Informationssicherheit und Datenschutz

Handbuch für Praktiker und Begleitbuch zum T.I.S.P.

2 Betriebswirtschaftliche Aspekte der Informationssicherheit

Einleitung

Jede unternehmerische Aktivität ist zahlreichen Risiken ausgesetzt. Daher ist unternehmerisches Handeln zu einem erheblichen Teil Risikomanagement: Jede unternehmerische Entscheidung soll Chancen ergreifen und zielt zugleich auf die Minimierung ganz unterschiedlicher Arten von Risiken. Dabei stehen vor allem Marktrisiken im Fokus; aber auch finanzielle Risiken (Liquiditätsrisiko, Zahlungsausfälle bei Kunden) und rechtliche Risiken (Patente, gesetzliche Anforderungen, Prozessrisiken) spielen im Kontext der Globalisierung und steigender Erwartungen der Marktteilnehmer an den unternehmerischen Erfolg eine immer wichtigere Rolle.

Das gilt insbesondere für die Besserung der Kreditwürdigkeit oder wenn der Unternehmenswert ermittelt wird, z. B. im Vorfeld eines Unternehmensverkaufs oder bei einer Börsennotierung. Dabei kommt der Bewertung der bestehenden Risiken und der Einschätzung der diesbezüglichen Stärke des Unternehmens ein erhebliches Gewicht zu. Seit einigen Jahren spielen dabei neben externen Risiken auch sogenannte operationelle Risiken eine immer größere Rolle. Darunter werden alle betrieblichen Risiken innerhalb eines Unternehmens mit wirtschaftlichen Auswirkungen verstanden. In der Eigenkapitalvereinbarung Basel II, nach der seit Inkrafttreten von Kreditinstituten erstmals auch operationelle Risiken bei der Eigenkapitalhinterlegung zu berücksichtigen sind, werden diese definiert als »*Risiko von Verlusten, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen oder durch externe Ereignisse verursacht werden.*« [Wiki_23]. In diese Kategorie fallen insbesondere alle Ausfälle und Fehler der Informationstechnik – unabhängig davon, ob diese durch technisches Versagen, durch gezielte oder ungezielte, externe oder interne Manipulation verursacht werden.

Alle Arten von Bedrohungen der Informationssicherheit zählen daher zu den operationellen Unternehmensrisiken. Daher wird – auch vor dem Hintergrund zunehmender Compliance-Anforderungen – die Informationssicherheit inzwischen in vielen Unternehmen als aktives Risikomanagement verstanden. Zum einen, weil in einer globalisierten Wirtschaft ein unkontrollierter Abfluss von Informationen irreparable wirtschaftliche Schäden verursachen kann, zum anderen, weil immer mehr Geschäftsprozesse von dem störungsfreien Funktionieren der Informationstechnik abhängen. Selbst aus dem Datenschutz können Risiken mit betriebswirtschaftlichen Auswirkungen erwachsen: Beschwerden von Kunden oder Mitarbeitern bei der Aufsichtsbehörde wegen Verstößen gegen geltendes Datenschutzrecht oder meldepflichtige Datenschutz-Vorfälle können nicht nur die Einleitung von Untersuchungen der Aufsichtsbehörde, sondern auch schmerzhafte Bußgelder und Schadensersatzforderungen der Betroffenen zur Folge haben.

Damit hat auch die betriebswirtschaftliche Bewertung von Maßnahmen der Informationssicherheit und des Datenschutzes an Bedeutung gewonnen. Der Schlüssel zu einer angemessenen betriebswirtschaftlichen Betrachtung und Bewertung ist dabei die vollständige

Erfassung und eine adäquate Quantifizierung der bestehenden Risiken einerseits sowie der Kosten und Wirksamkeit von Risiko senkenden Maßnahmen andererseits. Unternehmerisch lässt sich nur auf der Grundlage möglichst konkreter, quantitativ unterlegter Bedrohungsszenarien und Lösungsalternativen entscheiden, wie mit bestimmten Risiken zu verfahren ist. Dazu lassen sich im Wesentlichen vier Möglichkeiten der Risikobehandlung unterscheiden: ignorieren, verringern, versichern oder verhindern (s. a. Abschnitt 2.3.3).

Eine solche Quantifizierung liefert zugleich eine einfache Bewertung des erreichten Sicherheitsniveaus: Dieses ist angemessen, wenn alle nicht akzeptablen Risiken durch geeignete Maßnahmen ausgeschlossen und alle verbleibenden durch passende Maßnahmen in ihren Auswirkungen begrenzt werden. Leider scheitert dieser Ansatz an zwei praktischen Schwierigkeiten: So ist erstens in den meisten Fällen eine hinreichend präzise Quantifizierung der Risiken nicht möglich, und es gelingt zweitens nur mit wenigen Maßnahmen, ein bestimmtes Risiko mit vertretbarem Aufwand treffsicher und vollständig auszuschließen.

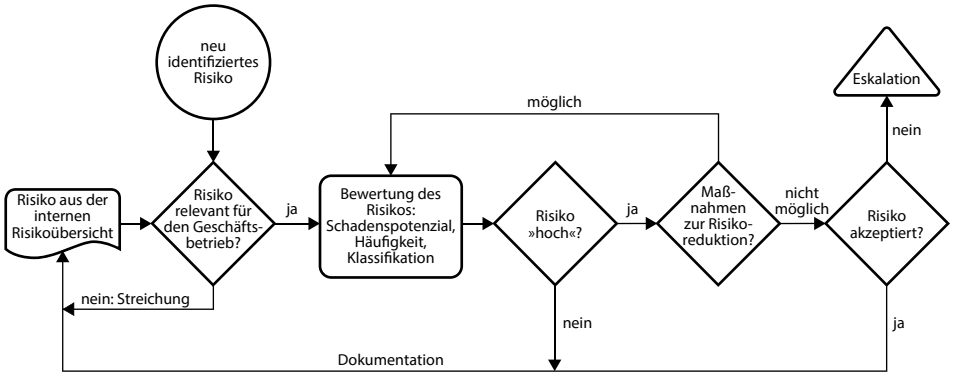
Die folgenden Abschnitte zeigen, dass die Betrachtung der Informationssicherheit aus betriebswirtschaftlicher Perspektive trotz verschiedener praktischer Schwierigkeiten dennoch einige wertvolle Ansätze bereithält. Unvermeidlich ist die Beschäftigung mit dieser Perspektive ohnehin, da mit der steigenden Bedeutung der Informationstechnik und immer umfangreicherer Verarbeitung personenbezogener Daten die Informationssicherheit und der Datenschutz zu immer wichtigeren Elementen des Risikomanagements werden.

2.1 Risikomanagement

Unter Risikomanagement werden alle Prozesse eines Unternehmens zum Umgang mit Geschäftsrisiken verstanden. Die ISO 31000 definiert das Risikomanagement als die »koordinierte Aktivität zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken« [ISO_18]. Das beginnt bei der Identifikation und Analyse von Risiken, ihrer Bewertung, des Umgangs mit den identifizierten Risiken und ihrer Überwachung. Große Unternehmen fassen meist die Behandlung aller Risiken in einem übergreifenden Risikomanagementprozess zusammen, um eine einheitliche Risikobehandlung sicherzustellen. In vielen Branchen gibt es hier aufsichtsbehördliche Anforderungen, die zu erfüllen sind und sowohl eine Dokumentation der Risikobehandlung als auch eine regelmäßige interne und externe Auditierung des Risikomanagements erfordern. Ähnliche Anforderungen leiten sich aus einer Börsennotierung des Unternehmens ab.

Den Gesamtprozess des Risikomanagements kann man sich – vereinfacht – vorstellen, wie in Abbildung 2.1 gezeigt: Regelmäßig (z. B. jährlich) sowie anlassbezogen (beim Auftreten eines neuen Risikos, z. B. durch die technische Entwicklung oder eine Unternehmensakquisition) werden die Risiken aus der Risikoübersicht geprüft: Sind sie (noch) relevant? Wenn ja, wie sind die Risiken zu bewerten? Wenn sie als hohes Risiko zu bewerten sind: Können Maßnahmen getroffen werden, um das Risiko zu senken? Wenn nicht: Kann das (verbleibende) Risiko dennoch akzeptiert werden?

Abbildung 2.1: Risikomanagementprozess



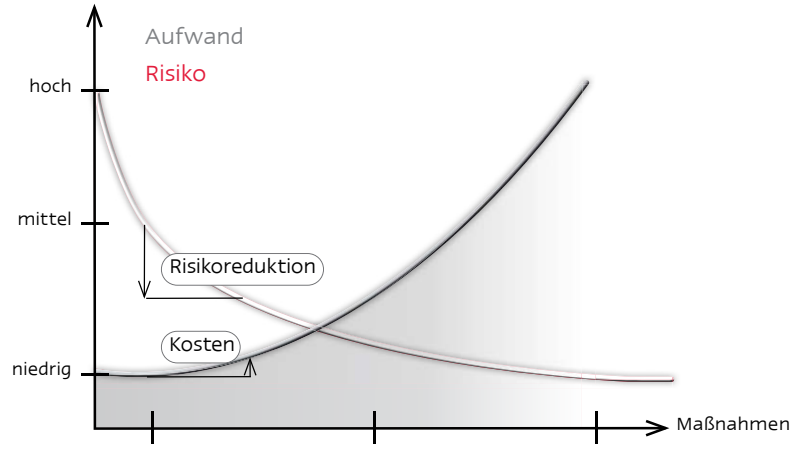
Bei der Identifikation von Risiken können Bedrohungsszenarien helfen, wie z. B. in der »Risiko-Toolbox« der Enisa vorgeschlagen [ENISA_23]. Die Klassifikation dieser (IT-Sicherheits-)Risiken erfolgt dann in der Regel durch eine Einordnung in eine Risikomatrix (Abb. 2.4): Schadenspotenzial (Schadenshöhe) und Eintrittswahrscheinlichkeit (Häufigkeit) werden in drei bis vier, selten auch fünf Stufen unterteilt (niedrig, mittel, hoch, ggf. sehr hoch) [BITKOM_05, BSI_17]. Die Zuordnung zu einer Stufe wird dabei entweder mit quantitativen Bewertungsmodellen oder qualitativ vorgenommen. Aus der resultierenden Risikoklasse leitet sich dann in der Regel ein unterschiedlicher Umgang mit den identifizierten Risiken ab. Die ISO/IEC 27005:2022 beschreibt einen solchen systematischen Prozess zur Identifikation, Bewertung, Behandlung und Überwachung der IT-Sicherheitsrisiken [ISO_22]. Dieses Management der IT-Sicherheitsrisiken sollte dann geeignet in den unternehmensweiten Risk-Management-Prozess (Enterprise Risk Management – ERM) integriert werden [NIST_20].

2.2 Quantitative Modelle

Aus betriebswirtschaftlicher Perspektive muss jeder Sicherheitsmaßnahme eine angemessene Risikoreduktion gegenüberstehen – der für die Umsetzung der Maßnahme erforderliche Aufwand muss sich »lohnen«. Für diese betriebswirtschaftliche Abwägung und Maßnahmenbewertung wurden Berechnungsmodelle zur Bestimmung eines quantitativen *Return on Security Investment* (ROSI) entwickelt.

Risiken und Sicherheitsmaßnahmen lassen sich betriebswirtschaftlich als Kosten ausdrücken: Risiken werden im Falle ihres Eintretens zu einem quantifizierbaren Schaden; Sicherheitsmaßnahmen hingegen verursachen unmittelbare direkte Kosten.

Abbildung 2.2: Verhältnis von Risikoreduktion und Kosten



Den Kosten für eine Sicherheitsmaßnahme sollte, damit die Investition wirtschaftlich ist, eine (nachhaltige) Risikoreduktion gegenüberstehen. Ziel dabei ist, eine hinreichende Risikoreduktion mit moderaten Kosten zu erreichen. Denn übersteigen die Kosten einer Sicherheitsmaßnahme das tatsächliche Risiko, ist es wirtschaftlicher, auf die Sicherheitsmaßnahme zu verzichten und das Risiko billigend in Kauf zu nehmen.

Abbildung 2.2 zeigt in einer vereinfachten Schemagrafik das idealtypische Verhältnis von Risiken, Kosten (Aufwand) und Sicherheitsmaßnahmen. Dabei wurde angenommen, dass die Maßnahmen nach »Wirkungsgrad« ergriffen wurden: Maßnahmen mit hoher Risikoreduktion, aber geringen Kosten wurden zuerst ergriffen, Maßnahmen mit hohen Kosten und geringer Risikoreduktion später – daher der stetige Verlauf der Kurven. Tatsächlich werden die Maßnahmen in der Praxis nicht in solcherart idealisierter Reihenfolge (die wirksamsten Maßnahmen zuerst) umgesetzt – einerseits aufgrund von Abhängigkeiten der Maßnahmen untereinander und der daraus resultierenden Schwierigkeit, die tatsächliche Risikoreduktion zu bestimmen, andererseits wegen der Abhängigkeit von externen Faktoren. Ein »realer« Kurvenverlauf wird in der Praxis daher nicht so stetig ausfallen (können).

