Eine Veröffentlichung des ISACA Germany Chapter e.V.

Bewertung der Leistung eines ISMS durch Schlüsselindikatoren

Praxisleitfaden für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016

ISACA Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Storkower Straße 158
10407 Berlin

www.isaca.de
info@isaca.de

Autorenteam:
- Nikolay Jeliazkov (CISA, CISM), Union Investment
- Andreas Kirchner (CISM), abat AG
- Dirk Meissner (CISA), Eaststep HK Limited
- Nico Müller BridgingIT GmbH
- Andrea Rupprich (CISA, CISM), usd AG
- Michael Schmid (CISM), Hubert Burda Media
- Holger Schrader (CISM, CRISC), ENFINA SECURITY s.r.o.

Stand: November 2020 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe Informationssicherheit)

Bewertung der Leistung eines ISMS durch Schlüsselindikatoren

Praxisleitfaden für ein zielorientiertes IS-Kennzahlensystem nach ISO/IEC 27004:2016

ISACA
Germany Chapter

Warum dieser Leitfaden?

Informationssicherheit ist unverzichtbar. Sie muss als Bestandteil der Unternehmensführung allerdings darauf ausgerichtet sein, die Geschäftsziele der Organisation optimal zu unterstützen.

Im Rahmen des Informationssicherheitsmanagementsystems (ISMS) definiert der Informationssicherheitsbeauftragte folglich Informationssicherheitsziele, die sich aus den Unternehmenszielen ableiten, und erarbeitet risikobasiert Steuerungsmaßnahmen (»Controls«), die in Summe geeignet sind, die Informationssicherheit in der Organisation zu steuern.

Die Steuerungsmaßnahmen müssen hierbei in der Lage sein, sowohl die Governance- und Compliance-Anforderungen der Organisation zu erfüllen als auch die vorhandenen Risiken der Organisation zu identifizieren und auf ein angemessenes Niveau zu senken (vgl. Abbildung 1).

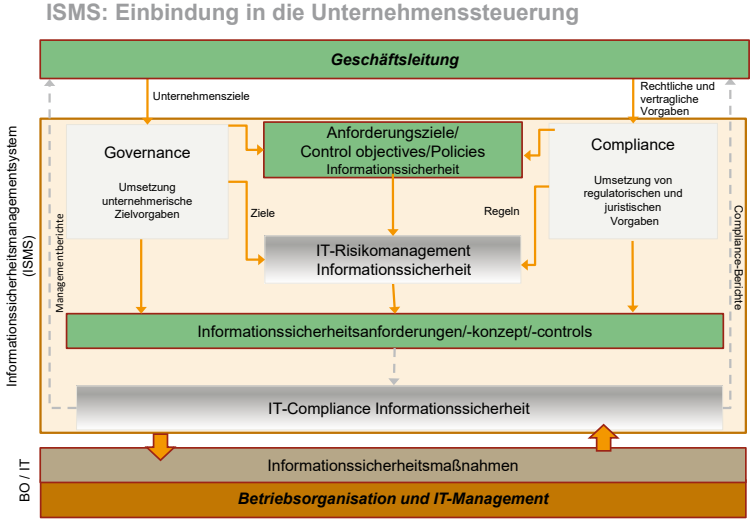

Abb. 1 GRC in der Unternehmenssteuerung

Es werden ISMS-Steuerungsprozesse in der Organisation eingeführt, die für die Mitarbeiter und die Prozesseigner auf operativer Ebene verbindlich sind (z. B. die Durchführung einer IS-Risikoanalyse auf operativer Ebene).

Der Informationssicherheitsbeauftragte definiert somit mit den Steuerungsmaßnahmen ein System von IS-relevanten Governance-Vorgaben, die in konkrete Aktivitäten (»Actions«) münden.

Schließlich hat der Informationssicherheitsbeauftragte zu überprüfen, ob die von ihm erlassenen Regelungen wirksam sind und ob sie dazu beitragen, die Informationssicherheitsziele und somit die Geschäftsziele der Organisation zu erreichen.

»Was man nicht messen kann, kann man nicht lenken«[1]

ist ein oft in diesem Kontext angeführtes Zitat.

Es ist folglich wichtig, dass der Informationssicherheitsbeauftragte ein IS-Kennzahlensystem etabliert, das anhand von Schlüsselindikatoren prüft, ob die Steuerungsmaßnahmen wirksam sind und die Ziele des ISMS erreicht werden.

Dieser Leitfaden zeigt auf, wie der Aufbau eines aussagekräftigen IS-Kennzahlensystems in der Informationssicherheit erfolgen sollte, welche Parameter aus welchen Gründen zu wählen sind und wie diese zu Schlüsselindikatoren *(Key Indicators)*, die den Erfolg und die Ziele des ISMS abbilden, zusammengeführt werden. Ein nach diesem Vorgehen aufgebauter ISMS-Bericht ermöglicht

- eine fundierte Entscheidungsfindung zur Steuerung innerhalb des ISMS durch den Informationssicherheitsbeauftragten und sein Team sowie
- eine fundierte Entscheidungsfindung im Topmanagement zum Einsatz von Finanz- und Personalressourcen mit Blick auf Aktivitäten zur Risikobehandlung in der Organisation.

1. »You can't manage what you can't measure«, Zitat wird W. Edwards Deming zugeschrieben.

Das IS-Kennzahlensystem trägt damit zur Erhöhung der Transparenz des Informationssicherheitsmanagements bei und das Vertrauen der Organisation in das ISMS wird gestärkt, dessen Fortschritte und Fehlentwicklungen werden aufgezeigt und ein nachhaltiger sowie kontinuierlicher Verbesserungsprozess (KVP) wird ermöglicht. Die Erkenntnisse aus der Auswertung der Kennzahlen dienen als Grundlage für den KVP. Ein derart gestaltetes IS-Kennzahlensystem ist auch in der Lage, Auskunft über die Effektivität und Wirtschaftlichkeit von bereits implementierten Sicherheitsmaßnahmen zu geben. Es kann beispielsweise folgende Fragen beantworten:

- Ist ein SIEM[2]-System in seiner derzeitigen Form effektiv (risikoreduzierende Wirksamkeit)?
- Ist es in seiner derzeitigen Form effizient (risikoreduzierender Nutzen im Verhältnis zu den entstehenden Kosten)?
- Existiert ein gutes Informationssicherheitsrisikomanagement in den operativen Geschäftsprozessen?

Im Besonderen ist ein IS-Kennzahlensystem als Teil des ISMS eine normative Anforderung der ISO/IEC 27001:2013, die dort in Kapitel 9.1 »Überwachung, Messung, Analyse und Auswertung« dokumentiert ist.

> *»Die Organisation muss die Leistung des Informationssicherheitssystems und die Wirksamkeit des Informationssicherheitsmanagementsystems auswerten.«*

Der vorliegende Leitfaden enthält praxisorientierte Empfehlungen und Hinweise für Organisationen, die entweder bereits ein IS-Kennzahlensystem für ein Informationssicherheitsmanagementsystem (ISMS) nach der internationalen **Norm ISO/IEC 27004:2016, Information Technology – Security Techniques – Information Security Management – Measurement**, betreiben oder ein solches aufbauen wollen.

2. Security Information and Event Management.

Danksagung

Das ISACA Germany Chapter e.V. bedankt sich bei der ISACA-Fachgruppe Informationssicherheit und bei den Autoren Nikolay Jeliazkov, Andreas Kirchner, Nico Müller, Andrea Rupprich und Michael Schmid für die Erstellung des Leitfadens sowie für die fachliche und redaktionelle Qualitätssicherung bei Julia Hermann, Angelika Holl, Melanie Holtz und Dr. Tim Sattler.

Projektkoordination und Redaktion: Holger Schrader/Dirk Meissner

Disclaimer

Die hier vorliegenden Informationen sind nach bestem Wissen durch Praxisexperten der Informationssicherheit, Auditoren und Informationssicherheitsverantwortliche erstellt worden. Jedoch wird an keiner Stelle ein Anspruch auf Vollständigkeit oder Fehlerfreiheit erhoben.

Alle in diesem Dokument aufgeführten Kennzahlen, deren Beschreibungen, Formeln und Zielvorgaben sind als Beispiele zu verstehen und sollten nicht unreflektiert übernommen werden. Jede Organisation muss die für sie passenden Kennzahlen und Werte für sich selbst ermitteln und bewerten.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Inhaltsverzeichnis

1 Einleitung und Aufbau des Praxisleitfadens

Der Zweck eines Informationssicherheitsmanagementsystems (ISMS) ist die Erreichung und Erhaltung der allgemeinen Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit. Zur Erreichung dieser Ziele werden risikoorientiert Steuerungsmaßnahmen etabliert, um die Informationssicherheitsrisiken der Organisation auf ein angemessenes Niveau zu reduzieren.

Allein die Einführung dieser Steuerungsmaßnahmen stellt aber nicht zwangsläufig sicher, dass ein Risiko effektiv und effizient behandelt wird und die Sicherheitsziele erreicht werden. Denn es muss auch geprüft werden, ob die etablierten Steuerungsmaßnahmen effektiv und effizient bei der Zielerreichung unterstützen und z. B. die Regelungen auf operativer Ebene (in den vom ISMS gesteuerten Geschäftsprozessen) umgesetzt werden.

Die Überprüfung der Wirksamkeit erfolgt mittels eines IS-Kennzahlensystems, welches das zentrale Werkzeug der Governance-Ebene für die in Kapitel 9.1 der ISO/IEC 27001:2013 geforderte »Performance-Überwachung« darstellt.

Die Notwendigkeit eines IS-Kennzahlensystems ergibt sich auch aus der geschäftlichen Anforderung, die Effektivität und die Effizienz der Steuerungsmaßnahmen eines Managementsystems sicherzustellen.

Damit das Management der Organisation eine fundierte Entscheidung treffen kann, benötigt das IS-Kennzahlensystem wohlbegründete Kennzahlen, welche die Ist-Situation des ISMS in Bezug auf die nachfolgenden Kernfragen transparent darstellen:

- Welche Steuerungsmaßnahmen des Managementsystems erfüllen derzeit ihre vordefinierten Zielsetzungen und wo gibt es Verbesserungspotenzial?
- Welche technischen und organisatorischen Maßnahmen (TOM) des Annex A oder der »Erklärung zur Anwendbarkeit« erfüllen den Zweck, der im jeweiligen Kontrollziel zur Maßnahme festgelegt ist?

In diesem Leitfaden stellen wir dar, wie Sie die Leistung der Informationssicherheit und die Wirksamkeit des ISMS bewerten und hierbei die Empfehlungen der ISO/IEC 27004:2016 anwenden können. Der Leitfaden dient damit auch der themenbezogenen Vertiefung des 2016 von der ISACA-Fachgruppe Informationssicherheit veröffentlichten Implementierungsleitfadens ISO/IEC 27001:2013 [ISACA 2016].

Themenbereiche

Der vorliegende Praxisleitfaden orientiert sich an den wesentlichen Themenbereichen der Norm ISO/IEC 27004:2016, allerdings ohne die Abschnittsstruktur des Standards identisch wiederzugeben. Vielmehr werden die relevanten Themenbereiche eines IS-Kennzahlensystems in den nachfolgenden drei Kennzahlklassen beschrieben, die sich in der Praxis als vorteilhaft erwiesen haben:

1. Key-Performance-Indikatoren (KPI) zur Steuerung der IS-Governance	In vielen Organisationen erfolgt die Wirksamkeitsprüfung zunächst auf Basis von KPIs, was ebenfalls ausreichend ist, um die Anforderungen der ISO/IEC 27001:2013 zu erfüllen. Die weitere Unterteilung der KPIs in die links aufgeführten Klassen bietet allerdings Vorteile, die in den nachfolgenden Kapiteln erläutert werden.
2. Key-Risk-Indikatoren (KRI) zur Steuerung des IS-Risikos (engl. Risk)	
3. Key-Control-Indikatoren (KCI) zur Steuerung der IS-Compliance	

Des Weiteren werden in den nachfolgenden Kapiteln zu allen Klassen die wesentlichen Erfolgsfaktoren für eine normkonforme Definition und Realisierung aufgezeigt.

Der zielgerichtete und wirtschaftliche Betrieb eines ISMS ist ein herausforderndes Unterfangen. Ein Managementsystem braucht »smarte«[3] Ziele, ausreichendes und fachkundiges Personal, einen befähigten Informationssicherheitsbeauftragten (»CISO«) und ein motiviertes und qualifiziertes Team in den Fachbereichen. Diese Aufzählung macht deutlich,

3. SMART: spezifisch, messbar, attraktiv/akzeptiert, realistisch, terminiert.

wie ressourcen- und kostenintensiv ein solches organisatorisches System sein kann.

