inge HANSCHKE

INFORMATIONS-SICHERHEIT UND DATENSCHUTZ

EINFACH & EFFEKTIV

Integriertes Management-instrumentarium systematisch aufbauen und verankern

HANSER

Hanschke

Informationssicherheit und Datenschutz – einfach & effektiv

Inge Hanschke

Informationssicherheit und Datenschutz – einfach & effektiv

Integriertes Managementinstrumentarium systematisch aufbauen und verankern

HANSER

Die Autorin:

Inge Hanschke, München
www.Lean24.com

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Petra Kienle, Fürstenfeldbruck
Layout: Manuela Treindl, Fürth
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © fotolia.com/RealVector
Datenbelichtung, Druck und Bindung: Kösel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

Print-ISBN: 978-3-446-45818-5
E-Book-ISBN: 978-3-446-45973-1
E-Pub-ISBN: 978-3-446-46300-4

Inhalt

Vorwort

Am besten erledigt man die Dinge systematisch.

Hesiod von Böotien (um 700 v. Chr.)

Anforderungen an die Informationssicherheit (u. a. ISO 27001 oder BSI), den Datenschutz (EU-Datenschutz-Grundverordnung) und Sicherheitsbedrohungen sowie die durch diese verursachten Schäden nehmen immer weiter zu. Ein in alle Planungs-, Entscheidungs- und Durchführungsprozesse verankertes, handhabbares und integriertes Managementinstrumentarium ist für deren nachhaltige Bewältigung notwendig. Im Buch werden sowohl die Herausforderungen adressiert als auch Hilfestellungen für eine systematische Gestaltung und nachhaltige Verankerung in der Organisation gegeben.

Im Buch werden sowohl die Anforderungen der EU-Datenschutz-Grundverordnung als auch die aus dem Kontext Informationssicherheit sowie wesentliche Normen und gesetzliche Regelungen eingeführt. Wegen der ständig zunehmenden Bedrohungslage im Cyberspace wird auch das Themenfeld Cyber-Security adressiert, um dessen wachsender Bedeutung gerecht zu werden. Cyber-Security beschreibt den Schutz vor technischen, organisatorischen und naturbedingten Bedrohungen, die die Sicherheit des Cyberspace inklusive Infrastruktur- und Datensicherheit gefährden. Es beinhaltet alle Konzepte und Maßnahmen, um Gefährdungen[1] zu erkennen, zu bewerten, zu verfolgen, vorzubeugen sowie Handlungs- und Funktionsfähigkeit möglichst schnell wiederherzustellen.

Neben den Herausforderungen für Datenschutz und Informationssicherheit finden Sie in diesem Buch sowohl Best-Practices für ein integriertes und ganzheitliches einfaches und effektives Management-Instrumentarium für Datenschutz und Informationssicherheit als auch einen Leitfaden, um Ihr individuelles Instrumentarium abzuleiten. Mithilfe eines

[1] Gefährdung = Bedrohung und Schwachstelle

Schritt-für-Schritt-Leitfadens werden Hilfestellungen für die individuelle Ableitung und für die Umsetzung gegeben. Die Schritte werden anhand von Beispielen erläutert.

Sowohl der Datenschutz als auch die Informationssicherheit, einschließlich der Cyber-Security, benötigen eine möglichst vollständige, konsistente und aktuelle Aufstellung aller Assets (fachliche und technische Werte des Unternehmens wie Geschäftsprozesse, Organisationsstrukturen, Applikationen, technische Bausteine und Configuration Items) für Analysen und Schutzbedarfsfeststellung.

So sind für den Datenschutz Informationen über die Verwendung von Daten (Geschäftsobjekte) in Prozessen oder Applikationen essenziell. Fragestellungen wie „Welche Prozesse oder Applikationen verwenden personenbezogene Daten in welcher Art und Weise?“ sind relevant. Auf Basis des Asset-Registers erfolgen zudem die Schutzbedarfsfeststellung und die Gefährdungsanalyse sowie die Analyse von Abhängigkeiten und Auswirkungen von technischen Schwachstellen (siehe Abschnitte 4.1 und 4.2).

Das Asset-Management kann maßgeblich durch Enterprise Architecture Management (EAM) und eine Configuration Management Database (CMDB) unterstützt werden. Durch die Kombination vom integrierten Managementsystem für Datenschutz und Informationssicherheit mit EAM und einer CMDB werden sowohl die Wirksamkeit als auch die Effizienz deutlich erhöht. Daher wird diesem Zusammenspiel ein eigenes Kapitel in diesem Buch gewidmet.

