Informationssicherheitsmanagement nach ISO 27001

Norm, Umsetzung, Best Practices

Kapitel 4
Begriffe zur Informationssicherheit

Informationen sind für Unternehmen heute Gold wert. Daher müssen sie ihre Informationen über den gesamten Lebenszyklus steuern und schützen. Dabei geht es nicht nur um die Vertraulichkeit, sondern auch um die Integrität und die Verfügbarkeit dieser Informationen im richtigen Moment.

4.1 Was sind Informationen?

Der Begriff *Information* ist heutzutage allgegenwärtig und wird häufig im Zusammenhang mit »Informationszeitalter« oder »Informationsaustausch« verwendet – aber was bedeutet er eigentlich genau? Besonders im Bereich der Informationssicherheit ist ein klares Verständnis dieses Begriffs von entscheidender Bedeutung: Alle Maßnahmen und Schutzkonzepte zielen letztendlich darauf ab, Informationen zu sichern. Ohne eine genaue Vorstellung davon, was eine Information ist, bleibt unklar, was überhaupt gesichert werden soll.

Praxistipp

In der Informationssicherheit werden die Begriffe *Daten* und *Informationen* oft synonym verwendet, obwohl sie nicht dasselbe bedeuten:

- **Daten** sind zunächst einmal rohe, unverarbeitete Zeichen, Zahlen oder Messwerte, die noch keine unmittelbare Bedeutung haben.
- **Informationen** entstehen erst durch Kontext, Interpretation und Nutzung.

Abbildung 4.1 zeigt, wie aus Zeichen Information entsteht. Der Mensch hat schon früh begonnen, Zeichen zu malen. So zum Beispiel die Ägypter. Nur wer wusste, wie diese Zeichen zu interpretieren sind, konnte aus ihnen etwas herauslesen. Diesen Zeichen wurde somit eine Bedeutung zugewiesen. Daraus entstand Information.

Eine *Information* ist also mehr als nur ein Datenpunkt. Sie entsteht erst durch Kontext, Interpretation und Bedeutung. *Daten* sind zunächst nur rohe, ungeordnete Zeichen, etwa Zahlen, Wörter oder Symbole. Erst wenn diese Daten in einen sinnvollen Zusammenhang gebracht werden, also wenn sie von einem Menschen oder einer Maschine interpretiert werden können, sprechen wir von Information. Ein Beispiel macht das deutlich: Die Zahl »42« ist für sich genommen ein Datum. Erst wenn wir wissen, dass sie sich auf das Alter einer Person, den Preis eines Produkts oder die Temperatur in Grad Celsius bezieht, wird daraus eine Information.

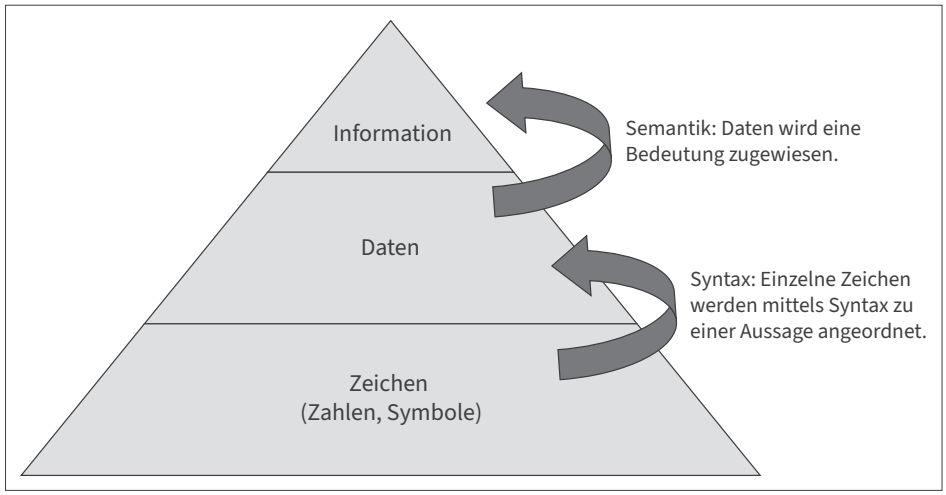

Abbildung 4.1: Entstehen von Information (angelehnt an Raffael Herrmann, http://www.derwirtschaftsinformatiker.de)

Information kann in verschiedenen Formaten existieren, digital als E-Mail oder als Datensätze sowie physisch auf Papier oder Whiteboards. Sie kann sogar mündlich in Besprechungen oder Gesprächen in der Kaffeeküche übermittelt werden. Für die Sicherheit von Informationen ist es wichtig zu beachten, dass nicht nur digitale Systeme geschützt werden sollten.

Ein wesentlicher Aspekt von Informationen ist ihr *Wert*. Nicht alle Informationen sind gleich schützenswert. Der Schutzbedarf einer öffentlich verfügbaren Marketingbroschüre ist ein anderer als der Schutzbedarf eines vertraulichen Vertragsdokuments oder eines Konstruktionsplans. Die Schutzwürdigkeit einer Information hängt dabei maßgeblich von ihrer Vertraulichkeit, ihrem Einfluss auf das Unternehmen und ihrer Relevanz für Dritte ab. Aus diesem Grund ist es in der Informationssicherheit von entscheidender Bedeutung, Informationen zu klassifizieren. Um geeignete Schutzmaßnahmen definieren und umsetzen zu können, ist es unerlässlich, im Vorfeld festzulegen, welche Informationen als besonders kritisch einzustufen sind. In Abschnitt 7.2.12, »NA A.5.12 – Klassifizierung von Informationen«, gehe ich genauer auf die Klassifizierung von Informationen ein.

Weiter zu berücksichtigen ist die Abhängigkeit von der Zeit und dem Kontext. Eine Information kann heute wertvoll, aber morgen ohne Nutzen sein oder umgekehrt. Ein einmaliger Zugangscode, zum Beispiel aus einer SMS oder einer Authenticator-App, ist nur für kurze Zeit gültig. Ebenso kann eine Information, die in einem Zusammenhang harmlos erscheint, in einem anderen schützenswert sein. Nehmen wir als Beispiel eine Liste mit Namen und Telefonnummern: Im internen Firmenverzeichnis mag sie unkritisch sein (aber bitte nicht offen herumliegen lassen), im Zusammenhang mit einem Projekt aber einen hohen Schutzbedarf aufweisen.

Informationen können auch miteinander verknüpft werden. Ein einzelnes Dokument, ein Gespräch oder ein Screenshot wirken auf den ersten Blick unscheinbar. In Kombination mit weiteren Informationen entsteht jedoch möglicherweise ein vollständiges Bild, das weitreichende Schlussfolgerungen erlaubt. Das Zusammenführen von Informationen stellt eine besondere Herausforderung dar, weil Sicherheitslücken häufig nicht in der einzelnen Information, sondern in ihrer Verbindung liegen.

Außerdem gilt es, den Lebenszyklus von Informationen zu kennen. Dieser kann in dem Kreislauf aus Abbildung 4.2 zusammengefasst werden:

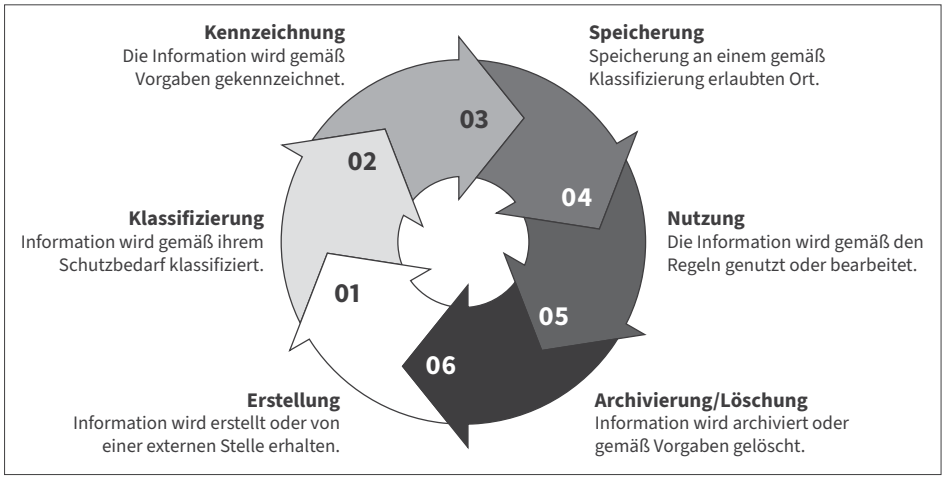

Abbildung 4.2: Kreislauf einer Information

1. **Erstellen** (oder Erhalt von einer externen Stelle): Die involvierte Person übernimmt die Rolle des Eigentümers der Information und ist dafür verantwortlich, dass diese Information gemäß den bestehenden Richtlinien behandelt wird.
2. Das **Klassifizieren** erfolgt gemäß dem Wert, den die Information für das Unternehmen hat.
3. Dann folgt die **Kennzeichnung** der Information (falls technisch möglich), damit die Klassifizierung auch für andere Personen ersichtlich ist.
4. Die **Speicherung** wird in einem Speicherort entsprechend der Klassifizierung vorgenommen.
5. Die **Nutzung** geschieht unter Berücksichtigung der Handlungsregeln, die für die jeweilige Klassifizierung gelten.
6. Die **Archivierung** erfolgt unter Berücksichtigung gesetzlicher und regulatorischer Anforderungen.
7. Die **Löschung** der Information findet statt, sobald diese nicht mehr benötigt wird oder die gesetzliche Aufbewahrungsfrist abgelaufen ist.