Sollten die Kennzahlen zeigen, dass sich das ISMS außerhalb der Zielvorgaben bewegt, ist dies der Auslöser für ein notwendiges korrektives Eingreifen des Managements. Die Kennzahlen müssen die momentane Ist-Situation im Verhältnis zu deren definierten Sollwerten aufzeigen.

Kennzahlen ohne Sollwerte sind nutzlos, da sie keine Steuerung ermöglichen.

Die entsprechenden Sollwerte bestimmen sich aus den Geschäftszielen, den Unternehmensrisiken sowie den rechtlichen und vertraglichen Vorgaben.

Konventionen

Der Begriff »Anhang« wird bei Verweisen auf Anhänge dieses Leitfadens, die Begriffe »Annex« bzw. »Annex A« werden bei Verweisen auf den Annex A der Norm ISO/IEC 27001:2013 oder der Annexe der ISO/IEC 27004:2016 verwendet.

2 Klassen von Kennzahlen innerhalb eines ISMS

Damit der Informationssicherheitsbeauftrage in die Lage versetzt werden kann, auf Basis valider Daten die Informationssicherheit zu steuern, kann er sich an einem bewährten Konzept der Unternehmenssteuerung orientieren: dem Berichtswesen.

Das Berichtswesen sammelt betriebswirtschaftlich orientierte Unternehmensdaten, bereitet sie auf und stellt sie dem Topmanagement und anderen leitenden Mitarbeitern zur Verfügung. Es arbeitet abteilungs- und bereichsübergreifend und erhebt Daten aus allen relevanten Sparten eines Unternehmens. Das Berichtswesen ermöglicht ein effizientes Controlling und eine erfolgsorientierte Lenkung des Unternehmens. Analog können auch alle für die Informationssicherheit relevanten Informationen aus internen und externen Quellen im Berichtwesen gesammelt und abgelegt werden. In größeren Unternehmen werden diese Informationen meist durch ein Managementinformationssystem (MIS) zur Verfügung gestellt.

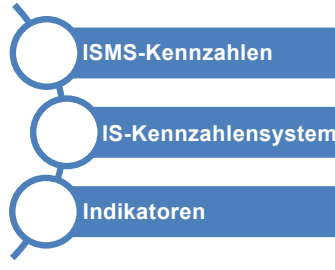

Abb. 2–1 Steuerung Informationssicherheit

Auf Grundlage dieser Datenbasis kann eine Vielzahl von Kennzahlen (Indikatoren) entwickelt werden. Diese Kennzahlen werden im ISMS-Kennzahlensystem zusammengefasst und in Beziehung gesetzt (vgl. Abbildung 2–1). Die erfassten Messwerte der Kennzahlen müssen mit definierten Schwellwerten hinterlegt werden (vgl. Abbildung 2–2), was dann in eine

Metrik mündet. Kennzahlen können für sämtliche messbaren und steuerbaren Bereiche verwendet werden (vgl. Kapitel 5).

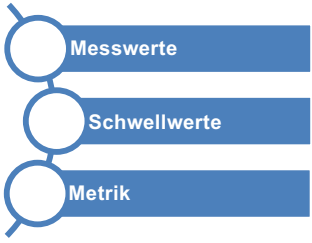

Abb. 2–2 Zusammensetzung von Indikatoren

Um Vergleichbarkeit, Kontinuität und Nachvollziehbarkeit herzustellen, sollten alle Ziele, deren Erreichung anhand von Kennzahlen gemessen werden soll, den SMART-Kriterien[4] genügen:

- **S**pezifisch
- **M**essbar
- **A**ttraktiv/Akzeptiert
- **R**ealistisch
- **T**erminiert

Dadurch wird sichergestellt, dass diese Ziele exakt, eindeutig und für jeden verständlich beschrieben werden.

Der Informationssicherheitsbeauftragte ist nun in der Lage, anhand der unterschiedlichen Kennzahlen, z. B. mithilfe einer Dashboard-Ansicht, die Informationssicherheit zu bewerten und zu steuern. Bei der Vielzahl der Kennzahlen konzentrieren wir uns im Hinblick auf die Informationssicherheit auf die folgenden drei Kennzahlklassen:

4. *https://de.wikipedia.org/wiki/SMART_(Projektmanagement)*

2.1 KPI – Key-Performance-Indikatoren

Ein Key-Performance-Indikator ist ein Wert (Soll-Ist-Vergleich), der anzeigt, wie erfolgreich ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse in Bezug auf die Erreichung der Informationssicherheitsziele umsetzt. Erfolgreich ist eine Maßnahme, wenn das gewünschte Leistungsniveau innerhalb der vorgegebenen Zeit und mit möglichst geringem Aufwand erreicht wird.

Beispielformeln:

- Benötigte Zeit im Vergleich zur geplanten Zeit bei der vorgegebenen Umsetzungsrate (z. B. 80 % der Mitarbeiter) einer Awareness-Kampagne.
- Benötigtes Budget im Vergleich zum geplanten Budget für die Umsetzung einer Awareness-Kampagne.

2.2 KRI – Key-Risk-Indikatoren

Ein Key-Risk-Indikator ist ein Wert (Soll-Ist-Vergleich), der anzeigt, ob Veränderungen im Risikoprofil die gewünschten Toleranzgrenzen potenziell überschreiten und damit die Zielerreichung gefährden. Er ist damit ein Maß dafür, wie risikoorientiert ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Eine Situation, die den Risikoappetit des Unternehmens überschreitet, wird durch gegensteuernde Maßnahmen wieder in den akzeptablen Risikobereich gebracht.

Beispielformeln:

- Prozentsatz der Mitarbeiter, die einen präparierten Phishing-Link während einer Awareness-Kampagne klicken.
- Prozentsatz der IT-Systeme mit Schwachstellen, die nicht im vorgesehenen Zeitfenster geschlossen wurden.
- Prozentsatz der produktiven IT-Systeme, für die kein Herstellersupport mehr besteht.

2.3 KCI – Key-Control-Indikatoren

Ein Key-Control-Indikator ist ein Wert (Soll-Ist Vergleich), der anzeigt, wie **effektiv** in Bezug auf die Zielerreichung ein Unternehmen die relevanten technischen und organisatorischen Maßnahmen sowie die Informationssicherheitsprozesse umsetzt. Effektiv ist eine Maßnahme, wenn die Steuerungsziele zuverlässig innerhalb der gewünschten Toleranzgrenzen erreicht werden.

Beispielformeln:

- Verhältnis der bisher geschulten Mitarbeiter im Vergleich zu den Planzahlen der zu schulenden Mitarbeiter bei einer Awareness-Kampagne.
- Anzahl der Mitarbeiter, die die Lernkontrolle am Ende der Awareness-Kampagne bestanden haben, im Vergleich zu den bereits geschulten Mitarbeitern bei einer Awareness-Kampagne.

3 Beziehungen der Kennzahlklassen

Aus den Definitionen in Kapitel 2 wird deutlich, dass diese drei Arten von Kennzahlen jeweils einen unterschiedlichen Schwerpunkt haben und unterschiedliche Managementindikatoren für unterschiedliche Zielgruppen bereitstellen. Im Umkehrschluss muss dies aber nicht bedeuten, dass die dreifache Menge an Daten erforderlich ist. Dies liegt im Wesentlichen daran, dass diese drei verschiedenen Arten von Indikatoren miteinander verknüpft sind und dass die gesammelten Daten oft für verschiedene Kennzahlklassen wiederverwendet werden können. Es wäre nicht ungewöhnlich, dass Daten für einen KCI beispielsweise für einen KRI wiederverwendet werden können, da sich lediglich der Blickwinkel auf die Daten ändert (vgl. Abbildung 3–1).

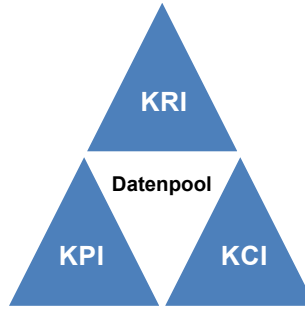

Abb. 3–1 Beziehung der Indikatoren zum Datenpool

Für Unternehmen ist es wichtig zu ermitteln, ob die Investitionen in die Informationssicherheit angemessen sind. Hierfür ist das Zusammenspiel zwischen den Kennzahlklassen KPI, KRI und KCI maßgebend. Nachdem die spezifische Verwendung für die einzelnen Arten von Kennzahlen definiert wurde, wird daher im Folgenden die Beziehung der Kennzahlklassen untereinander betrachtet.

KPIs überwachen den Grad der Zielerreichung, KRIs die Risikolage hinsichtlich einer Gefährdung der Zielerreichung und KCIs die Effektivität der Steuerungsmaßnahmen, die das Risiko auf ein angemessenes Niveau reduzieren sollen.

Während ein Unternehmen mithilfe der KCIs feststellen kann, wie wirksam die etablierten Steuerungsmaßnahmen in Bezug auf die Erreichung der Informationssicherheitsziele innerhalb der gesetzten Toleranzgrenzen sind, helfen KRIs dem Unternehmen, Risikosituationen zu identifizieren, die ein Überschreiten der Toleranzgrenzen wahrscheinlich erscheinen lassen und damit die Zielerreichung gefährden.

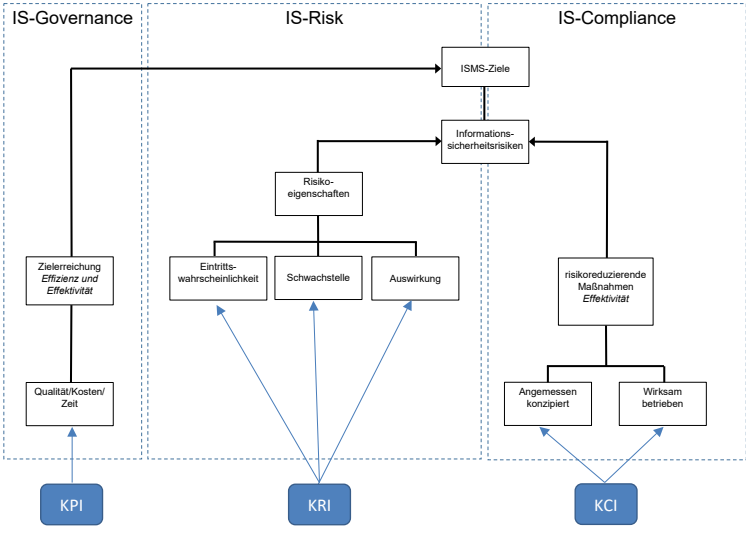

Abb. 3–2 Aufbau und Beziehung von KPI, KRI und KCI

KCIs haben eine starke Beziehung zu KRIs, denn wenn z. B. ein KCI auf das Versagen oder die Schwäche einer Kontrolle hinweist, dann ist es wahrscheinlich, dass das Risikoniveau ansteigt, was durch KRIs gemessen wird. Ein nicht erreichter KPI zeigt u.U. die Verzögerung bei der Umsetzung einer risikominimierenden Maßnahme. Der KCI wirkt hier ähnlich wie ein internes Kontrollsystem (IKS), das aus prozessintegrierten Maßnahmen wie Kontrollen und organisatorischen Sicherungsmaßnahmen besteht (vgl. COSO-Framework – Internal Control).

Ein weiterer interessanter Aspekt im Zusammenhang mit den Indikatoren ist die Zielgruppe, an die sie jeweils adressiert werden. Dies wird im folgenden Kapitel 4 betrachtet.

4 Zielgruppen der Kennzahlen

Als mögliche Zielgruppen für Kennzahlen kommen neben den verschiedenen Managementebenen eines Unternehmens weitere interessierte Parteien infrage, die Informationen über die Wirksamkeit eines ISMS oder einer Steuerungsmaßnahme anfordern (vgl. [ISO/IEC 27004:2016, Kapitel 6.5a]).

Dabei ist es wichtig, den Informationsbedarf der jeweiligen Zielgruppe zu treffen. Hierfür sollten zunächst die verschiedenen Verantwortlichkeiten im Zusammenhang mit der Informationssicherheit im Unternehmen geklärt werden, wie etwa die Festlegung der Verantwortlichen für den Schutz von Informationswerten und die Eigentümer des Informationswertes. Hierbei sind die Anliegen der Zielgruppen zu verstehen, um die richtige Auswahl von Kennzahlklassen/Kennzahlen zu treffen.

