1 Einführung

Die digitale Transformation

Waren bis vor wenigen Jahren noch Kostenreduzierung und Standardisierung sowie die Steuerung externer Dienstleister zentrale Herausforderungen an die Unternehmens-IT, dominieren heute Fragen der IT- und spezieller der Cybersicherheit, die Komplexitätsreduktion durch »passende« Unternehmensarchitekturen, Daten als »Vierter Produktionsfaktor«, der Plattformgedanke, Virtualisierung und Cloud sowie eine unbedingte 24/7-Verfügbarkeit zur Unterstützung neuer Geschäftsmodelle die Diskussion. Davon betroffen sind nicht nur Unternehmen, sondern Organisationen jeder Art. Alle öffentlichen (staatlichen und nicht staatlichen) Einrichtungen werden daher ebenso in die folgenden Überlegungen einbezogen wie gemeinnützige und alle sonstigen in der Öffentlichkeit sichtbaren Organisationen, auch wenn einheitlich der Begriff »Unternehmen« verwendet wird.

Denn die IT verändert jedes Unternehmen durch einen Prozess, der – auf Basis des technischen Fortschritts und einer immer besseren, auch mobilen Vernetzung – erst begonnen hat und noch lange nicht abgeschlossen ist und den wir als »digitale Transformation« wahrnehmen. Diese digitale Transformation führt dazu, dass bekannte und bewährte Produkte auf anderen Wegen vertrieben werden und/oder anders »funktionieren«. Sie hat aber auch zur Folge, dass viele neuartige Produkte und Dienstleistungen entstehen und sich die Zusammenarbeit zwischen Unternehmen wesentlich verändert. Als Beispiele für diese Entwicklungen dienen neuartige Mobilitätsdienste (etwa Uber) und Übernachtungs-/Urlaubsangebote (bspw. AirBnB), Streamingdienste, die das lineare Fernseh- und Rundfunkprogramm ablösen (etwa Netflix, Spotify), oder Unternehmen sowohl im B2B- als auch im Endkundenbereich, die nicht mehr ausschließlich ihre Produkte mit traditionell verstandener Wartung vertreiben, sondern vollkommen neuartige Abo-Dienstleistungen auf Basis ihrer Produkte oder in Kombination mit ihren Produkten verkaufen, einschließlich Konzepten der Predictive Maintenance. Die Geschäftsmodelle dieser Unternehmen folgen neuartigen Ansätzen oder verändern teilweise radikal bestehende Strukturen.

Fragen der Informationssicherheit und des Datenschutzes, aber auch weitere Risiken rücken damit zunehmend in den Vordergrund. Es vergeht praktisch kein Tag ohne neue Meldungen über identifizierte Sicherheitsprobleme in Hard- und Software, Datenlecks und einen zu sorglosen Umgang mit sensiblen Daten, aber auch Überlegungen einzelner Regierungen, auf verschiedenste Daten (etwa aus sozialen Medien oder von Smart-Home-Geräten) zugreifen zu können. Bekannte Beispiele sind etwa die Sicherheitslücken in Prozessoren und anderer Hardware großer Hersteller, teilweise politisch aufgeladene Datenschutzskandale, Manipulationen, die schwerpunktmäßig große Social-Media-Anbieter treffen, neue Einreisebestimmungen mit Offenlegungspflichten sowie eine mögliche Gefährdung unseres Alltags durch Cyberattacken auf wichtige Elemente unserer lebensnotwendigen Infrastruktur, etwa der Wasser- und Energieversorgung. Unter diesen Bedingungen IT erfolgreich zu steuern, setzt ein hohes Maß an fachlicher und sozialer Kompetenz, effektiven und effizienten Methoden, Erfahrung und Geschick voraus.