Für ein Unternehmen ist es also wichtig zu wissen, welche Informationen in welchem Status vorhanden sind und wie diese zu schützen sind. Ein klassischer Fehler ist es, sich dabei nur auf digitale Daten zu konzentrieren. Ein Beispiel aus der Praxis: Ein mittelständischer Maschinenbauer hatte seine CAD-Zeichnungen zwar verschlüsselt, doch ein Angreifer kopierte einfach die physischen Baupläne aus dem ungesicherten Archiv.

4.2 Die CIA-Triade

Wenn von Informationssicherheit die Rede ist, ist fast zwangsläufig die sogenannte *CIA-Triade* ein Thema. Hinter dieser Abkürzung verbirgt sich kein Geheimdienst, sondern ein Konzept, das die drei zentralen Schutzziele der Informationssicherheit zusammenfasst: *Confidentiality*, *Integrity* und *Availability* – auf Deutsch: Vertraulichkeit, Integrität und Verfügbarkeit. Abbildung 4.3 verdeutlicht ihr Zusammenwirken.

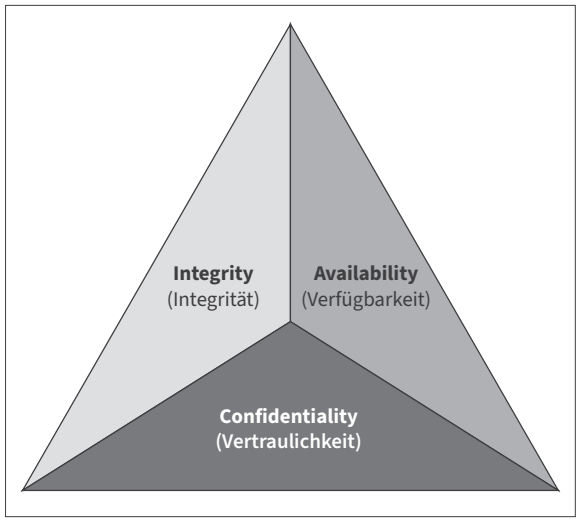

Abbildung 4.3: Die CIA-Triade

- **Vertraulichkeit** bezeichnet die Beschränkung des Zugangs zu Informationen auf autorisierte Personen, Systeme oder Prozesse. Das Ziel besteht darin, unbefugten Zugriff zu verhindern und damit die Inhalte vor Missbrauch, Spionage oder Datenabfluss zu schützen. In der Praxis ist dieses Ziel insbesondere im Umgang mit personenbezogenen Daten, Geschäftsgeheimnissen oder sensiblen Strategiedokumenten von Relevanz. Um die Vertraulichkeit der Informationen zu gewährleisten, werden verschiedene Maßnahmen ergriffen. Dazu zählen unter anderem Zugriffskontrollen, Verschlüsselung, Rollen- und Rechtemanagement sowie physische Schutzmaßnahmen. Ziel ist es, Informationen nur jenen zugänglich zu machen, die sie wirklich benötigen – nach dem sogenannten *Need-to-know*-Prinzip. Im Falle eines Verstoßes gegen die Vertraulichkeit können schwerwiegende Folgen entstehen. Sie können zu einem Vertrauensverlust bei den

Kunden, zu Imageschäden, zu rechtlichen Konsequenzen oder sogar zu wirtschaftlichen Nachteilen führen.

- **Integrität** beschreibt die Richtigkeit und Vollständigkeit von Informationen und ihrer Verarbeitung. Die unbeabsichtigte oder unbefugte Veränderung von Informationen, sei es durch technische Fehler oder gezielte Manipulation, ist zu verhindern. Der Fokus liegt also auf dem Schutz vor Datenverfälschung, Verlust von Genauigkeit oder vor unerwünschten Eingriffen. In Bezug auf gespeicherte Daten sowie während der Übertragung und Verarbeitung ist es von entscheidender Bedeutung, Integrität zu gewährleisten. Aus technischer Sicht wird sie beispielsweise durch Prüfsummen, digitale Signaturen oder Versionierung unterstützt. Auch organisatorische Maßnahmen, beispielsweise das Vier-Augen-Prinzip oder Änderungsprotokolle, tragen maßgeblich zu einem reibungslosen Ablauf bei. Ein Verlust der Integrität kann gravierende Auswirkungen haben. Dies kann etwa der Fall sein, wenn fehlerhafte Daten zu falschen Entscheidungen führen oder wenn manipulierte Informationen in automatisierten Prozessen unentdeckt weiterverarbeitet werden.
- **Verfügbarkeit** bezeichnet den Zustand, dass Informationen und die sie verarbeitenden Systeme dann zur Verfügung stehen, wenn sie benötigt werden. Es ist unerlässlich, dass die Verfügbarkeit sowohl im Alltagsbetrieb als auch im Krisenfall gewährleistet ist. Sollte es zu einem Ausfall eines E-Mail-Systems, einer Datenbank oder eines Kundenportals kommen, kann dies zu einem vollständigen Ausfall ganzer Geschäftsprozesse führen. Aus diesem Grund fokussiert sich dieses Schutzziel auf die Gewährleistung einer stabilen, zuverlässigen und belastbaren Infrastruktur. Die Verfügbarkeit wird durch redundante Systeme, Notfallpläne, Backup-Strategien, Monitoring oder auch durch Schutz vor physischen Schäden wie Feuer oder Wasser sichergestellt.

Diese drei Ziele sollten nicht isoliert voneinander betrachtet werden. Zwischen diesen Schutzzielen bestehen Verbindungen. Unter Umständen kann eine maximale Verfügbarkeit die Vertraulichkeit gefährden, etwa wenn der Zugriff auf Systeme zu wenig eingeschränkt wird, um jederzeit erreichbar zu sein. Eine sehr strikte Zugriffskontrolle kann sich ebenfalls negativ auf die Verfügbarkeit auswirken, wenn im Notfall kein schneller Zugriff auf benötigte Informationen möglich ist. Informationssicherheit erfordert daher stets einen ausgewogenen Ansatz, der sich an den spezifischen Anforderungen und Risiken des eigenen Unternehmens orientiert.

4.3 Authentizität und Verbindlichkeit

Neben der CIA-Triade gibt es weitere Schutzziele, die eine immer wichtiger werdende Rolle spielen. Zwei davon sind Authentizität und Verbindlichkeit. Sie erweitern die klassischen Konzepte um Aspekte, die besonders im Zusammenhang mit der digitalen Kommunikation, mit elektronischen Identitäten und mit rechtsverbindlichen Handlungen an Bedeutung gewinnen:

- Der Begriff *Authentizität* bezeichnet im Kern die Echtheit einer Information oder einer Identität. Es ist von Bedeutung, die Authentizität einer Information zu gewährleisten. Dies betrifft sowohl den Menschen als auch Systeme oder Prozesse. In der Praxis bedeutet Authentizität, dass ein empfangenes Dokument tatsächlich vom angegebenen Absender stammt und während des Transports nicht verändert oder ausgetauscht wurde. Ebenso ist es unerlässlich, dass sich Nutzerinnen und Nutzer eindeutig identifizieren lassen, bevor sie auf Systeme oder Informationen zugreifen dürfen.

  Der Schutz der Authentizität ist von Relevanz, da elektronische Informationen mit geringem Aufwand gefälscht oder manipuliert werden können. Während bei einem handschriftlich unterschriebenen Papierdokument oft bereits durch Haptik, Layout oder Unterschrift eine gewisse Sicherheit in Hinblick auf seine Echtheit gegeben ist, fehlen solche Merkmale bei einer E-Mail oder einem digitalen Dokument. Um die Authentizität in der digitalen Kommunikation sicherzustellen, sind technische Verfahren wie digitale Signaturen, Zertifikate oder kryptografische Hashwerte erforderlich. Der Einsatz von Zwei-Faktor-Authentifizierung oder biometrischer Identifikation verfolgt letztlich dasselbe Ziel: Nur wer nachweisen kann, die Person oder Entität zu sein, der er/sie vorgibt zu sein, erhält Zugriff oder kann eine Aktion ausführen.
- Der Begriff *Verbindlichkeit* ist eng mit dem der Authentizität verbunden. Im Englischen spricht man meist von *non-repudiation*. Verbindlichkeit bezeichnet die Nachweisbarkeit einer Handlung. Insbesondere bedeutet das, dass der Urheber seine Handlung nicht nachträglich abstreiten kann. Im Kontext der Informationssicherheit meint man damit, dass eine gesendete Nachricht oder eine durchgeführte Transaktion einer bestimmten Person oder Entität eindeutig zugeordnet werden kann und diese Zurechnung auch im Nachhinein beweisbar bleibt. Dies ist insbesondere dann relevant, wenn Verträge digital abgeschlossen, Zahlungen ausgelöst oder kritische Entscheidungen dokumentiert werden.

  Analog gilt dies auch in umgekehrter Richtung. Auch der Empfang einer Nachricht darf nicht abgeschritten werden können (siehe Abbildung 4.4 und Abbildung 4.5).

