

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                           |                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | DIN EN ISO/IEC 27005      |  |
| ICS 03.100.70; 35.030                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Einsprüche bis 2024-06-05 |                                                                                     |
| <div>Entwurf</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                           |                                                                                     |
| <p><b>Informationssicherheit, Cybersicherheit und Datenschutz –<br/>Leitfaden zur Handhabung von Informationssicherheitsrisiken<br/>(ISO/IEC 27005:2022);<br/>Deutsche und Englische Fassung prEN ISO/IEC 27005:2024</b></p> <p>Information security, cybersecurity and privacy protection –<br/>Guidance on managing information security risks (ISO/IEC 27005:2022);<br/>German and English version prEN ISO/IEC 27005:2024</p> <p>Sécurité de l’information, cybersécurité et protection de la vie privée –<br/>Préconisations pour la gestion des risques liés à la sécurité de l’information<br/>(ISO/IEC 27005:2022);<br/>Version allemande et anglaise prEN ISO/IEC 27005:2024</p> <p><b>Anwendungswarnvermerk</b></p> <p>Dieser Entwurf mit Erscheinungsdatum 2024-04-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.</p> <p>Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.</p> <p>Stellungnahmen werden erbeten</p> <ul style="list-style-type: none"><li>– vorzugsweise online im Norm-Entwurfs-Portal von DIN unter <a href="http://www.din.de/go/entwuerfe">www.din.de/go/entwuerfe</a> bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter <a href="http://www.entwuerfe.normenbibliothek.de">www.entwuerfe.normenbibliothek.de</a>, sofern dort wiedergegeben;</li><li>– oder als Datei per E-Mail an <a href="mailto:nia@din.de">nia@din.de</a> möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <a href="http://www.din.de/go/stellungnahmen-norm-entwuerfe">www.din.de/go/stellungnahmen-norm-entwuerfe</a> oder für Stellungnahmen zu Norm-Entwürfen der DKE unter <a href="http://www.dke.de/stellungnahme">www.dke.de/stellungnahme</a> abgerufen werden;</li><li>– oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.</li></ul> <p>Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.</p> <p>Gesamtumfang 148 Seiten</p> <p>DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)</p> |                           |                                                                                     |

## 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 prEN ISO/IEC 27005:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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](http://www.din.de)) durch eine Suche nach der Dokumentennummer aufgerufen werden.