Business-IT-Alignment

Zum Streben nach bestmöglicher IT-Unterstützung aller Geschäftsprozesse, dem bestmöglichen Business-IT-Alignment, kommt die Verpflichtung hinzu, das Unternehmen und seine Eigentümer vor Schaden durch die IT zu bewahren. Denn mit den vielfältigen neuen Herausforderungen gehen zwangsläufig ebenso vielfältige neue Bedrohungen und Schwachstellen einher. Was bedeutet es für uns und unseren Alltag, wenn die IT nicht verfügbar ist? Wenn sie Fehler in den Geschäftsprozessen verursacht, die Missbrauch, Datenmanipulation oder Datenspionage ermöglicht?

Nicht alles lässt sich durch verantwortungsvolle Führung verhindern, wohl aber darf (in besonders sensiblen Bereichen muss) verlangt werden, dass das Unternehmen vorbereitet ist und angemessene Gegenmaßnahmen ergreift. Sich über mögliche Bedrohungen und Schwachstellen sowie geeignete Gegenmaßnahmen zu informieren, ist deshalb eine zentrale Forderung an die IT-Leitungsebenen. Es geht dabei um einen zielorientierten und besonnenen Umgang mit einer *künftigen* Situation, auf die man sich bereits heute einstellen muss. Das erfordert eine genaue Kenntnis der *gegenwärtigen* Situation in der IT und im Gesamtunternehmen.

Gegenmaßnahmen kosten Zeit und Geld. Zu schnell kann aus übertriebener Sorge zu viel investiert werden. Dieser Endpunkt im Kontinuum des Aufwandes verbietet sich ebenso wie der Anfangspunkt geringstmöglichen Aufwandes, der auf zu großem Optimismus, Leichtsinn oder – noch schlimmer – Ahnungslosigkeit beruht.

Der Begriff »Wesentlichkeit«

Ziel aller Bemühungen und Überlegungen ist es, in **betriebswirtschaftlich vernünftiger Form *wesentliche* Risiken von der IT** und damit stets auch vom **Gesamtunternehmen und seinen Geschäftsprozessen fernzuhalten**, deutlich zu **reduzieren** oder ihre **Auswirkungen** zu **begrenzen**.

Das Informationssystem

Der Anwendungsbereich dieser Überlegungen (vgl. Abb. 1–1) erstreckt sich auf folgende Punkte:

- **Personen** und **Organisationseinheiten**, die in irgendeiner Form einen Bezug zu den weiteren Elementen haben. Der Begriff IT-Organisation im Speziellen umfasst dabei neben organisatorischen Regelungen (Ablauforganisation, siehe IT-Prozesse) alle Organisationseinheiten (Aufbauorganisation) mit IT-Bezug. Zur IT-Organisation gehören demzufolge die IT-Abteilung sowie Bereiche und Rollen in den Fachabteilungen mit IT-Bezug.
- **Daten** bzw. **Informationen**
  Eingeschlossen sind alle Daten zur Installation, Konfiguration und Administration von Software sowie Dokumente mit IT-Bezug.
- **Anwendungen**
  Unter diesem Begriff (engl.: Application oder kurz App) wird nach ISO/IEC 2382:2015 Software zur Unterstützung der unterschiedlichen Geschäftsprozesse zusammengefasst. Anwendungen haben stets einen fachlichen Fokus.
- **Industrial Automation Applications (IAA)**
  Diese Art Software wird im Fertigungsbereich zur Unterstützung der Planungs- und Steuerungsprozesse eingesetzt. Im Kontext von Industrie 4.0 und der damit verbundenen zunehmenden Vernetzung dieser Anwendungen untereinander und mit weiteren internen und externen Anwendungen gewinnt diese Gruppe nicht zuletzt aus IT-Sicherheits- und Risikosicht stark an Bedeutung (siehe dazu Normenreihe IEC 62443, NIST SP 800-82 Rev. 2).
- **Systemsoftware**
  Dazu zählt nach ISO/IEC 2382:2015 das Betriebssystem und andere für den IT-Betrieb notwendige Software (sog. Middleware), mitunter werden auch Datenbankmanagementsysteme in dieser Ebene eingeordnet, ebenso Spezialsoftware für Appliances und Mobilgeräte (sog. Firmware).
- **Hardware**
  Eingeschlossen sind Großrechner ebenso wie Server oder zentrale Speichersysteme (SAN/NAS) und Arbeitsplatzrechner, Bildschirme, Drucker und weitere Peripheriegeräte, aber auch alle mobilen Geräte.