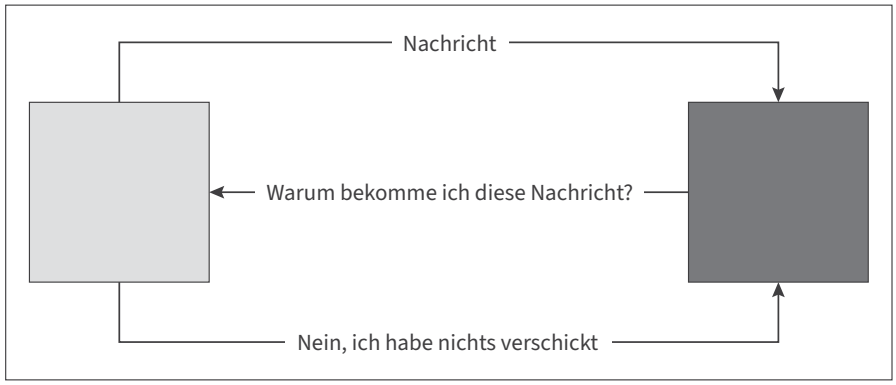

Abbildung 4.4: Bestreiten des Versands von Nachrichten (»non-repudiation of origin«). Hier bestreitet der Absender einer Nachricht, die Nachricht versandt zu haben.

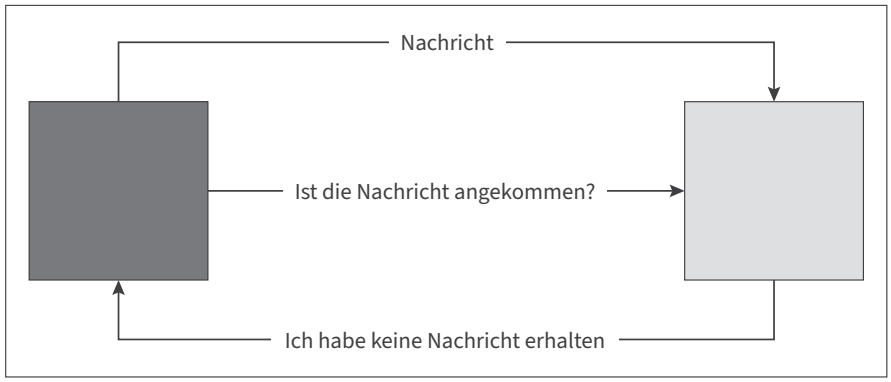

Abbildung 4.5: Bestreiten des Empfangs von Nachrichten (»non-repudiation of receipt«). Hier bestreitet der Empfänger einer Nachricht, die Nachricht erhalten zu haben.

Im Rechtsverkehr spielt die Verbindlichkeit eine zentrale Rolle. In vielen Ländern sind digitale Signaturen, die bestimmte Sicherheitsanforderungen erfüllen, juristisch den handschriftlichen Signaturen gleichgestellt. Dies bedeutet, dass bei einer digitalen Unterzeichnung die gleiche rechtliche Verpflichtung besteht wie bei einer physischen Unterschrift. Damit dies gelingt, sind neben technischen Lösungen auch Vertrauen in die Identitäten und Prozesse sowie in deren Zuverlässigkeit unerlässlich. Die Grundlage dieser Vertrauensinfrastruktur bilden Zertifizierungsstellen, Identitätsprovider und revisionssichere Protokollierungen.

In Organisationen bedeutet Verbindlichkeit zudem, dass Verantwortlichkeiten klar geregelt sind. Wer hat welche Entscheidung getroffen? Wer hat wann auf ein bestimmtes System zugegriffen oder eine Transaktion durchgeführt? Diese Fragen sind nicht nur im Kontext der Sicherheit, sondern auch für Audits, Haftungsfragen und Compliance-Anforderungen von zentraler Bedeutung.

4.4 Grundbegriffe

Bevor ich genauer auf das ISMS eingehe, muss ich noch einige Begriffe einführen. In der ISO 27001 wird in jedem Satz von »muss« gesprochen, in der ISO 27002 von »sollte«, »darf« oder »kann«. Was wird damit gemeint?

In der ISO 27000 werden die Verbformen wie folgt definiert:

- **muss** (engl. *shall*) bezeichnet eine Anforderung.
- **sollte** (engl. *should*) bezeichnet eine Empfehlung.
- **darf** (engl. *may*) bezeichnet eine Erlaubnis.
- **kann** (engl. *can*) bezeichnet eine Möglichkeit oder Fähigkeit.

Diese Begriffe orientieren sich am *Request for Comments* (RFC) 2119, der unter *https://www.ietf.org/rfc/rfc2119.txt* abrufbar ist.

Die Norm verwendet verschiedene Begriffe, die nachfolgend kurz erläutert werden:

- Die *interessierten Parteien* (engl. *interested parties*) sind natürliche oder juristische Personen, die von der Informationssicherheit einer Organisation betroffen sein können – direkt oder indirekt. Dazu zählen Mitarbeitende, Kunden, Partner, Aufsichtsbehörden oder Lieferanten. Das ISMS berücksichtigt ihre Erwartungen und Anforderungen, etwa in Bezug auf Datenschutz, Vertraulichkeit oder Verfügbarkeit von Diensten (siehe dazu Abschnitt 6.1.2, »NA 4.2 – Verstehen der Erfordernisse und Erwartungen interessierter Parteien«).
- Ein wichtiger Aspekt ist der *Kontext* (engl. *context*). Dies beinhaltet sowohl den internen, aber auch den externen Kontext. Damit ist das Umfeld gemeint, in dem die Organisation versucht, ihre Ziele zu erreichen (siehe dazu Abschnitt 6.1.1, »NA 4.1 – Verstehen der Organisation und ihres Kontextes«).
- Bei der *Geschäftsleitung* (engl. *executive management*) handelt es sich um eine Person oder Personengruppe, die die Verantwortung für die Umsetzung von Strategien und Richtlinien trägt, um die Ziele der Organisation zu erreichen. Die Geschäftsleitung wird manchmal auch als *oberste Leitung* bezeichnet. Dazu können die Geschäftsführer, Finanzverantwortlichen, die Verantwortlichen für die Informationsverarbeitung und ähnliche Rollen gehören.
- Bei der *Sicherheitsrichtlinie* (engl. *security policy*) handelt es sich um ein Statement der obersten Leitung, das die Absichten und Prinzipien im Umgang mit der Informationssicherheit schriftlich festhält. Die Richtlinie ist eine Art Grundgesetz des ISMS und bildet die Basis für die weiteren Maßnahmen (siehe dazu Abschnitt 6.2.2, »NA 5.2 – Politik«).

Praxistipp

Die drei Begriffe *Politik*, *Richtlinie* und *Leitlinie* werden oft vermischt. Es ist wichtig, diese im ISMS unterschiedlich zu verwenden:

- Die **Politik** (in der Norm wird der Begriff »Politik« verwendet, oft wird stattdessen **Strategie** benutzt) legt die langfristige Ausrichtung und die übergeordneten Ziele fest. Sie erläutert die Relevanz eines Themas und welche Bedeutung es im Gesamtbild des Unternehmens hat. Sie definiert unter anderem, welches Schutzniveau angestrebt wird, welche Risiken akzeptiert werden und wie die Informationssicherheit die Unterstützung der Geschäftsziele fördern soll. Die Strategie gibt die Richtung vor, ist aber bewusst nicht operativ.
- Eine Ebene tiefer sind die **Richtlinien** angesiedelt. Sie setzen die strategischen Vorgaben in verbindliche Regeln um und konkretisieren sie. Richtlinien bestimmen, was erlaubt ist, was verpflichtend eingehalten werden muss und wer die Verant-

wortung trägt. In der Informationssicherheit legen Richtlinien fest, wie beispielsweise mit Passwörtern, Zugriffsrechten oder mobilen Arbeitsplätzen umgegangen wird. Sie haben einen verbindlichen Charakter, gelten über die gesamte Organisation hinweg und sind die Basis für Kontrolle und Nachweisbarkeit.

- Im Gegensatz dazu sind **Leitlinien** dazu da, Orientierung zu bieten. Sie unterstützen die Mitarbeitenden dabei, die Richtlinien im Alltag umzusetzen.

- Ein *Asset* – oft als Vermögenswert oder kurz **Wert** übersetzt – bezeichnet in der Informationssicherheit alles, was für das Unternehmen von einem Wert ist. Das können nicht nur Informationen selbst sein, sondern auch Geräte, Software, Standorte, Personal oder auch die Reputation. Der Schutz dieser Assets ist ein Kernziel des ISMS (siehe dazu Abschnitt 7.2.9, »NA A.5.9 – Inventar der Informationen und anderen damit verbundenen Werte«).
- Der Begriff der *Risikobewertung* (engl. *risk assessment*) umfasst alle Aktivitäten, mit denen potenzielle Bedrohungen identifiziert, analysiert und bewertet werden. Das Ziel ist es, Risiken nachvollziehbar zu priorisieren, um angemessene Maßnahmen abzuleiten (siehe dazu Abschnitt 6.3.1, »NA 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen«).
- An verschiedenen Stellen verlangt die Norm *dokumentierte Informationen* (engl. *documented information*). Dies können Dokumentationen des ISMS, aber auch Informationen für den Betrieb sowie Audit-Nachweise sein. Diese dokumentierten Informationen müssen gelenkt und aufrechterhalten werden, inklusive des Mediums, auf dem sie gespeichert sind.
- Bei *sensitiven Personendaten* (engl. *sensitive personal data*) handelt es sich um Informationen, die Auskunft geben über ethnischen Ursprung, politische Meinungen, religiösen oder philosophischen Ansichten, Mitgliedschaft in einer Gewerkschaft, genetische oder biometrische Identifikationsdaten einer Person.
- Die Norm verlangt, dass in regelmäßigen Abständen *Audits* (engl. *audit*) durchgeführt werden. Ein Audit ist ein systematischer, unabhängiger und dokumentierter Prozess. Sein Ziel ist es, einen Nachweis über die Effektivität des ISMS zu erlangen. Dazu werden für jedes Audit Kriterien bestimmt (siehe dazu Abschnitt 6.7.2, »NA 9.2 – Internes Audit«).
- *Kontinuierliche Verbesserung* (engl. *continual improvement*): Die Informationssicherheit ist kein statischer Zustand, sondern ein dynamischer Prozess. Die Norm verlangt deshalb, dass das ISMS regelmäßig überprüft, angepasst und verbessert wird – sowohl auf der Basis interner Audits als auch durch Management-Reviews, Vorfallanalysen und neue Risikobewertungen (siehe dazu Abschnitt 6.8.1, »NA 10.1 – Fortlaufende Verbesserung«).