(Senior) Management

Der Geschäftsführer/Vorstandsvorsitzende hat die strategischen Auswirkungen der Informationssicherheitsaktivitäten und -risiken auf die Geschäftsziele zu bewerten und einzuordnen. Mögliche Fragestellungen sind: »Was sind unsere größten Bedrohungen?«; »Sind wir sicherer/unsicherer aufgestellt als vergleichbare Unternehmen?«. Die Antwort kann anhand von strategischen KRIs (z. B. »Bedrohungen haben tolerierbare Auswirkungen auf das Risikoprofil«) und KPIs (z. B. »Informationssicherheitsziele werden erreicht«) erfolgen.

Den Finanzvorstand/die Geschäftsleitung Finanzen interessieren Metriken mit Bezug zu finanziellen Risiken/Auswirkungen der Informationssicherheit auf das Unternehmen, die typischerweise über strategische KPIs und KRIs adressiert werden. Diese Indikatoren dienen beispielsweise der Vermeidung von Strafzahlungen bei Nichteinhaltung von gesetzlichen und regulatorischen Anforderungen (z. B. PCI DSS, DSGVO, BAIT).

Dem Informationssicherheitsbeauftragten und dem IT-Leiter geben die strategischen Kennzahlen für die Leitungsebene nicht nur Aufschluss über die Risikolage und den Grad der Zielerreichung, sondern diese Metriken bilden häufig auch eine Grundlage für die persönliche Leistungsbewertung.

Darüber hinaus ist der IT-Leiter an operativen KPIs interessiert, die Auskunft über den Ressourceneinsatz im Informationssicherheitsumfeld geben. Beispiel: »Wie hoch sind die Leistungseinbußen auf einem Produktivsystem nach Einführung einer technischen Sicherheitslösung?«

Für den Informationssicherheitsbeauftragten sind wiederum KCIs relevant, die einen Hinweis liefern, ob eine spezifische Steuerungsmaßnahme nicht effektiv umgesetzt oder nicht korrekt befolgt wurde.

Return on Security Investment (ROSI)

Seit 2002 wird die Problematik der Kosten-Nutzen-Evaluation häufig unter dem Schlagwort des »Return on Security Investment« (ROSI) diskutiert, dessen Grundidee – analog zum klassischen ROI – der Vergleich des finanziellen Gewinns eines Investitionsprojekts mit seinen Gesamtkosten ist. Eine wichtige Grundlage für ROSI-Berechnungen bildet z. B. das Konzept der jährlichen Verlusterwartung, »Annual Loss Expectancy« (ALE), das bereits Ende der 1970er-Jahre vom »US National Bureau of Standards« auf den Bereich der Informationssicherheit übertragen wurde (vgl. Abbildung 4-1). Um derartige Kosten-Nutzen-Betrachtungen durchführen zu können, müssen Kosten und Nutzen von Informationssicherheit messbar gemacht werden.

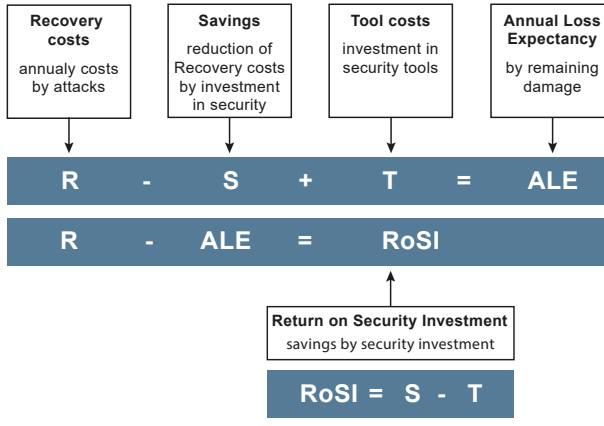

Abb. 4–1 Berechnung des Return on Security Investment (ROSI)

Fachbereiche

Die Fachbereiche haben unterschiedliche Anforderungen an ein ISMS-Kennzahlensystem. Sie benötigen Kennzahlen, die Aufschlüsse über die bestehenden Risiken (KRI) und die Wirksamkeit definierter Maßnahmen zur Risikoreduzierung (KCI) bzw. den Beitrag eingeführter Maßnahmen zur Zielerreichung (KPI) aufzeigen.

Weitere interessierte Parteien mit Bezug zur Informationssicherheit (Beispiele):

- Interne Revisoren und Auditoren
- Notfallmanager und Spezialisten für die Betriebskontinuität
- Verantwortliche für die physische Sicherheit (z. B. Leiter von Produktionsstätten)
- Betriebsrat/Personalrat

Mögliche interessierte Parteien außerhalb des Unternehmens:

- Geschäftspartner, insbesondere in Business-to-Business-Zulieferer-Netzwerken
- Aufsichtsbehörden
- Vergleichbare Unternehmen im freiwilligen Austausch und zum gegenseitigen Benchmarking
- Geschäftspartner, sofern die Erbringung von Informationssicherheitsmaßnahmen vertraglich gefordert ist

5 Sinnvoller Aufbau von Kennzahlen

Um eine zielorientierte Struktur und eine pragmatische Erstellung von Kennzahlen zu erreichen, benötigt man die folgenden Grundlagen:

- Eine fachliche Begründung der Kennzahl
- Einen Typ: Erreichungsgrad (performance) oder Effektivität (effectiveness)
  Anmerkung: Als Erweiterung der ISO/IEC 27004:2016 haben die Autoren noch die »Risikoorientierung« hinzugefügt.
- Einen definierten Prozess zur Sicherstellung von Nachvollziehbarkeit und Reproduzierbarkeit
- Definierte Eigenschaften (Kenndaten, Einflussgrößen und Bewertungen)

Der Zusammenhang zwischen den Anforderungen der zertifizierungsfähigen ISO/IEC 27001:2013 und der ISO/IEC 27004:2016 über das ISMS-Kennzahlensystem wird in Abbildung 5–1 verdeutlicht (vgl. [ISO/IEC 27004:2016, Structure and Overview (Clause 4)]).

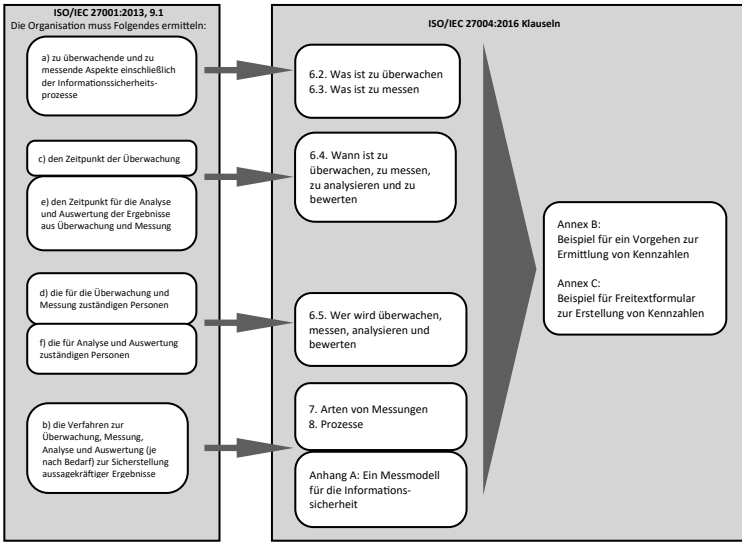

Abb. 5–1 Zuordnung zu ISO/IEC 27001:2013, 9.1 Anforderungen (Übersetzung durch die Autoren)

Die ISO/IEC 27004:2016 erläutert, dass durch eine Organisation für den Aufbau eines pragmatischen und dennoch aussagekräftigen ISMS-Kennzahlensystems die folgenden Punkte ermittelt und dokumentiert werden sollten:

1. Die relevanten Informationssicherheitsprozesse und -maßnahmen, die überwacht werden sollten. Dies sind beispielsweise eine fachliche Begründung (These) und der Typ der aus der Messung resultierenden Kennzahl: Erreichungsgrad, Effektivität bzw. Risikoorientierung. Darüber hinaus müssen die Aspekte der Prozesse und Maßnahmen identifiziert werden, die zum Gegenstand einer Messung herangezogen werden können.

   Da der Zweck einer Informationssicherheitsmaßnahme üblicherweise darin besteht, das Risiko zu reduzieren, können verschiedenste Attribute gemessen werden:

- Das Ausmaß, in dem eine präventive Maßnahme die Wahrscheinlichkeit des Auftretens eines Ereignisses verringert.
- Das Ausmaß, in dem eine reaktive Maßnahme die Konsequenz (Schaden) eines Ereignisses verringert.
- Die Häufigkeit von Ereignissen, die eine reaktive Maßnahme bewältigen kann, bevor sie versagt.
- Wie lange es nach dem Auftreten eines Ereignisses dauert, bis eine Überwachungsmaßnahme (Kontrolle) erkennt, dass das Ereignis aufgetreten ist.

2. Im nachfolgenden Schritt werden die Methoden zur Messung, Überwachung, Analyse und Auswertung definiert und dokumentiert. Dies stellt nachvollziehbare, aussagekräftige und wiederholbare Ergebnisse in Form von belastbaren Kennzahlen sicher.

3. Im dritten Schritt werden die Zeiträume und die zuständigen Personen für die einzelnen Phasen festgelegt. Dabei werden alle Details der Datensammlung, Datenauswertung und Berichterstellung dokumentiert:

   - Frequenz der Datensammlung – z. B. wöchentlich
   - Frequenz der Datenauswertung – z. B. monatlich
   - Frequenz der Ergebnisberichte – z. B. vierteljährlich

4. Im finalen Schritt wird festgelegt, wie lange die oben festgelegte Messstruktur gültig sein soll und ob in der Zwischenzeit ein Nachjustieren der Mess- oder Analysemethode stattfinden soll.

Diese Art der Dokumentation führt zu einem Kennzahlen-Steckbrief, wie er später in diesem Kapitel an einem Beispiel gezeigt wird. Dieser Kennzahlen-Steckbrief dient bei einem zertifizierten ISMS, zusammen mit den Nachweisen der Überwachungs- und Messergebnisse, als dokumentierte Information und sollte daher sorgfältig aufbewahrt werden.

Abbildung 5–2 zeigt das zugrunde liegende Messmodell der Informationssicherheit zur Sicherstellung von Nachvollziehbarkeit und Reproduzierbarkeit, das in [ISO/IEC 27004:2016, Annex A] dargestellt ist.

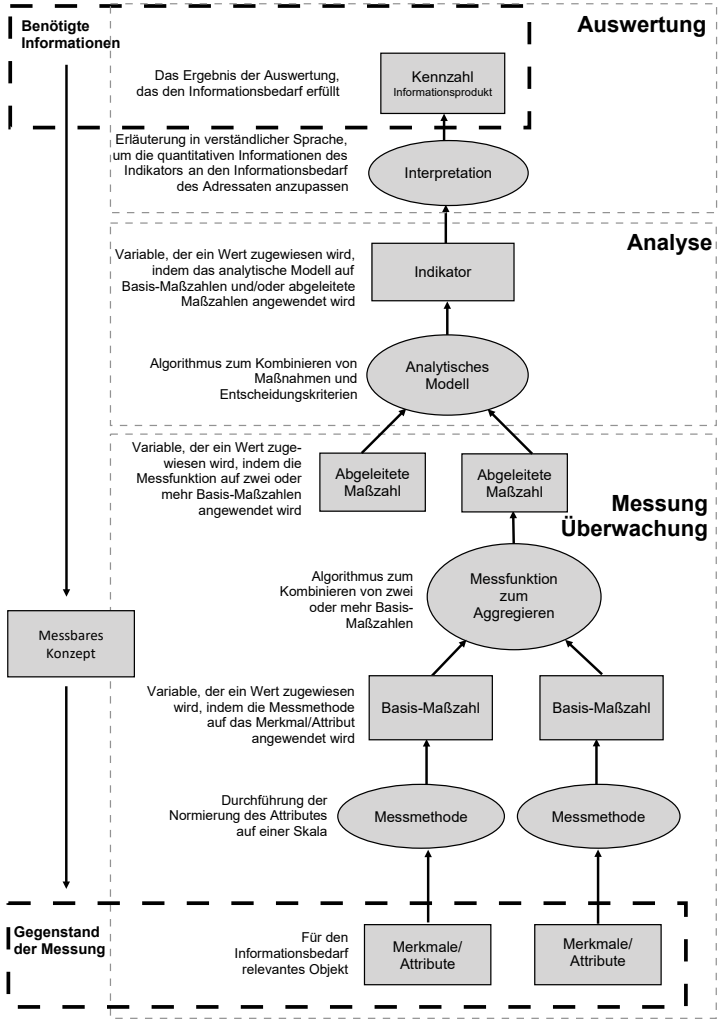

Abb. 5–2 Messmodell der Informationssicherheit zur Sicherstellung von Nachvollziehbarkeit und Reproduzierbarkeit (nach [ISO/IEC 27004:2016, Annex A], Übersetzung durch die Autoren)

Dieses Messmodell führt dann zu einem Profil des Kennzahlen-Steckbriefs.