In den folgenden Abschnitten werden Modelle zur Quantifizierung der Kosten von Risiken und Maßnahmen vorgestellt.

2.2.1 Kosten von Risiken

Die Festlegung eines akzeptablen Risikolevels ist eine unternehmerische Frage, die im Zweifel von der Geschäftsleitung beantwortet werden muss. Eine vernünftige Einschätzung ist allerdings nur dann möglich, wenn das Risiko in einer finanziellen Größenordnung ausgedrückt werden kann. Im Risikomanagement wird dafür üblicherweise der zu erwartende jährliche Verlust (*Annual Loss Expectancy*, ALE) bestimmt. Der ALE errechnet sich aus der finanziellen Höhe (*Loss*, L) und der Eintrittswahrscheinlichkeit (*Probability*, P) eines möglichen Schadens:

$$ALE = L \cdot P$$

Der erwartete Gesamtverlust ergibt sich als Summe der Erwartungswerte aller betrachteten Einzelrisiken:

$$ALE_{tot} = \sum_{i=1}^{n} L_i \cdot P_i$$

Die Anwendung der Berechnung des ALE für Bedrohungen der Informationstechnik geht auf die (inzwischen zurückgezogene) Richtlinie FIPS PUB 65 des NIST aus dem Jahr 1979 zurück [FIPS65]. Sie bildet die Grundlage für zahlreiche Ansätze von Kosten-Nutzen-Modellen der Informationssicherheit, insbesondere auch des ROSI-Ansatzes (s. u.). Die Reduktion eines spezifischen Risikos kann danach auf zweierlei Weise erfolgen:

- Entweder wird durch geeignete Gegenmaßnahmen die Eintrittswahrscheinlichkeit des Schadens verringert, z. B. durch einen Viren-Scanner auf einem E-Mail-Server oder den Betrieb einer Firewall,
- oder es werden Maßnahmen ergriffen, die die Auswirkungen des Schadens begrenzen, wie z. B. die konsequente Umsetzung des Need-to-know-Prinzips bei der Berechtigungsvergabe oder ausgearbeitete und trainierte Notfallpläne, betriebsbereite Ersatzsysteme und ausgefeilte Wiederanlaufprozesse.

Damit ist das Problem der Quantifizierung eines Risikos jedoch noch nicht gelöst, denn

- für die Eintrittswahrscheinlichkeit eines Schadens in der Informationstechnik existieren – anders als für viele andere, versicherbare Schäden – keine belastbaren Erfahrungswerte,
- durch die Schnelllebigkeit und die kurzen Innovationszyklen der Informationstechnik ändern sich sowohl die tatsächlichen Risiken als auch die möglichen Auswirkungen und deren Eintrittswahrscheinlichkeiten in sehr kurzen Zeiträumen und
- der errechnete erwartete Verlust ist eine rein statistische Größe – er kann im Einzelfall erheblich über- oder unterschritten werden.

Da sich mit diesem Berechnungsansatz nur ein einzelnes Risiko betrachten lässt, geht das ALE-Modell außerdem implizit von der Annahme aus, dass einzelne Bedrohungen und Gegenmaßnahmen isoliert betrachtet werden können. Das ist in der Praxis jedoch in den meisten Fällen eine grobe Vereinfachung. So gibt es Gegenmaßnahmen, die Schutz vor mehreren Bedrohungen bieten, wie z. B. eine Firewall (externer Denial-of-Service-Angriff auf Client-Systeme, Missbrauch des E-Mail-Servers, unberechtigter externer Zugriff auf vertrauliche Daten), und es gibt Maßnahmen, die neue Risiken verursachen, wie z. B. die Auslagerung von Backups.

Schließlich berücksichtigt das ALE-Modell keine kumulativen Effekte: Die Einzelrisiken werden einfach addiert. In der Praxis aber wird sich die Zahl der verlorenen Kunden aufgrund eines einstündigen Ausfalls des Onlinebankings bei einem Kreditinstitut in Grenzen halten; kommt es hingegen in kurzer Zeit wiederholt zu solchen Ausfällen, kann dies einen erheblichen Image-Schaden mit schmerzlichem Kundenverlust zur Folge haben – und einen Schaden verursachen, der die Summe der erwarteten Einzelschäden erheblich übersteigt.

Nicht zuletzt kann in dem Modell nicht zwischen großen Schäden mit geringer Eintrittswahrscheinlichkeit und geringen Schäden mit hoher Eintrittswahrscheinlichkeit unterschieden werden – obwohl sich Letztere meist sehr gut kontrollieren lassen, Erstere aber existenzbedrohend sein können und ihr Eintritt daher durch geeignete Maßnahmen in jedem Fall verhindert werden sollte.

Daher wurde das ursprüngliche ROSI-Modell mehrfach verfeinert, um verwertbarere Aussagen zu erhalten.

2.2.2 Kosten von Sicherheitsvorfällen

Die Kosten eines Sicherheitsvorfalls sind meist – insbesondere, wenn es tatsächlich zum Eintritt eines Schadens gekommen ist – deutlich einfacher zu quantifizieren. Leider bestimmen und dokumentieren nur die wenigsten Unternehmen die tatsächlichen Kosten eines Schadensfalls hinreichend genau, und das oft nicht einmal wegen des damit verbundenen Aufwands. Dabei ergäben sich aus diesen Erfahrungswerten sowohl eine hilfreiche Datenbasis für die finanzielle Abschätzung bestimmter Schäden als auch die Chance, geeignete Maßnahmen zu ergreifen, mit denen sich bei ähnlichen Vorfällen zukünftig das Schadensausmaß gezielt verringern ließe.

Die Kosten eines Sicherheitsvorfalls setzen sich aus den folgenden Einzelkosten zusammen:

- **Umsatzeinbußen und Wertverlust**
  unmittelbar durch Ausfallzeiten (diese Kosten sind in der Regel größer als die Gemeinkosten, d. h. die Betriebskosten während der Ausfallzeit) und mittelbar durch den Verlust von Kunden oder Aufträgen, bspw. aufgrund eines nachfolgenden Image-Schadens. Wertverlust und Umsatzrückgang oder -ausfall (*Loss*, L) lassen sich in Abhängigkeit von der Dauer t der Wirkung ausdrücken: Li(t).

- **Wiederherstellungskosten**
  Ersetzung oder Wiederanlauf der betroffenen Systeme, Wiedereinspielen von Images, Betriebssystemen oder Daten von Backups, gegebenenfalls Rettung teildefekter Datenträger. Die Wiederherstellungskosten setzen sich aus externen (leicht exakt quantifizierbaren) Kosten (Recovery, Re) für Unterstützungsleistungen beim Wiederanlauf und internem Aufwand (überwiegend investierte Arbeitszeit, also Personalkosten) Ri(t) zusammen.

- **Schadensersatzleistungen**
  Vertragsstrafen bei Lieferverzögerungen infolge eines Defekts oder Systemausfalls, Kosten für Rückrufe und Ersatzlieferungen, Haftung für verursachte Schäden Dritter (bspw. durch ungewollte Verbreitung von Schadsoftware). Dies sind leicht quantifizierbare Einmal-Kosten (*Fine*, F), deren Höhe unabhängig ist von der Dauer des Vorfalls.

Daraus ergibt sich eine einfache Formel für den Gesamtverlust (L) in Abhängigkeit von der Dauer eines Vorfalls (respektive seiner Auswirkungen):

Weitere, manchmal »immateriell« genannte Schäden sind betriebswirtschaftlich nicht relevant. Denn sofern sie Kosten verursachen, fließen sie »automatisch« in eine der drei oben genannten Schadenskategorien ein. So ist z. B. ein Imageschaden, der keine Umsatz-

einbußen zur Folge hat, kein betriebswirtschaftlich zu berücksichtigender Schaden – sondern eine (wenn auch ungeplante) Marketingmaßnahme. Führt er hingegen zu Umsatzausfällen, ist er in Li(t) bereits berücksichtigt. Anders ausgedrückt: Jeder relevante Schaden ist ein materieller Schaden – und lässt sich einer der drei Schadenskategorien zuordnen.

2.2.3 Kosten von Sicherheitsmaßnahmen

Auch die Kosten einer Sicherheitsmaßnahme setzen sich aus unterschiedlichen Elementen zusammen. Dabei sollte eine Gesamtkostenbetrachtung angestellt werden (*Total Cost of Ownership*, TCO), die nicht nur die Anschaffungskosten, sondern auch alle weiteren direkten und indirekten (Folge-)Kosten einer Sicherheitsinvestition berücksichtigt:

- **Konzeptionskosten C_c**
  Architektur, Lösungsauswahl, Testbetrieb, gegebenenfalls Anpassungen an der eigenen Infrastruktur (Konfiguration, Dokumentation) oder der gewählten Lösung
- **Investitionskosten C_i**
  Hardware, Software, Installation und Konfiguration, Dokumentation, Inbetriebnahme und Mitarbeiterschulungen (Administratoren, Benutzer)
- **Betriebskosten C_m**
  Support, Updates, jährliche Lizenzkosten, Betriebsprozesse (Betreuung, Hotline)

Aus diesen drei Kostenblöcken werden die Gesamtkosten der Sicherheitsinvestition (TCOSI) berechnet. Dabei werden die Einmalkosten (Konzeption, Investition) über den Betriebszeitraum y (in Jahren) abgeschrieben, während die Betriebskosten jährlich anfallen:

$$TCO_{SI} = \frac{(C_c + C_i)}{y} + C_m$$

Sonnenreich und seine Mitautoren weisen in ihrer Arbeit [SoAS_06] zu Recht darauf hin, dass in der Regel mit der Einführung einer Sicherheitsmaßnahme auch Produktivitätsverluste bei den Anwendern einhergehen. So kann eine Maßnahme zur Folge haben, dass sich das Starten der Client-Rechner verlängert, die Eingabe eines zusätzlichen Passworts oder längere Reaktionszeiten beim Zugriff auf verschlüsselte Daten Bearbeitungsprozesse verlangsamen oder regelmäßige Backups wertvolle Arbeitszeit binden. Eine faire Berechnung sollte daher auch Produktivitätsverluste als Teil der »Betriebskosten« einer Sicherheitsmaßnahme in der Kalkulation berücksichtigen.

2.2.4 Das ROSI-Modell

Nach dem Platzen der »Dotcom-Blase« im Jahr 2000 sahen sich IT-Verantwortliche angesichts der (steigenden) Kosten der Informationstechnik zunehmend dem kritischen Blick der Controller ausgesetzt. Wie bei anderen Investitionen auch wurde in vielen Unternehmen die Berechnung eines Return on Investment (ROI) als Bewertungsverfahren für die Wirtschaftlichkeit einer IT-Investition eingefordert. Die Kennzahl ROI geht auf Donaldson Brown (1885 – 1965) zurück, der sie im Jahr 1913 einführte. Sie sollte die Bewertung der Wirtschaftlichkeit (Rendite) einer unternehmerischen Investition ermöglichen und ist

definiert als das Produkt aus Umsatzrendite (= Gewinn/Nettoumsatz · 100) in Prozent und dem Kapitalumschlag (= Nettoumsatz/Gesamtkapital). Daraus ergibt sich die folgende einfache Berechnungsformel:

$$ROI = \frac{Gewinn}{Gesamtkapital} \cdot 100\ [\%]$$

Der ROI gibt also das prozentuale Verhältnis des Gewinns zum eingesetzten Kapital an. Diese Kennzahl kann sowohl zur Bestimmung der Wirtschaftlichkeit einer Gesamtinvestition (Unternehmen) als auch zur Bewertung des betriebswirtschaftlichen Erfolgs einer Periode (Monat, Quartal, Jahr) verwendet werden.

Ein erweitertes Verständnis des ROI erlaubt außerdem Wirtschaftlichkeitsbetrachtungen von Einzelinvestitionen, sofern der einer bestimmten Investition anteilig zuzurechnende Gewinn separiert werden kann:

$$ROI = \frac{Gewinnanteil}{Kapitaleinsatz} \cdot 100\ [\%]$$

Dabei wird der Gewinnanteil über die Nutzungsdauer der getätigten Investition berechnet. Diese Entwicklung blieb nicht ohne Auswirkung auf die IT-Sicherheit. So basiert der Ansatz zur Berechnung eines *Return on Security Investment* (ROSI), der auf Arbeiten von Kevin J. Soo Hoo an der Stanford University [Hoo_00] und (unabhängig von Hoo) Huaqiang Wei an der University of Idaho zurückgeht [WeFr_01], auf Browns ROI-Kennzahl. Darin stellen die Autoren eine Risk-Management-basierte Kosten-Nutzen-Berechnung für Sicherheitsinvestitionen vor. Wei gibt ein Rechenbeispiel für ein Intrusion-Detection-System, Hoo berechnet die Einsparungen für ein ganzes Bündel von Sicherheitsmaßnahmen. Allgemein bekannt wurde das ROSI-Konzept im Jahr 2002 durch eine Veröffentlichung von Scott Berinato im CIO Magazin [Beri_02].