- Ein *Control*, auf Deutsch oft als »Maßnahme« übersetzt, ist jede organisatorische oder technische Handlung, die ein Informationssicherheitsrisiko minimieren oder ausschließen soll. In ISO 27001 sind diese Controls in Anhang A aufgelistet, und sie werden in ISO 27002 ausführlich beschrieben. Controls reichen von Zugangskontrollen über die Verschlüsselung bis hin zu Sicherheitsrichtlinien, Mitarbeiterschulungen oder Notfallplänen.
- Der *Informationssicherheitsvorfall* (engl. *information security incident*) beschreibt jede beobachtete oder vermutete Schwachstelle oder Verletzung der Sicherheitsrichtlinien, die die Schutzziele gefährden könnte. Dies umfasst sowohl technische Vorfälle – etwa einen Malware-Befall – als auch organisatorische oder menschliche Fehler, wie das unbefugte Offenlegen von sensiblen Informationen (siehe dazu Abschnitt 7.2.24, »NA A.5.24 – Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen«).

Wenn Sie den Gebrauch dieser Begriffe verinnerlicht haben, sind Sie in der Lage, sich um den Aufbau des ISMS zu kümmern.

Kapitel 5

Einführung in die Normenreihe ISO 27000

Bereits Anfang der 1990er-Jahre wurde der Grundstein für die heutige ISO-27000-Normfamilie gelegt. Aus dem British Standard 7799 wurden in den vergangenen Jahren über 75 Normen rund um die Informationssicherheit erstellt.

Die Geschichte der ISO-27000-Normenreihe beginnt nicht in Genf, wo der Sitz der Internationalen Organisation für Normung (ISO) ist, sondern in London. Die Wurzeln der Normenreihe liegen in der britischen Norm *BS 7799*, die Anfang der 1990er-Jahre vom *Department of Trade and Industry* (DTI) entwickelt und 1995 erstmals von der *British Standards Institution* (BSI) veröffentlicht wurde. Das Internet steckte zu diesem Zeitpunkt noch in den Kinderschuhen, doch dass Sicherheit kein Nischenthema mehr war, zeigten die ersten Hackerangriffe und Datenpannen. BS 7799 wurde in zwei Teile gegliedert: Teil 1 listete Best Practices für Sicherheitsmaßnahmen auf, Teil 2 definierte Anforderungen an Managementsysteme.

Aufgrund der großen internationalen Bedeutung und Akzeptanz der BS 7799 wurde dieser Standard Anfang der 2000er-Jahre von der ISO übernommen und überarbeitet. Der erste Teil der ursprünglichen BS 7799 wurde als ISO/IEC 17799 übernommen, die die empfohlene Sammlung von Sicherheitsmaßnahmen (*Controls*) enthielt. Diese Norm wurde später zur heutigen ISO/IEC 27002 weiterentwickelt. Im Jahr 2005 erschien die erste Version von ISO/IEC 27001, die den zweiten Teil der BS-7799-Reihe ablöste und als offizieller internationaler Standard für die Zertifizierung eines ISMS anerkannt wurde.

Im Laufe der Zeit hat sich aus der ursprünglichen Norm ein umfassendes Normenwerk entwickelt: die ISO/IEC-27000-Familie. Diese umfasst heute über 75 Einzelnormen, die spezifische Aspekte der Informationssicherheit vertiefen: themenspezifische wie etwa Risikomanagement (ISO 27005), Monitoring und Messung (ISO 27004, siehe dazu Kapitel 9, »Informationssicherheit messen«), Sicherheitsaspekte in der Lieferkette (ISO 27036) oder sektorspezifische Anforderungen wie im Gesundheitswesen (ISO 27799) oder in Cloud-Umgebungen (ISO 27017).

Die ISO/IEC 27000 selbst, d. h. die gleichnamige Norm innerhalb der Reihe, definiert die Begriffe, die in allen Normen dieser Familie verwendet werden, und stellt eine übergeordnete Einführung in das Normensystem dar. Sie bildet somit die Grundlage für ein einheitliches Vokabular und eine gemeinsame Sichtweise auf Informationssicherheit.

Ein wichtiger Meilenstein in der Weiterentwicklung war die Revision der ISO/IEC 27001 im Jahr 2013, bei der die Norm an die sogenannte *High-Level Structure* (HLS) der ISO angepasst wurde (siehe Abschnitt 2.2, »Abgrenzung zu anderen Managementsystemen«). Bei der Überarbeitung wurde zudem ein Fokus auf ein risikobasiertes Vorgehen gelegt.

Die aktuelle Version der ISO/IEC 27001 wurde 2022 veröffentlicht und enthält zahlreiche inhaltliche und strukturelle Anpassungen, unter anderem eine Modernisierung des Kontrollkatalogs (Annex A).

Praxistipp

Die Jahreszahlen der Normen stellen eine erste Herausforderung dar.

Die englischen Ausgaben der ISO 27001 und der ISO 27002 stammen aus dem Jahr 2022. Die Schweizer Ausgabe der ISO 27001 datiert aus dem Jahr 2023, die ISO 27002 aus dem Jahr 2022. Die deutschen Ausgaben der ISO 27001 und 27002 sind aus dem Jahr 2024. Die österreichische ISO 27001 stammt aus dem Jahr 2024 und die ISO 27002 aus dem Jahr 2023.

Alles klar?

5.1 Inhalt und Aufbau

Die Normen ISO/IEC 27000, 27001 und 27002 bilden den Kern der 27000er-Normenfamilie. Sie ergänzen sich gegenseitig, adressieren aber unterschiedliche Ebenen. Zusammen bilden sie die Grundlage für ein strukturiertes und effektives ISMS. An dieser Stelle werden die drei Normen kurz beschrieben, inklusive des PDCA- und des Security-Kreislaufs.

5.1.1 ISO/IEC 27000

Die ISO/IEC 27000 (offizieller Titel: *Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie*) bietet einen Einstieg in das Thema ISMS.

Im dritten Kapitel der Norm werden über 70 zentrale Begriffe rund um das ISMS definiert, beispielsweise »Zugangssteuerung«, »Audit« oder »Risiko«. Die Begriffsdefinitionen sind mit Anmerkungen versehen. Einige dieser Begriffe habe ich bereits in Kapitel 4, »Begriffe zur Informationssicherheit«, erklärt.

Das Kernstück der Norm ist ihr viertes Kapitel, das sich ausschließlich mit dem Verständnis und der Implementierung eines ISMS befasst. Es beginnt mit einer allgemeinen Einführung in das Konzept und beschreibt dessen Grundprinzipien. Die Norm erläutert, was unter einem Managementsystem zu verstehen ist und warum ein prozessorientierter Ansatz für das effektive Erreichen von Informationssicherheitszielen entscheidend ist. Dieses Kapitel hat folgende Struktur:

- **4.1 Allgemeines:** Überblick über die Rolle und Bedeutung von ISMS
- **4.2 Was ist ein ISMS:** Definition und Grundprinzipien, inklusive Begriffe wie Information, Informationssicherheit, Management und Managementsystem
- **4.3 Prozessorientierter Ansatz:** Erläuterung der Steuerung durch Prozesse
- **4.4 Warum ein ISMS wichtig ist:** Beschreibung des Nutzens eines ISMS zur Risikobeherrschung
- **4.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS:** Leitfaden für Implementierung, Identifizierung, Beurteilung und Behandlung von Informationssicherheitsanforderungen und -risiken, Überwachung und kontinuierliche Verbesserung, inklusive Maßnahmen-Definition
- **4.6 Kritische Erfolgsfaktoren:** notwendige Voraussetzungen für ein wirksames ISMS
- **4.7 Nutzen der ISMS-Normenfamilie:** Erklärung, wie die verschiedenen Normen der 27000er-Familie zusammenwirken

In Kapitel 5 der Norm folgt schließlich eine systematische Einordnung der gesamten ISMS-Normenfamilie (siehe Abbildung 5.1):