Zunächst schauen wir in Tabelle 5–1 auf die rudimentären und unbedingt notwendigen Werte und ihre Zweckbestimmung.

Informationsbeschreibung	Bedeutung oder Zweck
ID der Maßnahme	Spezifische Kennung
Informationsbedarf	Übergreifendes Verständnis, zu welcher Erkenntnis die Messung beiträgt.
Messung	Spezifikation der Messung, gewöhnlich mit Worten wie »Prozentsatz«, »Anzahl«, »Häufigkeit« und »Durchschnitt« beschrieben.
Formel/Wertung	Wie die Messung ausgewertet, berechnet oder bewertet werden soll.
Ziel	Das gewünschte Ergebnis der Messung, z. B. ein Meilenstein oder eine statistische Messung oder ein Satz von Schwellwerten. Zu beachten ist, dass eine fortlaufende Überwachung erforderlich sein kann, um sicherzustellen, dass das Ziel nachhaltig erreicht wird.
Umsetzungsnachweise	Beweise, die bestätigen, dass die Messung: ◗ durchgeführt wird, ◗ geeignet ist, mögliche Ursachen für schlechte Ergebnisse zu identifizieren, und ◗ einen Beitrag für den Prozess leistet. Daten, die einen Beitrag für die Formel leisten.
Frequenz	Legt fest, wie oft die Daten gesammelt und gemeldet werden sollen. Es kann einen Grund für mehrere Frequenzen geben.
Verantwortliche Stellen	Die Stelle (Rolle), die für die Erfassung und Verarbeitung der Messung verantwortlich ist. Zumindest sollten ein Informationseigentümer, ein Informationssammler und der Adressat der Kennzahlen identifiziert werden.

→

Datenquelle	Mögliche Datenquellen können Datenbanken, Tracking-Tools, andere Teile der Organisation, externe Organisationen oder bestimmte individuelle Rollen sein.
Berichtsformat	Wie die Kennzahl erfasst und gemeldet werden soll, z. B. als Text, numerisch, grafisch (Kreisdiagramm, Liniendiagramm, Balkendiagramm usw.) als Teil eines »Dashboards« oder einer anderen Form der Präsentation.

Tab. 5–1 Profil des Kennzahlen-Steckbriefs (vgl. [ISO/IEC 27004:2016, Processes (Clause 8)], Übersetzung durch die Autoren)

Im Annex B wird dieser rudimentäre Steckbrief in mehreren Beispielen mit Inhalten gefüllt.

Hinweis:
Im Anhang A dieses Leitfadens befindet sich noch ein weiteres sehr detailliertes Beispiel für einen Kennzahlen-Steckbrief.

B.11 ISMS-Training oder ISMS-Sensibilisierung

Informationsbeschreibung	Bedeutung oder Zweck
ID der Maßnahme	… wird durch die Organisation vergeben.
Informationsbedarf	Um zu messen, wie viele Mitarbeiter ein ISMS-bezogenes Sensibilisierungstraining erhalten haben, und um [mit der Messung] die Einhaltung der Informationssicherheitsrichtlinie der Organisation zu kontrollieren.
Messung	Prozentsatz der Mitarbeiter, die an einem ISMS-Sensibilisierungstraining teilgenommen haben.
Formel/Wertung	◗ I1 = (Anzahl der Mitarbeiter, die eine ISMS-Schulung erhalten haben/Anzahl der Mitarbeiter, die eine ISMS-Schulung erhalten müssen) * 100 ◗ I2 = (Anzahl der Mitarbeiter, die ihre ISMS-Schulung im letzten Jahr erneuert haben/Anzahl der Mitarbeiter im Gültigkeitsbereich) * 100

→

Ziel	◗ Grün: wenn I1 > 90 % und I2 > 50 %, ◗ sonst Gelb: wenn I1 > 60 % und I2 > 30 %, ◗ sonst Rot Rot – Intervention ist erforderlich, Ursachenanalyse muss durchgeführt werden, um Gründe für Nichteinhaltung und schlechte Leistung zu ermitteln. Gelb – Die Anzeige sollte genau auf ein mögliches Abrutschen nach Rot überwacht werden. Grün – Keine Aktion erforderlich.
Umsetzungsnachweise	Teilnahmelisten aller Sensibilisierungstrainings, Anzahl der Felder/Zeilen mit dem Inhalt »Erhalten« in den Protokollen/Registern der ISMS-Schulungen.
Frequenz	◗ Sammeln: monatlich, erster Arbeitstag des Monats ◗ Analyse: vierteljährlich ◗ Bericht: vierteljährlich ◗ Eichung der Messung (Revision): jährliche Überprüfung ◗ Messzeitraum: jährlich
Verantwortliche Stellen	◗ Informationseigentümer: Manager für Trainings – Personalabteilung ◗ Informationssammler: Trainingsmanagement – Personalabteilung ◗ Adressat/Kunde der Messung: Verantwortlicher Manager für das ISMS, Informationssicherheitsbeauftragter
Datenquelle	Mitarbeiterdatenbank, Schulungsunterlagen, Teilnehmerlisten der Sensibilisierungstrainings
Berichtsformat	Balkendiagramm mit farbcodierten Balken basierend auf dem Ziel. Dem Balkendiagramm sollte eine kurze Zusammenfassung der Bedeutung der Messung und mögliche Gegenmaßnahmen beigefügt werden. **ODER** Kreisdiagramm über die aktuelle Situation und Liniendiagramm für die Darstellung der Entwicklung zur Konformität.

Tab. 5–2 Beispiel für einen Kennzahlen-Steckbrief

Um sicherzustellen, dass die Datensammlung, Analyse und Berichterstellung kein einmaliges Ereignis bleiben, sondern wie bei Managementsystemen üblich einem kontinuierlichen Prozess folgen, gibt es auch für das IS-Kennzahlensystem einen am Deming-Kreis orientierten Prozess (vgl. Abbildung 5–3).

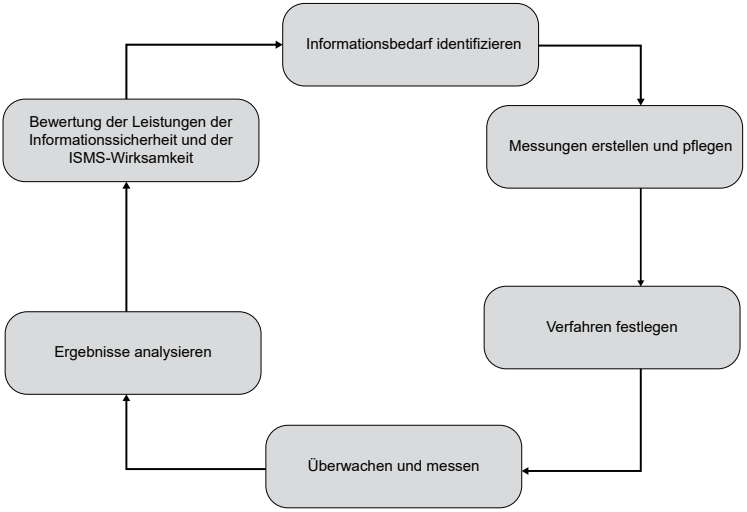

Abb. 5–3 Deming-Kreis der Schlüsselindikatoren (vgl. [ISO/IEC 27004:2016, Processes (Clause 8)])

6 Steuerung durch Kennzahlen

Auf Basis der Anforderungen der verschiedenen Zielgruppen unterstützt das IS-Kennzahlensystem die Entscheidungsfindung der jeweiligen Zielgruppe.

Die Steuerungsmaßnahmen müssen daher in der Lage sein, sowohl die Governance- und Compliance-Anforderungen der Organisation zu befriedigen als auch die vorhandenen Risiken der Organisation zu identifizieren und auf ein angemessenes Niveau zu senken.

Welches Ziel verfolgt also dieser Prozess zur Erstellung und zum Betrieb eines IS-Kennzahlensystems?

Eine Kennzahl dient dazu, anzuzeigen, ob ein Informationssicherheitsprozess oder eine Informationssicherheitsmaßnahme sich selbst regeln kann oder ob ein Eingreifen (Steuern) erforderlich ist. Da das Management in einem Managementsystem die Verpflichtung zur angemessenen Reaktion hat, ist außerhalb definierter Schwellwerte regulierend einzugreifen. Dies soll ein vereinfachtes Diagramm darstellen.

Ist die Kennzahl

- grün, so arbeitet der Prozess im Normbereich.
- gelb, so arbeitet der Prozess oder die Maßnahme im Toleranzbereich und sollte durch vordefinierte Kontrollprozesse eigenständig wieder in den Normbereich zurückfinden.
- rot, so arbeitet der Prozess außer Kontrolle.
  Er wird sich eigenständig nicht mehr in den Normbereich bewegen.

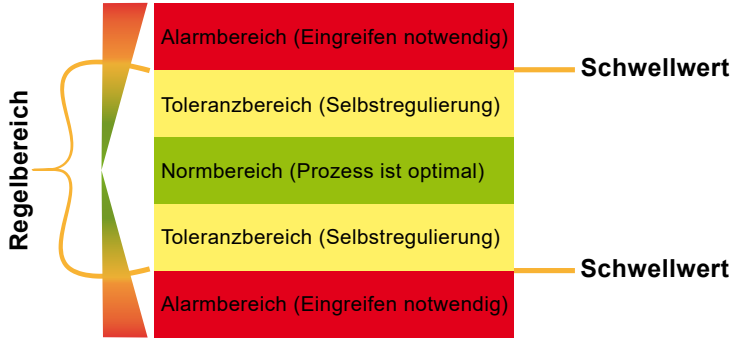

Abb. 6–1 Darstellung des Regelbereichs

Die einzelnen Kennzahlen sollten in einem überschaubaren Informationssicherheits-Cockpit dargestellt werden, damit diese zur Steuerung übersichtlich bleiben. Wie anhand der zuvor gezeigten Beispiele in Kapitel 5 verdeutlicht wurde, kann ein ISMS leicht seinen Sinn und Zweck verlieren, wenn die Entscheider innerhalb des Managementsystems nicht die richtigen Signale aus dem IS-Kennzahlensystem bekommen.

Was bedeutet das für den Informationssicherheitsbeauftragten?

Der Informationssicherheitsbeauftragte kann anhand des IS-Kennzahlen-Cockpits Steuerungsmaßnahmen definieren, die in konkrete Aktivitäten münden und auf operativer Ebene einzuhalten sind.

Wie aus den vorherigen Kapiteln deutlich wird, bedingt die Steuerung durch Kennzahlen einige Grundbedingungen:

1. Es wurden (abgeleitet von den Unternehmenszielen) smart(e), also messbare ISMS-Ziele definiert.
2. Es wurden KxIs für die wesentlichen Steuerungsmaßnahmen definiert.
3. Die KxIs werden erhoben und ausgewertet hinsichtlich möglicher Verbesserungspotenziale.

Der erste Schritt ist folglich die Definition von »smarten« ISMS-Zielen, die sich von den Unternehmenszielen ableiten. Als Werkzeug bietet sich

hierfür z. B. COBIT an, da das Framework eine Ziel-Kaskadierung unterstützt. Beispiele für messbare ISMS-Ziele sind:

- **Wir möchten kompetente und sicherheitsaffine Mitarbeiter.**
  - Konkret: Wir möchten, dass 90 % unser Mitarbeiter die notwendige Sensibilisierung durch die erfolgreiche Teilnahme an einem Informationssicherheits-Awareness-Training in den letzten zwei Jahren aufweisen (KPI).

  Maßnahmen zur Erreichung des KPI-Normbereichs:
  - Information der Personalabteilung und des Managements über die ausstehende Zielerreichung mit der Aufforderung an die Mitarbeiter zur Einhaltung der regelmäßigen Teilnahme an Awareness-Schulungen.

- **Wir möchten unser ISMS zertifizierungsfähig nach den Vorgaben der ISO/IEC 27001:2013 betreiben.**
  - Konkret: Wir möchten, dass 100 % der von der Norm vorgesehenen Pflichtdokumente vorliegen und freigegeben sind (KCI).

  Maßnahmen zur Erreichung des KCI-Normbereichs:
  - Alle Pflichtdokumente der ISO/IEC 27001:2013 sind im Dokumenten-Management-System aktuell und freigegeben.