Der Kern des ROSI-Berechnungsmodells ist einfach: Jede wirksame Sicherheitsinvestition (SI) reduziert entweder die Eintrittswahrscheinlichkeit (P) oder die Höhe eines bestimmten Schadens (L). Damit sinkt der erwartete Schaden, die *Annual Loss Expectancy* (ALE). Der »Gewinn« einer Sicherheitsmaßnahme ergibt sich damit aus der Verringerung dieses Erwartungswerts minus den Gesamtkosten der Maßnahme (TCOSI) und die Kennzahl ROSISI als Quotient aus Gewinn und Kosten [Enisa_12]:

$$ALE_{neu} = L_{neu} \cdot P_{neu}$$

$$\text{"Gewinn"} = ALE_{alt} - ALE_{neu} - TCO_{SI}$$

$$ROSI = \frac{ALE_{alt} - ALE_{neu} - TCO_{SI}}{TCO_{SI}} \cdot 100\ [\%]$$

2.2.5 Grenzen des ROSI-Ansatzes

Eine grundsätzliche Schwierigkeit ist zunächst einmal, dass der »Gewinn« einer Sicherheitsinvestition selten in eine *messbare* Verminderung von Ausgaben oder eine Erhöhung von Einnahmen mündet. Der Gewinn besteht in einer Verminderung eines operationellen Risikos, also eines Erwartungswerts für die Kosten von Sicherheitsvorfällen – ob dadurch tatsächlich Einsparungen erzielt worden sind, lässt sich selbst ex post nicht zuverlässig feststellen. Denn auch wenn – bspw. bei häufigen Schadensereignissen – ein Rückgang beobachtet werden kann, ist der ursächliche Zusammenhang mit der Sicherheitsmaßnahme in der Regel nicht belegbar.

Beispiel 1
Sie investieren in ein modernes, mehrstufiges Firewall-System. Wenn anschließend die Zahl der Angriffsversuche sinkt, kann das auch daran liegen, dass andere Angriffsziele vielversprechender waren, oder schlicht die Zahl der breit gestreuten Angriffe insgesamt abgenommen hat.

Beispiel 2
Sie führen eine Security-Awareness-Kampagne durch, die insbesondere für einen sicherheitssensiblen Umgang mit mobilen Geräten wirbt. Wenn anschließend die Zahl der entwendeten Laptops zurückgeht, kann das auf die Kampagne zurückzuführen sein – oder aber darauf, dass Ihre Laptop-Modelle inzwischen einen geringeren Diebstahlanreiz bieten.

Aber auch die berechneten Erwartungswerte besitzen eine systematische Schwäche: Sie beruhen – anders als bei der Berechnung von zahlreichen anderen, versicherbaren Risiken – auf keinen verlässlichen und ausreichend vergleichbaren Daten aus der Vergangenheit. Damit sind sie zumeist sehr grobe »Bauchschätzungen«. Je geringer die Schadenswahrscheinlichkeit, desto weniger Erfahrungswerte gibt es und dementsprechend größer ist die Ungenauigkeit der Schätzung.

Zudem besitzen die Schätzungen der Höhe der Kosten eines Vorfalls eine sehr große »Unschärfe« (Varianz). So hängen bspw. die Kosten eines Recoverys von Client-Systemen u. a. davon ab, ob virtuelle Maschinen, vereinheitlichte Images oder sehr heterogene, individuell konfigurierte oder dezentral betreute Systeme betroffen sind. Auch gibt es insbesondere bei der Erfassung tatsächlicher Angriffe eine hohe Dunkelziffer: Die Zahl erfolgreicher Angriffe, entdeckter erfolgreicher Angriffe und berichteter erfolgreicher Angriffe differieren erheblich (s. z. B. [Hoo_00]).

Schließlich liegt dem Modell eine vereinfachende Annahme zugrunde, durch die die durchgeführten Kalkulationen im Einzelfall Makulatur werden können. So werden im ROSI-Modell Einzelrisiken und darauf bezogene Sicherheitsmaßnahmen jeweils isoliert betrachtet – dabei wirken Sicherheitsmaßnahmen in der Praxis häufig auf zahlreiche Einzelrisiken, umgekehrt treten in einem Schadensfall erfahrungsgemäß meist Folgen aus kumulierten Risiken ein.

Nicht zuletzt sorgt die hohe Entwicklungsgeschwindigkeit in der Informationstechnik dafür, dass für die Amortisation einer Sicherheitsinvestition in der Regel nur kurze Zeit bleibt, da die ständige Veränderung der IT-Infrastrukturen die Wirksamkeit einer Sicherheitsmaßnahme erheblich beeinträchtigen kann. Werden bspw. mobile Geräte (Laptops, Smartphones) mit direktem Internet-Zugang eingeführt, benötigen sie Personal Firewalls,

will man das durch die Firewall-Infrastruktur erreichte Sicherheitsniveau nicht absenken – eine zusätzliche Investition, die die ROSI-Erfolgsrechnung der Firewall verschlechtern kann.

Auf einen wichtigen, allerdings ebenfalls schwer kalkulierbaren, in den Modellen von Hoo und Wei unberücksichtigten Kostenfaktor bei Sicherheitsinvestitionen weisen Sonnenreich et. al. [SoAS_06] hin: den Produktivitätsverlust, der mit einigen Sicherheitsmaßnahmen einhergeht. In Einzelfällen kann eine Sicherheitsmaßnahme auch durch Seiteneffekte produktivitätsfördernd wirken, so bspw., wenn eine systematische Vergabe von Benutzerrechten und die Etablierung von Prozessen den Aufwand für die Administration (bspw. durch Gruppenbildung) verringert oder Single Sign-On (SSO) die Authentisierungsprozesse beschleunigt.

2.2.6 Alternative quantitative Modelle

In den vergangenen Jahren wurden zahlreiche Erweiterungen oder Anpassungen des ROSI-Modells vorgestellt, die einige der Nachteile des ursprünglichen Modells abschwächen. Zwei dieser Modelle sind besonders vielversprechend und werden im Folgenden vorgestellt: ein Ansatz, der eine statistische Verteilung von Eintrittswahrscheinlichkeit und Schadenshöhe berücksichtigt, und ein zweiter, der die betriebswirtschaftliche Sicht eines Angreifers modelliert.

Der Lockstep-Ansatz

Dem Problem der »Unschärfe« widmet sich ein Ansatz der Australischen Bundesbehörden, der von Lockstep Consulting entwickelt wurde [GCIO_04]. Er basiert auf dem Australischen Risikomanagement-Standard AS 4360, der eine Klassifikation von Eintrittswahrscheinlichkeiten für IT-Sicherheitsvorfälle sowie die Schadenshöhe bietet (*Threat & Risk Assessment*, TRA). Anstatt nun feste Werte für die Eintrittswahrscheinlichkeit und die Kosten eines Schadensereignisses zu verwenden, wird für jede Klasse ein Bereich definiert (minimale/maximale Häufigkeit/Kosten). Mit einem Zufallsgenerator werden dann über mehrere Iterationen unterschiedliche Werte nach einer vorgegebenen statistischen Verteilung gewählt und die Erwartungswerte für den jährlichen Verlust mit und ohne Sicherheitsmaßnahmen berechnet.

Ergebnis dieser Kalkulation sind Histogramm-Darstellungen, die die Häufigkeitsverteilung der erwarteten Schadenshöhen und der Einsparungen durch Sicherheitsmaßnahmen angeben. Die Genauigkeit des Ergebnisses steigt dabei mit der Zahl der berechneten Iterationen. Über die Summierung der Häufigkeiten lässt sich aus den Histogrammen bspw. ablesen, wie hoch die Schadenssumme in 90 % der Fälle maximal ist, und dass man mit einer 50 %igen Wahrscheinlichkeit eine bestimmte Mindesteinsparung durch Sicherheitsmaßnahmen erzielt.

Auch dieses Modell beruht auf einer vereinfachenden Annahme: Für die Eintrittswahrscheinlichkeit wurde eine uniforme Verteilung angenommen, für die Kosten eine Dreiecksverteilung zwischen Minimum, Maximum und wahrscheinlichstem Wert. Diese Einschränkung, die den als Excel-Erweiterung genutzten Freeware-Tools geschuldet ist, kann durch entsprechende Anpassungen leicht reduziert werden.

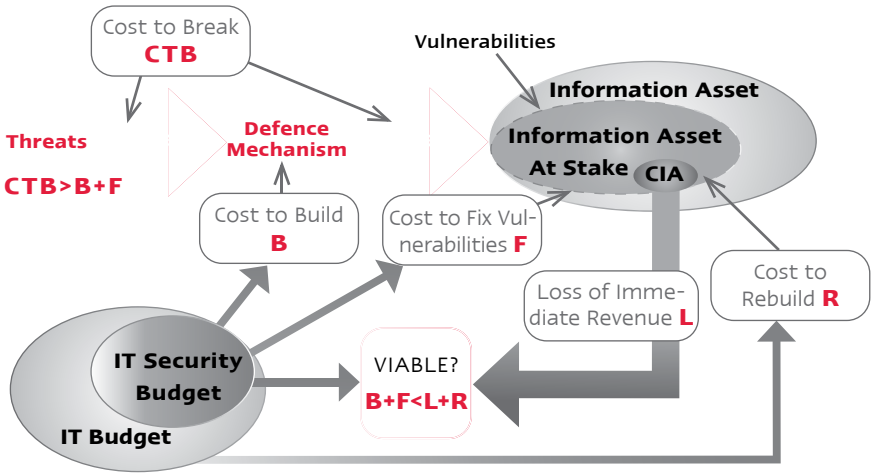
Das Modell schwächt einen erheblichen Nachteil des ursprünglichen ROSI-Modells ab. Allerdings sind auch hier bestimmte Annahmen wie die Definition des Wertebereichs

und der statistischen Verteilung der Ausgangswerte (Eintrittswahrscheinlichkeit und Schadenshöhe) entscheidend für die Qualität des Resultats – und für diese Zahlen gibt es keine belastbaren Erfahrungswerte.

Das Mizzi-Modell

Von Adrian Mizzi [Mizz_05] stammt ein Berechnungsmodell, das die ROSI-Kalkulation um eine interessante Perspektive ergänzt (Abb. 2.3): Die betriebswirtschaftliche Perspektive des Unternehmens wird ins Verhältnis gesetzt zu betriebswirtschaftlichen Betrachtungen aus der Sicht eines potenziellen Angreifers. Denn auch dem Angreifer entstehen Kosten – nämlich der Aufwand zur Konzeption des Angriffs (Identifikation einer Schwachstelle, C_a; abhängig von der Kompetenz des Angreifers können die dafür erforderlichen Kosten erheblich differieren) und für deren Umsetzung (also der konkreten Ausnutzung einer gefundenen Schwachstelle, C_b), für die er Zeit benötigt und Investitionen in Hardware und Software tätigen muss.

Abbildung 2.3: Das Mizzi-Modell – ROSI-Kalkulation des Angreifers



Grafikvorlage: Adrian Mizzi [Mizz_05]

Diesen Kosten muss aus Sicht des Angreifers ein Wert gegenüberstehen, der die Kosten deutlich übersteigt und ihn zur Durchführung des Angriffs motiviert.[1] Betriebswirtschaftlich gesehen kann dies entweder der Wert einer durch den Angriff gewonnenen Information (I) sein, oder aber die Höhe des Schadens, den er dem angegriffenen Unternehmen dabei zufügen kann (L_{tot}). Bei einem (betriebs)wirtschaftlich handelnden Angreifer ist ein Angriff genau dann zu erwarten, wenn gilt:

$$I + L_{tot} \gg C_a + C_b$$

1. Diese betriebswirtschaftliche Perspektive blendet »irrationale« Motive eines Angreifers (Fanatismus, Wahnvorstellungen usw.) aus.

Eine große Stärke dieses Ansatzes ist die Unabhängigkeit von wenig verlässlichen Wahrscheinlichkeitsannahmen, die die Aussagekraft der Ergebnisse beim ROSI-Modell erheblich einschränken. Auch ermöglicht der Ansatz, aktuelle Entwicklungen zu berücksichtigen, wie z. B. die Veröffentlichung einer kritischen Schwachstelle einer Standard-Anwendung und die Verbreitung von daran angepasster Exploit-Software, durch die der Aufwand des Angreifers sinken kann.

Gewichtig sind aber auch die Nachteile des Modells: Die Risikoberechnung basiert auf erheblich vereinfachenden Annahmen über die Angreifermotivation. Denn viele Hacker denken keineswegs betriebswirtschaftlich – zwar versuchen sie möglicherweise, eine (vor allem in der Szene) beeindruckende Wirkung mit einem Hack zu erzielen; viele zielen aber keineswegs auf Schadensmaximierung oder Informationsgewinnung. Dennoch ist der Ansatz wertvoll, denn er dient dazu, die Kosten-Nutzen-Situation des Angreifers zu prüfen, die für einen gezielten Angriff relevant sein dürfte. Daraus kann folgen, dass einem theoretisch denkbaren Angriffsszenario nur eine geringe praktische Bedeutung zuzumessen ist. Außerdem zwingt das Modell dazu, den Wert bestimmter Informationen zu quantifizieren.