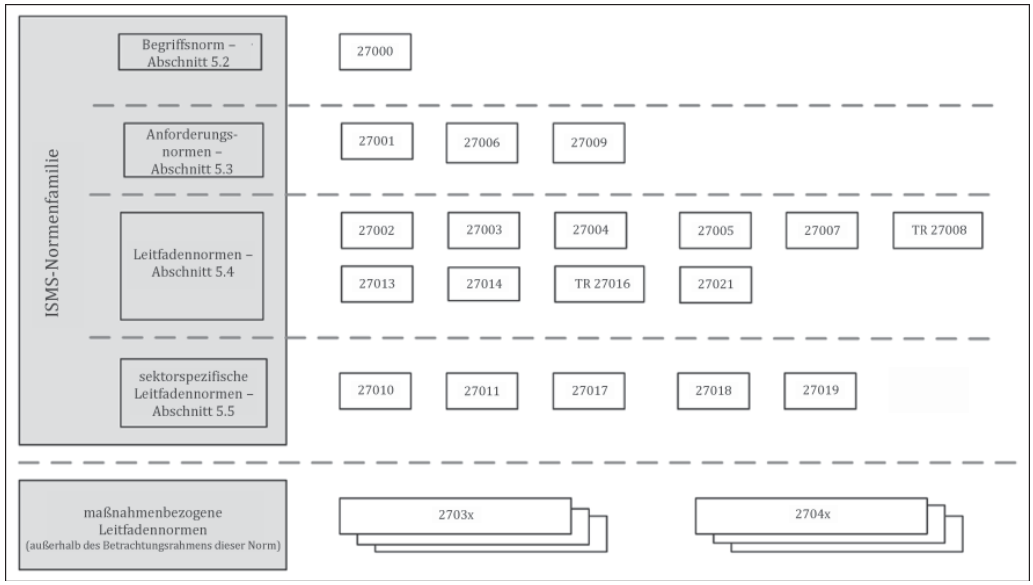

Abbildung 5.1: Zusammenhänge der ISMS-Normenfamilie (Quelle: ISO/IEC 27000:2020)

- **5.1 Allgemeines:** Einführung in die ISMS-Normenfamilie
- **5.2 Norm, die einen Überblick und die Terminologie beschreibt:** Damit ist die ISO/IEC 27000 selbst gemeint.
- **5.3 Normen, die Anforderungen festlegen:** z. B. ISO/IEC 27001 (Anforderungen an ISMS), ISO/IEC 27006 (Zertifizierungsstellen), ISO/IEC 27009 (sektorspezifische Anpassung)

- **5.4 Normen, die allgemeine Leitfäden beschreiben:** z. B. ISO/IEC 27002 (Maßnahmenkatalog), ISO/IEC 27003 bis ISO/IEC 27021
- **5.5 Normen, die branchenspezifische Leitfäden beschreiben:** z. B. für Telekommunikation, Cloud, Energie, Gesundheitswesen (u. a. ISO/IEC 27010 bis 27799)

5.1.2 ISO/IEC 27001

Die Norm ISO/IEC 27001 mit dem offiziellen Titel *Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagement-systeme – Anforderungen* umfasst zehn Kapitel und einen normativen Anhang. Ihre Kapitel 1 bis 3 enthalten allgemeine Informationen (Anwendungsbereich, normative Verweise und Begriffe). Ab Kapitel 4 beginnt der normative Teil, der die Anforderungen an ein ISMS beschreibt:

- **Kapitel 4 – Kontext der Organisation:** Verlangt die systematische Auseinandersetzung mit internen und externen Rahmenbedingungen (Kontext), interessierten Parteien und dem Geltungsbereich des ISMS.
- **Kapitel 5 – Führung:** Legt die Verantwortung der obersten Leitung fest, etwa durch die Definition der Informationssicherheitspolitik, das Setzen von Zielen und das Zuweisen von Rollen.
- **Kapitel 6 – Planung:** Beinhaltet die Risikobewertung, die Risikobehandlung sowie die Ableitung und Planung von Maßnahmen. Ebenfalls wird die Erstellung einer Erklärung zur Anwendbarkeit verlangt.
- **Kapitel 7 – Unterstützung:** Regelt Ressourcen, Kompetenzen, Schulungen, Kommunikation sowie die Dokumentation im Rahmen des ISMS.
- **Kapitel 8 – Betrieb:** Beschreibt die konkrete Umsetzung und Steuerung der geplanten (Risiko-)Maßnahmen und Prozesse im operativen Alltag.
- **Kapitel 9 – Bewertung der Leistung:** Verlangt Messung, Überwachung und Bewertung der Wirksamkeit des ISMS. Hier sind interne Audits und das Management-Review zentrale Elemente.
- **Kapitel 10 – Verbesserung:** Behandelt den Umgang mit Nicht-Konformitäten, das Ergreifen von Korrekturmaßnahmen und die kontinuierliche Weiterentwicklung des ISMS.

Zusätzlich enthält Anhang A einen Verweis auf eine strukturierte Liste von 93 Sicherheitsmaßnahmen (*Controls*), die zur Risikobehandlung herangezogen werden können. Diese Controls werden jedoch nicht in der Norm selbst erklärt. Jedes Control ist einem einzigen Satz beschrieben. Details zur Umsetzung sind in der ISO/IEC 27002 zu finden.

5.1.3 Der PDCA-Kreislauf

Ein zentrales Prinzip eines ISMS ist der *PDCA-Kreislauf*, ein Modell zur kontinuierlichen Verbesserung, das sich in vielen Managementsystemen der ISO-Welt wiederfindet (siehe

Abbildung 5.2). Die vier Buchstaben stehen für *Plan–Do–Check–Act*. Der Zyklus beschreibt die kontinuierliche Steuerung und Weiterentwicklung von Prozessen, Maßnahmen und Zielen und bildet das Herzstück des ISMS.

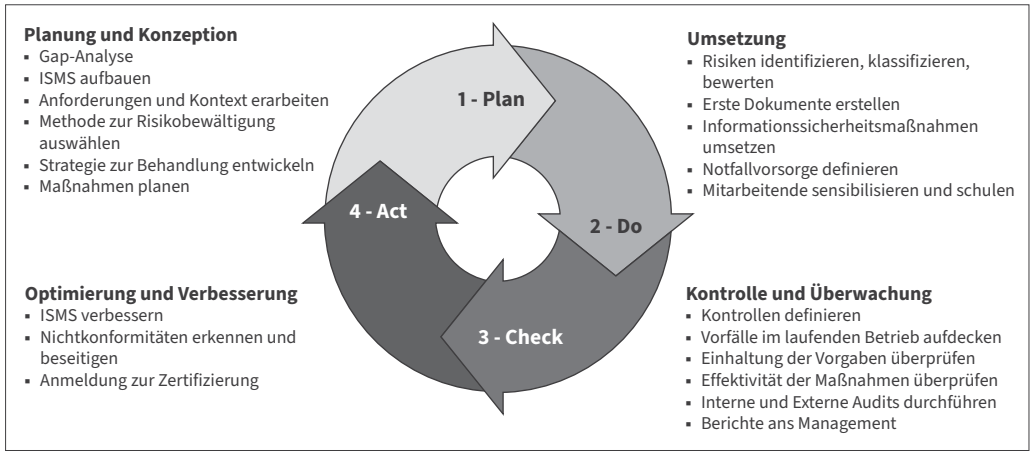

Abbildung 5.2: Der PDCA-Kreislauf

- In der **Plan-Phase** plant die Organisation ihr ISMS. Dazu gehört zunächst die Erfassung des organisatorischen Kontextes: Welche internen und externen Faktoren beeinflussen die Informationssicherheit? Welche Anforderungen stellen Gesetze, Kunden oder Partner? Darauf aufbauend werden Risiken identifiziert, bewertet und priorisiert. Die Organisation setzt sich Ziele, definiert Sicherheitsrichtlinien, identifiziert notwendige Ressourcen und entscheidet, welche Maßnahmen zur Risikobewältigung umgesetzt werden sollen. Diese Phase bildet das strategische Fundament des ISMS und setzt den Rahmen für alle weiteren Aktivitäten.
- In der **Do-Phase** werden die geplanten Maßnahmen umgesetzt. Verantwortlichkeiten werden zugewiesen, Mitarbeitende geschult, Prozesse eingeführt sowie technische und organisatorische Kontrollen etabliert. Dabei geht es nicht nur um Einzelmaßnahmen, sondern um die Integration der Sicherheitsaktivitäten in den täglichen Betrieb. Die Wirksamkeit der Umsetzung hängt in dieser Phase stark davon ab, inwieweit das ISMS von der gesamten Organisation getragen wird.
- In der **Check-Phase** wird die Wirksamkeit der getroffenen Maßnahmen überprüft. Dies geschieht durch interne Audits, Kennzahlen, Überwachung von Sicherheitsvorfällen und regelmäßige Bewertungen. Auch der Fortschritt in Bezug auf die gesetzten Ziele wird erfasst. Die Organisation fragt sich in dieser Phase: Funktionieren unsere Maßnahmen? Sind die Sicherheitsziele erreicht? Gibt es Schwachstellen oder Verbesserungsmöglichkeiten?
- In der **Act-Phase** werden die Erkenntnisse aus dem Audit in konkrete Maßnahmen umgesetzt. Zeigt ein Audit beispielsweise Lücken im Zutrittsmanagement auf, werden Verbesserungsmaßnahmen abgeleitet und umgesetzt. Auch geänderte gesetzliche An-

forderungen oder neue Bedrohungen können Anlass sein, das ISMS anzupassen. Die Organisation reagiert auf Veränderungen und stellt sicher, dass sich das Managementsystem kontinuierlich weiterentwickelt.