## 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 –

April 2024

**prEN ISO/IEC 27005**

**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)

## Inhalt

|                                                                                                                                                      | Seite |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort . . . . .                                                                                                                       | 4     |
| Vorwort . . . . .                                                                                                                                    | 5     |
| Einleitung . . . . .                                                                                                                                 | 7     |
| 1 Anwendungsbereich . . . . .                                                                                                                        | 8     |
| 2 Normative Verweisungen . . . . .                                                                                                                   | 8     |
| 3 Begriffe . . . . .                                                                                                                                 | 8     |
| 3.1 Begriffe im Zusammenhang mit Informationssicherheitsrisiken . . . . .                                                                            | 8     |
| 3.2 Begriffe im Zusammenhang mit der Handhabung von Informationssicherheitsrisiken . . . . .                                                         | 12    |
| 4 Aufbau dieses Dokuments . . . . .                                                                                                                  | 14    |
| 5 Handhabung von Informationssicherheitsrisiken . . . . .                                                                                            | 15    |
| 5.1 Prozess zur Handhabung von Informationssicherheitsrisiken . . . . .                                                                              | 15    |
| 5.2 Zyklen des Informationssicherheitsrisikomanagements . . . . .                                                                                    | 17    |
| 6 Kontextfestlegung . . . . .                                                                                                                        | 18    |
| 6.1 Organisatorische Aspekte . . . . .                                                                                                               | 18    |
| 6.2 Identifizierung grundlegender Anforderungen von interessierten Parteien . . . . .                                                                | 18    |
| 6.3 Anwendung der Risikobeurteilung . . . . .                                                                                                        | 19    |
| 6.4 Festlegung und Aufrechterhaltung der Informationssicherheitsrisikokriterien . . . . .                                                            | 19    |
| 6.4.1 Allgemeines . . . . .                                                                                                                          | 19    |
| 6.4.2 Risikoakzeptanzkriterien . . . . .                                                                                                             | 19    |
| 6.4.3 Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen . . . . .                                                        | 21    |
| 6.5 Wahl eines angemessenen Verfahrens . . . . .                                                                                                     | 24    |
| 7 Prozess zur Beurteilung von Informationssicherheitsrisiken . . . . .                                                                               | 25    |
| 7.1 Allgemeines . . . . .                                                                                                                            | 25    |
| 7.2 Identifizierung von Informationssicherheitsrisiken . . . . .                                                                                     | 26    |
| 7.2.1 Identifizierung und Beschreibung von Informationssicherheitsrisiken . . . . .                                                                  | 26    |
| 7.2.2 Identifizierung von Risikoeigentümern . . . . .                                                                                                | 28    |
| 7.3 Analyse von Informationssicherheitsrisiken . . . . .                                                                                             | 29    |
| 7.3.1 Allgemeines . . . . .                                                                                                                          | 29    |
| 7.3.2 Beurteilung potentieller Folgen . . . . .                                                                                                      | 29    |
| 7.3.3 Beurteilung der Wahrscheinlichkeit . . . . .                                                                                                   | 30    |
| 7.3.4 Bestimmung der Risikoniveaus . . . . .                                                                                                         | 32    |
| 7.4 Bewertung der Informationssicherheitsrisiken . . . . .                                                                                           | 32    |
| 7.4.1 Vergleich der Ergebnisse der Risikoanalyse mit den Risikokriterien . . . . .                                                                   | 32    |
| 7.4.2 Priorisierung der analysierten Risiken für die Risikobehandlung . . . . .                                                                      | 33    |
| 8 Prozess zur Informationssicherheitsrisikobehandlung . . . . .                                                                                      | 34    |
| 8.1 Allgemeines . . . . .                                                                                                                            | 34    |
| 8.2 Auswahl geeigneter Optionen zur Behandlung von Informationssicherheitsrisiken . . . . .                                                          | 34    |
| 8.3 Festlegung aller Maßnahmen, die zur Umsetzung der gewählten Optionen für die Informationssicherheitsrisikobehandlung erforderlich sind . . . . . | 35    |
| 8.4 Vergleich der festgelegten Maßnahmen mit denen in ISO/IEC 27001:2022, Anhang A . . . . .                                                         | 38    |
| 8.5 Erstellung einer Erklärung zur Anwendbarkeit . . . . .                                                                                           | 39    |
| 8.6 Handlungsplan für Informationssicherheitsrisiken . . . . .                                                                                       | 39    |
| 8.6.1 Ausarbeitung des Risikobehandlungsplans . . . . .                                                                                              | 39    |
| 8.6.2 Zustimmung durch die Risikoeigentümer . . . . .                                                                                                | 41    |
| 8.6.3 Akzeptanz der Restrisiken für die Informationssicherheit . . . . .                                                                             | 41    |
| 9 Betrieb . . . . .                                                                                                                                  | 42    |
| 9.1 Durchführung des Prozesses zur Risikobeurteilung der Informationssicherheit . . . . .                                                            | 42    |
| 9.2 Durchführung des Prozesses zur Risikobehandlung der Informationssicherheit . . . . .                                                             | 43    |
| 10 Nutzung verbundener ISMS-Prozesse . . . . .                                                                                                       | 43    |
| 10.1 Kontext der Organisation . . . . .                                                                                                              | 43    |
| 10.2 Führung und Verpflichtung . . . . .                                                                                                             | 44    |

