

## Gute Steuerung als Basis für Erfolg

*Der Erfolg kommt nur über die Brücke der Planung zu Dir.  
(Adolf Loos, österr. Architekt)*

---

### Zusammenfassung

In diesem Kapitel soll ein Verständnis für die Anforderungen einer effektiven *Information Security Governance* (kurz: *IS-Governance*), sowie Kenntnis der Elemente und Vorgehensweisen bei der Entwicklung und Implementierung einer Information Security Strategie (kurz: *IS-Strategie*) vermittelt werden. Damit wird in diesem Kapitel auch die Grundlage für eine angemessene Betrachtung von Risiken gelegt und die Voraussetzungen dafür geschaffen, dass das IS-Management die notwendige Rückendeckung bei der Entwicklung und Implementierung einer organisationsweiten Informationssicherheit von Seiten des Managements bekommt.

---

## 2.1 Grundlagen der Information Security Governance

Unter *Information Security Governance* (siehe beispielsweise [1] für eine weitergehende Beschreibung) versteht man eine Sammlung von Verantwortlichkeiten (engl.: *responsibilities*) und Vorgehensweisen (engl.: *practices*) des Vorstands bzw. der Aufsichtsgremien und des Managements (engl.: *board*) bzw. der Geschäftsführung (engl.: *executive management*) einer Organisation, die die Zielsetzung haben, die Organisation in der Art und Weise strategisch auszurichten, dass die (betrieblichen) Ziele der Organisation erreicht werden und dabei gleichzeitig die Risiken gemanagt und alle Ressourcen verantwortungsbewusst eingesetzt werden.

**Aufbau der Informationssicherheit** In diesem Kapitel werden wir – wie bereits der Beschreibung der Ziele zu entnehmen – die Grundlagen kennenlernen, auf deren Basis die Informationssicherheit<sup>1</sup> organisationsweit effektiv aufgebaut werden kann. Der *Manager der Informationssicherheit* (kurz: *IS-Manager*) treibt diesen Prozess voran und ist dafür verantwortlich, dass die hier zunächst zusammenfassend dargestellten und in den folgenden Abschnitten weiter ausgeführten Teilschritte umgesetzt werden.

Nach der Strukturierung der ISACA (vgl. dazu auch [2]) handelt es sich bei diesen Teilschritten um:

1. Die Erstellung einer Strategie im Bereich der Informationssicherheit, die an den Geschäftszielen und den Geschäftszwecken des Unternehmens ausgerichtet ist,
2. den Aufbau und die Aufrechterhaltung eines IS-Rahmenwerks, das alle Aktivitäten so steuert, dass sie die IS-Strategie unterstützen,
3. die Ausrichtung der IS-Strategie an der Unternehmensstrategie unter Berücksichtigung der IS-Governance auf Basis der Corporate Governance,
4. den Aufbau und Aufrechterhaltung von IS-Leitlinien,
5. die Entwicklung von geschäftlich relevanten Fällen, die die IS-Investitionen stützen und rechtfertigen, wie beispielsweise für eine Notfallvorsorge,
6. die Identifizierung aktueller und zukünftig möglicher rechtlicher und regulatorischer Anforderungen bzw. Randbedingungen bei der IS-Einführung,
7. die Identifizierung möglicher treibender Kräfte für die Informationssicherheit im Rahmen einer Stakeholder-Analyse,
8. die Definition und Zuordnung von Kompetenzen und Verantwortlichkeiten (engl.: *roles and responsibilities*) und
9. den Aufbau von internen und externen Kommunikationskanälen.

Die weiteren Abschnitte dieses Kapitels gehen nun auf die konkreten Fragen bei der Umsetzung dieser einzelnen Teilschritte ein. Dabei werden wir uns zunächst mit der Frage beschäftigen, warum eine IS-Governance notwendig ist, welche Aufgaben der IS-Manager übernehmen muss und welche spezifischen Aufgaben im Bereich der IS-Governance eine Rolle spielen. Zur besseren Einordnung in den Gesamtkontext werden wir auch die wesentlichen Sicherheitskonzepte nochmals kurz stichpunktartig vorstellen.