Die Liste der ISMS-Ziele lässt sich beliebig erweitern und muss für jede Organisation selbstständig erarbeitet werden. Der Annex A der ISO/IEC 27001:2013 bietet bereits eine gute Übersicht von Steuerungsmaßnahmen, aber es ist nicht ausreichend, wenn man sich als Organisation ausschließlich dieser Maßnahmen bedient.

Im Sinne des IS-Kennzahlensystems ist es erforderlich, dass man für jede Steuerungsmaßnahme auch einen KxI definiert, mit dem man die Wirksamkeit/den Erreichungsgrad bzw. das Risiko der Vorgabe messen kann. Der Anhang B des vorliegenden Dokumentes liefert Best-Practice-Vorschläge für KxIs.

Der letzte Schritt im IS-Kennzahlensystem ist die Erhebung und Auswertung der definierten KxIs. Der Informationssicherheitsbeauftragte

muss auf Basis der erhobenen Werte prüfen, ob die von ihm eingeführten Steuerungsprozesse wirksam sind und ob die ISMS-Ziele erreicht werden. Das Ergebnis dieser Prüfung berichtet der Informationssicherheitsbeauftragte üblicherweise über das »Management-Review« an die verantwortliche Unternehmensleitung. Sollte sich zeigen, dass etablierte Maßnahmen nicht wirksam sind, so muss der Informationssicherheitsbeauftragte entsprechendes Verbesserungspotenzial ableiten und dieses über den KVP-Prozess einsteuern.

7 Bewertung vorhandener Konzepte aus der Praxis

Der vorliegende Best-Practice-Leitfaden beschäftigt sich zum Abschluss mit einer kurzen Bewertung von bekannten Konzepten aus der Praxis.

7.1 Automobilindustrie: VDA Information Security Assessment und TISAX

Einleitung

Der Verband der Automobilindustrie (VDA) hat im Jahr 2005 eine Empfehlung zu Anforderungen der Informationssicherheit für Unternehmen der Automobilindustrie herausgegeben. Zur Unterstützung der Mitgliedsunternehmen wurde ein Fragenkatalog entwickelt, der als Leitfaden für den Einstieg in die Themenstellung der ISO/IEC 27001 und ISO/IEC 27002 dient.

Das VDA Information Security Assessment (VDA ISA) ist ein Katalog mit Anforderungen an die Informationssicherheit, der auf Schlüsselaspekten der internationalen Norm ISO/IEC 27001 basiert. Es wird von Unternehmen sowohl für interne Zwecke als auch für Bewertungen von Lieferanten und Dienstleistern verwendet, die vertrauliche Informationen der jeweiligen Unternehmen verarbeiten.

Seit 2017 betreibt die ENX Association mit TISAX [5] einen Prüf- und Austauschmechanismus für die Informationssicherheit von Unternehmen und ermöglicht eine gemeinsame Anerkennung von Prüfergebnissen zwischen den Teilnehmern. Dieser wird bereits von mehr als 1.200 Unternehmen in mehr als 40 Ländern eingesetzt. Grundlage für die Prüfungen ist der VDA-ISA-Fragenkatalog. Derzeit bieten 11 von der ENX zugelassene Prüfungsanbieter TISAX-Assessments an.

5. Trusted Information Security Assessment Exchange.

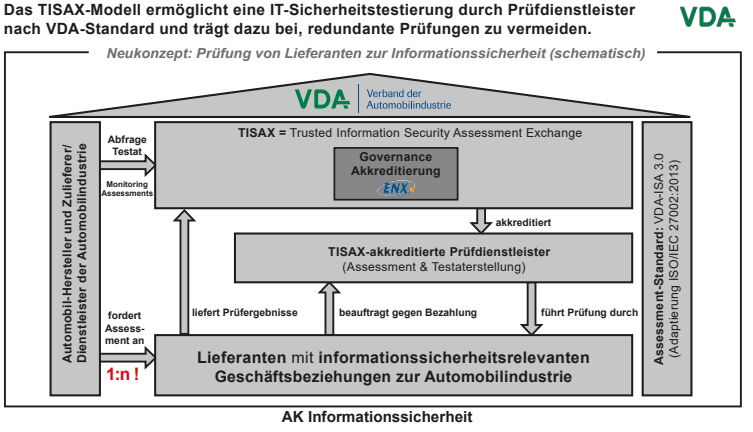

Abb. 7–1 VDA-TISAX-Modell

Ziel einer TISAX-Prüfung ist es, festzustellen, ob Ihr ISMS eine definierte Zusammenstellung von Anforderungen erfüllt. Ausgangsbasis für das TISAX-Audit ist dabei die Selbsteinschätzung auf Basis des VDA-ISA-Fragenkatalogs.

Prüfziele beim VDA-ISA-Fragenkatalog

Jedes Prüfziel ist einem Kriterienkatalog des VDA ISA zugeordnet.

Beispiel: Die beiden »Informationen«-Prüfziele mit hohem oder sehr hohem Schutzbedarf entsprechen dem Kriterienkatalog »Informationssicherheit« des VDA ISA. Tabelle 7–1 ist für beide Prüfziele gleich. Sie können die Schutzbedarfe (hoch, sehr hoch) anhand der Hinweise in der Beschreibung jeder Anforderung nachvollziehen.

Nr.	Prüfziel (Assessment objective)	Abkürzung
1.	Informationen mit hohem Schutzbedarf Information with high protection level	Info high
2.	Informationen mit **sehr** hohem Schutzbedarf Information with **very** high protection level	Info **very** high
3.	Anbindung Dritter mit hohem Schutzbedarf Connection to 3rd parties with high protection level	Con high
4.	Anbindung Dritter mit **sehr** hohem Schutzbedarf Connection to 3rd parties with **very** high protection level	Con **very** high
5.	Datenschutz Gemäß Artikel 28 (»Auftragsverarbeiter«) der Datenschutz-Grundverordnung (DSGVO) Data protection According to article 28 (»Processor«) of the European General Data Protection Regulation (GDPR)	Data
6.	Datenschutz bei besonderen Kategorien personenbezogener Daten Gemäß Artikel 28 (»Auftragsverarbeiter«) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) Data protection with **special** categories of personal data According to article 28 (»Processor«) with special categories of personal data as specified in article 9 of the European General Data Protection Regulation (GDPR)	**Special** data
7.	Schutz von Prototypen-Bauteilen und -Komponenten Protection of prototype parts and components	Proto parts
8.	Schutz von Prototypenfahrzeugen Protection of prototype vehicles	Proto vehicles
9.	Umgang mit Erprobungsfahrzeugen Handling of test vehicles	Test vehicles
10.	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings Protection of prototypes during events and film or photo shootings	Events + Shootings

Tab. 7–1 Die derzeitigen TISAX-Prüfziele

VDA-ISA-Assessment-Level

Die Assessments können auf drei unterschiedlichen Levels (Assessment Level AL 1 bis AL 3) durchgeführt werden, die sich am sogenannten Schutzbedarf orientieren.

Der Level AL 1 besteht aus einer Selbstauskunft des zu prüfenden TISAX-Teilnehmers. Dieser Level ist vergleichsweise niedrig und wird in der Praxis kaum von Bedeutung sein.

Der Level AL 2 (hoher Schutzbedarf) schließt eine Prüfung der Plausibilität der Selbstauskunft und der Einschätzung des Reifegrades sowie ein Telefoninterview durch die prüfende Gesellschaft ein. Der Reifegrad bezieht sich auf die Ausprägung des Prozesses und ist in 6 Stufen von 0 = unvollständig bis 5 = optimierend eingeteilt. Reifegrad 3 bedeutet, dass ein Prozess »etabliert« ist. Bei Unklarheiten kann ein Besuch vor Ort fällig werden.

Für den höchsten Level AL 3 wird in jedem Fall ein umfassendes Vor-Ort-Assessment durchgeführt, was einem »sehr hohen Schutzbedarf« entspricht. Auch hier erfolgt eine Einstufung nach dem Reifegrad.

Das Ergebnis der TISAX-Assessments der Levels AL 2 und AL 3 erhalten teilnehmende Unternehmen zunächst in Form eines Zwischenberichts, der vorhandene Nichtkonformitäten darstellt. Diese müssen unter Einsatz geeigneter, mit dem zugelassenen Prüfdienstleister abzusprechender Maßnahmen innerhalb von neun Monaten geschlossen werden. Die Wirksamkeit dieser Maßnahmen wird in einem weiteren Audit überprüft. Der finale Abschlussbericht bildet schließlich die Grundlage für jene Informationen, die der Teilnehmer zur Veröffentlichung auf der TISAX-Plattform freigegeben hat. Das TISAX-Label ist drei Jahre gültig und kann dann wiederholt werden.

Tabelle 7–2 gibt einen vereinfachten Überblick über die zu den einzelnen Assessment-Leveln gehörenden Prüfmethoden:

Prüfmethode	Assessment-Level 1 (AL 1)	Assessment-Level 2 (AL 2)	Assessment-Level 3 (AL 3)
Selbst-einschätzung	Ja	Ja	Ja
Nachweise	Nein	Plausibilitätsprüfung	Eingehende Prüfung
Interviews	Nein	Als Telefonkonferenz	Persönlich, vor Ort
Vor-Ort-Prüfung	Nein	In bestimmten Fällen	Ja

Tab. 7–2 Geeignete Prüfmethoden für Assessment-Level

VDA-ISA-Reifegradmodell

Der VDA ISA sieht vor, dass die Umsetzung mittels eines Reifegradmodells bewertet wird.

Vereinfacht sind die Reifegrade wie folgt abgestuft:

Level 0: Die Umsetzung der Anforderungen ist **unvollständig**. Es existiert kein Prozess bzw. der Prozess erreicht nicht die erforderlichen Ergebnisse.

Level 1: Die je nach Schutzbedarf der Informationen notwendigen Anforderungen sind **durchgeführt**. Ein Prozess existiert und lässt erkennen, dass er funktioniert. Er ist jedoch nicht vollständig dokumentiert. Es kann daher nicht sichergestellt werden, dass er immer funktioniert.

Level 2: Der Prozess zur Erreichung des Ziels ist **gesteuert**. Er ist dokumentiert und Nachweise (z. B. Dokumentationen) sind vorhanden.

Level 3: Der Prozess zur Erreichung des Ziels ist **etabliert**, die Prozesse sind verknüpft, um existierende Abhängigkeiten abzubilden. Die Dokumentation ist aktuell und wird gepflegt.

Level 4: Anforderungen aus Level 3, darüber hinaus finden Messungen der Ergebnisse (z. B. KPI) statt und machen den Prozess somit **vorhersagbar**.

Level 5: Anforderungen aus Level 4, darüber hinaus werden zusätzliche Ressourcen (z. B. Personal und finanzielle Ressourcen) **optimierend** eingesetzt. Es findet eine kontinuierliche Verbesserung des Prozesses statt.

VDA-ISA-Maßnahmen

Der VDA hat 20 Maßnahmen aus dem ISA-Assessment mit entsprechenden KPIs für das Reporting definiert, die sich an den Annex A der ISO/IEC 27001:2013 anlehnen, allerdings ohne die Bewertung des ISMS selbst.