- **Netzwerk**
  Hierunter fallen alle Netzwerkgeräte, beispielsweise sogenannte Appliances wie Firewalls, Router sowie alle aktiven und passiven Komponenten zur Datenübertragung.
- **IT-Prozesse** zur unmittelbaren Unterstützung von **Geschäfts- und Produktionsprozessen**, aber auch von **administrativen IT-Betriebsabläufen**, etwa Datensicherungen oder die Durchsicht von Protokollen.
- **Geschäfts-/Produktionsprozesse und ergänzende organisatorische Regelungen.** Sie beschreiben die **Logik** aller Produktions- und Geschäftsprozesse und legen **Berechtigungen** und **Verantwortlichkeiten** sowie prozessunabhängige und -übergreifende **Regelungen** fest.
- **Sonstige, nicht IT-bezogene Ressourcen** als Bestandteile von Geschäfts- und Produktionsprozessen.

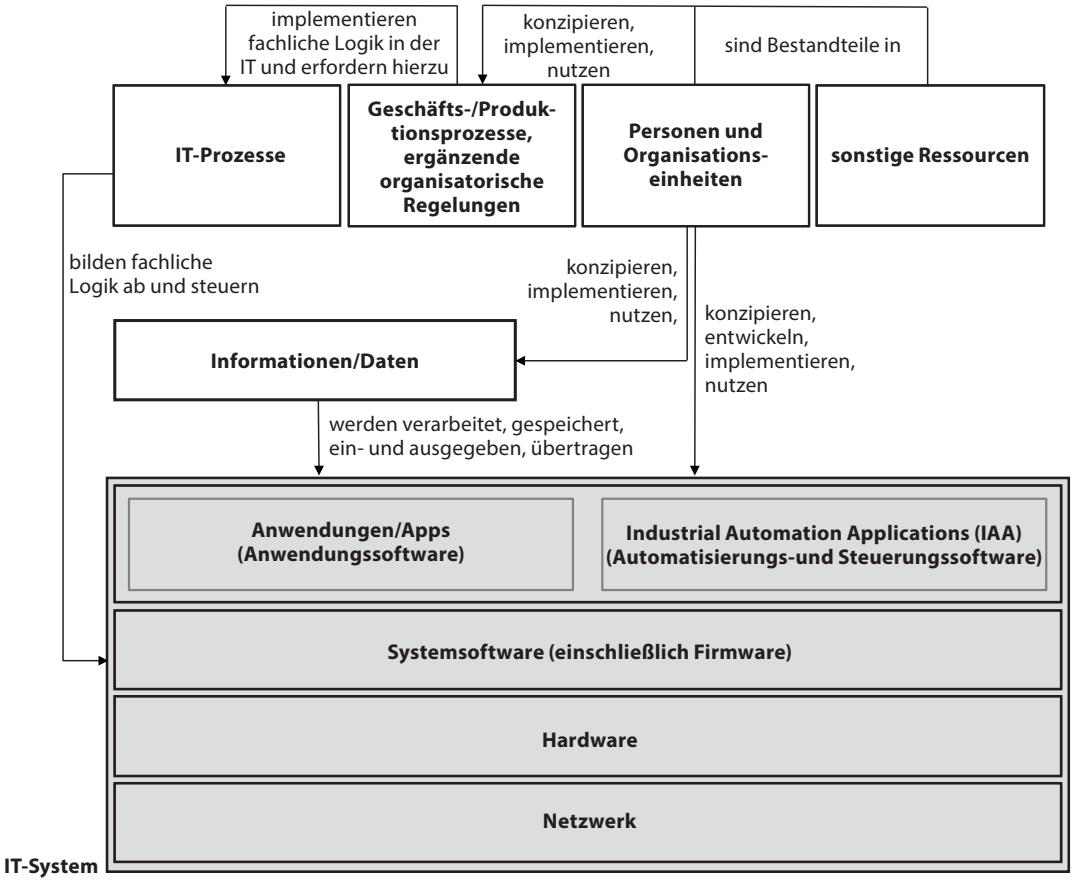

Abb. 1–1 *Informationssystem*

Alle Elemente in Abbildung 1–1 zusammen beschreiben ein **Informationssystem** als soziotechnisches System, in dem der Mensch, die von ihm entwickelten Regelungen bzw. fachlichen/technischen Prozesse, alle Daten sowie die unterstützenden IT-Systeme zusammengefasst sind.

Definition

Die Disziplin, die sich mit **Risiken aus Entwicklung, Betrieb und Nutzung** solcher **Informationssysteme** befasst, wird **IT-Risikomanagement** genannt.

Die fünf grau hinterlegten Elemente beschreiben zusammengenommen ein **IT-System**. Das IT-System lässt sich nach seiner Unterstützung für betriebswirtschaftliche oder technische Aufgaben entsprechend differenzieren.

Zur Systematisierung von betriebswirtschaftlich genutzten IT-Systemen (etwa ERP-, CRM-, BI- oder E-Commerce-Systeme sowie weitere Systeme mit Endkundenfokus) existieren in der Wirtschaftsinformatik mehrere Ansätze, meist wird nach Anwendungsbereichen oder nach Vernetzungsfähigkeiten