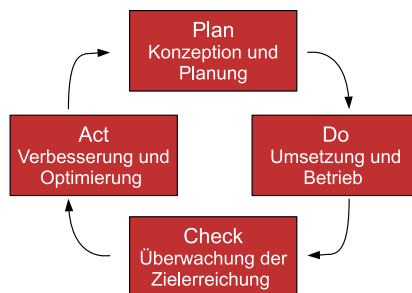
### 2.1.1 Die Idee des Managementprozesses

Im Rahmen eines planvollen Vorgehens bei der Bearbeitung von ganzen Projekten und/oder Teilaufgaben innerhalb dieser wird häufig der Ansatz eines *Managementprozesses* genutzt. Grundlegend besteht jeder Managementprozess aus vier Phasen, die auch in Abb. 2.1 dargestellt sind.

---

<sup>1</sup> Der Begriff „Informationssicherheit“ wird im weiteren Verlauf des Textes – insbesondere aufgrund der besseren Lesbarkeit – häufig durch die Kurzform „IS“ ersetzt.

**Abb. 2.1** Darstellung und Beschreibung eines PDCA-Zyklus mit den vier Phasen *Plan*, *Do*, *Check* und *Act* nach Deming [3]



- Phase 1: Jeder Zyklus eines Managementprozesses beginnt mit der *Planung*, in der Abbildung als *Plan* bezeichnet. In dieser Phase werden die Anforderungen, die der Prozess erfüllen soll, erhoben und auf Basis dieser die Leistungsmerkmale des Prozesses festgelegt. Gleichzeitig wird auch definiert, wie eine nachfolgende Bewertung des Erfolgs bei der Umsetzung des Prozesses erfolgen soll.
- Phase 2: In der Phase der *Umsetzung*, in der Abb. 2.1 als *Do* bezeichnet, erfolgt die konkrete Umsetzung der in Phase 1 erhobenen Anforderungen.
- Phase 3: Die nächste Phase der *Überprüfung*, in der Abb. 2.1 als *Check* bezeichnet, besteht aus der Kontrolle der Umsetzung aus Phase 2.
- Phase 4: In der abschließenden Phase der *Anpassung*, in der Abb. 2.1 als *Act* bezeichnet, werden die Ergebnisse aus Phase 3 sowie Änderungen, die sich aus geänderten Rahmenbedingungen ergeben haben, umgesetzt.

Wichtig ist aber nun, dass mit Schritt 4 der Prozess nicht zu Ende ist. Vielmehr entsteht ein Kreislauf: Der Gesamtzyklus wird, wenn immer es notwendig ist, wiederholt. Dadurch erreicht man eine kontinuierliche Anpassung des Prozesses an geänderte Bedingungen und somit einen kontinuierlichen Verbesserungsprozess.

**PDCA-Zyklus** Dieser Managementprozess wird alternativ oft auch als PDCA-Zyklus<sup>2</sup> beschrieben, wenngleich die Bezeichnung der einzelnen Phasen hier etwas anders definiert ist. Von William Edwards Deming [3] auf Grundlage der Arbeiten von Walter Andrew Shewhart [4] eingeführt, beschreibt der PDCA-Kreislauf mit seinen vier Phasen *Plan*, *Do*, *Check* und *Act* einen ähnlichen Ansatz.

Ursprünglich ging es Deming darum, betriebswirtschaftlich sinnvolle Abläufe bei der Einführung von Software im Unternehmen zu schaffen (vgl. dazu auch [5]). Es liegt auf der Hand, dass vor Entwicklung der Software eine Erhebung stattfinden sollte, was die Software überhaupt leisten soll (*Plan*). Im anschließenden *Do* ist dann – entgegen der häufig getroffenen Annahme – nicht das Roll-out gemeint, vielmehr geht es darum, die

<sup>2</sup> Auch in den einschlägigen ISO/IEC-Standards zur Informationssicherheit ist der PDCA-Zyklus – entgegen der häufigen Annahme – im Rahmen der Kapitelstruktur immer noch vorhanden, lediglich die Grafik zum PDCA-Zyklus wurde entfernt.