2.3 Qualitative Betrachtungen

2.3.1 Grenzen betriebswirtschaftlicher Betrachtungen

Nicht erst seit dem »Gesetz zur Kontrolle und Transparenz im Unternehmensbereich« (KonTraG, 1998) sind Geschäftsführer und Vorstände von Kapitalgesellschaften zur Reduktion unternehmenskritischer Risiken verpflichtet. Einen planvollen Umgang mit operationellen Risiken gebietet allein schon die allgemeine Sorgfaltspflicht (»Sorgfalt des ordentlichen und gewissenhaften Geschäftsleiters«, § 93 Aktiengesetz und § 43 GmbH-Gesetz).

Tatsächlich gibt es darüber hinaus gesetzliche Einzelbestimmungen wie bspw. die Datenschutz-Grundverordnung (DSGVO), das Telekommunikationsgesetz (TKG) oder das Kreditwesengesetz (KWG), die z. T. sehr konkrete Anforderungen an den Informationsschutz und die IT-Sicherheit stellen. Diese gesetzlichen Anforderungen sind damit einer rein betriebswirtschaftlichen Bewertung als Entscheidungsgrundlage entzogen, da ihre Umsetzung gesetzlich geboten ist.

Neben gesetzlichen Erfordernissen (Compliance) gibt es einen zweiten Bereich, in dem die Investition in Sicherheitsmaßnahmen außer Frage steht: neue Onlineangebote, seien es E-Commerce-Lösungen oder Kunden-Services. Denn ohne ein Minimum an geeigneten Sicherheitsmaßnahmen ist das Vertrauen von Nutzern in Onlineangebote nachweislich schwer zu gewinnen – man stelle sich Onlinebanking ohne PIN, TAN und andere Sicherheitsmechanismen vor.

Die betriebswirtschaftliche Perspektive hilft jedoch auch in diesen Fällen, in denen die Umsetzung von Sicherheitsmaßnahmen nicht infrage steht, dabei, die dafür erforderlichen Investitionsentscheidungen zu treffen.

2.3.2 Wirtschaftlichkeit von Investitionsentscheidungen

Grundsätzlich lassen sich drei Wirtschaftlichkeitsprinzipien unterscheiden, an denen eine einzelne Investitionsentscheidung ausgerichtet werden kann:

- **Minimierungsprinzip**
  Ist das Ziel konkret vorgegeben, werden die Maßnahmen ergriffen, die das Ziel mit einem möglichst geringen Aufwand erreichen.
- **Maximierungsprinzip**
  Sind die maximal einsetzbaren Mittel (Budget) zur Erreichung eines Ziels vorgegeben, werden die Maßnahmen ergriffen, die eine möglichst große Wirkung erzielen.
- **Extremumsprinzip**
  Das Extremumsprinzip zielt auf eine Optimierung des Kosten-Nutzen-Verhältnisses – mit möglichst geringem Mitteleinsatz soll ein möglichst gutes Ergebnis erzielt werden. Da die Kostenkurve sich nicht bei jeder Investition proportional zum Sicherheitsgewinn entwickelt, kann es mehrere »lokale« Extrema geben – die Bestimmung des Optimums ist in solchen Fällen gegebenenfalls aufwendig.

In der Praxis stehen vor einer Investitionsentscheidung zumeist das Ziel (Risikoreduktion) und die Mittel (festzulegender Anteil an einem Gesamtbudget) nur ungenau fest. Daher sind Investitionsentscheidungen in der IT-Sicherheit im Ganzen zunächst eine allgemeine und sehr komplexe Optimierungsaufgabe nach dem Extremumsprinzip.

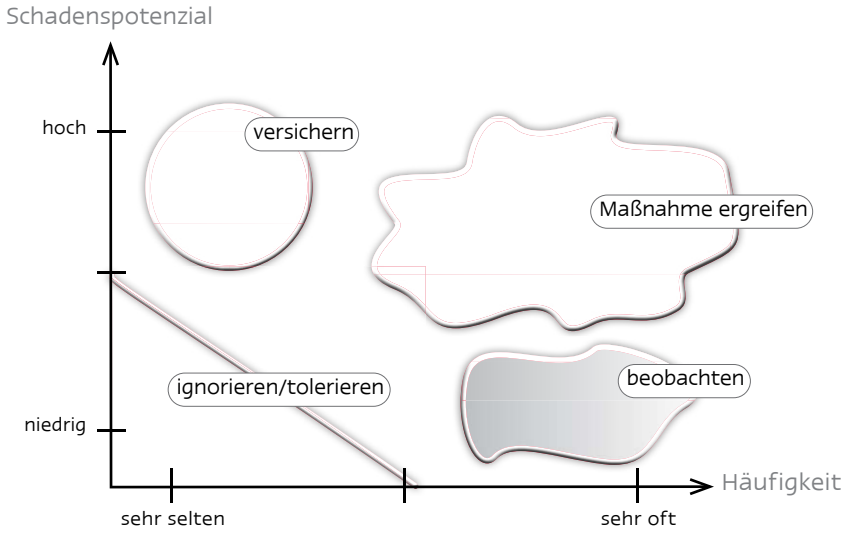
Sind die (Jahres-)Ziele konkretisiert, wird deren Erfüllung meist nach dem Minimierungsprinzip umgesetzt: Bei der Wahl einer konkreten Lösung zur Erreichung eines präzisierten Teilziels gilt es, mit möglichst geringen Ressourcen auszukommen. Häufig aber steht auch der Budgetrahmen fest, z. B. als festgelegter Anteil des IT-Budgets: Dann gilt es, mit begrenzten Mitteln einen möglichst großen Sicherheitsgewinn zu erzielen – nach dem Maximierungsprinzip.

2.3.3 Risikomatrix

Eine Alternative zur quantitativen Risikobewertung ist die Einordnung von Risiken in eine »Risikomatrix«, in der die potenzielle Schadenshöhe und die Eintrittswahrscheinlichkeit eines Risikos lediglich grob und im Vergleich zu anderen Risiken eingeschätzt werden.

Anschließend werden die Risiken durch Gruppierung bestimmten »Klassen« zugeordnet: Risiken mit eher kleiner Schadenshöhe und geringer Wahrscheinlichkeit werden toleriert; Risiken mit höherer Wahrscheinlichkeit beobachtet. Gegen Risiken mit höherem Schaden und höherer Eintrittswahrscheinlichkeit werden Maßnahmen ergriffen, und Risiken mit erheblicher Schadenshöhe, aber geringer Eintrittswahrscheinlichkeit können z. B. mit einer Versicherung transferiert werden (Abb. 2.4).

Abbildung 2.4: Risikomatrix



Die Risikomatrix hat den Vorteil, dass alle Risiken überblicksartig erfasst und dokumentiert werden; damit fällt es leichter, den Überblick über offene (Rest-)Risiken zu behalten. Auch hier handelt es sich bei der Eintrittswahrscheinlichkeit um eine grobe Schätzung – allerdings beansprucht diese keine quantitative Genauigkeit. Unberücksichtigt bleiben bei dieser Betrachtung mögliche Abhängigkeiten zwischen einzelnen Risiken und die Kosten von Gegenmaßnahmen.

Die Aufstellung einer Risikomatrix ergänzt jedoch eine quantitative Betrachtung um eine wertvolle Gesamtübersicht und sollte daher grundsätzlich erstellt werden.

2.3.4 Pareto-Prinzip

Auch für die IT-Sicherheit gilt das Gesetz vom abnehmenden Grenznutzen (Gossen'sches Gesetz): Der Zusatznutzen (Sicherheitsgewinn) sinkt mit der Zahl der Maßnahmen. In der Praxis hilft es daher, sich bei Investitionen in die Informationssicherheit am Pareto-Prinzip, auch 80/20-Regel genannt, zu orientieren: So erreicht man erfahrungsgemäß mit ca. 20 % des Aufwands etwa 80 % des angestrebten Ziels; die verbleibenden 20 % verursachen hingegen ein Vielfaches dieses Aufwands. Übertragen auf die Informationssicherheit bedeutet dies, dass der größte Sicherheitsgewinn in der Regel mit vergleichsweise moderatem Aufwand erreicht wird. Betriebswirtschaftlich ist es daher sinnvoll, in allen von IT-Risiken betroffenen Bereichen die Maßnahmen zu ergreifen, die ein sehr gutes Kosten-Nutzen-Verhältnis aufweisen – und erst später das Sicherheitsniveau in Bereichen mit besonders großem Risiko zu maximieren.

Auch der BSI-Ansatz des IT-Grundschutzes nutzt das Pareto-Prinzip: Der für den Grundschutz angenommene »normale« Schutzbedarf sollte die untere Grenze für schutzwürdige Infrastrukturen darstellen und sich mit einer vergleichsweise moderaten Investition erreichen lassen. Als vordefinierter Soll-Zustand bietet er eine gute Vergleichbarkeit und die Möglichkeit, das eigene Sicherheitsniveau zu bewerten. Zusätzliche Investitionen in Individualmaßnahmen sind nur dann erforderlich, wenn ein höherer Schutzbedarf vorliegt. Abbildung 2.4 zeigt, dass sich das Kosten-Nutzen-Verhältnis ergänzender Sicherheitsmaßnahmen typischerweise immer weiter verschlechtert – so lange, bis der erforderliche Aufwand den Gewinn an Sicherheit nicht mehr rechtfertigt.

Allerdings ist dabei zu berücksichtigen, dass der Sicherheitsgewinn einer Maßnahme schwierig zu quantifizieren ist – daher ist die Entscheidung, welche Maßnahme das bessere Kosten-Nutzen-Verhältnis aufweist, meist nicht leicht zu treffen.

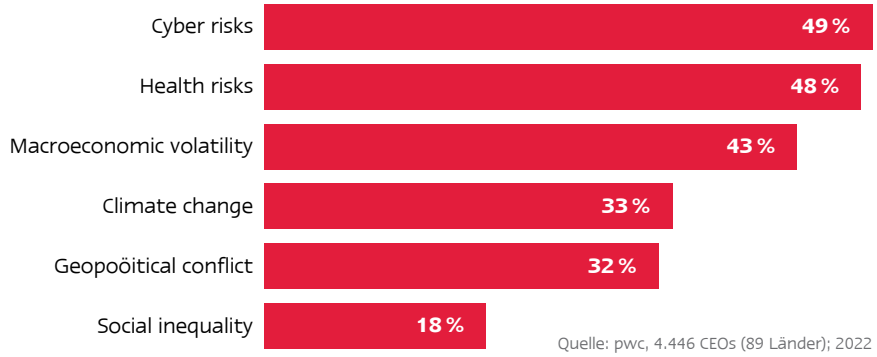
2.3.5 Erfahrungswerte – Best Practice

Zwar gibt es wenige allgemeine oder verallgemeinerbare Erfahrungswerte über Eintrittswahrscheinlichkeiten von Schadensereignissen und Schadenshöhen im Bereich der Informationssicherheit; auch die Angaben über die Höhe der Investitionen von Unternehmen in Sicherheitsmaßnahmen in Studien schwanken stark und sind meist schlecht vergleichbar, da nicht klar abgegrenzt wird, welche Ausgaben der IT-Sicherheit zugeordnet werden. So kann bspw. das Patch-Management sowohl aus dem Budget der IT-Sicherheit als auch aus dem des IT-Betriebs finanziert sein. Eine Orientierung an solchen Angaben ist daher nur sehr eingeschränkt möglich. Eine grobe Orientierung können solche Angaben aber dennoch bieten. Im Jahr 2017 lag nach einem Global Enterprise Security Survey von Fortinet das IT-Sicherheitsbudget bei 36 % der Unternehmen unter 10 %, bei ebenso vielen (36 %) hingegen bei über 15 % des IT-Budgets.

Insgesamt lässt sich allerdings – selbst bei Unterstellung eingeschränkter statistischer Signifikanz solcher Untersuchungen – über alle Studien hinweg ein eindeutiger Trend erkennen: Der Anteil der Ausgaben für IT-Sicherheit gemessen am IT-Budget steigt bei den meisten Unternehmen signifikant; bei Banken und Versicherungen liegt er außerdem deutlich höher als bei Unternehmen anderer Branchen.

Und ein zweiter deutlicher Trend ist erkennbar: Die Bedeutung von IT-Sicherheitsrisiken steigt in den Augen des Managements angesichts der wachsenden Anzahl erfolgreicher Angriffe auf Unternehmen in den vergangenen Jahren (z. B. durch Verschlüsselungstrojaner). Im 25. »Annual Global CEO Survey« von PwC aus dem Jahr 2022, in dem 4446 CEOs aus 89 Ländern befragt wurden, rangierten »Cyber Risks« unter den »Risiken der kommenden 12 Monate« an erster Stelle – vor Gesundheits- und (global verursachten) wirtschaftlichen Risiken (Abb. 2.5).