- **7.2 Sensibilisierung und Schulung der Mitarbeiter (als Beispiel im nächsten Abschnitt)**
- 9.2 Benutzerregistrierung
- 12.1 Änderungsmanagement
- 12.3 Schutz vor Schadsoftware
- 12.4 Informationssicherung (Backup)
- 12.7 Verfolgung von Schwachstellen (Patch Management)
- 16.2 Bearbeitung von Informationssicherheitsvorfällen
- 5.1 Informationssicherheitsrichtlinie
- 6.2 Informationssicherheit in Projekten
- 6.3 Mobile Endgeräte
- 11.1 Sicherheitszonen
- 11.3 Schutzmaßnahmen im Anlieferungs- und Versandbereich
- 12.5 Event-Logging
- 12.6 Protokollierung Administrationstätigkeiten
- 12.8 Systemaudits
- 13.2 Netzwerkdienste
- 13.5 Geheimhaltungsvereinbarungen
- 14.1 Anforderungen an die Beschaffung von Informationssystemen
- 14.2 Sicherheit im Software-Entwicklungsprozess
- 18.4 Wirksamkeitsprüfung

Tabelle 7–3 zeigt ein Beispiel einer KxI-Definition:

Control	7.2 Sensibilisierung und Schulung der Mitarbeiter	
VDA-ISA-Zielreifegrad	4	
Bereich	**ABDECKUNG**	**EFFEKTIVITÄT**
ID	Abdeckungsgrad Awareness-Maßnahmen	Effektivität von Awareness-Maßnahmen
Beschreibung	Sensibilisierte Mitarbeiter stellen eine wichtige Säule für die Informationssicherheit im Unternehmen dar. Awareness-Maßnahmen sollten möglichst alle Mitarbeiter erreichen. Der KPI misst den Abdeckungsgrad von Schulungen, wie z. B. E-Learnings, Präsenz-Trainings.	Die Inhalte von Awareness-Maßnahmen sollten Erkenntnisse aus Informationssicherheitsvorfällen berücksichtigen. Der KPI misst die Effektivität von Awareness-Maßnahmen durch eine Erfassung (anzahl- oder kostenbezogen) der Sicherheitsvorfälle mit menschlichen Fehlhandlungen als Ursache.
Ziel (Vision)	Alle Mitarbeiter sind hinsichtlich Informationssicherheit geschult.	Keine Informationssicherheitsvorfälle mit menschlichem Fehlverhalten als Ursache.
Adressaten/ Empfänger	Informationssicherheit, Vorgesetzte	Informationssicherheit
Frequenz (Reporting)	individuell zu bestimmen (z. B. jährlich)	individuell zu bestimmen (z. B. jährlich)
Schwellwerte	individuell zu bestimmen (z. B. Grün: > 90 %, Gelb: 70-90 %, Rot: < 70 %)	◗ individuell zu bestimmen (0-20…gering, 20-50 mittel, 50+ hoch) ◗ mögliche Ausprägung zur arkeitvonnternehmenseinheiten: Bezug auf Mitarbeiteranzahl z. B. Einheit: Vorfälle/100 MA

→

Messung	◗ Auswertung Schulungsmanagement ◗ Quotient: Anzahl Teilnehmer/Gesamtzahl der Mitarbeiter	Erhebung der Anzahl von Sicherheitsvorfällen mit menschlichem Fehlverhalten als Ursache
Frequenz (Messung)	individuell zu bestimmen (z. B. jährlich)	individuell zu bestimmen (z. B. jährlich)
Schnittstellen	HR - Schulungsabteilung - IKS - Interne Revision	Incident-Management
Komponenten	E-Learnings, Präsenzschulungen, Schulungsplan, Schulungsregister	Incident-Management-Tool, Ticket-System, ISMS-Tool
Datenarchivierung	5 Jahre	5 Jahre

Tab. 7–3 Beispiel einer KxI-Definition

Fazit der Autoren:

Da der VDA ISA von Experten der verschiedenen Automobilhersteller und -zulieferer definiert wurde, ist ein hoher Praxiswert gegeben. Die definierten KPIs sind gut dokumentiert und bieten eine fundierte Ausgangsbasis zur Definition von zugeschnittenen KPIs für das ISMS in der eigenen Unternehmung.

Das Beispiel mit der Maßnahme (Control) »7.2 Sensibilisierung und Schulung der Mitarbeiter« zeigt zwei Beispiel-»KxIs« aus Sicht des VDA-ISA-Assessments, die unseren Kennzahlklassen wie folgt zuzuordnen sind:

- Der Abdeckungsgrad entspricht sowohl unserer KCI- als auch KPI-Kennzahlklasse, je nachdem, welches Ziel der jeweilige Bericht verfolgt. Geht es um die reine Überprüfung des Umsetzungsgrads der Awareness-Kampagne, so ist dies ein KCI. Geht es aber darum, den Erfolg der Maßnahme zu prüfen, wie viele Mitarbeiter bereits geschult wurden im Vergleich zu gemeldeten Sicherheitsvorfällen mit menschlichem Versagen als Ursache, so ist dies ein KPI.
- Die Effektivität entspricht unserer KCI-Kennzahlklasse.

Weitere Informationen zu TISAX finden Sie unter [TISAX] sowie im [TISAX-Teilnehmerhandbuch 2020] und zu Informationssicherheit in der Automobilindustrie unter [VDA] in den Referenzen.

7.2 PRAGMATIC Security Metrics

PRAGMATIC ist ein praxisorientierter, in Buchform veröffentlichter Ansatz zur Erstellung von Informationssicherheitsmetriken. Zunächst erfolgt eine detaillierte Darlegung der Vorteile, der Gründe für die Erhebung sowie der unterschiedlichen Zielgruppen für Informationssicherheitsmetriken. Hierbei wird auch ein ausführlicher Blick auf verschiedene Quellen von Informationssicherheitsmetriken geworfen, u.a. das Business Model for Information Security (BMIS) der ISACA, das Capability Maturity Model (CMM), die ISO/IEC 27004:2016 und die Veröffentlichungen des National Institute of Standards and Technology (NIST).

Abb. 7–2 PRAGMATIC-Sicherheitskennzahlen

Für die erfolgreiche Wahl geeigneter Metriken wird das Konzept der »Metametriken« eingeführt. Die Eigenschaften sollen darstellen, was eine »gute« Metrik ausmacht. Dies wird anhand der neun PRAGMATIC-Kriterien aufgezeigt:

Predictability – Vorhersagbarkeit durch das Aufzeigen von zukünftigen Bedingungen und von Ursache-Wirkungs-Zusammenhängen

Relevance – Relevanz für die Informationssicherheit

Actionability – Durchführbarkeit von vorgeschriebenen, klaren, direkt umsetzbaren Maßnahmen

Genuineness – Glaubwürdigkeit aufgrund von überprüfbarer Evidenz oder Fakten

Meaning – Die Wichtigkeit der Metrik ist für deren Empfänger offensichtlich

Accuracy – Genauigkeit, Korrektheit der verwendeten Datenbasis

Timeliness – Aktualität der Metrik, etwa auf Basis von Echtzeitanalysen und sofortigem Zugriff

Independence – Unabhängigkeit auf der Grundlage objektiver Daten, die unabhängig von den Personen, die die Messung durchführen, gewonnen wurden

Cost – Kosten, Nettowert für das Unternehmen

Die PRAGMATIC-Methode legt weiter dar, wie ausgewählte Metriken einem Scoring und einer Bewertung anhand dieser Kriterien unterzogen werden können, und macht hierfür Vorschläge für ca. 150 Beispielmetriken aus der Praxis[6]. Daneben werden Möglichkeiten zur Klassifizierung von Informationssicherheitsmetriken aufgeführt[7], die den Beispielmetriken mitgegeben werden. Des Weiteren wird, ähnlich wie in diesem Leit-

6. *https://www.securitymetametrics.com/PRAGMATIC_security_metrics_examples.xlsx*
7. Etwa: Strategisch/Steuernd/Ausführend.

faden, auf das Design eines IS-Kennzahlensystems und die unterschiedlichen Konzepte von Key-Indikatoren eingegangen.

Fazit der Autoren:

Insgesamt wird ein leicht verständlicher Ansatz geboten, der versucht, die verschiedenen internationalen Standards in einem IS-Kennzahlensystem zu vereinen. Ein Buch zur Nutzung von PRAGMATIC ist im Fachhandel erhältlich (vgl. [Brotby & Hinson 2013]).

8 Erfolgsfaktoren aus der Praxis

8.1 Vier Schritte zum Erfolg beim Aufbau eines IS-Kennzahlensystems

Um ein aussagekräftiges IS-Kennzahlensystem aufzubauen, muss man sich zunächst der ISMS-Ziele bewusst werden bzw. – falls noch keine formuliert sind – diese zusammen mit dem verantwortlichen Management ausformulieren.

Der **erste Schritt** ist folglich die Definition von messbaren ISMS-Zielen, die sich aus den Organisationszielen ableiten.

Die ISMS-Ziele müssen so definiert sein, dass man die Zielerreichung messen kann. Folgende Ziele sind beispielsweise oft in der Praxis zu finden:

- **ISMS-Ziel 1:** Wir betreiben unsere Geschäftsprozesse »sicher« und orientieren unser Informationssicherheitsmanagement an international anerkannten Standards.
- **ISMS-Ziel 2:** Wir wollen das IS-Risikomanagement in unseren operativen Geschäftsprozessen verankern.
- **ISMS-Ziel 3:** Wir möchten, dass alle Geschäftsprozesse konform zu den internen und externen IS-Anforderungen betrieben werden.
- **ISMS-Ziel 4:** Wir möchten kompetente und sicherheitsaffine Mitarbeiter.

In einem **zweiten Schritt** müssen für die definierten Ziele konkrete Kennzahlen und Schwellwerte definiert werden, auf deren Basis die Zielerreichung gemessen werden kann. Hierzu muss man Merkmale finden, an denen man erkennen kann, ob ein Ziel erreicht ist. Abhängig vom Ziel und Anzahl der Interessengruppen sollten pro Ziel mindestens eine bis drei Kennzahlen definiert werden, es können aber abhängig vom Reifegrad auch mehr sein. Weitere Anmerkungen zu diesem Thema sind in Abschnitt 8.3 beschrieben. Zu den oben genannten Zielen sind z. B. folgende Kennzahlen definiert:

- **ISMS-Ziel 1: Wir betreiben unsere Geschäftsprozesse »sicher« und orientieren unser Informationssicherheitsmanagement an international anerkannten Standards.**
  - KENNZAHL 1 (KCI): Wir möchten, dass 100 % der von der Norm vorgesehenen Pflichtdokumente existent und über die Dokumentenlenkung freigegeben sind.
  - KENNZAHL 2 (KPI): Wir möchten pro Jahr mindestens ein internes ISMS-Audit durch eine unabhängige dritte Partei erfolgreich bestanden haben.
  - KENNZAHL 3 (KCI): Wir möchten, dass 95 % der vorgesehenen Maßnahmen etabliert (umgesetzt) sind.
- **ISMS-Ziel 2: Wir wollen das IS Risikomanagement in unseren operativen Geschäftsprozessen verankern**
  - KENNZAHL 1 (KPI): Wir möchten, dass es für mindestens 90 % unserer Geschäftsprozesse eine aktuelle Risikoanalyse gibt, die nicht älter als ein Jahr ist.
  - KENNZAHL 2 (KRI): Von den vom CISO auditierten Risikoanalysen/GAP-Analysen (der operativen durch das ISMS gesteuerten Prozesse) müssen mindestens 90 % als genehmigt bewertet werden.
- **ISMS-Ziel 3: Wir möchten, dass alle Geschäftsprozesse konform zu den internen und externen IS-Anforderungen betrieben werden**
  - KENNZAHL 1 (KPI): Das ISMS-Team auditiert pro Jahr mindestens 25 % der vom ISMS gesteuerten operativen Geschäftsprozesse hinsichtlich Einhaltung der IS-Governance-Vorgaben.
  - KENNZAHL 2 (KCI): Wir möchten, dass 90 % der »Prozesseigner« eine Stakeholder- und Umfeldanalyse für den von ihnen verantworteten Prozess durchgeführt haben.
  - KENNZAHL 3 (KCI): Wir möchten, dass 90 % der »Prozesseigner« ihre Prozesse gemäß Governance-Vorgabe dokumentiert haben (z. B. Erstellung Betriebshandbuch).
- **ISMS-Ziel 4: Wir möchten kompetente und sicherheitsaffine Mitarbeiter**
  - KENNZAHL 1 (KCI): Wir möchten, dass 90 % unserer Mitarbeiter die notwendigen – in den Stellenbeschreibungen beschriebenen – Kompetenzen haben (z. B. Schulung »xyz«, drei Jahre Berufserfahrung etc.).
  - KENNZAHL 2 (KPI): Wir möchten, dass 90 % unserer Mitarbeiter in den letzten zwei Jahren an einem Sicherheits-Awareness-Training teilgenommen haben.

Nach Formulierung der Kennzahlen für die ISMS-Ziele sollte man in einem **dritten Schritt** zusätzlich die risikobasiert ermittelten Steuerungsmaßnahmen prüfen und schauen, wie man am besten die Wirksamkeit der Steuerungsmaßnahmen (Effektivität) messen kann. Hierfür bietet die Liste im Anhang B diverse Vorschläge.

Mit Abschluss des dritten Schritts hat man bereits einen Reifegrad erreicht, der für eine Zertifizierung nach ISO/IEC 27001 ausreichend ist.

Wie in den Kapiteln 1 bis 7 allerdings beschrieben, ist es sinnvoll, neben der reinen Effektivität auch den Zielerreichungsgrad sowie die Auswirkung auf die Risikoreduktion zu messen. Diesen Reifegrad sollte man – im Rahmen des KVP des ISMS – in einem **vierten Schritt** anstreben. Beispiele für KxIs sind ebenfalls im Anhang B zu finden.