Hier setzt dieses Buch an. Das Buch liefert einerseits einen ganzheitlichen schlanken und handhabbaren Ordnungsrahmen und andererseits einen Schritt-für-Schritt-Leitfaden für die systematische maßgeschneiderte Ableitung Ihres individuellen Datenschutz- und Informationssicherheitsinstrumentariums sowie deren Operationalisierung durch direkt anwendbare Hilfestellungen.

München, im Herbst 2019

Inge Hanschke

Danksagung

Vielen Dank an die vielen Datenschutz- und Informationssicherheitsexperten und Kollegen aus befreundeten Unternehmen für den intensiven Austausch.

Danke an meine Diskussionspartner, Reviewer und Unterstützer, die durch wertvolle Kommentare und Feedback das Buch maßgeblich mitgestaltet haben. Hier sind insbesondere Sebastian Hanschke, Christiane Charrad und auch Frau Brigitte Bauer-Schiewek sowie Frau Irene Weilhart vom Hanser-Verlag für ihr wertvolles Feedback und ihre Unterstützung zu nennen.

Besonderen Dank an Jörg Krüger, meine Familie und Freunde, die mir den Rücken freigehalten haben und mich auch durch Feedback tatkräftig unterstützt haben.

Wegweiser durch dieses Buch

Die Gliederung des Buchs ist im folgenden Bild dargestellt. Sie können die Kapitel in der genannten Reihenfolge oder aber auch selektiv lesen. Sie sind inhaltlich in sich abgeschlossen.

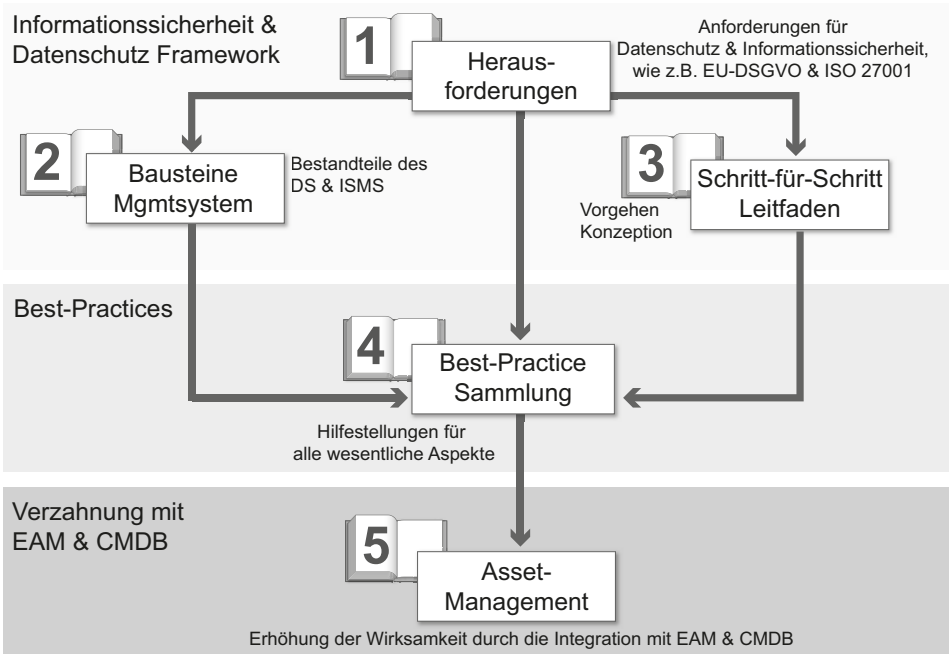

Bild 1 Kapitelstruktur

- Kapitel 1 erläutert die Herausforderungen im Datenschutz und in der Informationssicherheit mit allen relevanten Sicherheitsvorgaben, wie z. B. ISO 27001, IT-Grundschutz und EU-DSGVO sowie der Cyber-Security.
- Kapitel 2 skizziert die Bausteine eines integrierten Datenschutz- und Informationssicherheitssystems.
- In Kapitel 3 finden Sie den Schritt-für-Schritt-Leitfaden für die Konzeption Ihres integrierten Instrumentariums.
- Kapitel 4 liefert Ihnen eine Best-Practice-Sammlung zur Operationalisierung Ihres Instrumentariums.
- Kapitel 5 widmet sich dem Asset-Management mit Hilfe vom Enterprise Architecture Management und einer CMDB.