Abbildung 2.5: Größte Risiken aus Sicht von Unternehmensleitungen



Quelle: pwc, 4.446 CEOs (89 Länder); 2022

Zusammenfassung

Die Qualität der mit den unterschiedlichen Modellen kalkulierbaren quantitativen Aussagen steht und fällt mit der Genauigkeit der Angaben zur Eintrittswahrscheinlichkeit, Schadenshöhe und den Gesamtkosten einer geeigneten Sicherheitsmaßnahme. Da aus den genannten Gründen in absehbarer Zeit auf keine hinreichend verlässliche Zahlenbasis aus Erfahrungswerten für die unterschiedlichen IT-Risiken zurückgegriffen werden kann, lassen sich auch in nächster Zukunft nur für Schadensereignisse mit hoher Eintrittswahrscheinlichkeit aussagekräftige ROSI-Berechnungen durchführen.

Gerade für häufige Schadensereignisse ist jedoch der »Return« einer Sicherheitsmaßnahme meist offensichtlich und auch ohne ein ausgefeiltes Modell sehr leicht abzuschätzen. So liegt es auf der Hand, dass ein wirksamer Spam-Filter, der unerwünschte elektronische Nachrichten (oft mit maliziösem Anhang) mit einer hohen Trefferquote und ohne *False Positives* (fälschlich als »Spam« deklarierte E-Mails) aussortiert, einen unmittelbaren »Return« in Form gesteigerter Produktivität und einer Abnahme des Risikos eines erfolgreichen Angriffs bewirkt.

Hingegen wäre für die seltenen Schadensereignisse mit hohem Schadenspotenzial, die sich einer »Pi mal Daumen«-Schätzung entziehen, eine ROSI-Kalkulation besonders wertvoll. Genau das leisten jedoch auch die quantitativen Modelle nicht.

In der Praxis kommen daher überwiegend qualitative Ansätze zur betriebswirtschaftlichen Steuerung von Sicherheitsstrategien zum Einsatz, wie die Checklisten des IT-Grundschutzes oder die Erfahrungswerte und Strategien aus vergleichbaren Unternehmen.

Literatur

[BBS_07] *Brocke, Jan; Buddendick, Christian; Strauch, Gereon*: Return on Security Investments – Design Principles of Measurement Systems Based on Capital Budgeting, AMCIS Proceedings 2007, S. 4

[Beri_02] *Berinato, S.*: Finally, a Real Return on Security Spending, CIO Magazine, 08.04.2002

[BITKOM_05] *BITKOM*: IT-Risiko- und Chancenmanagement im Unternehmen. Ein Leitfaden für kleinere und mittlere Unternehmen. 23.05.2006; *https://www.bitkom.org/sites/main/files/file/import/060601-Bitkom-Leitfaden-IT-Risikomanagement-V10-final.pdf* (Stand: 17.01.2024)

[BSI_18] *Bundesamt für Sicherheit in der Informationstechnik (BSI)*: Risikoanalyse auf der Basis von IT-Grundschutz. BSI-Standard 200-3, Oktober 2018

[Enisa_12] *Enisa*: Introduction to Return on Security Investment, Dec. 2012; *https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment* (Stand: 25.01.2024)

[Enisa_23] *Enisa*: Interoperable EU Risk Management Toolbox, Feb. 2023; *https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox* (Stand: 25.01.2024)

[FIPS_65] *National Institute of Standards and Technology (NIST)*: Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65, 01.08.1975 (zurückgezogen am 25.08.1995, abgelöst durch SP 800-30 [NIST_12])

[Fox_11] *Fox, Dirk*: Betriebswirtschaftliche Bewertung von Security Investments in der Praxis, Datenschutz und Datensicherheit (DuD), 1/2011, S. 50 – 55

[GCIO_04] *Government Chief Information Office*: A Guide for Government Agencies Calculation Return on Security Investment; New South Wales Government, Department of Commerce; Version 2.0, 13.06.2004; *https://webarchive.nla.gov.au/awa/20091124224132/http://pandora.nla.gov.au/pan/111462/20091125-0940/www.gcio.nsw.gov.au/products-and-services/policies-guidelines/Lockstep_ROSI_Guideline_SGW_282_2_29.pdf* (Stand: 25.01.2024)

[Hoo_00] *Hoo, Kevin J. Soo*: How Much Is Enough? A Risk-Management Approach to Computer Security, Working Paper, CRISP, Stanford University, June 2000; *https://cisac.fsi.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security* (Stand: 17.01.2024)

[ISO_18] *International Organisation for Standardization (ISO)*: Risk management – Guidelines. ISO 31000:2018, 2018

[ISO_22] *International Organisation for Standardization (ISO)*: Information technology – Security techniques – Information security risk management. ISO/IEC 27005:2022, Oktober 2022

[Mizz_05] *Mizzi, A.*: Return on Information Security Investment – Are you spending enough? Are you spending too much? Januar 2005; *http://adrianmizzi.com/ROISI-Paper.pdf* (Stand: 17.01.2024)

[MöTe_06] *Möricke, M.; Teufel, S. (Hrsg.)*: Kosten & Nutzen von IT-Sicherheit, Praxis der Wirtschaftsinformatik, HMD Heft 248, April 2006, dpunkt.verlag 2006

[NFKP_05] *Nowey, T.; Federrath, H.; Klein, C.; Plößl, K.:* Ansätze zur Evaluierung von Sicherheitsinvestitionen, In: Sicherheit 2005, Lecture Notes in Informatics, P-62, Köllen-Verlag, Bonn 2005, S. 15–26

[NIST_11] *National Institute of Standards and Technology (NIST):* Managing Information Security Risks. NIST Special Publication 800-39, March 2011; *https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf* (Stand: 17.01.2024)

[NIST_12] *National Institute of Standards and Technology (NIST)*: Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Rev. 1, September 2012; *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf* (Stand: 17.01.2024)

[NIST_20] *Stine, K.; Quinn, S.; Witte, G.; Gardner, R. K.*: Integrating Cybersecurity and Enterprise Risk Management (ERM). National Institute of Standards and Technology (NIST) Interagency Report, NIST IR 8286, October 2020; *https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf* (Stand: 17.01.2024)

[ROSI_11] *Return on Security Investment (ROSI)*: Calculator; *http://www.iso27001standard.com/en/rosi/return-on-security-investment* (Stand: 17.01.2024)

[SoAS_06] *Sonnenreich, W.; Albanese, J.; Stout, B.*: Return On Security Investment (ROSI) – A Practical Quantitative Model. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006, S. 55–66; *https://www.scitepress.org/papers/2005/25802/25802.pdf* (Stand: 25.01.2024)

[WeFr_01] *Wei, H.; Frinke, D. et al.*: Cost-Benefit Analysis for Network Intrusion Detection Systems. In: Proceedings of the 28th Annual Computer Security Conference October 2001; *http://www.csds.uidaho.edu/deb/costbenefit.pdf* (Stand: 17.01.2024)

[Wiki_23] *Wikipedia*: Operationelles Risiko, 2023

6 ISO 27001 und ISO 27002

Einleitung

Im Jahr 2005 wurde durch die International Organization for Standardization (ISO) ein Standard veröffentlicht, der sich dediziert dem Thema »Managementsystem für Informationssicherheit« widmet. Wie auch andere Managementstandards (z. B. ISO 900x für Qualitätsmanagement oder ISO 1400x für ein Umweltmanagementsystem) bietet dieser Standard Unternehmen und Behörden die Möglichkeit einer Zertifizierung. Hierzu definiert ISO 27001 [ISO27001] verbindliche und konkrete Anforderungen an zu etablierende Prozesse und umzusetzende Maßnahmen. Überarbeitete Fassungen von ISO 27001 wurden 2013 und 2022 veröffentlicht. Neben einigen inhaltlichen Änderungen erfolgte insbesondere eine formelle Anpassung des Standards an Annex SL der ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO. Dort werden Vorgaben definiert für den Aufbau und die Struktur für ISO-Standards zu Managementsystemen.

Im Jahr 2000 wurde durch die ISO bereits mit ISO/IEC 17799 [ISO17799] ein »Leitfaden für das Management von Informationssicherheit« veröffentlicht und im Jahr 2007 in die ISO-27xxx-Reihe als ISO 27002 [ISO27002] überführt. ISO 27002 enthält eine Sammlung sogenannter Best-Practice-Maßnahmen, die im Rahmen eines angemessenen Security Managements berücksichtigt werden sollten. Aufgrund des fehlenden Prozessgedankens und der mangelnden Verbindlichkeit ist, im Gegensatz zur ISO 27001, eine Zertifizierung nicht möglich. Analog zu ISO 27001 wurde auch ISO 27002 überarbeitet und 2013 sowie 2022 in einer neuen Version veröffentlicht.

Dieses Kapitel beschreibt die Entstehungsgeschichte und Inhalte von ISO 27001 und ISO 27002. Ferner wird beschrieben, wie ISO 27001 in das Qualitätsmanagement einer Organisation integriert werden kann. Abschließend werden die entsprechenden Prüf- und Zertifizierungsprozesse erläutert.

6.1 Entstehungsgeschichte

Die Ursprünge von ISO 27001 und ISO 27002 reichen zurück zu den Tagen des britischen Department of Trade and Industry (DTI) Commercial Computer Security Centre (CCSC). Gegründet im Mai 1987, hatte das CCSC zwei Hauptaufgaben: Herstellern von IT-Sicherheitsprodukten dabei zu helfen, international anerkannte Kriterien zur Evaluierung von Sicherheitsprodukten und ein darauf basierendes Evaluierungs- und Zertifizierungsschema zu entwickeln. Diese Bemühungen flossen letztendlich in die Entwicklung der »Information Technology Security Evaluation Criteria« (ITSEC) ein.

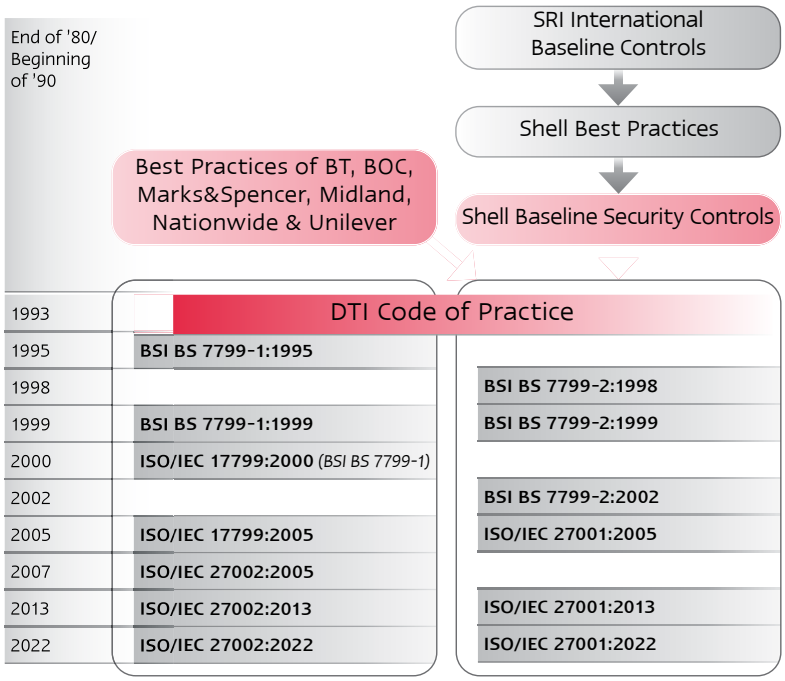
Der zweite Schwerpunkt des CCSC lag in der Entwicklung eines *Code of Good Security Practice* und resultierte 1989 in der Veröffentlichung des *Users Code of Practice*. Diese Verhaltensrichtlinie wurde später vom National Computing Centre (NCC) und einer Gruppe von führenden Unternehmen und Organisationen weiterentwickelt; es sollte auf diesem Wege sichergestellt werden, dass der Code sinnvoll und aus Benutzersicht auch praktisch anwendbar war. Das Resultat wurde schließlich als Public Document (PD) 0003,

A Code of Practice for Information Security Management veröffentlicht und mündete nach einiger Umgestaltung 1995 in den durch das British Standard Institution (BSI) herausgegebenen britischen Standard BS 7799 Teil 1.

Dieser »Leitfaden zum Management von Informationssicherheit«, der Sicherheitsmaßnahmen und Hinweise für ein sinnvolles Vorgehen enthielt, sollte Industrie und Behörden bei der Umsetzung von Informationssicherheit unterstützen. Im Jahr 1998 wurde dann ein zweiter Teil, BS 7799-2 »Information Security Management Systems – Specification with guidance for use« [BS77992], veröffentlicht, der den Prozess zur Entwicklung eines Informationssicherheitsmanagementsystems (ISMS) beschreibt und als Grundlage für eine Zertifizierung diente.

Im Jahr 1998 wurde BS 7799 einer gründlichen Revision unterzogen. Ziel dieser Überarbeitung war, neue Entwicklungen, z. B. E-Commerce oder mobiles Arbeiten, und entsprechende Maßnahmen hinzuzufügen. Außerdem sollte die internationale Akzeptanz des Standards erhöht werden, bspw. durch das Entfernen aller »UK-spezifischen Verweise« innerhalb des Dokuments. Die neue Fassung des Standards wurde schließlich im März 1999 veröffentlicht.