5.1.4 Der Security-Kreislauf

Um den PDCA-Kreislauf optimal in ein ISMS umzusetzen, habe ich einen Security-Kreislauf erstellt (siehe Abbildung 5.3). Die verschiedenen Themengebiete der ISO/IEC 27001 werden in ihm berücksichtigt.

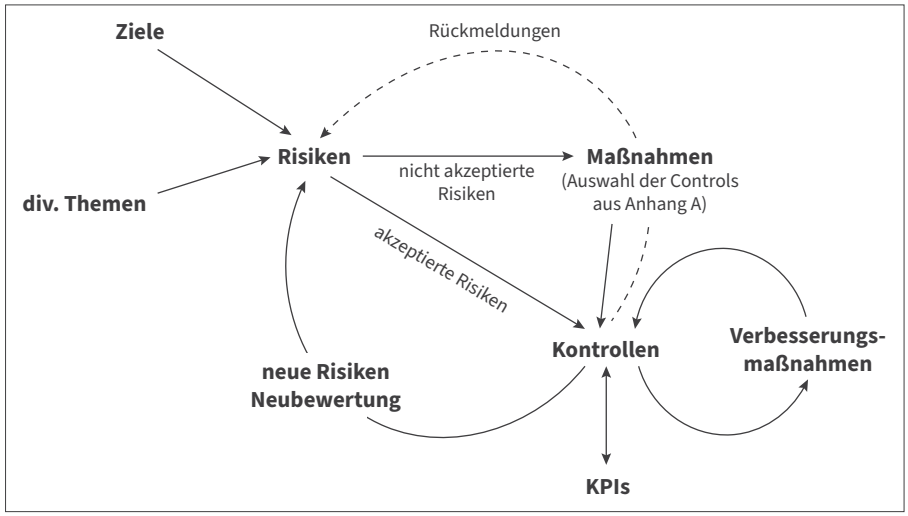

Abbildung 5.3: Der Security-Kreislauf

Nachfolgend werden die einzelnen Schritte kurz beschrieben:

- **Ziele:** Die Ziele des ISMS werden von der Firmenvision, -mission und -strategie abgeleitet. Sie bestimmen die Vorgaben zur Implementierung und zum Betrieb des ISMS.
- **Risiken:** Die Ziele des ISMS sind einer Vielzahl von Bedrohungen ausgesetzt, die ihrer Erreichung entgegenstehen. Das Schadenspotenzial dieser Bedrohungen hängt von verschiedenen Faktoren ab: einerseits von den Zielen selbst, andererseits von dem Geschäftsumfeld, der IT-Landschaft, dem Benutzerverhalten, externen Bedürfnissen etc. Die Analyse wird in einem Risikoregister festgehalten, das als Grundlage für die Behandlung ebendieser Risiken dient.
- **Maßnahmen:** Die Risiken werden entweder durch Maßnahmen reduziert oder gar eliminiert oder sie werden ohne Behandlung akzeptiert, weil eine Reduktion nicht möglich ist oder unverhältnismäßigen Aufwand erfordert.
- **Kontrollen:** Die getroffenen Maßnahmen basieren entweder auf den Controls im Anhang A der ISO-27001-Norm oder auf anderen Quellen. Sie bilden die Kontrollpunkte, die in regelmäßig stattfindenden Audits überprüft werden.

- **KPI:** *Key Performance Indicators* (KPIs, dt. *Leistungskennzahlen*) sind quantitative Beurteilungskriterien für die Kontrollen, mit deren Hilfe die Wirksamkeit des ISMS gemessen werden kann.
- **Verbesserungsmaßnahmen:** Durch die Implementierung der getroffenen Maßnahmen soll die Wirksamkeit des ISMS stetig verbessert werden.
- **Neubeurteilung von Risiken:** Es ist notwendig, die Risiken regelmäßig neu zu überprüfen, da sowohl die Bedrohungen selbst als auch das Geschäftsumfeld der Organisation in stetigem Wandel begriffen sind.

Beispiel: Das Ziel der Organisation ist es, keinen Datenverlust zu erleiden. Mögliche Risiken, die im Weg stehen, sind zum Beispiel Hacker-Angriffe, Fehlbedienung, Systemausfall etc.

Als Maßnahme wird daher ein Backup erstellt. Die Kontrolle kann lauten: »Ist das Backup letzte Nacht erfolgreich durchgelaufen?«.

Der KPI könnte sein: »Wie viele Backups sind im letzten Monat fehlgeschlagen?«

In einer grafischen Anzeige könnten 0 Fehlschläge als Grün definiert sein, 1 Fehlschlag könnte als Orange dargestellt werden, ab 2 Fehlschlägen könnte das Resultat in Rot markiert sein. Durch die Umsetzung des Backups kann das Risiko entsprechend reduziert werden.

5.1.5 ISO/IEC 27002

Die ISO/IEC 27002:2022 (offizieller Titel: *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen*) ist die Ergänzung zur ISO/IEC 27001. Während die ISO/IEC 27001 das »Was« vorgibt, beantwortet ISO/IEC 27002 die Fragen nach dem »Wie«.

Im Zentrum der Norm stehen 93 konkrete Maßnahmen (*Controls*), die auf Basis internationaler Erfahrungen entwickelt wurden. Diese Maßnahmen sind in vier Themenbereiche unterteilt:

- Bei den **organisatorischen Maßnahmen** stehen übergeordnete Steuerungs- und Managementthemen im Vordergrund. Dazu gehören unter anderem die Formulierung und Pflege einer Informationssicherheitspolitik und entsprechender Richtlinien, die klare Definition von Rollen und Verantwortlichkeiten, der strukturierte Umgang mit externen Dienstleistern sowie das Management von Sicherheitsvorfällen und Notfällen. Auch Vorgaben zur sicheren Gestaltung von Projekten und Veränderungen, etwa im Change-Management, sind verankert.
- Die **personenbezogenen Maßnahmen** umfassen alle Aspekte, die direkt das Verhalten und die Einbindung der Mitarbeiterinnen und Mitarbeiter betreffen. Dazu gehören verpflichtende Schulungen zur Sensibilisierung für Sicherheitsrisiken, Regelungen zum vertraulichen Umgang mit Informationen, das strukturierte Ausscheiden von Mitarbei-

tenden (*Offboarding*) sowie Richtlinien für sicheres Arbeiten im Home-Office oder unterwegs. Das Ziel dieser Maßnahmen ist es, ein Sicherheitsbewusstsein zu schaffen und menschliche Fehler zu minimieren.

- Die **physischen Maßnahmen** betreffen den Schutz der Infrastruktur und der Umgebung, in der Informationen verarbeitet oder gespeichert werden. Dazu gehören die Einrichtung von Zugangskontrollen, die Sicherung besonders schützenswerter Bereiche (z. B. des Serverraums) innerhalb von Gebäuden, die sichere Aufbewahrung von Informationswerten (z. B. in abschließbaren Schränken) sowie der Schutz von Geräten vor Diebstahl, Manipulation oder Umwelteinflüssen.
- Bei den **technologischen Maßnahmen** geht es um den direkten Schutz von IT-Systemen, Netzwerken und Anwendungen. Dazu gehören der Einsatz starker Authentisierungsverfahren, der gezielte Einsatz kryptografischer Methoden wie Verschlüsselung und digitale Signaturen, die Absicherung von Netzwerken, ein regelmäßiges Schwachstellenmanagement sowie Anforderungen an die sichere Entwicklung von Software.

Diese Gliederung in vier Kapitel ersetzt die frühere Struktur mit 14 Domänen. Zusätzlich wurden bei der letzten Überarbeitung sogenannte Attribute eingeführt, mit denen sich jede Maßnahme mehrfach klassifizieren lässt, und zwar nach Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit), nach ihrer Funktion im Sicherheitsprozess (präventiv, detektiv, korrektiv) oder nach ihrer Zuordnung zu Cybersecurity-Konzepten wie *Identifizieren*, *Schützen* oder *Reagieren* (siehe Abbildung 5.4).

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Ökosystem #Resilienz

Abbildung 5.4: Attributtabelle für das Control 5.1, »Informationssicherheitspolitik und -richtlinien«

Jede einzelne Maßnahme ist in der Norm nach einem festen Schema aufgebaut:

- **Maßnahmenüberschrift:** ein kurzer, prägnanter Titel
- **Attributtabelle:** eine Übersicht, welche Eigenschaften mit der Maßnahme verknüpft sind
- **Beschreibung der Maßnahme:** Was soll konkret getan werden?
- **Zweck:** Warum ist die Maßnahme relevant?
- **Anleitung:** Beschreibt, wie die Umsetzung in der Praxis erfolgen kann.
- **Weitere Informationen:** Erläuterungen, Beispiele oder Querverweise zu anderen Normen

Kapitel 6
Die ISO 27001 verstehen

In diesem Kapitel erhalten Sie einen Überblick über die wichtigsten Anforderungen der ISO 27001, indem die wesentlichen Inhalte der Normkapitel 4 bis 10 erläutert werden. Die Struktur der Norm wird verständlich dargestellt, und die Beziehungen zwischen den verschiedenen Abschnitten werden aufgezeigt.