Jedes Kapitel enthält darüber hinaus zahlreiche Literaturhinweise als Empfehlung für die Vertiefung des jeweiligen Themas.

Wer sollte dieses Buch lesen?

Das Buch adressiert alle Personengruppen im Kontext Informationssicherheit und Datenschutz, die „Kümmerer“ und die „Betroffenen“, wie z. B. der Datenschutz- oder Informationssicherheitsbeauftragte sowie die Bereiche Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge. Folgende Personengruppen werden besonders adressiert:

- *Chief Information Security Officer (CISO), Informationssicherheitsbeauftragter (ISB), Beauftragte für IT-Sicherheit, Bereichs- oder Projektsicherheitsbeauftragter*
  - Wie kann das ISMS initiiert, implementiert und überwacht werden?
  - Welche Sicherheitsanforderungen bestehen? Welche Normen, wie z. B. ISO 27001, sind für das Unternehmen relevant?
  - Wie werden Sicherheitsziele und Geltungsbereich festgelegt?
  - Welche Sicherheitsmaßnahmen sind zur Umsetzung der Anforderungen erforderlich?
  - Welche Dokumente sind unter welchen Vorgaben verpflichtend? Welche Inhalte haben die Dokumente, wie z. B. die Informationssicherheitsleitlinie? Wie können diese handhabbar gestaltet werden?
  - Wie muss eine Sicherheitsorganisation für den jeweiligen Kontext gestaltet werden?
  - Wie sieht ein Sicherheitskonzept aus? Welche Best-Practices gibt es hierzu?
  - Wie kann wirksam ein Instrumentarium aufgebaut und betrieben werden?
  - Wie erfolgt die Erstellung von Plänen zur Umsetzung und Kontrolle von Sicherheitsmaßnahmen?
  - Wie kann die Wirksamkeit überprüft werden?
  - Wie kann ein ausreichendes Sicherheitsniveau definiert und implementiert werden?
  - Wie kann Informationssicherheit effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, und organisatorische Strukturen muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?
- *Datenschutzbeauftragte (DSB)*
  - Wie kann der Datenschutzbeauftragte der obersten Leitungsebene bei der Wahrung der Persönlichkeitsrechte und der Vermeidung von Zwischenfällen, die dem Ansehen des Unternehmens schaden, unterstützen?
  - Wie sieht ein Datenschutzkonzept aus?
  - Welche Dokumente/Meldewege sind verpflichtend? Welche Inhalte und Struktur haben diese Dokumente? Wie können diese handhabbar gestaltet werden?
  - Welche technischen und organisatorischen Maßnahmen sind relevant für die Umsetzung des Datenschutzkonzepts? Wie kann deren Wirksamkeit überprüft werden?
  - Welche organisatorischen Voraussetzungen müssen geschaffen werden?
  - Wie kann ein ausreichendes Datenschutzniveau definiert und implementiert werden?
  - Wie kann Datenschutz effizient und effektiv kontinuierlich sichergestellt werden?
  - In welche Prozesse, wie z. B. Risikomanagement, muss sich das Instrumentarium verzahnen? Auf welche Art und Weise?