mit externen Partnern differenziert. In diese Gruppe fallen auch alle IT-Systeme, die den Plattform-Ansatz unterstützen, etwa Social-Media-, Streaming-, Mobilitäts- und weitere Angebote, die verschiedene Anbieter mit Kunden verbinden. Dazu zählen auch Smartphones und Tablets mit den jeweiligen App-Stores.

Ein IT-System zur Unterstützung technischer Aufgaben wird Steuerungssystem für Industrieanlagen bzw. **Industrial Control System** (ICS) genannt. In diese Gruppe fallen – als separate Elemente oder als Bestandteil von ICS – auch alle Elemente des sogenannten **Internet der Dinge** (engl.: **Internet of Things, IoT**, vgl. Abschnitte 7.4 und 8.5). Neben produktionsunterstützenden Systemen rund um Fertigungs- und Logistikanlagen fallen alle für die **Gebäudeautomation/Smart Home** eingesetzten Systeme darunter. Die Beispiele reichen dabei von einem Aktor oder Sensor mit Netzwerkanbindung bis hin zu einer vollständigen Lösung zur Steuerung/Überwachung von Gebäuden und Anlagen mit Benutzeroberfläche und Schnittstellen zu betrieblichen Anwendungen. Zu dieser Gruppe gehören spätestens mit der (beinahe) flächendeckenden Einführung von Voice-over-IP-Technologien (VoIP) und der damit einhergehenden Einbindung in das bestehende Netzwerk auch alle Telekommunikationsanlagen und -endgeräte in den Unternehmen, die zuletzt noch vollkommen separat betrachtet wurden.

IT-Systeme wie Smart TVs oder Wearables (etwa Smart Watches) lassen sich meist nicht exakt einordnen, vielmehr liegen sie je nach Anwendungsschwerpunkt entsprechend näher an betriebswirtschaftlichen bzw. endkundenorientierten oder produktions- und steuerungsnahen Anwendungen. So erfüllt beispielsweise ein Smart TV in einem

Besprechungsraum eine andere Aufgabe als in der Produktion oder im Privathaushalt.