Zum Einstieg jedes Abschnitts finden Sie den Originaltext der Norm, den ich im Anschluss kontextualisieren und einordnen möchte. Die Normtexte sind mit einem grauen Balken markiert. Den gesamten Text der Norm finden Sie in Anhang B. Folgende Abkürzungen werden in den Überschriften verwendet, um Ihnen die Orientierung zu erleichtern:

- NK: Norm-Kapitel
- NA: Norm-Abschnitt

Und ein wichtiger Hinweis schon einmal vorab …

Hinweis
Gemäß den Vorgaben der Norm ist es bei der Gestaltung eines ISMS nicht zulässig, Anforderungen aus Kapitel 4 bis Kapitel 10 auszuschließen. Alle Normanforderungen sind umzusetzen!

6.1 NK 4 – Kontext der Organisation

Das erste relevante Normkapitel beinhaltet die vier Schwerpunkte *Kontext*, *interessierte Parteien*, den *Anwendungsbereich* und das *ISMS*.

Der Kontext umfasst alle relevanten Fakten, Vorgaben und Erwartungen, die das ISMS und dessen Ergebnisse beeinflussen und steuern könnten. Zunächst werden Informationen über den Zweck und die (geschäftlichen) Tätigkeiten einer Organisation bereitgestellt. Es werden auch Erwartungen, Ziele und Vorgaben festgelegt, die das ISMS betreffen.

Erfahrungsgemäß benötigt die Erarbeitung des Kontexts einiges an zeitlichem Aufwand. Hierzu kann nicht nur die Firmenwebseite kopiert werden, sondern das Unternehmen sollte sich vertiefter mit diesem Thema auseinandersetzen. Es handelt sich um mehr als nur um eine einfache Umfeldanalyse: Es ist entscheidend, das ISMS an die aktuelle Situation und die Besonderheiten der eigenen Organisation anzupassen.

6.1.1 NA 4.1 – Verstehen der Organisation und ihres Kontextes

> **4.1 Verstehen der Organisation und ihres Kontextes**
>
> Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagementsystems zu erreichen.
>
> Die Organisation muss bestimmen, ob Klimawandel ein relevantes Thema ist.

Der *Kontext* einer Organisation umfasst interne und externe Faktoren, die für das Erreichen der Sicherheitsziele von Relevanz sind. Der Kontext ist jedoch nicht konstant, er ändert sich mit dem Umfeld, je nach technologischer oder wirtschaftlicher Entwicklung sowie abhängig von der rechtlichen Basis. Daher verlangt die Norm, dass der Kontext ständig überwacht wird, damit das ISMS immer auf dem aktuellen Stand basiert.

Die Analyse hat folgende Ziele:

- Verständnis des Kontexts, um den Umfang des ISMS festzulegen,
- Analyse des Kontexts, um Risiken und Chancen zu ermitteln, und
- Sicherstellung, dass das ISMS an sich ändernde externe und interne Themen angepasst ist.

Externe Faktoren sind solche, die außerhalb der Kontrolle der Organisation liegen. Dies wird oft als »das Umfeld der Organisation« bezeichnet. Die externen Faktoren umfassen gesetzliche Vorschriften, Marktanforderungen, technologische Entwicklungen, politische Ereignisse oder soziale Erwartungen. Auch der Klimawandel bzw. die Folgen für das eigene Unternehmen sind dabei in die Überlegungen miteinzubeziehen. Ein Unternehmen im stark regulierten Finanzdienstleistungs- oder Gesundheitsbereich steht vor ganz anderen Herausforderungen als ein Start-up im Modebereich. Selbst kleine Organisationen unterliegen aber dem Einfluss von Kunden, Partnern, Lieferanten oder staatlichen Organisationen. Auf Basis dieser Faktoren wird ein angemessenes Niveau der Informationssicherheit dargestellt.

Der von der Arbeitsgruppe ISO/IEC JTC 1/SC27 herausgegebene *Practical Guide* listet folgende Beispiele auf:

- **wirtschaftliche Faktoren**, die sich auf das Unternehmen und sein ISMS auswirken können, wie z. B. die Wirtschaft im Allgemeinen, Wechselkurse, Zinssätze, Inflation, Verfügbarkeit von Krediten, Löhne, Transportkosten
- **soziale Faktoren**, wie z. B. Arbeitslosenquoten, Sicherheitsanforderungen, Bildungsniveau, Öffentlichkeit, Kultur
- **politische Bedingungen**, wie z. B. politische Stabilität, öffentliche Investitionen, lokale Infrastruktur, internationale Handelsabkommen

- **technologische Trends**, die sich auf das Unternehmen und sein ISMS auswirken können, z. B. neue Technologien, neue Softwareversionen, neue Hardware
- **vertragliche Beziehungen** zu Kunden und Lieferanten und Berücksichtigung der jeweiligen Anforderungen an die Informationssicherheit, soweit dies für die Dienstleistungen und Produkte relevant ist
- **gesetzliche und regulatorische Faktoren**, wie z. B. Datenschutzbestimmungen, Cybersicherheitsgesetze, Arbeitsrecht, Wettbewerbsvorschriften, Import-/Exportbeschränkungen oder Branchenvorschriften

Im Februar 2024 wurde eine Änderung veröffentlicht (»Amendment 1«). Sie verlangt, dass in Kapitel 4.1 am Ende des Unterabschnitts folgender Satz hinzugefügt wird: »Die Organisation muss feststellen, ob der Klimawandel ein relevantes Thema ist.«

Je nach akkredierter Zertifizierungsstelle wird diese Anforderung enger oder weiter aufgefasst. Jedes Unternehmen muss diesen Punkt bei den Faktoren berücksichtigen.

Interne Faktoren sind genauso wichtig und beziehen sich auf die organisatorische Struktur, Ressourcen, Unternehmenskultur, strategische Ausrichtung sowie auf bereits vorhandene Managementsysteme. Eine Organisation mit starken Hierarchien wird ein anderes Sicherheitsverständnis haben als eine Organisation mit flachen Hierarchien und agilen Praktiken. Die IT-Landschaft, die Fähigkeiten der Mitarbeitenden oder bereits gemachte Erfahrung mit Sicherheitsvorfällen spielen ebenfalls eine Rolle im Kontext.

Die ISO 27003 listet auch für interne Faktoren einige Beispiele auf. Es handelt sich dabei um:

- Kultur der Organisation
- Richtlinien, Ziele und Strategien
- Governance, Organisationsstruktur, Rollen und Verantwortlichkeiten
- Standards, Leitlinien und Modelle innerhalb der Organisation
- Prozesse und Verfahren
- physische Infrastruktur und Umgebung
- Informationssysteme, Informationsflüsse und Entscheidungsprozesse
- frühere Audits und frühere Ergebnisse der Risikobewertung

Die Norm ist jedoch nicht spezifisch dazu, wie alles dokumentiert oder aufgezeichnet werden soll. In der Praxis sind strukturierte Analysen des Kontexts üblich, beispielsweise durch eine *SWOT*-Analyse, durch das *PESTEL-Framework* (das Kürzel steht für: politisch, wirtschaftlich, sozial, technologisch, ökologisch, rechtlich) oder durch eine Umfeldanalyse mit Bezug auf die interessierten Parteien. Die Analysen sollten helfen, das abstrakte Konzept zu konkretisieren und seinen Einfluss besser zu verstehen.

Die organisatorische Kontextanalyse bedeutet jedoch auch, dass diese Erkenntnisse in alles einfließen, was die Organisation tut. Nur einmal eine Analyse zu erstellen, bringt nur

kurzfristig einen Erfolg. Die gewonnenen Erkenntnisse müssen die Grundlage für alles sein, was zu tun ist, um die Informationssicherheit sicherzustellen und auf einem hohen Niveau zu halten.

Schließlich kann das Verstehen des Kontexts dazu beitragen, dass die Risikobeurteilung angemessen ist, und es kann helfen, Aktivitäten und Anforderungen zu priorisieren.

6.1.2 NA 4.2 – Verstehen der Erfordernisse und Erwartungen interessierter Parteien

> **4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien**
>
> Die Organisation muss Folgendes bestimmen:
>
> a) die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind;
>
> b) die relevanten Anforderungen dieser interessierten Parteien;
>
> c) welche dieser Anforderungen durch das Informationssicherheitsmanagementsystem behandelt werden.
>
> ANMERKUNG Die Anforderungen interessierter Parteien können gesetzliche und regulatorische Vorgaben sowie vertragliche Verpflichtungen beinhalten.
>
> ANMERKUNG 2 Relevante interessierte Parteien können Anforderungen in Bezug auf den Klimawandel haben.

Ein ISMS ist nicht nur für das eigene Unternehmen gedacht. Es ist wichtig, Informationen zu schützen, weil ihr Verlust oder ihre Veränderung schwerwiegende Folgen für eine Vielzahl von Beteiligten haben kann.

Deshalb verlangt die ISO/IEC 27001:2022 in Abschnitt 4.2, dass Organisationen sich mit den Stellen auseinandersetzen, die von ihrer Informationssicherheit betroffen sind oder Erwartungen daran haben. Diese werden als *interessierte Parteien* oder auch als *Stakeholder* bezeichnet. Das können Kunden, Lieferanten, Behörden oder weitere Interessensgruppen sein.