- *Betriebsrat*
  - Wie können die Mitbestimmungsrechte gewahrt werden?
  - Wie können Mitarbeiter vor Sanktionen geschützt werden?
  - Wie können Mitarbeiter vor unklaren Regelungen und einschränkenden Maßnahmen geschützt werden?
- *Oberste Leitungsebene („Informationssicherheit und Datenschutz ist Chefsache")*
  - Ist ein ISMS im Wettbewerb ein Vorteil oder ein Hygienefaktor?
  - Wie können die Unternehmenswerte hinreichend gesichert werden?
  - Wie können die Unternehmensrisiken und persönlichen Risiken beherrscht werden?
  - Wie können Informationssicherheit und Datenschutz hinreichend umgesetzt werden? Mit welcher Organisation? Ohne zu viele Aufwände? Ohne zu viele Formalismen? Wie viele Rollen und Ressourcen sind notwendig?
  - Welche Aufgaben bestehen für die oberste Leitungsebene? Welche Aufgaben können delegiert werden? Welche Verantwortung verbleibt?
- *Leiter Organisation und Führungskräfte*
  - Welche organisatorischen Voraussetzungen müssen für Informationssicherheit und Datenschutz geschaffen werden?
  - Welche organisatorischen und personellen Anforderungen bestehen und wie können diese durch angemessene Sicherheitsmaßnahmen umgesetzt werden?
  - Wie können Datenschutz- und Informationssicherheitsrisiken in das unternehmensübergreifende Risikomanagement integriert werden?
- *Einkauf*
  - Wie kann das Sicherheitsrisiko durch Lieferanten gesenkt werden? Wie können Auftragnehmer zu den für das Unternehmen festgelegten Sicherheits- und Datenschutzrichtlinien verpflichtet und in geeigneter Weise zur Einhaltung „gezwungen" werden?
  - Wie stellt man sicher, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber unverzüglich informiert?
  - Wie kann der Aufwand bei der Lieferanten-Auditierung reduziert werden?
- *Fachverantwortliche für Geschäftsprozesse und Fachverfahren*
  - Wie können die geschäftliche Relevanz/Kritikalität der verarbeitenden Informationen, der Verarbeitungen und deren Schutzbedarf festgelegt werden?
  - Welche Sicherheits- und Kontrollmaßnahmen sind zur Verwaltung und zum Schutz der im Verantwortungsbereich befindlichen Informationen zu implementieren?
  - Wie können durch den Fachverantwortlichen der Zugang zu Informationen sowie der Umfang und die Art der Autorisierung in den Verarbeitungen definiert werden? Was ist dabei zu berücksichtigen? Wie ist die Autorisierung zu dokumentieren?
  - Welche Informationen haben welche geschäftliche Relevanz und wie können diese adäquat geschützt werden?
  - Welche Aufbewahrungsfristen müssen entsprechend der gesetzlichen Vorschriften eingehalten werden?

- *Mitarbeiter*
  - Welche Verhaltensregeln gibt es im Kontext Informationssicherheit und Datenschutz?
  - Was muss beachtet werden? Wo findet man die jeweils gültige Richtlinie und Verfahrensanweisung?
- *IT-Verantwortliche*
  - Welche Richtlinien und Verfahrensanweisungen sind für sichere IT-Unterstützung der Geschäftsprozesse relevant? Wie können diese mit den vorhandenen IT-Prozessen integriert werden?
  - Wie können IT-Servicemanagement und Informationssicherheit zusammenwirken?
  - Wie sollte eine ordnungsgemäße IT-Administration erfolgen? Welche Verhaltensregeln und Sicherheitshinweise sollten für Administratoren festgelegt werden?
  - Wie können über Sicherheitsgateways oder Firewalls Schutzzonen erstellt werden? Welche sind erforderlich?
  - Wie kann ein hinreichender Virenschutz zum Schutz vor Schadprogrammen erreicht werden?
  - Wie kann die Notfallvorsorge aussehen?
  - Was ist bei der Datensicherung zu beachten?
  - Welche Daten sind zu archivieren? Welche Aufbewahrungsfristen gelten?
  - Wie kann die sichere Nutzung von E-Mail und Groupware gewährleistet werden?
  - Was ist bei Outsourcing und externen Dienstleistern zu beachten?

Webseite zum Buch

Weitergehende Informationen zum Buch finden Sie auf den Webseiten https://Lean42.com und https://LeanISMS.de, außerdem unter https://www.hanser-fachbuch.de/978-3-446-45818-5. Auf dieser Buchdetailseite klicken Sie auf die Registerkarte Links.

1 Herausforderungen in Informationssicherheit und Datenschutz

Man wächst mit der Herausforderung.

Quelle: Unbekannt

Die Informations- und Kommunikationstechnik hat alle Lebensbereiche durchdrungen. Die Geschäftsprozesse von Unternehmen kommen kaum mehr ohne IT-Unterstützung aus. Die horizontale und vertikale Vernetzung von Partnern bis zu Maschinen nimmt immer weiter zu. Nur so kann schnell auf Kundenanfragen und sich ändernde Kundenbedürfnisse reagiert werden. Die hohe Durchdringung mit Informations- und Kommunikationstechnik erhöht jedoch gleichzeitig die Abhängigkeit und die Anfälligkeit für die kontinuierlich zunehmenden Sicherheitsbedrohungen, zum Beispiel im Kontext von Cyber-Security.

Sicherheits- und Datenpannen, wie Massen-E-Mails mit Viren, Veröffentlichung von vertraulichen Daten oder manipulierte, missbräuchlich verwendete, mutwillig zerstörte oder kompromittierte Daten, können für die Unternehmen zu ernsthaften rechtlichen oder wirtschaftlichen Konsequenzen führen. Insbesondere aber auch die Nichtverfügbarkeit von Systemen hat erhebliche wirtschaftliche Auswirkungen. Ein Beispiel hierzu ist die Unterbrechung einer Lieferkette in einer Just-in-time-Fertigung (JIT-Fertigung) aufgrund eines Systemabsturzes, der zu einem Produktionsstillstand führt, da wesentliche Rohstoffe oder Teile nicht angefordert werden und somit fehlen.