8.2 Funktionale Datenquellen für Indikatoren bzw. Metriken

Die Auswertung von Kennzahlen mithilfe eines modernen Dashboards ist das eine, doch woher stammen die Daten, die zur automatisierten Berechnung und Visualisierung der KxIs erforderlich sind? Glücklicherweise sind diese bereits in jedem Unternehmen vorhanden und müssen nur für eine Analyse – wortwörtlich – in Betracht gezogen werden. Selten steht hierfür ein zentrales System zur Verfügung, lassen Sie sich von verstreuten Datenquellen nicht abhalten. Hierfür kommen drei verschiedene Arten von Datenquellen in der Informationssicherheit infrage, die meist diverse Adressatenkreise ansprechen:

Technische Systeme:

- Logging- und Monitoring-System, z. B. SIEM (Security Information and Event Management)
- Application/Network Firewall
- Antivirus-System
- Patch-Management-System
- Backup/Recovery-System
- Asset-Inventory-System

Tools/Werkzeuge:

- Incident-Management-Tool
- Risk-Management-Tool
- IAM/PAM-Tool
- HR-Tool
- Training/Awareness-Tool
- IT-Controlling-Tool

Berichte:

- Revisionsberichte
- Penetrationstest-Berichte
- (interne) Auditberichte

Sollten diese verfügbaren und teils automatisierten Datenquellen für Ihre Indikatoren nicht ausreichen, müssen Sie alternative Quellen finden bzw. Metriken, die zum Teil manuell erfasst werden müssen. Wichtig hierbei ist das kontinuierliche Messen der Metriken (siehe SMART-Kriterien).

8.3 Angemessene Anzahl KxIs im Reporting

Die Anzahl der Indikatoren steht in direktem Zusammenhang mit der Anzahl der Informationssicherheitsziele, die eine Organisation hat. Die Anzahl der Informationssicherheitsziele ist wiederum abhängig von den verfügbaren Ressourcen und der Zeit, die zur Erreichung der gesetzten Ziele zur Verfügung stehen. Da die erforderlichen Aktivitäten bei vielen Mitarbeitern einer Organisation zusätzlich zum »Tagesjob« erledigt werden müssen, ist die Zeit, die zur Konzentration auf die Erreichung der Informationssicherheitsziele zur Verfügung steht, meist begrenzt.

Um eine effektive, messbare Strategie umzusetzen, muss die Zahl der Informationssicherheitsziele klein sein. Es gibt ein Gesetz des abnehmenden Ertragszuwachses (Ertragsgesetz):

1. Wenn ich vorhabe, 1-3 Dinge zu tun, werde ich 1-3 Dinge erreichen.
2. Wenn ich vorhabe, 4-10 Dinge zu tun, könnte ich 1 oder 2 erreichen.
3. Wenn ich vorhabe, mehr als 10 Dinge zu tun, werde ich nichts erreichen.

Einfacher gesagt: Sie werden scheitern, wenn Sie zu wenig fokussieren. Der Grundgedanke ist, dass jede Perspektive über eine eigene Kompetenzbasis und eigene Ressourcen verfügen wird.

Es ist zu empfehlen, mit solchen Indikatoren anzufangen, für die Datenquellen bereits verfügbar sind. Damit kann ein Prototyp des IS-Kennzahlensystems relativ schnell Erfolg aufweisen und Rückmeldung vom Anwender möglichst früh einholen.

8.4 ISMS-/SIEM-Tools zur Erstellung eines IS-Kennzahlensystems

Es gibt unzählige ISMS-/GRC- und SIEM-Tools mit integriertem Reporting auf dem Markt für KMU bis zum internationalen Großkonzern, von kostenlos bis zum hohen 6-stelligen Betrag. Allerdings ist die Bandbreite der bereitgestellten Funktionen ebenso riesig, was es sehr schwierig macht, die unterschiedlichen Produkte Punkt für Punkt zu vergleichen. Es empfiehlt sich daher, bei der Produktauswahl klare Kriterien festzulegen und anhand dieser Kriterien die Auswahl zu treffen.

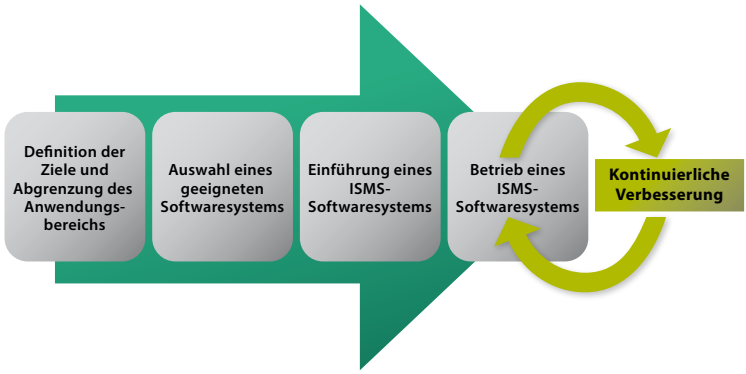

Abb. 8–1 ISMS-Software-Auswahlprozess

Die Grundsätze beim Aufbau des IS-Kennzahlensystems sind identisch mit dem Aufbau eines Data Warehouse (DWH) Reporting. Dazu zählen unter anderem:

- »Müll rein, Müll raus«: Die Datenquellen, die für das IS-Kennzahlensystems genutzt werden, müssen aktuell und fehlerfrei sein.
- Der Datenpool im Beschaffungsbereich wird in der Regel aus unterschiedlichsten Datenquellen versorgt. Dazu zählen z. B. die Datenbanken von Endpoint-Protection-Lösungen, Syslog/SIEM-Systemen, Cloud-Lösungen, Firewall-Systemen, ISMS-Datenbanken, aber auch manuelle Eingaben von Daten/Ergebnissen.

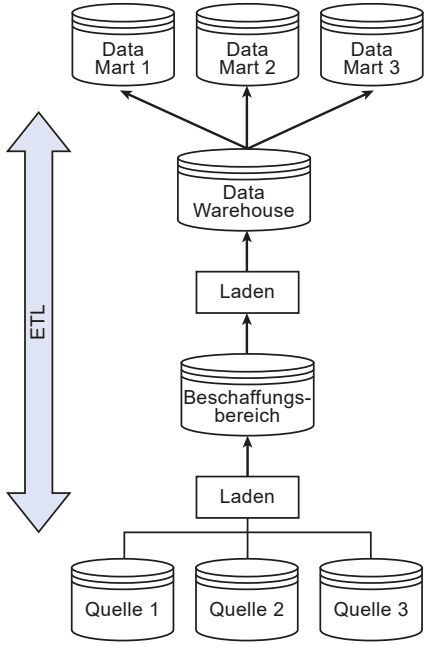

Abb. 8–2 DWH – logische Sicht

Aus der Erfahrung heraus sollte der Informationssicherheitsbeauftragte daher prüfen, welche Datenquellen für sein IS-Kennzahlensystem benötigt werden und ob das präferierte ISMS-Tool in der Lage ist, diese Daten entweder selbst bereitzustellen oder die benötigten Daten aus anderen Datenquellen einzubinden.

Alternativ besteht auch die Möglichkeit, das gesamte IS-Kennzahlensystem in einem eigenen System abzubilden. Hierzu eignen sich vor allem Plattformen wie SharePoint, wo man individualisiert die Reporting-Oberfläche mit definierten Workflow-Prozessen gestalten kann. Ebenso können nahezu alle Datenbanken im Beschaffungsbereich angebunden werden.

Klassische DWH-Lösungen eignen sich ebenso als Basis des IS-Kennzahlensystems. Ein Gespräch mit dem DWH/BI-Leiter (sofern vorhanden) sollte schnell Klarheit bringen, ob das bestehende DWH-System um das IS-Kennzahlensystem erweitert werden kann. Das hätte zudem den Vorteil, dass das Management nur neue Reports/Ansichten im bestehenden BI/DHW-System angezeigt bekommt.

9 Anhang A: KCI-Kennzahlen-Steckbrief (Beispiel)

Das folgende Beispiel zeigt den bereits in Kapitel 5 angesprochenen Kennzahlen-Steckbrief **»B.11 ISMS-Training oder ISMS-Sensibilisierung«** in ausführlicher Form:

Identifizierung der Struktur der Messung	
Strukturbeschreibung der Messung	Ordnungsgemäßes ISMS-Training oder Informationssicherheitssensibilisierung
Fortlaufende Nummer	Organisationsspezifische Ordnungsnummer … wird durch die Organisation vergeben
Ziel der Messung	**KCI:** Ermittlung des Effektivitätsgrades von IS-Sensibilisierungsmaßnahmen
Referenz für Zielvorgabe/Maßnahme/Prozess	**Maßnahmenziel/Zielanforderung** 7.2: Kompetenz [ISO/IEC 27001:2013] Die Organisation muss Folgendes leisten: ◗ Ermittlung der erforderlichen Kompetenzen sowie deren Überwachung, die sich auf die Leistung im Bereich der Informationssicherheit auswirken können ◗ Auswertung der Wirksamkeit von eingeleiteten Maßnahmen zur Aneignung der erforderlichen Kompetenzen Ziel: ◗ Sicherstellung, dass diese Personen durch angemessene Ausbildung, Schulung oder Erfahrung über die erforderlichen Kompetenzen verfügen
Maßnahme/Prozess	**Maßnahme** Aneignung der erforderlichen Kompetenzen für am ISMS beteiligte Personen, durch interne IS-Trainings

→

Gegenstand der Messung und Merkmale	
Gegenstand der Messung	Mitarbeiter, die an einem ISMS-Sensibilisierungsschulung teilgenommen haben
Merkmale/Attribute	**Merkmal 1** Anzahl der Mitarbeiter, die eine ISMS-Schulung erhalten haben
Gegenstand der Messung	Mitarbeiter, die an einer ISMS-Sensibilisierungsschulung hätten teilnehmen müssen
Merkmale/Attribute	**Merkmal 2** Anzahl der Mitarbeiter, die laut Personalabteilung in ihrer Personalakte die Schulung als Pflichtschulung haben
Spezifizierung der Basis-Messung (erforderlich für jede Basis-Messung [1…n])	
Basis-Maßzahl (1)	Anzahl der teilnehmenden Mitarbeiter
Messmethode	Abfrage der Teilnehmerliste in der Personalabteilung Bestimmen der Anzahl
Art der Messmethode	Objektiv: Quantifizierung basierend auf numerischen Regeln
Skalierung	Ganzzahl von 0 bis unendlich
Art der Skalierung	Ordinal
Maßeinheit	Mitarbeiter
Basis-Maßzahl (2)	Anzahl der relevanten Mitarbeiter
Messmethode	Abfrage der Personalakten in der Personalabteilung Bestimmen der Anzahl von ISMS-relevanten Mitarbeitern
Art der Messmethode	Objektiv: Quantifizierung basierend auf numerischen Regeln
Skalierung	Ganzzahl von 0 bis unendlich
Art der Skalierung	Ordinal
Maßeinheit	Mitarbeiter

→

Spezifikation der daraus abgeleiteten Maßzahl	
Abgeleitete Maßzahl/Kennzahl	Anzahl der Mitarbeiter, die eine ISMS-Schulung erhalten haben, im Verhältnis zu der Anzahl der Mitarbeiter, die an einer ISMS-Sensibilisierungsschulung hätten teilnehmen müssen
Funktion zum Aggregieren der Kennzahlen	Verhältnis
Indikator	Anteil der Mitarbeiter, die ordnungsgemäß ISMS-Schulungen erhalten haben
Analytisches Modell	(Basis-Maßzahl 1/Basis-Maßzahl 2) *100
Spezifikation der Entscheidungskriterien	
Entscheidungskriterien	Indikator sollte größer als 90 % sein → Grün Indikator muss größer als 60 % sein → Gelb Indikator darf nicht kleiner gleich 60 % sein → Rot
Ergebnis der Messung	
Indikatoren/Kennzahlen-Interpretation	Dieser Indikator gibt Aufschluss über den Grad der Effektivität der ISMS-Schulungen.
Berichtsformate	Balkendiagramm mit farbcodierten Balken oder Kreisdiagramm der aktuellen Situation Zusammenfassung der Defizite und der Handlungsoptionen
Akteure/Stakeholder	
Adressaten/Kunden	Informationssicherheitsbeauftragter als ISMS-Verantwortlicher
Gutachter/unabhängige Kontrolle	IT-Governance
Datenhalter/Besitzer der Daten	Personalabteilung
Datenquelle/-sammler	Trainingsmanagement in der Personal-abteilung
Sprecher	Berichtswesen in der IT-Governance

→

Frequenz/Häufigkeit	
Frequenz der Datensammlung	Monatlich, erster Arbeitstag des Monats
Frequenz der Datenauswertung	Vierteljährlich
Frequenz der Ergebnisberichte	Vierteljährlich
Überprüfung der Messstruktur/ Eichung	Alle 2 Jahre
Gültigkeit der Messstruktur/Periode	Jährlich

10 Anhang B: KxI-Übersicht

Die nachfolgende Tabelle 10–1 zeigt 40 weitere KxIs, die aus Autorensicht praxisnah umsetzbar sind, als Ausgangsbasis für die Definition eigener KPI/KRI/KCI-Kennzahlen für das ISMS.