Anforderungen und die Leistungsfähigkeit der Software abzugleichen und potenzielle Lücken zu identifizieren. Man kann daher beim *Do* auch von einem Test in kleiner Umgebung sprechen, dieser Tatsache wird heute im Bereich der IT durch Testumgebungen Rechnung getragen. Der Teilschritt des *Check* überprüft nun, ob die im *Plan* gesetzten Anforderungen durch die im *Do* ausgerollte Software erfüllt werden können. Erst im folgenden Schritt des *Act* hat Deming vorgesehen, dass die Software nunmehr ausgerollt wird, nachdem die während des *Check* aufgedeckten Defizite beseitigt wurden. Der Kreislauf schließt sich, und der Prozess ist – ebenso wie im klassischen Managementprozess – kontinuierlich. Dieser Aspekt ist gerade im Bereich der IT besonders relevant, da hier bedingt durch neue IT-Prozesse oder durch Software-Releases häufig geänderte Bedingungen vorliegen.

**Informationssicherheit ist ein Prozess** Nachdem nun klar geworden ist, warum das Management der IT und insbesondere auch der IS keine einmalige Angelegenheit ist, sondern einen kontinuierlichen Prozess darstellt, bleibt noch offen, wie oft die Phasen der Vorbereitung der Umsetzung, der Umsetzung und der Kontrolle der Umsetzung durchlaufen werden sollen. Dies ist eine oft und zudem kontrovers diskutierte Frage, denn letztendlich benötigt auch der Managementprozess Ressourcen und darf daher nicht überstrapaziert werden.

- **Tipp** Als goldene Regel hat sich in der Praxis folgendes Vorgehen bewährt: Immer wenn es zu Änderungen in den Geschäftsprozessen kommt, mindestens aber einmal pro Jahr, werden alle Managementprozesse auf ihre Wirksamkeit hin überprüft.

**Priorisierung notwendig** Bei der Vielzahl der in einer Organisation anzutreffenden Teilprozesse muss bei der Umsetzung dieser goldenen Regel aber ebenfalls planvoll vorgegangen werden: Es ist eine *priorisierte Liste* notwendig, da ansonsten nicht sichergestellt werden kann, dass bei der Vielzahl der Prozesse auch wirklich alle wesentlichen angemessen berücksichtigt werden.

Die Priorisierung innerhalb dieser Liste kann wiederum auf unterschiedlichsten Parametern beruhen, beispielsweise der Relevanz des zu betrachtenden Prozesses für das Unternehmen. Hier sind diejenigen Aktivitäten von größerer Bedeutung, die einen hohen Anteil an der Wertschöpfung bzw. für den Geschäftszweck haben.

Bei der Umsetzung einer IS-Governance leistet der IS-Manager Hilfestellung. Damit dies sinnvoll funktionieren kann, sollte er einige Voraussetzungen erfüllen: Zunächst ist die Kenntnis der Anforderungen des Geschäftsbetriebs eine unabdingbare Voraussetzung für den Aufbau einer IS-Governance und den sich daraus ergebenden weiteren Aspekten im Bereich IS-Management.

- **Achtung** Wenngleich oft falsch verstanden, verfolgt die IT einer Organisation keinen Selbstzweck – sie dient vielmehr zur Unterstützung des Geschäftsbetriebs und erfüllt damit eine Dienstleistungsfunktion. Selbiges gilt nun auch für

die IS, die sowohl der IT als auch den Anforderungen aus dem Geschäftsbetrieb folgt. Dieser Grundsatz muss bei allen weiteren Planungen entsprechend berücksichtigt werden.