|                                                                                                 |                                                                      |    |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----|
| 10.3                                                                                            | Kommunikation und Konsultation                                       | 45 |
| 10.4                                                                                            | Dokumentierte Informationen                                          | 47 |
| 10.4.1                                                                                          | Allgemeines                                                          | 47 |
| 10.4.2                                                                                          | Dokumentierte Informationen über Prozesse                            | 47 |
| 10.4.3                                                                                          | Dokumentierte Informationen über Ergebnisse                          | 48 |
| 10.5                                                                                            | Überwachen und Überprüfen                                            | 48 |
| 10.5.1                                                                                          | Allgemeines                                                          | 48 |
| 10.5.2                                                                                          | Überwachung und Überprüfung der die Risiken beeinflussenden Faktoren | 49 |
| 10.6                                                                                            | Managementbewertung                                                  | 50 |
| 10.7                                                                                            | Korrekturmaßnahme                                                    | 51 |
| 10.8                                                                                            | Fortlaufende Verbesserung                                            | 51 |
| Anhang A (informativ) Beispiele für Techniken zur Unterstützung des Risikobeurteilungsprozesses |                                                                      | 54 |
| A.1                                                                                             | Risikokriterien für die Informationssicherheit                       | 54 |
| A.1.1                                                                                           | Kriterien im Zusammenhang mit der Risikobeurteilung                  | 54 |
| A.1.2                                                                                           | Risikoakzeptanzkriterien                                             | 59 |
| A.2                                                                                             | Praktische Verfahren                                                 | 60 |
| A.2.1                                                                                           | Risikokomponenten für die Informationssicherheit                     | 60 |
| A.2.2                                                                                           | Vermögenswerte                                                       | 60 |
| A.2.3                                                                                           | Risikoquellen und gewünschter Endzustand                             | 62 |
| A.2.4                                                                                           | Ereignisbasierter Ansatz                                             | 65 |
| A.2.5                                                                                           | Auf Vermögenswerten basierender Ansatz                               | 67 |
| A.2.6                                                                                           | Beispiele für Szenarien, die in beiden Ansätzen anwendbar sind       | 74 |
| A.2.7                                                                                           | Überwachung risikobehafteter Ereignisse                              | 75 |
| Literaturhinweise                                                                               |                                                                      | 78 |

## Bilder

|          |                                                                  |    |
|----------|------------------------------------------------------------------|----|
| Bild 1   | Prozess zur Handhabung von Informationssicherheitsrisiken        | 16 |
| Bild A.1 | Komponenten für die Risikobeurteilung der Informationssicherheit | 60 |
| Bild A.2 | Beispiel eines Diagramms der Abhängigkeiten von Vermögenswerten  | 62 |
| Bild A.3 | Identifizierung der interessierten Parteien des Ökosystems       | 66 |
| Bild A.4 | Risikobeurteilung anhand von Risikoszenarien                     | 75 |
| Bild A.5 | Beispiel für die Anwendung des SFDT-Modells                      | 77 |

## Tabellen

|              |                                                                                     |    |
|--------------|-------------------------------------------------------------------------------------|----|
| Tabelle A.1  | Beispiel einer Folgenskala                                                          | 54 |
| Tabelle A.2  | Beispiel einer Wahrscheinlichkeitsskala                                             | 55 |
| Tabelle A.3  | Beispiel für einen qualitativen Ansatz bei den Risikokriterien                      | 56 |
| Tabelle A.4  | Beispiel einer logarithmischen Wahrscheinlichkeitsskala                             | 58 |
| Tabelle A.5  | Beispiel einer logarithmischen Folgenskala                                          | 58 |
| Tabelle A.6  | Beispiel für eine Bewertungsskala in Kombination mit einer Drei-Farben-Risikomatrix | 59 |
| Tabelle A.7  | Beispiele und übliche Angriffsmethoden                                              | 62 |
| Tabelle A.8  | Beispielhafte Klassifizierung von Motivationen, die den DES zum Ausdruck bringen    | 64 |
| Tabelle A.9  | Beispiele für Zielvorgaben                                                          | 64 |
| Tabelle A.10 | Beispiele für typische Bedrohungen                                                  | 67 |
| Tabelle A.11 | Beispiele für typische Schwachstellen                                               | 69 |
| Tabelle A.12 | Beispiele für Risikoszenarien in beiden Ansätzen                                    | 75 |
| Tabelle A.13 | Beispiel für ein Risikoszenario und eine Überwachung risikobehafteter Ereignisse    | 76 |