Praxistipp

In der ISO 27000:2020 steht in der nationalen Fußnote N1: »In ISO/IEC 27001 wird anstatt des Begriffes ›Stakeholder‹ durchgängig der Begriff ›interessierte Partei‹ verwendet.«

Somit dürfen diese Begriffe als Synonym benutzt werden. Der Begriff wird wie folgt definiert: »Person oder Organisation, die eine Entscheidung oder Tätigkeit beeinflussen, davon beeinflusst werden oder sich davon beeinflusst fühlen kann.«

Diese *Interessengruppen*, im Englischen auch als *Interested Parties* bezeichnet, umfassen alle Personen, Gruppen oder Organisationen, die einen Bedarf an Informationssicherheit haben oder von einer Verletzung der Informationssicherheit betroffen sein könnten. Dabei sollte nicht nur an Kunden oder Behörden gedacht werden, sondern auch an Mitarbeitende, Eigentümer, Geschäftspartner, Lieferanten, Versicherungen oder sogar an die Öffentlichkeit. Interessierte Parteien einer Organisation haben oft sehr unterschiedliche Interessen, Einflussmöglichkeiten und rechtliche Verbindungen zum Unternehmen. Aufgrund dieser Vielfalt ist es umso wichtiger, sich strukturiert mit deren Erwartungen zu beschäftigen.

Die Norm verlangt, dass Organisationen zunächst herausfinden müssen, wer ihre interessierten Parteien sind. Dies kann durch interne Workshops, Interviews, Stakeholder-Analysen oder durch die Nutzung bereits verfügbarer Informationen aus Verträgen oder Vorschriften erfolgen. Darüber hinaus ist es wichtig, die relevanten Bedürfnisse und Erwartungen dieser Gruppen zu verstehen. Dabei werden bewusst nicht nur gesetzliche Anforderungen berücksichtigt, sondern auch vertragliche Verpflichtungen, ethische Erwartungen oder branchenspezifische Standards. So erwartet beispielsweise ein Kunde, dass seine Daten vertraulich behandelt werden, während eine Aufsichtsbehörde den Nachweis verlangt, dass die gesetzlichen Anforderungen an den Datenschutz erfüllt sind. Mitarbeitende legen Wert darauf, dass ihre persönlichen Daten nicht ohne ihre Zustimmung weitergegeben oder eingesehen werden.

Ein nicht zu unterschätzender Aspekt ist, dass sich die Erwartungen interessierter Parteien im Laufe der Zeit ändern können. Neue Gesetze, Sicherheitsvorfälle, technologische Entwicklungen oder gesellschaftliche Veränderungen führen dazu, dass bisherige Anforderungen angepasst oder neue formuliert werden. Aus diesem Grund muss auch diese Analyse regelmäßig durchgeführt und aktualisiert werden. Sie ist ein wichtiger Teil der kontinuierlichen Verbesserung des ISMS.

Der dritte Punkt der Normanforderung verlangt, dass aufgezeigt wird, welche Anforderungen durch das ISMS behandelt werden. Es empfiehlt sich, eine Tabelle zu erstellen: Die interessierten Parteien werden in der ersten Spalte aufgeführt, die relevanten Anforderungen in der zweiten, und in der dritten Spalte steht, welche dieser Anforderungen behandelt werden – beziehungsweise besser *wie* diese behandelt werden.

In der Praxis zeigt sich immer wieder, dass viele Sicherheitsanforderungen, die an ein Unternehmen gestellt werden, auf den ersten Blick nicht als solche zu erkennen sind. Kundenverträge mit Vertraulichkeitsklauseln, IT-Dienstleistungsverträge mit Anforderungen an die Verfügbarkeit oder branchenspezifische Audit-Anforderungen beinhalten häufig indirekte Anforderungen an das ISMS. Nur wer sich die Mühe macht, diese sorgfältig zu analysieren und zu systematisieren, wird in der Lage sein, diese im ISMS zu berücksichtigen.

Wie bereits im vorherigen Abschnitt erwähnt, wurde im Februar 2024 eine Änderung veröffentlicht (»Amendment 1«). Diese hat auch eine Erweiterung dieses Normpunkts zur

Folge. Am Ende des Unterabschnitts muss folgender Hinweis ergänzt werden: »Relevante interessierte Parteien können Anforderungen im Zusammenhang mit dem Klimawandel haben.« Daher gehören auch diese Anforderungen in die Auflistung der möglichen Anforderungen.

6.1.3 NA 4.3 – Festlegen des Anwendungsbereichs des ISMS

> **4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems**
>
> Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.
>
> Bei der Festlegung des Anwendungsbereichs muss die Organisation Folgendes berücksichtigen:
>
> a) die unter 4.1 genannten externen und internen Themen;
>
> b) die unter 4.2 genannten Anforderungen;
>
> c) Schnittstellen und Abhängigkeiten zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten, die von anderen Organisationen durchgeführt werden.
>
> Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

Die erarbeiteten Punkte bilden in der Folge die Grundlage für den *Anwendungsbereich* (im Englischen als *Scope* bezeichnet) und somit für alle weiteren Maßnahmen im ISMS. Der Anwendungsbereich legt fest, welche Informationen, Prozesse, Standorte, Systeme und Einheiten in das Schutzkonzept mit einbezogen werden – und welche nicht. Diese Entscheidung beeinflusst direkt den Umfang der Risikoanalyse, die anzuwendenden Sicherheitsmaßnahmen und die Aussagekraft eines möglichen Zertifikats.

Die Bestimmung des Anwendungsbereichs sollte gut geplant sein. Die Grundlage sind die Ergebnisse aus Kapitel 4.1 (»Verstehen des Kontexts der Organisation«) und Kapitel 4.2 (»Verstehen der interessierten Parteien und ihrer Anforderungen«). Nur wenn die Struktur der Organisation, bestehende Abhängigkeiten und Risiken sowie zu erfüllende Anforderungen bekannt sind, kann sinnvoll bestimmt werden, was das ISMS tatsächlich beinhalten muss. Die Norm schreibt ausdrücklich vor, dass die Organisation interne und externe Themen, interessierte Parteien sowie deren Anforderungen berücksichtigt, um einen fundierten und begründbaren Geltungsbereich zu bestimmen.

Praktisch heißt das, dass nicht unbedingt die gesamte Organisation abgedeckt werden muss. Insbesondere größere Unternehmen wählen häufig den Weg, das ISMS zunächst auf bestimmte Geschäftsbereiche, Länderorganisationen oder sogar einzelne Services zu beschränken. Solange diese Einschränkung begründet, dokumentiert und transparent kommuniziert wird, ist sie zulässig. Ein häufiges Kriterium ist zum Beispiel die entschei-

dende Bedeutung eines Bereichs für das Kerngeschäft, besonders hohe regulatorische Anforderungen oder die Notwendigkeit, schnell auf Kundenanforderungen reagieren zu können.

Die Norm mahnt jedoch zur Vorsicht: Der Anwendungsbereich darf nicht absichtlich verkleinert werden, um kritische Systeme oder Bereiche gezielt auszuschließen. Auslassungen dieser Art würden das ISMS als unglaubwürdig erscheinen lassen und bei einer Zertifizierung wahrscheinlich auffallen. Ausschlüsse, die nicht abgedeckte Aspekte darstellen, sind nur dann erlaubt, wenn sie keine Auswirkungen auf die Fähigkeit des ISMS haben, die angestrebten Ergebnisse zu erzielen. Die Organisation selbst trägt die Verantwortung für die Abgrenzung und muss erklären können, warum der gewählte Anwendungsbereich angemessen ist.

Ein wichtiger Aspekt bei der Bestimmung des Anwendungsbereichs ist der Abschnitt c). Die Organisation muss die Schnittstellen und Abhängigkeiten zwischen intern durchgeführten Tätigkeiten und solchen, die von Dritten übernommen werden, berücksichtigen. Diese Anforderung nimmt Bezug darauf, dass die Informationsverarbeitung selten vollständig selbstständig erfolgt. Externe IT-Dienstleister, Cloud-Anbieter, Supportfirmen, ausgelagerte Geschäftsprozesse sowie globale Lieferketten – all diese Konstellationen erzeugen technische und organisatorische Abhängigkeiten, die direkte Auswirkungen auf die Informationssicherheit haben.

Praktisch heißt das: Wenn ein externes Unternehmen beispielsweise für den Betrieb von IT-Systemen, das Hosting von Anwendungen oder den Support von Endbenutzern verantwortlich ist, muss das Unternehmen die Informationssicherheit dieser Tätigkeiten trotzdem überprüfen. Selbst wenn der technische Betrieb extern vergeben ist, muss das ISMS diese Schnittstellen einbeziehen. Die Kontrolle kann beispielsweise durch Lieferanten-Audits erfolgen.

Es ist erforderlich festzulegen, wer welche Aufgaben übernimmt, wo die Übergabepunkte genau liegen und wie Kontrollmechanismen an den Schnittstellen definiert sind. Nicht nur für die Sicherheit, sondern auch für die Auditierbarkeit des Systems zu einem späteren Zeitpunkt sind diese Überlegungen relevant. Auch der Auditor wird überprüfen, ob ausgelagerte Prozesse ausreichend in das ISMS integriert sind – beispielsweise durch vertragliche Verpflichtungen, Zugriffsregelungen oder Kontrollrechte.

Wichtig ist bei allen Überlegungen, dass der Anwendungsbereich nicht nur intern bekannt ist, sondern auch dokumentiert und veröffentlicht wird.

Praxistipp

Die Beschreibung des Anwendungsbereichs erscheint auch auf dem Zertifikat. Dieser Satz könnte beispielsweise wie folgt lauten: »Das ISMS umfasst die Planung, den Betrieb und die Überwachung aller IT-Systeme der Hauptniederlassung an Standort A, die für die Verarbeitung von Kundendaten der X AG zuständig sind.«