### 2.1.2 Die Rolle des IS-Managers

Eine der wesentlichen Aufgaben des IS-Managers ist es, dafür Sorge zu tragen, dass die Maßnahmen im Rahmen des Aufbaus des ISMS umgesetzt werden, und zudem fortlaufend zu kontrollieren, dass die *Sicherheitsleitlinien* (engl.: *information security policies*), *Sicherheitsstandards* (engl.: *information security standards*) und *Sicherheitsarbeitsanweisungen* (engl.: *information security procedures*) an der Geschäftsstrategie ausgerichtet sind und damit auch die Geschäftsziele des Unternehmens unterstützen.

**Verständnis für den Geschäftsbetrieb** Dazu muss der IS-Manager natürlicherweise die Anforderungen des Geschäftsbetriebs verstehen und – das ist jetzt der wesentliche Schritt – diese in Bezug auf das Thema Informationssicherheit so umsetzen, dass die notwendigen Sicherheitsmaßnahmen etabliert werden. Neben dem „Verständnis“ der Governance muss der IS-Manager zudem dazu in der Lage sein, die entsprechenden Anforderungen an die Beteiligten kommunizieren zu können.

- **Achtung** Für die Tätigkeit des IS-Managers ist der Aspekt der Kommunikation mit allen Beteiligten vor allem deswegen relevant, weil nicht der IS-Manager alle notwendigen Schritte selbst umsetzen wird. Vielmehr ist er der Vermittler (zwischen den Anforderungen des Geschäftsbetriebs und den eigentlichen Akteuren) und Kontrolleur (der Einhaltung der Anforderungen, die sich aus der IS-Governance ergeben).

### 2.1.3 IS-Governance im Überblick

Im Rahmen der IS-Governance werden alle (am Prozess) Beteiligten darüber informiert, was von ihnen erwartet wird und welche Regeln dabei einzuhalten sind. Damit wird gleichzeitig die Basis für kontinuierliche und wiederholbare Prozesse in der Organisation gelegt. Da die Anforderungen dokumentiert sind, wird zugleich auch ein „moving target“ vermieden und es stehen entsprechende Kriterien für ein Audit zur Verfügung. Darüber hinaus übernimmt die Managementebene auch die Verantwortung und demonstriert gegenüber Mitarbeitern, Geschäftspartnern, Kunden und weiteren Interessengruppen die *angemessene Sorgfalt* (engl.: *due care*).

**Zahlreiche Governance-Aktivitäten** Entsprechende Governance-Aktivitäten, insbesondere die Festlegung formalisierter Regeln, sind in allen (Geschäfts-)Prozessen einer Organisation unabdingbar, beispielsweise in den Ein- und Verkaufsprozessen oder den Prozessen zur Einstellung bzw. Versetzung von Mitarbeitern. Dies gilt auch – sogar insbesondere – im Bereich der IS, wo die Komplexität der Regeln höher ist und daher ein besonderes

Augenmerk darauf zu legen ist, diese den Mitarbeitern „nahezubringen“ (Stichwort: Training und Awareness).

- **Tipp** Beachtet werden muss dabei aber, dass Governance auf Prinzipien bzw. Grundsätzen basiert, die „technologieneutral“ und vielmehr in „vernünftigen“ Zielen und Idealen verankert sind. So ist beispielsweise die Anforderung, dass „Informationswerte vor unbefugtem Zugriff zu schützen sind“, technologieneutral formuliert und geht vielmehr davon aus, dass zum jeweiligen Zeitpunkt eine dazu angemessene Technologie (früher beispielsweise rein passwortbasierte Systeme, heute eher Systeme auf Basis einer Zwei-Faktor-Authentifizierung) eingesetzt wird.

**Finanzierung der Governance-Aktivitäten** Wer innerhalb der Organisation die Aktivitäten im Bereich der IS-Governance finanziert, an wen also der Verantwortliche für den Bereich IS berichtet, hängt von der Eingliederung der IS in der Organisation ab. Generell gilt, dass das Reporting so hoch wie möglich im Management angesiedelt sein sollte. Allerdings wird dies je nach Organisationsstruktur unterschiedlich gehandhabt, teilweise berichten die IS-Verantwortlichen (engl.: *Chief Information Security Officer*, kurz: *CISO*) dem Security-Komitee oder der Rechtsabteilung, häufig aber auch direkt an die Geschäftsführung bzw. Leitungsspitze.