Externe Vorgaben wie Gesetze, Regulatoren und Normen sowie Anforderungen interessierter Parteien (z. B. BDSG, UWG, TMG, Regulierungsbehörden) und Verträge erfordern ein angemessenes Sicherheitsniveau und die Einhaltung von Formalien. Vorstände und Geschäftsführer haften persönlich für viele Versäumnisse und mangelnde Risikovorsorge. Ein Beispiel sind die hohen Bußgelder bei Datenpannen im Kontext der EU-DSGVO (europäische Datenschutzgrundverordnung). Imageschäden und Folgekosten erhöhen die Schadensauswirkungen noch erheblich. Die Gewährleistung der Persönlichkeitsrechte Betroffener und die Sicherstellung der Rechenschaftspflicht sind daher Grundanforderungen an ein Datenschutz-Managementsystem.

Informationssicherheit und Datenschutz sind unerlässlich, um sowohl personenbezogene Daten als auch Geschäfts- und Unternehmensgeheimnisse zu schützen und einen zuverlässigen Geschäftsbetrieb und die kontinuierliche Weiterentwicklung des Geschäftsmodells zu gewährleisten. Es geht letztendlich darum, mit Informationssicherheitsmanagement und Datenschutz den Erfolg des Unternehmens abzusichern (siehe Bild 1.1). Gerade im Zeitalter der digitalen Transformation sind „sichere“ Daten- und Integrationsplattformen mit vielen Automatismen als integraler Bestandteil des Managementsystems unerlässlich. Nur so kann der Mehrwert aus Daten gehoben und Big Data, Business-Analytics rechtssicher und berechtigt genutzt werden.

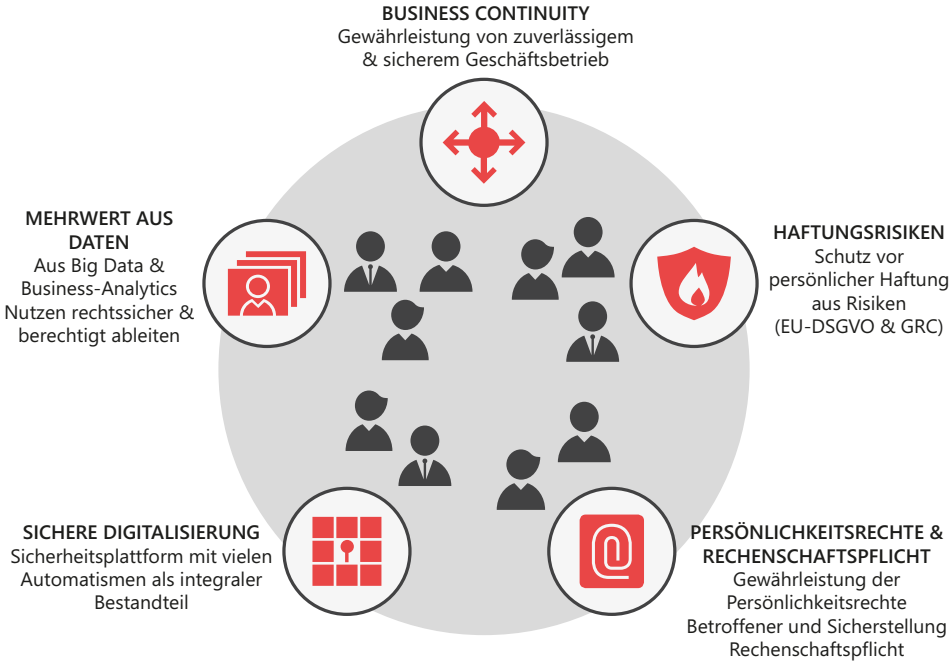

Bild 1.1 Nutzenorientiertes Management von Datenschutz und Informationssicherheit

Die Informationssicherheit und der Datenschutz eines Unternehmens müssen einen Handlungsrahmen und Hilfestellungen liefern, um den kontinuierlichen Geschäftsbetrieb und auch die Geschäftsmodellweiterentwicklung hinreichend sicher zu ermöglichen. Um hinreichend sicher einschätzen zu können, müssen wir uns in diesem Kapitel die Anforderungen und Normen im Kontext der Informationssicherheit und des Datenschutzes etwas näher anschauen. Da die Begrifflichkeiten nicht ganz einfach sind, widmen wir uns im folgenden Abschnitt zunächst diesen. Eine Kurzfassung der Anforderungssammlung finden Sie in [Han19].