## **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 prEN ISO/IEC 27005:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

### **Anerkennungsnotiz**

Der Text von ISO/IEC 27005:2022 wurde von CEN als prEN 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](http://www.iso.org/directives) oder [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In der IEC, siehe [www.iec.ch/understanding-standards](http://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 Vermögenswerten basierenden Ansatz zur Risikoidentifizierung gegenübergestellt;
- der Inhalt der Anhänge wurde überarbeitet und in einem einzigen Anhang zusammengefasst.

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

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](http://www.iso.org/members.html) und [www.iec.ch/national-committees](http://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 helfen soll,

- 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 Ungewissheit 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 eines *Ereignisses* (3.1.11) oder Wissen über ein *Ereignis* (3.1.11), seine *Folgen* (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 alleine 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 *Folgen* (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 einem bestimmten Zeitraum) beschrieben wird.

Anmerkung 2 zum Begriff: Der englische Begriff „likelihood“ hat in einigen Sprachen keine direkte Entsprechung, wo für „likelihood“ (subjektive Wahrscheinlichkeit) und „probability“ (objektive, mathematische Wahrscheinlichkeit) oft ein und dasselbe Wort verwendet wird. In der englischen Sprache ist der Begriff „probability“ jedoch oftmals sehr eng als mathematischer Begriff definiert. 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), das 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 *Folgen* (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

#### **Maßnahme**

Mittel, das das *Risiko* (3.1.3) beibehält und/oder verändert

Anmerkung 1 zum Begriff: Maßnahmen umfassen unter anderem alle Prozesse, Richtlinien, Geräte, Verfahren oder andere Bedingungen und/oder Aktionen, die Risiken beibehalten oder verändern.

Anmerkung 2 zum Begriff: Maßnahmen haben möglicherweise nicht immer den erwünschten oder angenommenen verändernden Effekt.

[QUELLE: ISO 31000:2018, 3.8]

### 3.1.17

#### **Restrisiko**

*Risiko* (3.1.3), das nach einer *Risikobehandlung* (3.2.7) übrig bleibt

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 -absprache**

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 Absprachen 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 Absprache 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 zum Finden, Erkennen und Beschreiben von *Risiken* (3.1.3)

Anmerkung 1 zum Begriff: Die Risikoidentifizierung beinhaltet die Identifizierung der *Risikquellen* (3.1.6), der *Ereignisse* (3.1.11), ihrer Ursachen und möglichen *Folgen* (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, der die Ergebnisse der *Risikoanalyse* (3.2.5) mit den *Risikokriterien* (3.1.7) vergleicht, 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 *Folgen* (3.1.14);
- Teilen des Risikos mit einer anderen Partei oder anderen Parteien (einschließlich Verträgen und Risikofinanzierung); und
- Beibehalten des Risikos auf Grundlage einer fundierten 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.

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

Anmerkung 3 zum Begriff: Risikobehandlungen, die sich mit negativen Folgen beschäftigen, werden manchmal auch als „Risikominderung“, „Risikoeeliminierung“, „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**

fundierte 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), die die eine 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: Nutzung 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.