Das IT-Risikomanagement schließt deshalb neben der betriebswirtschaftlichen Sicht auf die IT auch die Sicht auf Steuerungen und Produktionsanlagen sowie alle weiteren oben beschriebenen Komponenten mit IT-Anteilen (bspw. VoIP-Telefonanlagen) ausdrücklich mit ein. Die IT in diesen Bereichen wird aufgrund des gekapselten und häufig proprietären Charakters der darin enthaltenen Hard- und Software bislang in vielen Unternehmen als *Schatten-IT* bezeichnet, auch wenn dieser Begriff eher aus dem betriebswirtschaftlichen Kontext (in den Fachabteilungen entwickelte Office-Anwendungen) bekannt ist. Sie untersteht in solchen Fällen nicht der Verantwortung der IT, sondern vielfach noch der Produktionsleitung (Fertigungsanlagen), spezialisiertem Leitstellenpersonal (Steuerungsanlagen, etwa in der Energie-/Wasserversorgung), dem Facility Management (Gebäudeautomation, Telekommunikationsanlagen) oder medizinisch-technischem Fachpersonal in entsprechenden Einrichtungen (medizinisch-technische Geräte). Entsprechend waren und sind solche IT-Systeme vielfach vom IT-Risikomanagement nicht erfasst worden. Das ändert sich aktuell, nicht zuletzt aufgrund zunehmender Sicherheitsvorfälle (etwa Angriffsmöglichkeiten auf Herzschrittmacher, Insulinpumpen und andere Geräte).

Diese Entwicklung ist positiv zu bewerten, denn eine intensive Betrachtung wird zwingend notwendig, weil IT-Systeme, die nicht in die Lebenszyklus-, Service- und Supportprozesse und -strukturen der IT eingebunden sind, zunehmend eine Bedrohung für das einsetzende Unternehmen, aber auch für dessen Kunden werden können. Anlagen und Produkte einschließlich darauf basierender digitaler Dienstleistungen könnten fehlerhaft oder nicht verfügbar sein, mit allen Folgen bis hin zur Gefahr für Leben oder Gesundheit der jeweiligen Nutzer.

Aufbau des Buches und Hinweise zur Nutzung der Praxiselemente

Struktur des Buches

Das Buch gliedert sich in vier größere Themenbereiche (vgl. Abb. 1–2).