**Wesentliche Ziele der IS-Governance** Die ISACA führt in [2] insgesamt sechs Aspekte an, die zu den wesentlichen Zielen der IS-Governance gezählt werden und im Folgenden kurz zusammenfassend dargestellt werden. Diese sechs Aspekte sind

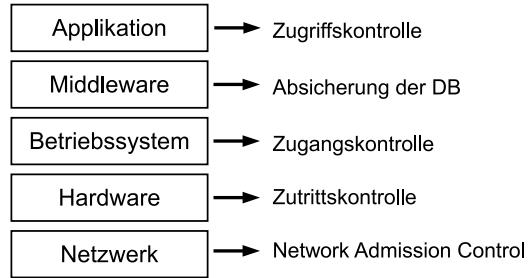
1. die *strategische Ausrichtung* (engl.: *strategic alignment*) an der (Geschäfts-) Strategie der Organisation (engl.: *business strategy*), um auch im Rahmen der IS die (Geschäfts-)Ziele der Organisation zu unterstützen,
2. die Etablierung eines *Risikomanagements* (engl.: *risk management*), das dazu dient, die Risiken so weit zu reduzieren, dass ihre Auswirkungen für die Organisation „tragbar“ sind,
3. die *Schaffung von Mehrwerten* (engl.: *value delivery*) durch Investitionen in IS, die die (strategischen) Ziele der Organisation optimal unterstützen,
4. der Aufbau eines *Ressourcenmanagements* (engl.: *ressource management*), das dazu dient, Wissen und Infrastruktur im Bereich der IS effektiv und effizient zu nutzen,
5. die *Messung der Leistung* (engl.: *performance management*), um die Zielerreichung bzw. den Fortschritt der Umsetzung der IS durch regelmäßige bzw. kontinuierliche Überwachung und Dokumentation sicherzustellen und so ggf. rechtzeitig gegen steuern zu können sowie
6. die *Einbindung von „Sicherungsfunktionen“* (engl.: *assurance integration*), um sicherzustellen, dass die Prozesse wie vorgesehen funktionieren.

## 2.2 Wichtige Sicherheitskonzepte

Da die Umsetzung des IS-Prozesses ohne entsprechende Maßnahmen nicht möglich ist, diese aber auf grundlegenden Sicherheitskonzepten beruhen, ist ein Verständnis dieser Konzepte für eine effektive Arbeit des IS-Managers eine unerlässliche Voraussetzung. Daher wollen wir im Folgenden die wichtigsten Konzepte kurz zusammenfassend darstellen:

- *Vertraulichkeit* (engl.: *confidentiality*) ist die Tatsache, dass sichergestellt werden kann, dass nur Berechtigte Zugriff auf Informationen haben. Zur Sicherstellung der Vertraulichkeit werden häufig kryptografische Mechanismen (beispielsweise in Form einer Verschlüsselung) eingesetzt.
- *Integrität* (engl.: *integrity*) ist die Verhinderung von unbemerkten Veränderungen – während sämtlicher Phasen des Lebenszyklus der Daten – durch Einsatz von Integritätssicherungsmaßnahmen. Wichtig ist, dass etwaige Veränderungen selber nicht verhindert, wohl aber Methoden zur Verfügung gestellt werden können, die es erlauben, diese Veränderungen zu bemerken. Häufig werden zur Sicherstellung der Integrität kryptografische Maßnahmen, beispielsweise durch Einsatz einer digitalen Signatur, genutzt.
- *Verfügbarkeit* (engl.: *availability*): Im Rahmen der Verfügbarkeit muss sichergestellt werden, dass *Befugte in angemessener Zeit* auf die Daten zugreifen können. Die Frage, wie schnell auf die Daten zugegriffen werden können muss, hängt dabei von der *Kritikalität* (engl.: *criticality*) des Geschäftsprozesses ab, der diese Daten benötigt.
- *Nichtabstreitbarkeit* (engl.: *non-repudiation*) beinhaltet zwei Aussagen: Der empfangende Kommunikationspartner kann sicher sein, dass die Nachricht auch tatsächlich vom Absender stammt, und dieser kann nicht bestreiten, die Nachricht verschickt zu haben. Zur Umsetzung der Nichtabstreitbarkeit werden häufig kryptografische Mechanismen, insbesondere digitale Signaturen, eingesetzt.
- *Authentifizierung* (engl.: *authentication*) ist die Überprüfung der Identität. Dies kann anhand von *Wissen* (etwa einem Passwort), *Besitz* (etwa einer Chipkarte) oder *Sein* (etwa einem Fingerabdruck) geschehen. Je nach Anzahl der verwendeten Merkmale spricht man von einer Einfaktor- oder Zwei-/Mehrfaktorauthentifizierung. Der Unterschied zur Authentisierung besteht darin, dass die agierende Partei eine andere ist. Während sich der Nutzer an einem System *authentisiert*, *authentifiziert* das System den Nutzer.
- *Zugangskontrolle* (engl.: *access control*) meint im Deutschen i. d. R. die Überprüfung von Berechtigungen an einem System, also beispielsweise den Login-Prozess an einem Betriebssystem. Soll dieser Sachverhalt im Englischen ausgedrückt werden, so spricht man – um Missverständnisse zu vermeiden – auch von *logical access control*. Demgegenüber steht die *Zutrittskontrolle* (engl.: *physical access control*), die beim Zutritt zu

**Abb. 2.2** “Layered Defense“  
am Beispiel der Absicherung  
oberhalb und unterhalb der  
Betriebssystemebene



Räumlichkeiten zum Einsatz kommt. Der eigentliche Zugriff auf Daten wird durch die *Zugriffskontrolle* (engl.: *data access control*) beschränkt.

- *Authorisierung* (engl.: *authorization*) legt fest, welches Subjekt wie auf welches Objekt zugreifen bzw. wie es dieses benutzen darf. Authorisierungsinformationen werden beispielsweise vom Betriebssystem (etwa in Form der Metadaten im Dateisystem) abgelegt und dann im Rahmen des Zugriffsversuchs überprüft. Dazu muss sichergestellt sein, dass das Subjekt einwandfrei identifiziert worden ist – was durch eine ordnungsgemäße Authentifizierung erreicht werden kann.
- *Layered Defense* ist der Ansatz in der IS, Sicherheitsmaßnahmen in unterschiedlichen Schichten des Gesamtsystems einzubringen. Betrachtet man dazu etwa das *ISO/OSI-Referenzmodell*, so bedeutet Layered Defense in diesem Fall, dass beispielsweise sowohl auf der *Vermittlungsschicht* (engl.: *network layer*, Layer 3), als auch auf der *Transportschicht* (engl.: *transport layer*, Layer 4) und der *Anwendungsschicht* (engl.: *application layer*, Layer 7) Sicherheitsmaßnahmen eingesetzt werden. Dadurch wird sichergestellt, dass auch bei Versagen einer der Sicherheitsmaßnahmen ein Angreifer Zugriff auf die „Nutzdaten“ erlangen kann. Zu beachten ist dabei allerdings, dass ein Versagen von Sicherheitsmaßnahmen in einer der unteren Schichten i. d. R. nicht mehr durch Sicherheitsmaßnahmen in einer der höheren Schichten kompensiert werden kann.

Ein weiteres Beispiel ist in Abb. 2.2 gezeigt, bei dem die Sicherheitsmechanismen nicht nur im Betriebssystem, sondern auch in den darunter und darüber liegenden Schichten, beispielsweise in der Middleware (beispielsweise durch Absicherung einer Datenbank), eingebracht werden.