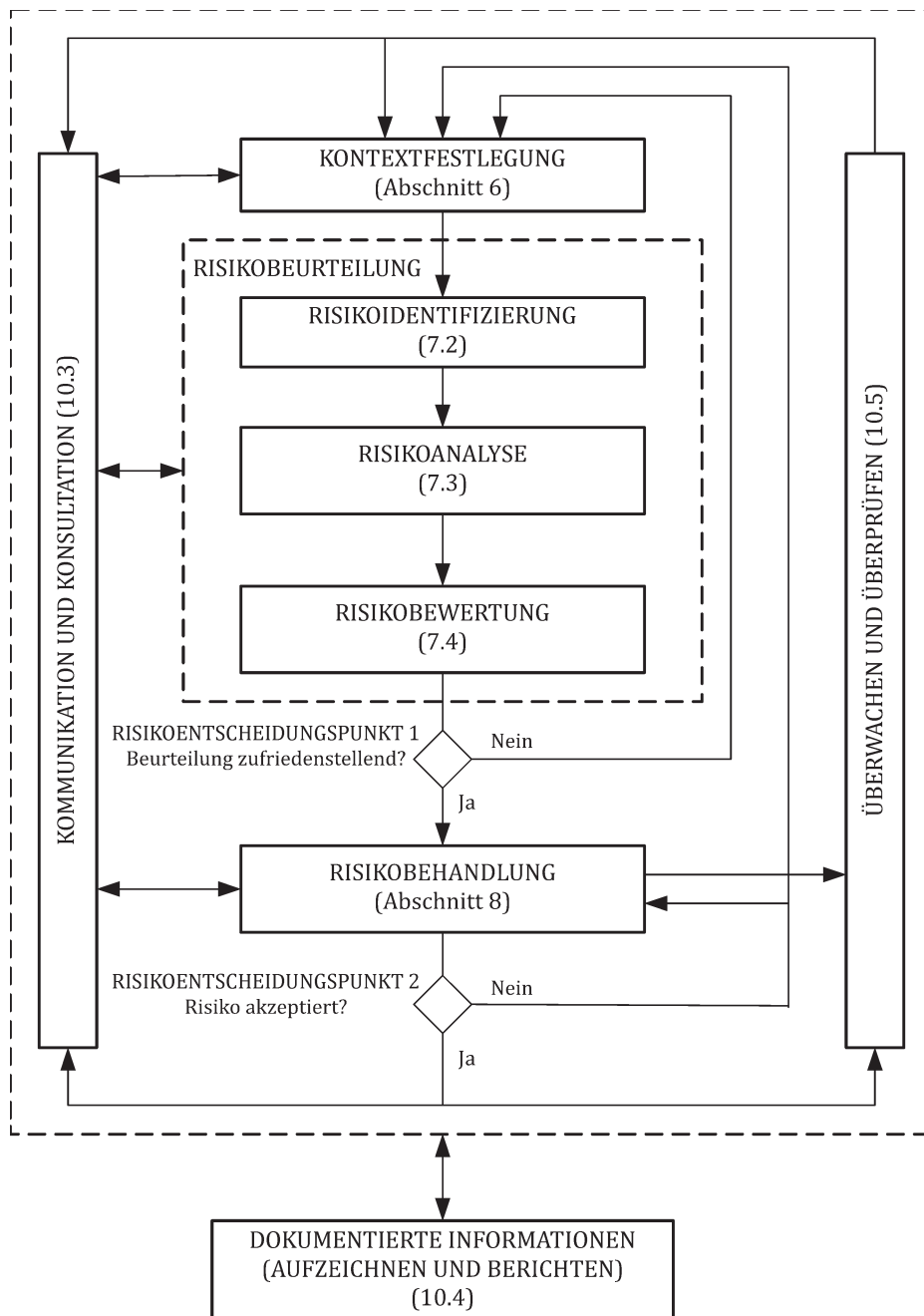


**Bild 1 — Prozess zur Handhabung von Informationssicherheitsrisiken**

Wie 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 auf der Grundlage von 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 Folgen 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;
- Betriebszyklus, 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 des 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 gelten (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 Aufgaben zur Risikobehandlung umgesetzt wurden.

Sämtliche Compliance-Verstöße gegen die 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, spezifisches Thema. Unabhängig davon, wie die Risikobeurteilungen durchgeführt werden, sollten sie insgesamt 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 Kapazität 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).

