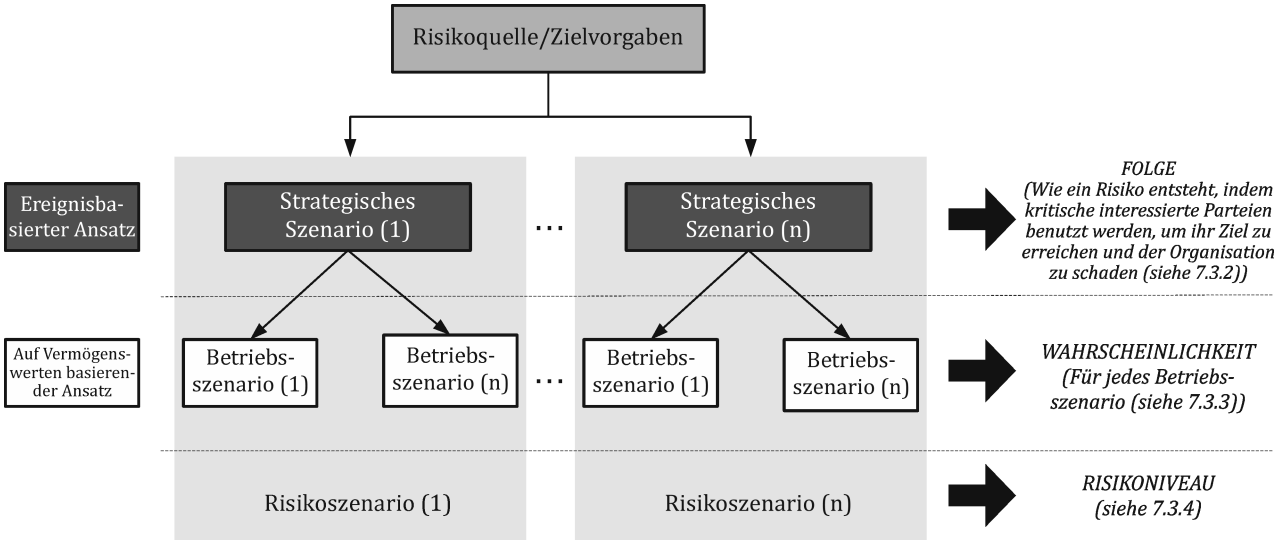


Bild A.4 — Risikobeurteilung anhand von Risikoszenarien

Tabelle A.12 zeigt Beispiele für Risikoszenarien und die Verbindungen zu den auf Werten basierenden bzw. ereignisbasierten Ansätzen und Risikoquellen.

Tabelle A.12 — Beispiele für Risikoszenarien in beiden Ansätzen

Risikoquelle	Zielvorgabe DES	Strategisches Risikoszenario (Ereignisbasierter Ansatz)	Operatives Risikoszenario (Auf Werten basierender Ansatz)
Autoritärer Staat	Aneignung eines strategischen Angriffsvektors	Unterwanderung kritischer Infrastruktur	Einsatz von versteckter und dauerhafter Schadsoftware in der Lieferkette
Organisierte Kriminalität	Entwicklung illegaler Tätigkeiten	Nutzung von Hafeninfrastruktur	Unterwanderung der Hafenarbeitergewerkschaft
			Übernahme der Kontrolle über ein computergestütztes System zur Steuerung des Warenflusses
		Steuerkarussellbetrug	Gründung von Briefkastenfirmen zur Durchführung von Scheinbörsen auf dem Emissionshandelsmarkt
		Erpressung	Verbreitung von Ransomware
Aggressive Geschäfte	Erlangung eines Marktmonopols	Einflussnahme auf die Regulierungsbehörde	Bestechung eines Entscheidungsträgers
		Ausschaltung von Wettbewerbern	Verleumdungskampagne in sozialen Netzwerken

A.2.7 Überwachung risikobehafteter Ereignisse

Die Überwachung risikobehafteter Ereignisse dient der Identifizierung von Faktoren, die ein Risikoszenario für die Informationssicherheit wie in 10.5.2 definiert beeinflussen können.