Abbildung 6.1: Von BS 779 BS 7799 zu ISO 2700x – die historische Entwicklung im Überblick



Das internationale Interesse an BS 7799 führte schließlich im Dezember 2000 dazu, dass BS 7799 Teil 1 [BS77991] als sogenannter Fast Track in die ISO-Standardisierung (International Organization for Standardization) eingebracht wurde und unter der Bezeichnung ISO 17799:2000 als internationaler Standard veröffentlicht wurde. Fast Track bedeutet, dass, mit Ausnahme einiger unbedeutender editorischer Änderungen, die ursprüngliche Fassung von BS 7799 Teil 1 ohne weitere inhaltliche Korrekturen übernommen wurde.

ISO 17799 umfasst jedoch nicht den zweiten Teil der BS 7799, der den Bereich der Umsetzung abdeckt und die Grundlage für eine Auditierung und Zertifizierung bildet. Dieser wurde 2005 dann in ISO 27001 überführt (vgl. Abb. 6.1). Im Juni 2005 wurde dann die neue Revision ISO 17799:2005 verabschiedet, die einige wesentliche Änderungen mit sich brachte, dazu später mehr.

Im Jahr 2002 wurde ferner eine überarbeitete Fassung von BS 7799 Teil 2 (BS 77792:2002) vorgelegt. Ziel dieser Revision war die Harmonisierung mit anderen Management-Standards, bspw. ISO 9001:2000 und ISO 14001:2004. Die Ausrichtung des zweiten Teils von BS 7799 an international anerkannte Managementstandards führte schließlich zur Überführung von BS 7799-2 in ISO 27001. Im Jahr 2007 erfolgte schließlich die Überführung von ISO 17799 in die ISO-27xxx-Reihe als Standard ISO 27002.

2013 wurden beide Standards noch einmal überarbeitet. Primäres Ziel der Überarbeitung war dabei, ISO 27001 kompatibel zu den Vorgaben der ISO zu Standards für Managementsysteme zu gestalten, gemäß Anhang SL der ISO/IEC-Direktiven, Teil 1, »Consolidated ISO Supplement« [DirectiveP1] sowie den Regeln nach ISO/IEC Direktive, Teil 2 [DirectiveP2].

Eine weitere Überarbeitung erfolgte 2022. Hierbei wurden als wesentliche Änderungen in der ISO 27002 eine neue Struktur der Best Practices gewählt und zu einzelnen neuen Themengebieten wie Cloud Security neue Punkte ergänzt. Die ISO 27001 wurde im Annex A darauf abgestimmt.

6.2 Die Familie der ISO-27000-Standards

Stand 2022 umfasst die Familie der ISO-27000 über 20 Standards und weitere sind vorgesehen. Im Folgenden geben wir einen kurzen Überblick ausgewählter Standards, bevor in den weiteren Abschnitten dieses Kapitels die beiden Standards ISO 27002 und 27001 vertiefend dargestellt werden. Die fünf zentralen Standards für die Implementierung eines zertifizierbaren ISMS sind im Folgenden aufgeführt. Daneben hat die ISO bereits weitere Themen oder bereichsspezifische Standards verabschiedet (s. hierzu *http://www.iso.org*).

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

Der Standard ISO/IEC 27000 [ISO27000] gibt eine Einführung in die Familie der ISMS-Standards, stellt wichtige Definitionen vor und legt Begriffe fest. Er enthält:

- einen Überblick über die Familie von ISMS-Standards
- eine Einführung in das Information Security Management System
- ein Glossar der verwendeten Begriffe und Definitionen

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

Der Teil ISO/IEC 27001 spezifiziert die Anforderungen für den Aufbau, die Umsetzung und die Prozesse für Betrieb, Überwachung, Überprüfung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems sowie die Anforderungen an die Implementierung von Sicherheitsmaßnahmen, die an die individuellen Bedürfnisse eines Unternehmens angepasst werden müssen.

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

Dieser Teil bietet einen Leitfaden zum Management von Informationssicherheit und umfasst eine Sammlung von Empfehlungen für die Einführung, Durchführung, Aufrechterhaltung und Verbesserung eines ISMS.

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

ISO 27003 [ISO27003] konzentriert sich auf die Management-Aspekte bei der Einführung eines ISMS. Der Standard stellt eine Anleitung für die erfolgreiche Konzeption und Implementierung eines ISMS nach ISO 27001 dar.

ISO/IEC 27004:2016
Information technology – Security techniques – Information security management – Measurement

Der Teil ISO 27004 [ISO27004] der Standard-Familie definiert die Kennzahlensysteme für die Messung der Wirksamkeit eines nach ISO 27001 implementierten ISMS.

ISO/IEC 27005:2018
Information technology – Security techniques – Information security risk management

ISO 27005 [ISO27005] enthält Richtlinien für ein Information Security Risk Management, das den Anforderungen nach ISO 27001 gerecht wird.

6.3 ISO 27001

ISO 27001 »Information security, cybersecurity and privacy protection – Information security management systems – Requirements« liefert ein Modell zum Aufsetzen und Betrieb eines effizienten ISMS. ISO 27001 beschreibt hierzu notwendige Prozesse zur Implementierung, Überwachung, Prüfung, Instandhaltung und Verbesserung eines ISMS, die in den folgenden sieben zentralen Themenkomplexen erläutert werden. In Klammern sind jeweils die Kapitel aus dem Standard angegeben:

- Context of the organization (Kapitel 4)
- Leadership (Kapitel 5)
- Planning (Kapitel 6)
- Support (Kapitel 7)
- Operation (Kapitel 8)
- Performance Evaluation (Kapitel 9)
- Improvement (Kapitel 10)

Des Weiteren umfasst der Standard die folgenden Anhänge:

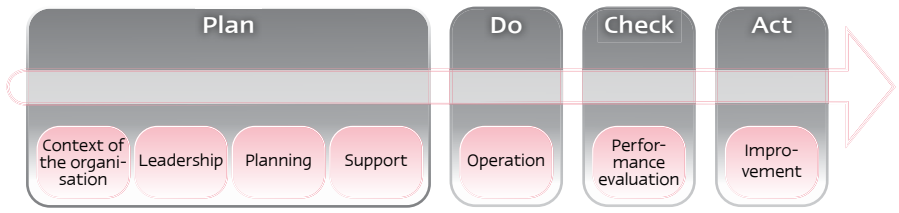
- Annex A (normative) Control objectives and controls
- Bibliography

Vorangetrieben durch die Bestrebungen der ISO, eine einheitliche Struktur und einen einheitlichen Aufbau für alle als ISO-Standard verabschiedeten Managementsysteme zu etablieren, erfolgte auch in ISO 27001:2013 sowohl eine formelle als auch inhaltliche Anpassung. So wurde bspw. das in ISO 27001:2005 eingeführte Plan-Do-Check-Act-Modell (PDCA-Modell) nicht mehr grafisch aufgeführt, ergibt sich aber aus der Gliederung. Auch enthält ISO 27001:2013 keine Begriffsdefinitionen mehr, sondern verweist hierzu nur noch auf ISO 27000. Diese Maßnahmen führten letztlich dazu, dass der gesamte Standard ISO 27001:2013 gerade einmal 30 Seiten umfasst. Die überarbeitete Fassung ISO 27001:2022 wurde im Annex A an die neue ISO 27002:2022 angepasst.

6.3.1 Vorgehensweise und Anwendungen

Auch wenn die explizite Beschreibung des prozessorientierten Ansatzes (PDCA-Modell) in ISO 27001:2013 und neuer nicht mehr enthalten ist, so spiegelt sie sich doch in der strukturellen Gestaltung wider (s. Abb. 6.2).

Abbildung 6.2: Vorgehen nach ISO/IEC 27001



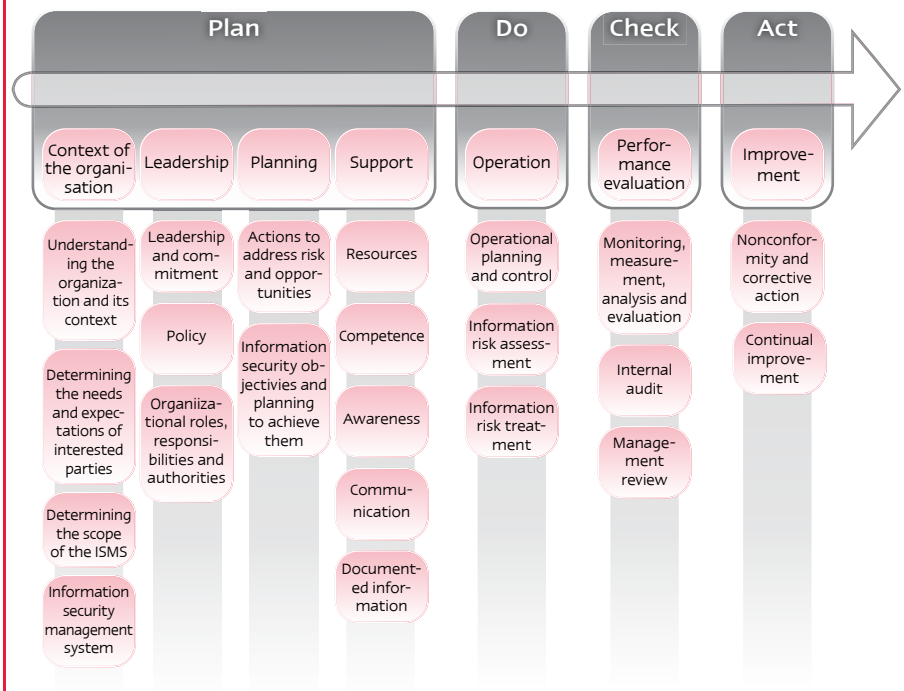
Zuordnung der PDCA-Phasen nach ISO 27001:2005 zum Vorgehen nach ISO 27001:2013.

Dies ist insbesondere für bereits zertifizierte Unternehmen von Relevanz, die im Rahmen einer bevorstehenden Re-Zertifizierung die notwendigen Schritte zur Anpassung des bereits etablierten ISMS an die Anforderungen der ISO 27001 vornehmen müssen. Unternehmen, die eine Zertifizierung nach ISO 27001 anstreben, müssen alle in den Kapiteln 4 bis 10 geforderten Anforderungen bis zum Zertifizierungszeitpunkt umsetzen. Gegenüber älteren Versionen von ISO 27001 haben Unternehmen nun etwas mehr Gestaltungsfreiheit, um die spezifischen ISMS-Zielsetzungen und zu erfüllenden Anforderungen an die jeweiligen Gegebenheiten des Unternehmens anzupassen.

6.3.2 Inhaltliche Elemente der ISO 27001

Die folgende Abbildung 6.3 zeigt, welche Elemente ein ISMS nach ISO 27001 umfassen sollte.

Abbildung 6.3: Inhaltliche Elemente der ISO/IEC 27001



Context of the organisation

Die Basis für das zu etablierende ISMS bildet der spezifische Kontext des Unternehmens. Hierzu sind:

- relevante interne und externe Themen hinsichtlich der ISMS-Zielsetzungen zu bestimmen
- Anforderungen und Erwartungen von Beteiligten zu berücksichtigen

- gesetzliche und regulatorische Anforderungen zu identifizieren
- den Scope (Geltungsbereich) des ISMS festzulegen
- das eigentliche Informationssicherheitsmanagementsystem in Übereinstimmung mit den Anforderungen von ISO 27001 einzuführen, zu implementieren, aufrechtzuerhalten und kontinuierlich zu verbessern

Dies führt letztlich dazu, dass der Standard kein generelles Mindestmaß an Informationssicherheit bestimmt, sondern dies durch jedes Unternehmen selbst ermittelt und fixiert werden muss.

Der Verantwortung des obersten Managements für Etablierung, Implementierung, Betrieb sowie für Monitoring, Review und die Verbesserung des ISMS wird ein hoher Stellenwert beigemessen. Das Management demonstriert die Übernahme der Verantwortung durch die:

- Festlegung von Sicherheitszielen und der Informationssicherheitspolitik
- Einbindung von Informationssicherheit in die Prozesse der Organisation
- Bereitstellung notwendiger Ressourcen
- Sicherstellung, dass die durch das ISMS verfolgten Ziele erreicht werden
- Führung und Unterstützung der Mitarbeiter und Manager
- Förderung der kontinuierlichen Verbesserungen
- Zuweisung von Rollen, Verantwortlichkeiten und Befugnissen

Planning

Den Schwerpunkt dieses Schritts bilden die Ermittlung und Adressierung von Chancen und Risiken, um

- die angestrebten ISMS Ziele erreichen zu können,
- unerwünschte Effekte vermeiden oder reduzieren zu können und
- eine stetige Verbesserung erzielen zu können.

Das Risikomanagement muss dabei essenziell in die ISMS-Prozesse integriert und auf ausreichende Effektivität geprüft werden. Hierzu sind geeignete Prozesse zur Risikobewertung und Risikobehandlung zu etablieren. Schließlich muss ein Abgleich der identifizierten Maßnahmen mit den in Annex A gelisteten Controls erfolgen.