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

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 der Wahrscheinlichkeit und den Folgen 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 Folgen). Es kann jedoch Umstände geben, unter denen es notwendig ist, Schwellenwerte für die Akzeptanz extremer Folgen unabhängig von ihrer Wahrscheinlichkeit oder extrem hoher Wahrscheinlichkeiten ungeachtet der Folgen festzulegen, wobei die Auswirkungen 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 Anforderung 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 Folgen unabhängig voneinander sowie die Kosten für die Handhabung berücksichtigen und nicht nur die Höhe des Risikos als eine Kombination aus Wahrscheinlichkeit und Folgen.

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 Folgen, 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 Folgen 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 Folgen;
- 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 Folgen, 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 Folgen verwendet werden, wie sie definiert werden und welche Folgen 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 Folgen 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 Folgen 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 gleichwertige Folgeniveaus 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 Folgen 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 Folgen, 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 Folgen 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. Die gebräuchlichsten Ansätze zur Handhabung von Informationssicherheitsrisiken verwenden das aktuelle Risiko, um die Wahrscheinlichkeit und die Folgen 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 Folgen 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 des Risikos 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 Folgen hat, und der Schweregrad dieser Folgen 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.

ISO/IEC 27001 schreibt keinen bestimmten Ansatz vor, 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 Vermögenswerten 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 versteht man den Prozess zum Finden, Erkennen und Beschreiben von Risiken. 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 Folgen identifiziert und beurteilt werden können. Ereignisse und Folgen lassen sich häufig durch Fest-

stellung 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 Folgen, sondern auch die Risikoeigentümer zu identifizieren.

Mit 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. Die Bewertung von Ereignissen nach diesem Ansatz kann auf historische Daten zurückgreifen, bei denen die Risiken über lange Zeitspannen unverändert bleiben, und ermöglicht es den interessierten Parteien, 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 Vermögenswerten basierenden Ansatz liegt das Konzept zugrunde, dass Risiken durch eine Prüfung von Vermögenswerten, Bedrohungen und Schwachstellen identifiziert und beurteilt werden können. Ein Vermögenswert ist alles, was einen Wert für die Organisation hat und daher geschützt werden muss. Bei der Identifizierung von Vermögenswerten ist zu berücksichtigen, dass ein Informationssystem aus Aufgaben, Prozessen und zu schützenden Informationen besteht. Die Vermögenswerte können je nach Art und Priorität als primäre und unterstützende Vermögenswerte 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 Vermögenswerts aus, um die Vertraulichkeit, Integrität und/oder Verfügbarkeit der entsprechenden Informationen zu gefährden. Wenn alle gültigen Kombinationen von Vermögenswerten, 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 Vermögenswerten erstellt werden, die mit Informationen und informationsverarbeitenden Einrichtungen verbunden sind.

Mit dem auf Vermögenswerten basierenden Ansatz können vermögenswertspezifische 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 Vermögenswerten basierenden Beurteilung in der Regel eine Aufwärtssuche vom Vermögenswert bis zum Szenario erfolgt, um einen Überblick darüber zu erhalten, wie sich die Folgen 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 er die Erzielung konsistenter, gültiger und vergleichbarer Ergebnisse sicherstellt und die Anforderung von ISO/IEC 27001:2022, 6.1.2 b) erfüllt.

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

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 Folgen) 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 Vermögenswerten 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, fundierte Entscheidungen zu treffen (z. B. über die Behandlung der Risiken).

Das Risikoniveau und die Frage, für welchen Vermögenswert 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. ISO/IEC 27001:2022, 6.1.2, schreibt vor, dass die Risikoanalyse für jedes identifizierte Risiko auf der Beurteilung der sich aus dem Risiko ergebenden Folgen und der Beurteilung der Wahrscheinlichkeit des Risikos beruht, um ein Risikoniveau zu bestimmen.

Techniken zur Risikoanalyse auf der Grundlage von Folgen 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 Folgen. Um eine effiziente Entscheidungsfindung beim Risikomanagement zu ermöglichen, kann es ausreichen, erste und grobe Schätzungen der Wahrscheinlichkeit und der Folgen vorzunehmen.