In diesem Zusammenhang werden Faktoren als eine Reihe von Elementen identifiziert, die es ermöglichen, ein unerwartetes Verhalten in Bezug auf einen bestimmten Wert zu erkennen, und die in die Überwachungsfähigkeiten und -instrumente der Organisation integriert werden können, um den Auslöser eines Risikoszenarios für die Informationssicherheit zu bestimmen.

Die Überwachung risikobehafteter Ereignisse kann anhand mehrerer Indikatoren definiert werden, die aus operativen oder strategischen Szenarien stammen und beide in 7.2.1 eingeführt wurden. Sie können unterschiedlicher Art sein (technisch, organisatorisch, verhaltensbezogen, Ergebnisse von Audits usw.). Die Überwachung von Ereignissen erfolgt nach festgelegten Prioritäten wie dem Ausmaß der Auswirkungen und der Wahrscheinlichkeit des Ereignisses.

Tabelle A.13 enthält ein Beispiel für die Beschreibung eines Risikoszenarios für die Informationssicherheit mit der zugehörigen Überwachung risikobehafteter Ereignisse.

Tabelle A.13 — Beispiel für ein Risikoszenario und eine Überwachung risikobehafteter Ereignisse

<table>
<tr><th>Risikokomponenten</th><th>Beispiele</th><th></th><th>Zu überwachende Ereignisse</th></tr>
<tr><td>Strategisches Szenario (ereignisbasiert)</td><td>Sensible Dokumente werden von einem Administrator vernichtet</td><td rowspan="13"></td><td rowspan="13"></td></tr>
<tr><td>Betroffene Ereignisse</td><td>Verlust wichtiger Dokumente</td></tr>
<tr><td>Schweregrad der Folge</td><td>Deskriptives Maß: hoch</td></tr>
<tr><td rowspan="3">Operative Szenarien (auf Werten basierend)</td><td>Nutzung von Administratorrechten, um die sensiblen Dokumente durch direkten Zugriff auf die Datenbank zu vernichten</td><td>– ></td><td>Erkennung eines direkten Zugriffs auf die Datenbank außerhalb der üblichen Arbeitszeiten</td></tr>
<tr><td>Root-Zugriff, um das Systemdatum/die Systemuhrzeit zu ändern</td></tr>
<tr><td>Infektion mit Schadsoftware des Arbeitsplatzes des Administrators mit Ausbreitung auf die Datenbank</td><td>– ></td><td>Erkennung von Operationen, die sich auf eine große Menge von Daten auswirken (Vernichtung)</td></tr>
<tr><td>Wahrscheinlichkeit</td><td>Deskriptives Maß: mittel</td></tr>
<tr><td>Risikoquelle</td><td>Administrator</td></tr>
<tr><td>Zielvorgabe</td><td>Kompromittierung der Verfügbarkeit sensibler Dokumente</td></tr>
<tr><td>DES</td><td>Kompromittierung des Systems</td></tr>
<tr><td rowspan="5">Sicherheitsmaßnahmen</td><td>Implementierung einer Sicherungsstrategie</td></tr>
<tr><td>Lösung zum Schutz vor Schadsoftware</td></tr>
<tr><td>NTP-Implementierung</td></tr>
<tr><td>Härtung des Betriebssystems</td></tr>
<tr><td>Einschränkung der Zugriffsrechte auf Betriebsdaten</td></tr>
</table>

Das Modell Quelle-Funktion-Ziel-Auslöser (SFDT, en: source-function-destination-trigger) ermöglicht die Überwachung risikobehafteter Ereignisse, wobei:

— Quelle: angibt, woher das Ereignis/die Technik kommt (wer und warum?) und mit A.2.3-Ressourcen in Verbindung gebracht werden kann;

— Funktion: angibt, welche Art von Ereignis/Technik der Angreifer nutzt (was?);

— Ziel: angibt, wo die Technik oder das Ereignis durchgeführt wird (auf welchen primären Hilfsmitteln?);

— Auslöser: angibt, unter welchen Bedingungen das Risikoszenario erkannt und identifiziert werden kann (Ergebnisse des Angriffs).

Ein Beispiel für die Anwendung des SFDT-Modells ist in Bild A.5 dargestellt.