ISO 27001 verfolgt einen risikobasierten Ansatz. Allerdings sind die Vorgaben für das Risikomanagement flexibel gehalten. Das Risikomanagement muss nicht zwingend auf der Ermittlung der organisationseigenen Werte (Assets) beruhen. Für ein Information-Security-Risk-Management nach ISO 27001 müssen

- Information-Security-Risk-Kriterien einschließlich der Kriterien für die Risikoakzeptanz (Festlegung von Risikostufen) und der Durchführung von Risk Assessments festgelegt werden,
- die verwendeten Verfahren konsistente, valide und vergleichbare Ergebnisse liefern,
- bestehende Risiken und verantwortliche Risk Owner identifiziert werden,
- mögliche Auswirkungen bei Eintreten der ermittelten Risiken analysiert sowie realistische Eintrittswahrscheinlichkeiten abgeschätzt werden und
- die Risiken mit den zu Beginn festgelegten Kriterien abgeglichen (Einstufung in die Risikostufen) und Prioritäten zum Umgang mit diesen Risiken festgelegt werden.

Zur Behandlung der Risiken muss ein entsprechender Risk-Treatment-Prozess etabliert werden, in dem die angemessenen Behandlungsoptionen ausgewählt werden. Notwendige Maßnahmen müssen identifiziert und ein Risk-Treatment-Plan erstellt werden. Im Rahmen des Prozesses ist ferner das sogenannte Statement of Applicability (SoA) zu erstellen, in dem die ausgewählten Maßnahmen mit den Maßnahmen aus Annes X abgeglichen werden.

Support

Die für das ISMS erforderlichen Unterstützungsleistungen müssen ermittelt und bereitgestellt werden und umfassen:

- notwendige Ressourcen zur Errichtung, Implementierung und Aufrechterhaltung des ISMS
- Bestimmung notwendiger Fähigkeiten der Mitarbeiter auf Basis angemessener Ausbildung oder Erfahrung und gegebenenfalls Ergreifung von Aus- und Weiterbildungsmaßnahmen
- Schaffung von Awareness für Informationssicherheit
- Bestimmung der internen und externen ISMS-Kommunikationsanforderungen
- Festlegung der notwendigen Dokumentationen sowie Etablierung einer Dokumentenlenkung

Operation

Im Rahmen des ISMS-Betriebs erfolgen

- Planung und Etablierung notwendiger Prozesse, um die Anforderungen der Informationssicherheit erfüllen zu können,
- Erstellung und Pflege der Dokumentation im erforderlichen Umfang,
- die Kontrolle von Änderungen und Bewertung von Konsequenzen unbeabsichtigter Änderungen,
- eine Bestimmung und Kontrolle ausgelagerter Prozesse,
- dokumentierte Information Security Risk Assessments, die sowohl regelmäßig als auch bei signifikanten Änderungen durchgeführt werden, sowie
- die Erstellung des dokumentierten Risikobehandlungsplans.

Performance evaluation

Um die Angemessenheit, Wirksamkeit und Nachhaltigkeit des ISMS gewährleisten zu können,

- sind die Performance der Informationssicherheit und ISMS-Effektivität zu bestimmen,
- muss festgelegt und dokumentiert werden, was, wie, wann durch wen überwacht und gemessen werden soll sowie auf welche Weise wann und durch wen gegebenenfalls eine Auswertung oder Analyse zu erfolgen hat,
- müssen interne Audits gemäß einem zu erstellenden Audit-Programm geplant und durchgeführt werden,
- muss das ISMS in regelmäßigen Intervallen durch das Management einem Review unterzogen werden.

Improvement

Im Rahmen der stetigen Verbesserung des ISMS müssen bei Auftreten von »Nonconformities« (Abweichungen) diese bewertet und beurteilt sowie Maßnahmen zur Korrektur ergriffen werden. Die Eignung, Angemessenheit und Wirksamkeit des Informationssicherheitsmanagementsystems müssen kontinuierlich verbessert werden.

6.3.3 Notwendige Dokumentation

Primäres Ziel von ISO 27001 ist die Etablierung eines *dokumentierten* Information Security Management Systems, in dem alle relevanten Strukturen, Prozesse und Abläufe für Planung, Steuerung und Kontrolle des ISMS beschrieben und schriftlich fixiert sind. Seit ISO 27001:2013 wird dabei allgemein »documented information« gefordert, was im Sinne der ISO sowohl die erforderlichen ISMS-Dokumente als auch die Aufbewahrung von Aufzeichnung (bspw. Schulungsnachweise oder Log-Einträge) umfasst. Aus dem Standard lassen sich direkt eine Reihe von zu erstellenden Dokumenten ableiten, siehe Tabelle 6.1.

Tabelle 6.1: Geforderte Referenzdokumente in einem ISMS

Documented Information	Kapitel
Scope of the ISMS	4.3
Information security policy	5.2
Risk assessment and risk treatment methodology	6.1.2
Statement of Applicability	6.1.3d
Risk treatment plan	6.1.3e
Risk treatment process	6.1.3
Information security objectives	6.2
Evidence of competence, training, skills, experience and qualifications	7.2
Operational planning and control	8.1
Risk assessment report	8.2
Risk treatment report	8.3
Monitoring and measurement results	9.1
Internal audit program and audit results	9.2
Results of the management review	9.3
Results of corrective actions	10.2

Allerdings lassen sich aus Annex A weitere Dokumentationsanforderungen ableiten, die bei der Umsetzung des jeweiligen Controls zu berücksichtigen sind.

Zu Art, Umfang, Ausgestaltung und Form der Dokumentation macht die ISO 27001 keine Vorschriften. Diese Merkmale orientieren sich in der Praxis einzig an den Gegebenheiten und Notwendigkeiten der Sicherheitsanforderungen für den betrachteten Anwendungsbereich.

Dokumentenmanagement (Lenkung von Dokumenten nach ISO 9001)

Der Standard gibt Hinweise zum Umgang mit dieser Dokumentation, die geschützt und kontrolliert werden muss. Es muss ein dokumentierter Prozess etabliert werden zur Festlegung der folgenden (Dokumenten-) Managementtätigkeiten:

- Überprüfung der Dokumente bezüglich ihrer Angemessenheit vor Herausgabe
- Überprüfung und Aktualisierung der Dokumente und deren erneuter Genehmigung
- Sicherstellung einer Versions- und Änderungskontrolle
- Bereitstellung der aktuellen Dokumente
- Sicherstellung der Lesbarkeit und Identifizierbarkeit der Dokumente
- Kennzeichnung externer Dokumente
- Kontrolle der Verteilung der Dokumente
- Entfernung obsoleter Dokumente
- Identifikation obsoleter Dokumente, falls sie aus irgendeinem Grund aufbewahrt werden

6.3.4 Prüfungs- und Zertifizierungsprozess

Das Zertifizierungsschema zur Erlangung einer ISO-27001-Zertifizierung ist streng reglementiert und in [ISO/IEC 27006] grundlegend festgeschrieben. Die Anwendung von ISO 27006[1] muss dabei in enger Verbindung mit ISO 19011[2] betrachtet werden, die generelle Richtlinien zur Auditierung von Managementsystemen definiert.

Die Zertifizierung darf nur durch speziell akkreditierte Institutionen, sogenannte Certification Bodies, erfolgen. Die Akkreditierung dieser Certification Bodies obliegt den nationalen Akkreditierungsstellen, in Deutschland ist dies die »Deutsche Akkreditierungsstelle« (DAkkS).

Die nationalen Akkreditierungsstellen treffen gegenseitige Anerkennungsvereinbarungen, sodass die in einem Land ausgestellten Zertifikate auch in anderen Ländern Anerkennung finden. Die Akkreditierung der Certification Bodies erfolgte früher – vor dem Bestehen von ISO 27006 – gemäß der Richtlinie EA 7/03 der »European co-operation for Accreditation«.

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

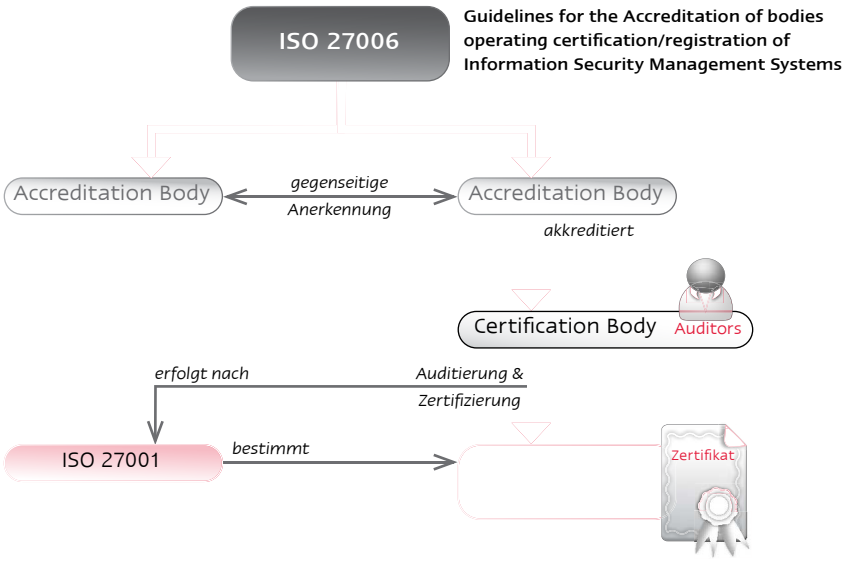
2 ISO 19011:2018 – Guidelines for auditing management systems.

Die eigentliche Zertifizierung erfolgt dann nach folgendem Ablaufschema:

- Das zu zertifizierende Unternehmen beauftragt ein akkreditiertes Unternehmen mit der Überprüfung des Information Security Management Systems.
- Das Audit-Team wird zusammengestellt.
- In einer ersten Phase erfolgen die Überprüfung und Beurteilung der Dokumentation.
- In einer zweiten Phase werden Vor-Ort-Audits durchgeführt.
- Es wird ein Audit-Bericht erstellt.
- Sofern der Audit-Bericht positiv ausfällt, wird das Zertifikat ausgestellt.

Ein erteiltes Zertifikat besitzt eine Gültigkeit von 3 Jahren, anschließend ist eine Re-Zertifizierung erforderlich, wodurch die Gültigkeit um weitere 3 Jahre verlängert wird.

Abbildung 6.4: Zertifizierungsschema nach ISO 27001



6.4 ISO 27002

ISO 27002 »Information security, cybersecurity and privacy protection – Information security controls« ist ein international anerkannter Leitfaden zum Management von Informationssicherheit und umfasst eine Sammlung von Empfehlungen für Informationssicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben (*Best Practices*). Der Standard orientiert sich dabei an einem Top-down-Ansatz mit generischen Standard-Sicherheitsmaßnahmen für annähernd alle relevanten Bereiche der Informationssicherheit. Er enthält keine produktorientierten, sondern nur allgemeine, technologieorientierte Maßnahmen und empfiehlt bewusst keine konkreten Sicherheitslösungen.

ISO 27002 adressiert kein spezielles Sicherheitsniveau, wodurch eine individuelle Anpassung an ein höheres oder niedrigeres Sicherheitsniveau jederzeit möglich ist. Eine konkrete Vorgehensweise gibt der Standard nicht vor, die Auswahl der Maßnahmen orientiert sich an den spezifischen Gegebenheiten des Unternehmens und ist so auch für kleinere Unternehmen problemlos anwendbar.

Der Leitfaden sieht sich als Basis zur Entwicklung organisationsbezogener Sicherheitsnormen und effektiver Managementpraktiken. Er eröffnet Unternehmen, Institutionen und Behörden den Weg zu einer formalen Zertifizierung des eigenen ISMS nach ISO 27001 und definiert die Zielsetzung der Informationssicherheit hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Zur Übersicht wird kurz auf die Inhalte der ISO 27002:2013 eingegangen und dann werden Änderungen in ISO 27002:2022 vorgestellt.

ISO 27002:2013 gliedert sich in 14 Managementgebiete und umfasst 35 Maßnahmenziele. Die Maßnahmenziele wiederum spezifizieren insgesamt 114 Maßnahmen (*Baseline Controls*), die zur Zielerreichung umgesetzt werden können. Die 14 Managementgebiete umfassen dabei die folgenden Punkte:

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development and maintenance
11. Supplier relationships
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Des Weiteren beinhaltet der Standard zu jeder Maßnahme Hinweise zur Umsetzung und weiterführende Informationen, bspw. Hinweise auf weiterführende Standards.

Die Inhalte und Ziele dieser Managementgebiete werden unten etwas näher dargestellt. ISO 27002:2022 weist eine geänderte Struktur auf, die Maßnahmen sind nun nur noch in vier Maßnahmenkategorien unterteilt:

- Organisatorische Maßnahmen
- Mitarbeiterbezogene Maßnahmen
- Physische Maßnahmen
- Technische Maßnahmen

Zur Strukturierung der Maßnahmen wurden Attribute (Tags) eingeführt, die verschiedene Sichtweisen auf die Maßnahmen erlauben.

Im Wesentlichen wurden die Maßnahmen neu sortiert, inhaltlich gibt es an den weiterhin geführten Maßnahmen nur geringfügige Änderungen. Neben der Änderung der Struktur wurden elf Maßnahmen neu hinzugefügt. Diese sind unten bei den Änderungen der Edition 2022 beschrieben.