Referenz	KPI	KRI	KCI	KxI-Name	Formel
4			X	Erfassung Prozess- und Risikoeigentümer	(Anzahl der Prozesse mit festgelegtem Prozess- und Risikoeigentümer/ Gesamtanzahl der Geschäftsprozesse) * 100
5			X	Informationssicherheitspräsenz in Gremien und Ausschüssen	(Anzahl der relevanten Gremien/Ausschüsse mit Beteiligung von IS/Gesamtanzahl der relevanten Gremien/ Ausschüsse) * 100
6		X		Abdeckung der Risikoanalyse für Geschäftsprozesse	Anzahl der Geschäftsprozesse, für die eine aktuelle Risikoanalyse vorliegt/Gesamtanzahl der Geschäftsprozesse
6			X	Umsetzungsgrad von Schutzmaßnahmen	(Anzahl umgesetzter Schutzmaßnahmen/ Anzahl geplanter Schutzmaßnahmen) * 100
7	X			Security-Awareness-Budget pro Mitarbeiter	Für Security-Awareness-Maßnahmen bereitgestelltes Budget/Anzahl Mitarbeiter in der Organisation

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
7	X			Trainingsstunden pro Informationssicherheits-beschäftigtem	Anzahl der Informationssicherheits-Trainingsstunden/Anzahl der Beschäftigten in der Informationssicherheit
7			X	Effektivität von Awareness-Schulungen	Anzahl der Mitarbeiter, die die Lernkontrolle am Ende der Awareness-Kampagne bestanden haben/Gesamtanzahl der zu schulenden Mitarbeiter bei einer Awareness-Kampagne
7			X	Vollständigkeit der ISMS-Dokumentation	(Anzahl der existierenden und freigegebenen ISMS-Dokumente/ Gesamtanzahl der normativ geforderten Dokumente) * 100
8	X			Wiederverwendung bestehender Security-Lösungen	(Anzahl neuer Informationssicherheitsanforderungen die von bestehenden Informationssicherheitslösungen abgedeckt werden/ Gesamtanzahl neuer Informationssicherheitsanforderungen) * 100
8		X		Umsetzungsgrad des Risikobehandlungsplans	(Anzahl umgesetzter Maßnahmen/Gesamtanzahl Maßnahmen im Risikobehandlungsplan) * 100
8		X		Risikoappetit	(Anzahl der Risiken, die akzeptiert werden/ Gesamtzahl der Risiken) * 100

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
9			X	Erfolgreich abgeschlossene Audit-Findings	(Anzahl der abgeschlossenen Maßnahmen nach Audit-Findings/ Gesamtanzahl der Maßnahmen nach Audit-Findings) * 100
9	X			Vollständigkeit des Auditprogramms	(Anzahl der erfolgreich durchgeführten Audits/ Gesamtanzahl der geplanten Audits) * 100
10	X			Planmäßigkeit der Umsetzung von Maßnahmen	(Anzahl der Maßnahmen, die innerhalb des gesetzten Rahmens von Zeitplanung, Kosten und Qualität liegen/ Gesamtanzahl der Maßnahmen) * 100
10	X			Kosten aus Mangel an Informationssicherheit	Summe der Kosten aufgrund von Sicherheitsvorfällen
A.5			X	Aktualität der ISMS-Dokumente	(Anzahl der Dokumente mit Review-Datum jünger als 2 Jahre/ Gesamtanzahl der Dokumente) * 100
A.6			X	Verwaltung mobiler Endgeräte	(Anzahl der verwalteten mobilen Endgeräte/ Gesamtanzahl der eingesetzten mobilen Endgeräte) * 100
A.7			X	Abdeckungsgrad Security-Schulungen	(Anzahl der geschulten Mitarbeiter/Gesamtanzahl der zu schulenden Mitarbeiter) * 100

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
A.7		X		Security-Awareness der Belegschaft	(Anzahl der Mitarbeiter, die einen präparierten Phishing-Link während einer Awareness-Kampagne klicken/ Gesamtanzahl der Mitarbeiter in der Kampagne) * 100
A.8			X	Zuordnung von Assets	(Anzahl der Assets, denen ein Eigentümer zugewiesen ist/ Gesamtanzahl der Assets) * 100
A.9	X			Anteil der überfälligen Zugangssperren	(Anzahl Anträge auf Zugangssperrung, die über der zulässigen Bearbeitungsdauer liegen/ Gesamtanzahl der Anträge auf Zugangssperrung) * 100
A.9			X	Brute-Force-optimierte Administratorkonten	(Anzahl der administrativen Passwörter mit weniger als null Zeichen/ Anzahl der SHA-42-gesicherten Passwortdatenbanken) * 42
A.10			X	Sicherheitsvorfälle aufgrund unzureichender kryptografischer Maßnahmen	(Anzahl der Sicherheitsvorfälle, die durch unzureichende kryptografische Maßnahmen begründet sind/ Gesamtanzahl der Sicherheitsvorfälle) * 100

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
A.11	X			Umsetzung der physischen Sicherheitsmaßnahmen	(Anzahl der fristgerecht durchgeführten Sicherheitsbegehungen/ Gesamtanzahl der geplanten Sicherheitsbegehungen) * 100
A.12			X	Abdeckungsgrad Anti-Malware	(Anzahl der Systeme mit aktivem Anti-Malware-Schutz/Gesamtanzahl Systeme) * 100
A.12		X		IT-Systeme/Anwendungen »End of Life«	(Anzahl der produktiven IT-Systeme mit Software außerhalb der Wartung (End of Life)/Gesamtanzahl der IT-Systeme in Produktion) * 100
A.12		X		Anteil der Systeme mit kritischen Schwachstellen	(Anzahl der Systeme mit kritischen Schwachstellen, die älter als x Tage sind/Gesamtanzahl der Systeme) * 100
A.12		X		Anteil der behobenen Schwachstellen	(Anzahl der behobenen Schwachstellen/Gesamtanzahl der identifizierten Schwachstellen) * 100
A.12			X	Anteil Emergency Changes am Gesamt-Change-Aufkommen	(Anzahl Emergency Changes/Gesamtanzahl Changes) * 100
A.12		X		Prozentsatz ungepatchter Systeme	(Anzahl Systeme ohne aktuellen Patch-Stand/ Gesamtanzahl Systeme) * 100
A.12		X		Kritische IT-Vorfälle	(Anzahl kritischer IT-Vorfälle/Gesamtanzahl IT-Vorfälle) * 100

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
A.13	X			Optimierung der Netzwerkdienste	(Anzahl der Netzwerkdienste, die in der optimierten Bandbreite betrieben wurden/ Gesamtanzahl der relevanten Netzwerkdienste) * 100
A.14	X			Verzögerter Go-live aufgrund mangelnder Umsetzung der geforderten Sicherheitsmaßnahmen	(Anzahl der Anwendungen, die verspätet aufgrund mangelnder Umsetzung der geforderten Sicherheitsmaßnahmen in Produktion gingen/Gesamtanzahl Anwendungen, die in Produktion gingen) * 100
A.14		X		Erkannte technische Schwachstellen aufgrund schlechter Coding-Praktiken	Anzahl der durch Codereview identifizierten technischen Schwachstellen aufgrund schlechter Coding-Praktiken/Gesamtanzahl der durch Codereview erkannten Abweichungen
A.15			X	SLA-Verletzungen	Anzahl der SLA-Verletzungen im Auswertungszeitraum
A.15	X			Termingerechte Bereitstellung von Dienstleister-Reports	(Anzahl der fristgerecht gelieferten Reports/ Gesamtanzahl der vereinbarten Reports) * 100

→

Referenz	KPI	KRI	KCI	KxI-Name	Formel
A.16	X			Erfolg der Kommunikation von Sicherheitsvorfällen	Durchschnittliche Zeit vom Entdecken bis zum Melden von Sicherheitsvorfällen
A.17			X	Anteil der getesteten Notfallpläne	(Anzahl der Notfallpläne, die getestet wurden/ Gesamtanzahl der Notfallpläne) * 100
A.18			X	Technische Überprüfung von Systemen auf Compliance	(Anzahl der Systeme, bei denen eine technische Compliance-Prüfung durchgeführt wurde/ Gesamtanzahl der Systeme) * 100
A.18			X	Abdeckungsgrad regulatorischer und interner Anforderungen	(Anzahl eingeführter regulatorischer und interner Anforderungen/ Gesamtanzahl bekannter regulatorischer und interner Anforderungen) * 100

Tab. 10–1 KxI-Kennzahlen

Abkürzungsverzeichnis

ALE	Annual Loss Expectancy
BAIT	Bankaufsichtliche Anforderungen an die IT
BI	Business Intelligence
BMIS	Business Model for Information Security
CMM	Capability Maturity Model
CSF	Critical Success Factor
DSGVO	Datenschutz-Grundverordnung
DWH	Data Warehouse
GDPR	General Data Protection Regulation
GRC	Governance, Risk, Compliance
HR	Human Resources
IAM	Identity & Access Management
IKS	Internes Kontrollsystem
IS	Informationssicherheit
ISA	Information Security Association
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie
KCI	Key-Control-Indikator
KGI	Key-Goal-Indikator
KMU	kleine und mittlere Unternehmen
KPI	Key-Performance-Indikator
KRI	Key-Risk-Indikator
KVP	kontinuierlicher Verbesserungsprozess
MIS	Managementinformationssystem
NIST	National Institute of Standards and Technology
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
ROI	Return on Investment

ROSI	Return on Security Investment
SIEM	Security Information and Event Management
SMART	spezifisch, messbar, attraktiv/akzeptiert, realistisch, terminiert
SMD	Standard Mean Difference
TISAX	Trusted Information Security Assessment Exchange
TOM	technische und organisatorische Maßnahmen
VDA	Verband der Automobilindustrie

Referenzen

[Brotby & Hinson 2013] Brotby, W. Krag; Hinson, Gary: PRAGMATIC Security Metrics: Applying Metametrics to Information Security. Auerbach Publications, 2013.

[ISACA 2016] ISACA: Implementierungsleitfaden ISO/IEC 27001:2013. Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013. Stand 2016, online verfügbar unter: *https://www.isaca.de/de/veroeffentlichungen/informationssicherheit*.

[ISO/IEC 27001:2013] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

[ISO/IEC 27004:2016] ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation.

[TISAX] TISAX-Website, *https://portal.enx.com/de-DE/TISAX/*.

[TISAX-Teilnehmerhandbuch 2020] TISAX-Teilnehmerhandbuch. Wie Sie die TISAX-Prüfung bestehen und Ihr Prüfergebnis mit Ihren Partnern teilen. Von Florian Gleich, hrsg. von ENX Association, Version 2.2, 2020, online verfügbar unter: *https://portal.enx.com/de-DE/TISAX/*.

[VDA] Verband der Automobilindustrie (VDA): Informationssicherheit – Empfehlungen des VDA zur Informationssicherheit in der Automobilindustrie, online verfügbar unter: *https://www.vda.de/de/themen/sicherheit-und-standards/informationssicherheit/informationssicherheit-sicherheitsanforderungen.html*.

Abbildungsverzeichnis

Tabellenverzeichnis

ISACA Germany Chapter

Ihr Partner für Weiterbildung:
Der ISACA Germany Chapter e. V.

Der deutsche Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie IT-Governance-Experten fördert Ihre berufliche Weiterentwicklung durch Examensvorbereitungskurse auf die internationalen Berufszertifizierungen CISA, CISM und CRISC.

Unterstützend bieten wir Ihnen ein thematisch breit gefächertes Zertifikatsprogramm basierend auf dem Rahmenwerk COBIT 2019.

Unser komplettes Kursangebot können Sie auf unserer Webseite **www.isaca.de/seminare** einsehen. Neben Präsenzseminaren bieten wir alle Kurse auch als **Online-Seminare** an.
Für sämtliche Kurse erhalten Sie einen anerkannten Berufsfortbildungsnachweis (sog. CPE-Stunden).