- *Auditierbarkeit* (engl.: *auditability*): Ein Audit ist ein Instrument für eine systematische, unabhängige und dokumentierte Untersuchung, bei der festgestellt werden soll, ob die geplanten Anforderungen und Ziele eingehalten werden. Der Begriff Auditierbarkeit bezeichnet also die Tatsache, dass das Auditobjekt über klar definierte Merkmale verfügt und dass entsprechende Kriterien zur Überprüfung bereits im Vorfeld eines Audits festgelegt werden. Im Rahmen der Auditierbarkeit spielt auch die sogenannten Policy-Pyramide eine Rolle.

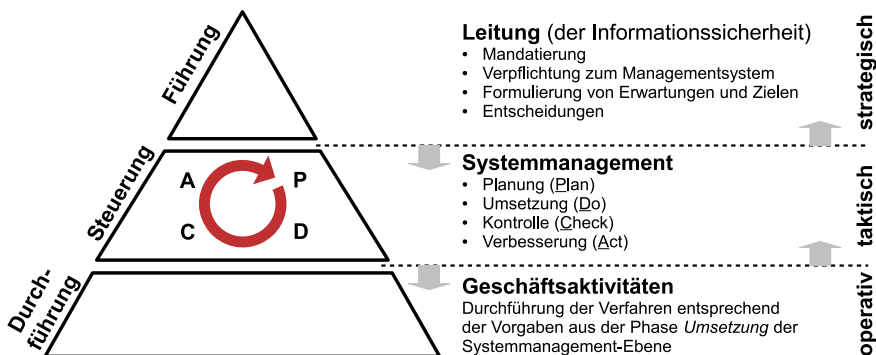


### 2.2.1 Die Policy-Pyramide

Wie bereits angesprochen bilden die IS-Leitlinie, IS-Standards sowie IS-Arbeitsanweisung und IS-Handlungsempfehlungen die sogenannte Policy-Pyramide<sup>3</sup>. Von der Spitze zur Basis nimmt die Änderungshäufigkeit und der Detailgrad der Dokumente zu: Die IS-Leitlinie ist demnach eher allgemein und übergreifend formuliert und wird sich – auch weil sie aus der IS-Strategie abgeleitet ist – eher im Drei- bis Fünf-Jahres-Takt ändern. Aufgrund des geringen Detailgrads reichen die Vorgaben der IS-Leitlinie aber somit auch nicht für ein Audit aus.

Im Gegensatz dazu geben die IS-Arbeitsanweisungen im Detail an, wie die Mitarbeiter vorzugehen haben; sie definieren also, wie die Mitarbeiter die Anforderungen, die sich aus IS-Standards und letztendlich auch aus der IS-Leitlinie ergeben, zu verstehen haben. Daraus wird auch ersichtlich, dass sich die IS-Arbeitsanweisungen häufiger ändern werden, etwa, weil sich die Parametrisierung von kryptografischen Algorithmen geändert hat. *Auditierbarkeit* ist ab der Ebene der IS-Standards gegeben, IS-Handlungsempfehlungen werden als „echte“ Empfehlung verstanden und müssen nicht zwingend befolgt werden.

**Von der Strategie zur Umsetzung** Abb. 2.3 zeigt diesen Sachverhalt nochmals in leicht anderer Form, so wie er in vielen großen Organisationen tatsächlich „gelebt“ wird: Ausgehend von der *strategischen* Ebene, in der die Leitung die Erwartungen und Ziele formuliert, erfolgt in der Systemmanagementebene die *taktische* Umsetzung unter Verwendung eines PDCA-Zyklus. In der *operativen* Ebene werden die Verfahren schließlich entsprechend der Vorgaben aus der Systemmanagementebene „im Betrieb“ umgesetzt. Neben dem *Top-down-Ansatz* sollte gleichzeitig auch im Rahmen eines *Bottom-up-Ansatzes* ein Rückfluss von den unteren in die oberen Ebenen stattfinden.