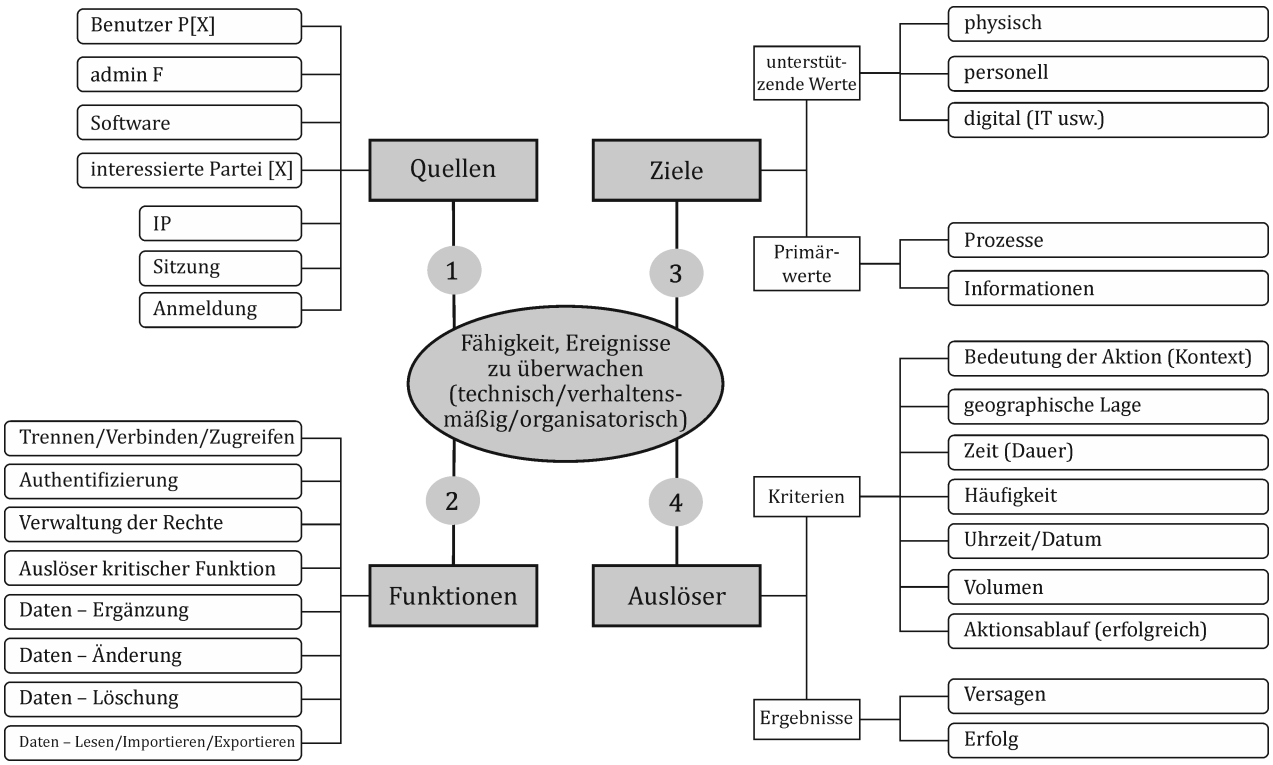


Bild A.5 — Beispiel für die Anwendung des SFDT-Modells

Um sicherzustellen, dass ein risikobehaftetes Überwachungsereignis effektiv und effizient ist, um ein Risikoszenario im Bereich der Informationssicherheit zu überwachen, ist es notwendig, die Indikatoren dafür zu bestimmen.

Indikatoren für die Überwachung risikobehafteter Ereignisse:

— Risikoniveau des überwachten Risikoszenarios;

— Wirksamkeit, Fähigkeit der risikobehafteten Ereignisse zur Überwachung eines Risikoszenarios;

— Effizienz, Verhältnis zwischen echten positiven Alarmen und falschen positiven Alarmen oder die Kosten der Charakterisierung.

Literaturhinweise

[1] ISO 17666:2016, *Space systems — Risk management*

[2] ISO/IEC 27001:2022, *Information technology — Security techniques — Information security management systems — Requirements*

[3] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[4] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27014, *Information security, cybersecurity and privacy protection — Governance of information security*

[6] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[7] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[8] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[9] ISO 31000:2018, *Risk management — Guidelines*

[10] IEC 31010:2019, *Risk management — Risk assessment techniques*

[11] ISO Guide 73:2009, *Risk management — Vocabulary*