Da die Maßnahmen aus den Managementgebieten der ISO 27002:2013 weitestgehend weiter bestehen bleiben und die meisten Institutionen sich Stand 2022 noch an diesem Standard ausgerichtet haben, werden sie hier vorgestellt. Wer sich bereits nach ISO 27002:2022 ausrichtet, wird die Ausführungen dennoch verwenden können.

Information Security Policies

Es sollen Information Security Policies verfasst werden, in denen die Richtungsvorgabe und Unterstützung des Managements für Informationssicherheit dokumentiert wird. Diese Policies müssen sowohl in Übereinstimmung mit Geschäftsanforderungen und den geltenden Gesetzen und Regelungen getroffen werden. Ein wesentliches Dokument hierbei ist die Information Security Policy. Sie dient der Festlegung der strategischen Ausrichtung und der Dokumentation der Unterstützung durch das Management hinsichtlich aller Belange der Informationssicherheit.

Diese Information Security Policies sollen an alle Mitarbeiter kommuniziert werden; eine regelmäßige Überprüfung und Bewertung der Policies stellt die Aktualität und Angemessenheit der getroffenen Maßnahmen sicher.

Organization of information security

Es sollte ein entsprechendes »Management Framework« etabliert werden, das Methoden, Verfahren und Prozesse zur Initiierung, Implementierung und Kontrolle von Informationssicherheit im Unternehmen zur Verfügung stellt. Neben dem Aufbau einer entsprechenden internen organisatorischen Infrastruktur und der Klärung von Verantwortlichkeiten werden hier auch die Themen »Mobile Endgeräte« und »Telearbeit« adressiert, für die entsprechende Nutzungsrichtlinien erlassen werden sollten.

Human Resources Security

Dieses Managementgebiet dient der Reduzierung von Risiken durch menschliche Fehler, Diebstahl, Betrug oder Missbrauch von Einrichtungen. Es umfasst sowohl Maßnahmen für interne und externe Mitarbeiter als auch für sonstige Auftragnehmer. Unterschieden werden hierbei grundlegende Maßnahmen, Maßnahmen während des Beschäftigungsverhältnisses als auch Maßnahmen, die bei der Beendigung des Beschäftigungsverhältnisses berücksichtigt werden sollten.

Asset Management

Um einen angemessenen Schutz der Unternehmenswerte erreichen zu können, bedarf es einer gründlichen und umfassenden Inventarisierung dieser Werte. Jeder Wert sollte einem eindeutigen Eigentümer zugewiesen sein. Um eine Einstufung und Zuordnung von Sicherheitsmaßnahmen durchführen zu können, sollte ein Klassifikationsschema erstellt und zur Kennzeichnung der Werte herangezogen werden.

Es sollten Vorgaben zur Handhabung von Speicher- und Aufzeichnungsmedien erstellt werden, um eine unerlaubte Veröffentlichung, Veränderung, Verwendung und Zerstörung von Informationen zu verhindern.

Access Control

Dieses Managementgebiet verweist auf die Bedeutung von Kontroll- und Überwachungsmaßnahmen für den Zugriff auf Informationen und Systeme zum Schutz vor Missbrauch durch interne Mitarbeiter oder externe Angreifer. Die Maßnahmenziele fokussieren auf eine Begrenzung des Zugangs und des Zugriffs entsprechend der Aufgaben aus Geschäftsprozessen, die geordnete Administration der Zugriffsrechte, die Verantwortung der Benutzer, bspw. zum Umgang mit Passwörtern, und die technische Zugriffskontrolle auf System- und Anwendungsebene.

Cryptography

Zum Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen durch Kryptografie ist eine Leitlinie zur Anwendung von Kryptografie zu erstellen. Für die Verwaltung von kryptografischen Schlüsseln sind Regelungen zu erlassen. Wesentlich in der Praxis ist, eine Übersicht zu haben, wo überall kryptografische Verfahren eingesetzt werden. Und dass prozessual sichergestellt wird, dass die Verfahren dem Stand der Technik entsprechen.

Physical and Environmental Security

Durch die Errichtung von Sicherheitszonen sollen vorbeugende Maßnahmen ergriffen werden, durch die unberechtigter Zugang und Beschädigung von Geschäftsgebäuden und Informationen vermieden werden. Des Weiteren werden Maßnahmen definiert, die vor Verlust, Beschädigung oder Kompromittierung von Wirtschaftsgütern und einer Unterbrechung der Geschäftstätigkeit schützen.

Operations Security

Zur Sicherstellung des korrekten und sicheren Betriebs informationsverarbeitender Einrichtungen sind entsprechende Verfahren und Verantwortlichkeiten festzulegen. Es müssen Maßnahmen zum Schutz vor Schadsoftware und zur Sicherung von Informationen (Backup) getroffen werden. Ferner adressiert dieses Managementgebiet die Themen Protokollierung und Überwachung, Kontrolle von Software im Betrieb, Umgang mit Schwachstellen und Audits von Informationssystemen.

Communications Security

Im Rahmen des Managementgebiet Communications Security werden Maßnahmen zum Management der Netzsicherheit und zum Erhalt der Sicherheit von Informationen und Software, die innerhalb einer Organisation oder mit Externen ausgetauscht werden, getroffen.

Systems Acquisition, Development & Maintenance

Vor der Entwicklung von informationsverarbeitenden Systemen müssen Sicherheitsanforderungen identifiziert und vereinbart werden. Bei der Wartung von Systemen müssen diese Anforderungen berücksichtigt werden. Hierzu sind

- Sicherheitsanforderungen an Systeme bereits während der Entwicklung zu berücksichtigen,
- Sicherheit bei Entwicklungs- und Supportprozessen zu integrieren sowie
- der Schutz von Testdaten sicherzustellen.

Supplier Relationship

Zum Schutz der organisationseigenen Werte müssen Anforderungen an die Informationssicherheit auch im Rahmen von Lieferantenbeziehungen berücksichtigt werden. Hier sind Maßnahmen zu ergreifen, um die Aufrechterhaltung der Sicherheit von Informationen und von informationsverarbeitenden Einrichtungen, die von Externen benutzt oder verwaltet werden, zu gewährleisten.

Des Weiteren soll ein Management der Dienstleistung von Dritten erfolgen, indem eine Überwachung und Überprüfung der Dienstleistungen und Dienstleister erfolgt.

Information Security Incident Management

Das Information Security Incident Management soll geeignete Prozesse zur Meldung, Behebung und Weiterverfolgung von Sicherheitsvorfällen umfassen, um rechtzeitig korrigierende Maßnahmen ergreifen zu können, sowie die Sicherung von Beweismaterial beinhalten.

Information security aspects of business continuity management

Es sollten präventive und reaktive Maßnahmen gegen Unterbrechungen der Geschäftsaktivitäten getroffen und kritische Geschäftsprozesse vor den Auswirkungen von Ausfällen und Katastrophen geschützt werden.

Compliance

Dieses Managementgebiet widmet sich der Einhaltung gesetzlicher Verpflichtungen, der Überprüfung der Sicherheitspolitik und der Einhaltung technischer Normen sowie Überlegungen zum Systemaudit. Die hier getroffenen Empfehlungen zur Regelkonformität dienen

- der Vermeidung von Verletzungen jeglicher Gesetze des Straf- oder Zivilrechts, gesetzlicher, behördlicher oder vertraglicher Verpflichtungen an die Informationssicherheit,
- der Sicherstellung der Erfüllung unternehmenseigener Sicherheits-Policies und -Standards sowie
- der Maximierung der Effektivität und Minimierung der Störungen beim System-Audit-Prozess.

Wesentliche Neuerungen der ISO 27002:2022

Die ISO 27002:2022 weist eine neue Struktur mit den oben aufgeführten vier Maßnahmenkategorien und nun 93 Maßnahmen auf. Die bisherigen Maßnahmen wurden zum Teil zu neuen Maßnahmen zusammengefasst. Neu aufgeführt sind zudem Maßnahmeneigenschaften oder -attribute, wie die Wirkungsweise (»präventiv«, »erkennend« oder »korri-

gierend«). Des Weiteren werden je Maßnahme unter anderem die Ziele, die die Maßnahme unterstützt (Verfügbarkeit, Integrität, Vertraulichkeit) benannt oder bspw. auch der Bereich der Informationssicherheit aufgeführt, den eine Maßnahme betrifft, z. B. »Governance«.

Elf der 93 Maßnahmen der ISO 27002:2022 sind neu hinzugekommen, unter anderem aufgrund der technischen Weiterentwicklung, verbesserter Schutzmaßnahmen oder neuer Schadensszenarien. Bestehende Managementsysteme und Sicherheitskonzepte sollten ggf. um diese neuen Maßnahmen ergänzt werden:

- 5.7 Threat Intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity
- 7.4 Physical security monitoring
- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Zusammenfassung

Die ISO 27001 stellt Anforderungen für ein zertifizierbares Information Security Management System und beschreibt die notwendigen Prozesse zur Implementierung, Überwachung, Prüfung, Instandhaltung und Verbesserung eines ISMS, das auf Basis eines etablierten Risikomanagements operiert. Ein ISO-27001-Zertifikat ist drei Jahre gültig, wobei ein jährliches Kontrollaudit zur Sicherstellung der geforderten Qualität notwendig ist.

Die ISO 27002 stellt einen generischen Maßnahmenkatalog zur Verfügung, der als Basis zur Entwicklung organisationsbezogener Sicherheitsnormen und effektiver Managementpraktiken herangezogen werden kann. Eine Zertifizierung nach ISO 27002 ist nicht möglich, allerdings ist die Gliederung der ISO 27002 als Annex A integraler Bestandteil der ISO 27001 und bildet somit das Grundgerüst für eine spätere Zertifizierung.

Literatur

[BS77991] *British Standards Institution (BSI):* BS 7799-1:1999, Information security management Code of practice for information security management

[BS77992] *British Standards Institution (BSI):* BS 7799-2:2002, Information security management systems – Specification with guidance for use

[DirectiveP1] *Annex SL Anhang SL der ISO/IEC-Direktiven*, Teil 1, »Consolidated ISO

[DirectiveP2] *Annex SL Anhang SL der ISO/IEC-Direktiven*, Teil 1, »Consolidated ISO Supplement«; *https://isotc.iso.org/livelink/livelink?func=ll&objId=4230452&objAction=browse&sort=subtype* (Stand: 17.01.2024)

[EA7/03] *European co-operation for Accreditation:* EA 7/03, Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems, November 1999;

Die Richtlinie EA 7/03 wurde zurückgezogen und durch ISO 27006 ersetzt. Hintergrund dieser Richtlinie ist, dass eine ISO-27001-Zertifizierung nur durch speziell akkreditierte, sogenannte Certification Bodies erfolgen darf. Die Akkreditierung dieser Certification Bodies erfolgte früher – vor dem Bestehen von ISO 27006 – gemäß dieser Richtlinie EA 7/03 der »European co-operation for Accreditation«.

[ISO17799] *International Organization for Standardization (ISO):* ISO/IEC 17799:2005, Information technology – Code of practice for information security management; *http://www.iso.org* (Stand: 17.01.2024)

[ISO27000] *International Organization for Standardization (ISO):* ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO/IEC 27000 gibt eine Einführung in die Familie der Informationssicherheitsmanagementsystem-Standards. Er enthält alle Begriffe und Definitionen, die in der ISO-27000-Serie verwendet werden.

[ISO27001] *International Organization for Standardization (ISO):* ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO 27001 beschreibt den Aufbau eines Informationssicherheitsmanagementsystems. Eine Zertifizierung nach ISO 27001 ist möglich.

[ISO27002] *International Organization for Standardization (ISO):* ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO 27002 bietet einen Leitfaden zum Management von Informationssicherheit und umfasst eine Sammlung von Empfehlungen für die Einführung, Durchführung, Aufrechterhaltung und Verbesserung eines Informationssicherheitsmanagementsystems.

[ISO27003] *International Organization for Standardization (ISO):* ISO/IEC 27003:2017, Information technology – Security techniques – Information security management system implementation guidance; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO 27003 konzentriert sich auf die kritischen Aspekte bei der Einführung eines Informationssicherheitsmanagementsystems. Der Standard stellt eine Anleitung für die erfolgreiche Konzeption und Implementierung eines ISMS nach ISO 27001 dar.

[ISO27004] *International Organization for Standardization (ISO):* ISO/IEC 27004:2016, Information technology – Security techniques – Information security management –Measurement; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO 27004 der ISO-2700er-Familie definiert die Kennzahlensysteme für die Messung der Wirksamkeit eines nach ISO 27001 implementierten Informationssicherheitsmanagementsystems.

[ISO27005] *International Organization for Standardization (ISO):* ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management; *http://www.iso.org* (Stand: 17.01.2024)

Der Standard ISO 27005 enthält Richtlinien für ein »Information Security Risk Management«, das den Anforderungen nach ISO 27001 gerecht wird. Dieser Standard ersetzt ISO/IEC 13335-3 und ISO/IEC 13335-4.

[ISO27006] *International Organization for Standardization (ISO):* ISO/IEC 27006:2015, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems; *http://www.iso.org* (Stand: 17.01.2024)