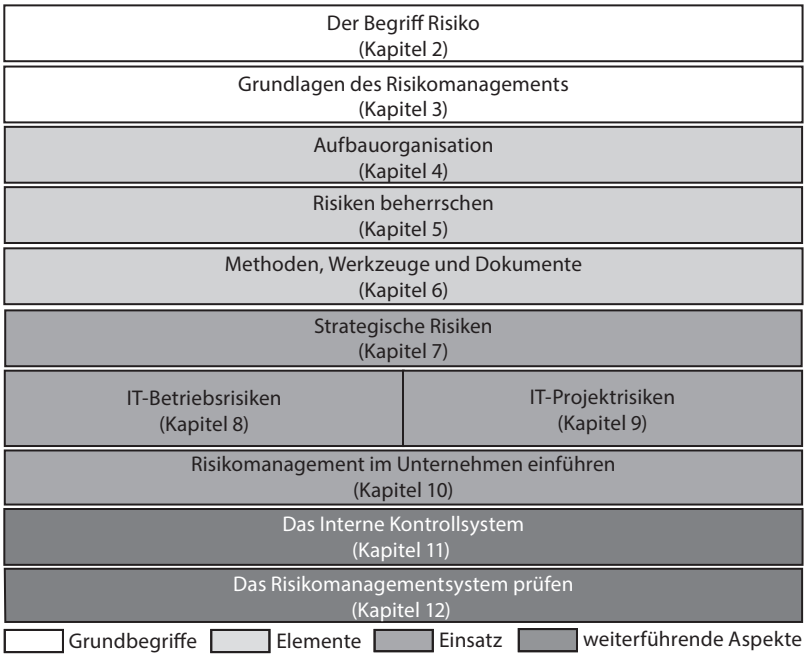

Abb. 1–2
Thematischer Aufbau des Buches

Der erste Themenbereich (Kap. 2 und 3) legt die begrifflichen Grundlagen. Der zweite Themenbereich (Kap. 4 bis 6) behandelt die Organisation des IT-Risikomanagements, den IT-Risikomanagementprozess sowie Methoden, Werkzeuge und Dokumente des IT-Risikomanagements. Der dritte Themenbereich (Kap. 7 bis 10) betrachtet das IT-Risikomanagement im strategischen Bereich und damit im Kontext des IT-GRC-Managements, dem IT-Betrieb und in IT-Projekten, an der Schnittstelle zwischen Entwicklung und Betrieb sowie die notwendigen Schritte zu seiner Einrichtung. Das Kapitel 8 befasst sich auch mit Fragen des IT-Risikomanagements beim Einsatz von Cloud-Angeboten für Endkunden sowie allen übrigen Dienstleistungen mit IT-Anteil, die den Endkunden direkt einbeziehen. Der vierte Themenbereich (Kap. 11 und 12) stellt das Interne Kontrollsystem und seine Bedeutung für das IT-Risikomanagement dar und erläutert die Prüfung des IT-Risikomanagements hinsichtlich Angemessenheit und Wirksamkeit.

Ein wichtiges Ziel ist es, die Theorie des IT-Risikomanagements für die Praxis aufzubereiten. Dazu hebt das Buch wichtige **Definitionen** hervor, ergänzt die Theorie durch kleine (**Anwendungs-**)**Beispiele** und hilft bei der Umsetzung durch **Praxishinweise**, konkrete **Handlungsempfehlungen** und Muster als Anregung für die Erstellung eigener **Checklisten**.

Ein **Praxishinweis** ist erkennbar am Hinweis in der Marginalspalte und einem grau unterlegten Kasten.

Praxishinweis

Konkrete Fragestellung

Als Antwort auf die jeweilige Fragestellung sind in einem Praxishinweis wichtige Erfahrungen in knapper Form zusammengefasst.

Handlungsempfehlungen sind gekennzeichnet durch einen Hinweis in der Marginalspalte und eine Schritt-für-Schritt-Empfehlung zur Umsetzung.

Handlungsempfehlung

Schritt-für-Schritt-Empfehlung für die Bearbeitung einer bestimmten Fragestellung	
Schritt 1	Handlungsempfehlung
Schritt 2	Inhaltlich nächste Aktivität, ggf. Alternativen, Bedingungen

Checklisten enthalten Punkte, die bei der Beschäftigung mit einer Aufgabe im eigenen Unternehmen sinngemäß Berücksichtigung finden sollten. Sie sind in der Marginalspalte gekennzeichnet und als Tabelle ausgestaltet.

Checkliste

Checkliste zur Aufgabenstellung		○ | ◗ | ●
1.	Zu beachtender Aspekt, ggf. mit Unterpunkten	Grad der Erfüllung/Abdeckung, Statusinformation
2.	Weitere Frage im Kontext	

○ nicht erfüllt, ◗ erfüllt, kann aber noch verbessert werden, ● erfüllt

Denn beim Auf- und Ausbau des eigenen IT-Risikomanagements gilt grundsätzlich, dass Vorlagen und Überlegungen aus Büchern, Zeitschriften und dem Internet hilfreich sein können. Allerdings ist eine direkte Übernahme von Inhalten erwartungsgemäß selten möglich. Für eine Nutzung sollten – etwa im Rahmen eines Workshops:

- Begriffe in die Sprachwelt des Unternehmens übertragen werden;
- inhaltliche Details zu Prozessen und der IT auf Übereinstimmung geprüft und angepasst werden – dies betrifft beispielsweise verwendete Systematisierungen, Klassifizierungen, Einheiten, Farbcodes und Symbole;
- Besonderheiten des eigenen Unternehmens ergänzt werden. Dabei handelt es sich meist um Spezifika aus der Geschäftstätigkeit, die (in einem Workshop) im Dialog mit den betroffenen Fachabteilungen ermittelt werden müssen. Dies gilt besonders in regulierten Branchen und im KRITIS-Umfeld.