### 7.3.2 Beurteilung potentieller Folgen

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

Auslöser: Die Beurteilung der Folgen wird notwendig, wenn:

- sie bisher noch nicht erfolgt ist;
- die durch die „Risikoidentifizierung“ erstellte Liste geändert wird;

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

- Risikoeigentümer oder interessierte Parteien die Einheiten geändert haben, in denen sie die Folgen festlegen wollen, oder
- Änderungen des Anwendungsbereichs oder des Kontexts festgestellt werden, die sich auf die Folgen auswirken.

Ausgabe: Eine Liste potentieller Folgen im Zusammenhang mit Risikoszenarien mit ihren Folgen für Vermögenswerte 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 Folgen für die Organisation und deren Ziele haben. Die Folgenanalyse kann ausgehend von den Folgen 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 Folgen abschätzen, wenn das Ereignis eintritt. Folgende Elemente sollte 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 Verwendungstatus.

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

Auslöser: Neben den Folgen 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 Folgen 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. Schwermriminalität, 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 bössartiger 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 Folgen eines Informationssicherheitsereignisses hängt in der Regel von der Wahrscheinlichkeit potentiell mehrerer untergeordneter Ereignisse und deren Folgen ab. Anstatt zu versuchen, die Wahrscheinlichkeit geschäftlicher Folgen 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 Folgen für Vermögenswerte oder Ereignisse und deren Wahrscheinlichkeit (quantitativ oder qualitativ).

Aktion: Das Risikoniveau sollte als eine Kombination aus der beurteilten Wahrscheinlichkeit und den beurteilten Folgen 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 Niveauewerten.

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 Folgen für alle maßgeblichen Risikoszenarien bestimmt. Alternative Berechnungen können sowohl einen Vermögenswert 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 Niveauewerten.

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 Folgen 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 einen bestimmten Zeitraum 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 Folgen 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 besteht. 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 man nachfragt,

- 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;

**E DIN EN ISO/IEC 27005:2024-05**  
**prEN ISO/IEC 27005:2024 (D)**

- 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, detektiv und korrektiv eingestuft werden:

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

- b) **detektive Maßnahme:** eine Maßnahme, die dazu dient, das Auftreten eines Informationssicherheitsereignisses zu erkennen;
- c) **korrektive Maßnahme:** eine Maßnahme, die die Folgen 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, detektive 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, detektiven und korrektiven Maßnahmen:

- detektive Maßnahmen sollten das Risiko mindern, wenn die präventiven Maßnahmen versagen;
- korrektive Maßnahmen sollten das Risiko mindern, wenn die detektiven 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 detektive Maßnahmen umgesetzt werden. Wenn es nicht möglich ist, ein Ereignis zu erkennen, können detektive 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 man nicht wissen, 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 detektive 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 detektiven Maßnahmen fehlschlagen, hat das wahrscheinlich eine oder mehrere unerwünschte Folgen. Die Implementierung der korrektiven Maßnahmen kann dazu beitragen, diese Folgen zu begrenzen. Obwohl korrektive Maßnahmen erst nach dem Eintreten der Folgen 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 Folgen. 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 Folgen 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 Folgen 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 Folgen 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 Maß-

nahmen 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 Ausschlüsse von Maßnahmen aus ISO/IEC 27001:2022, Anhang A.

Die SOA kann leicht erstellt werden, indem man die Risikobeurteilung untersucht, um die notwendigen Maßnahmen zu identifizieren, und indem man den Risikobehandlungsplan untersucht, um die Maßnahmen zu identifizieren, die umgesetzt werden sollen. 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 Vermögenswerten (z. B. verschiedene Pläne für verschiedene Klassifizierungen von Vermögenswerten) oder nach Ereignissen (wie bei der Risikobeurteilung nach der ereignisbasierten Methode) 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 Vermögenswert 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: Die 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 Folgen einfließen. Die in den Risikobehandlungsplänen vorgeschlagenen Maßnahmen und ihre Wirksamkeit sollten unter dem Gesichtspunkt betrachtet werden, ob sie die Wahrscheinlichkeit oder die Folgen 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.