**Abb. 2.3** Zur Umsetzung der Informationssicherheit ist ein durchgängiger Regelungsrahmen (i. S.v. einem Top-down- und Bottom-up-Ansatz) erforderlich

<sup>3</sup> Für die detaillierte Diskussion zur IS-Policy-Pyramide siehe auch Abschn. 2.6 „Aufbau und Fortschreibung eines IS-Policy Frameworks“.

Wenden wir uns – nach dieser Darstellung der Grundlagen der IS-Governance – in den nächsten Abschnitten nun den anfangs bereits angesprochenen Teilschritten beim Aufbau einer IS-Governance zu.

---

## 2.3 Aufbau und Aufrechterhaltung einer IS-Strategie

Der Aufbau und die Aufrechterhaltung einer an den Unternehmenszwecken und vor allem Unternehmenszielen ausgerichteten IS-Strategie ist eines der Kernkonzepte im Bereich des ISMS und vor allem während des Aufbaus eines ISMS wichtig. Ausgehend von der *IS-Strategie* wird das *IS-Programm* aufgebaut und entsprechend fortgeschrieben. Somit bildet die IS-Strategie die wesentliche Grundlage für alle Elemente des IS-Programms. Unterlaufen dem IS-Manager bzw. den sonstigen Verantwortlichen bei der Entwicklung der IS-Strategie Fehler, so pflanzen sich diese in allen Elementen des IS-Programms fort und verursachen damit erhebliche Korrekturaufwände.

Grundlegend ist zunächst die Frage, was überhaupt als *IS-Strategie* verstanden wird. Dass sich die IS-Strategie aus der Unternehmensstrategie ableitet, wurde bereits erwähnt. Was aber bedeutet „Strategie“ in diesem Fall? Zum einen ist eine Strategie im Gegensatz zu taktischen und operativen Maßnahmen grundsätzlich durch einen übergreifenden, längerfristigen und ganzheitlichen Ansatz geprägt. Auf der anderen Seite bezeichnet eine Strategie aber auch in weniger formaler Hinsicht eine Sammlung von Sicherheitszielen, Prozessen sowie Methoden, Werkzeugen und technischen Verfahren. Letztendlich führen aber beide Bedeutungen im Bereich des ISMS in die gleiche Richtung: Der Schaffung von übergreifenden Lösungsansätzen für spezifische Probleme.

**IS-Strategie leitet sich aus der Geschäftsstrategie ab** Ein wichtiger Aspekt ist, dass sich die IS-Strategie kongruent zur Geschäftsstrategie und damit zu den übrigen Geschäftsprozessen ausrichten muss. Konträre oder nicht angemessene Ansätze sind zum Scheitern verurteilt, da die Notwendigkeit nicht erkannt bzw. die Ansätze als Hemmnisse gesehen werden. So würde Sicherheit auf einem Niveau, das typischerweise im Bankensektor vorzufinden ist, von großen Teilen der mittelständischen Industrie schlichtweg nicht akzeptiert werden. Im Gegensatz dazu begünstigt eine an den sonstigen Geschäftsprozessen ausgerichtete IS-Strategie (und damit auch ein entsprechend ausgerichtetes IS-Programm) die Akzeptanz und damit letztendlich auch die (finanzielle) Unterstützung durch das Management.

- **Tipp** Nicht weniger wichtig ist aber auch der Aspekt, dass auch die Mitarbeiter einer Organisation erkennen, dass die Elemente eines ISMS sie nicht bei ihrer Arbeit hemmen, sondern letztendlich die Geschäftsprozesse sogar unterstützen. Erst dadurch wird die IS auch von den IT-Nutzern und den Mitarbeitern umgesetzt, sie wird im Unternehmen gelebt.

Informationssicherheits-Management  
Leitfaden für Praktiker und Begleitbuch zur  
CISM-Zertifizierung

Wegener, C.; Milde, Th.; Dolle, W.

2016, XXII, 211 S. 55 Abb., Hardcover

ISBN: 978-3-662-49166-9