In diesem Kapitel finden Sie die Antworten auf folgende Fragen

- Warum ist Informationssicherheit und Datenschutz wichtig?
- Was ist Informationssicherheit?
- Was ist Datenschutz?
- Welche Anforderungen leiten sich aus Gesetzen und Normen ab?

1.1 Einordnung von Informationssicherheit und Datenschutz

Wie bereits ausgeführt, sind Informationssicherheitsmanagement und Datenschutz essenziell, um den Erfolg des Unternehmens abzusichern. Was versteht man aber unter Informationssicherheit und Datenschutz?

Die **Informationssicherheit** zielt auf den angemessenen Schutz von Informationen und IT-Systemen in Bezug auf alle festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit, ab. Ein unbefugter Zugriff oder die Manipulation von Daten soll verhindert und soweit möglich vorgebeugt werden, um daraus resultierende wirtschaftliche Schäden zu verhindern. Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier als auch in IT-Systemen vorliegen.

IT-Sicherheit adressiert als Teilbereich der Informationssicherheit den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung inklusive Funktionssicherheit, also das fehlerfreie Funktionieren und die Zuverlässigkeit der IT-Systeme. Hier müssen auch Systeme einbezogen werden, die häufig nicht unmittelbar als IT-Systeme wahrgenommen werden, wie Steuerungs- (ICS) oder IoT-Systeme. Die IT-Sicherheit ist also Bestandteil der Informationssicherheit. Das Aktionsfeld der klassischen IT-Sicherheit wird bei der Cyber-Sicherheit auf den gesamten Cyber-Raum ausgeweitet.

Unter **Datenschutz** wird primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden, um das Recht des Einzelnen auf informationelle Selbstbestimmung zu stärken.

Es stellt sich hierbei nicht die Frage, ob man Informationssicherheit und Datenschutz adressiert, sondern nur wann und in welchem Umfang. Die Kernfrage ist hier: „Wann ist man hinreichend sicher?“

- *Welche Richtlinien, Verfahrensanweisungen und Arbeitsanweisungen sind erforderlich?*
  Mögliche Antwort: verpflichtende und empfohlene Dokumente aus Informationssicherheit und Datenschutz (u. a. ISO 2700X, BSI IT-Grundschutz und EU-DSGVO)
- *Wie kann man die IT-Systeme hinreichend „technisch“ absichern?*
  Hierauf gibt es eine einfache Antwort: „Systeme sind hinreichend sicher, wenn der Aufwand eines Angreifers dessen Nutzen erheblich übersteigt.“

  Widerstandsfähige Systeme überstehen absichtliche Angriffe ohne inakzeptablen Schaden für das Unternehmen. Für viele Systeme mit normalem Schutzbedarf reicht hierbei eine Absicherung nach dem „Stand der Technik“ aus (siehe Abschnitt 1.2.4).
- *Wann ist die Absicherung hinreichend?*
  Wie viel Schutz ist notwendig, um einen kontinuierlichen Geschäftsbetrieb sicherzustellen, die sichere Geschäftsmodell-Weiterentwicklung zu ermöglichen und Image-Schäden und Reputationsverlust zu vermeiden?
  So dürfen z. B. Hackerangriffe nicht zum Ausfall von Kernsystemen führen.

Schutz ist kein Selbstzweck. Es ist so viel Schutz notwendig, um einen kontinuierlichen Geschäftsbetrieb, keinen Reputationsverlust, die Kundenbindung und allgemein die Voraussetzungen für das Erreichen der Unternehmensziele zu gewährleisten.

Hinreichend ist hierbei das Schlüsselwort. Denn eine hundertprozentige Sicherheit ist auch mit noch so hohem Aufwand nicht zu erreichen. Eine extrem hohe Absicherung ist unverhältnismäßig teuer oder geschäftsverhindernd. Ein Beispiel sind hier nicht vernetzte Systeme. Diese sind natürlich einfacher abzusichern. Jedoch erfordern die meisten Geschäftsabläufe gerade im Zeitalter der Digitalisierung vernetzte Systeme. Ein Kappen der Vernetzung verhindert oder erschwert den Geschäftsbetrieb so stark, dass wahrscheinlich auf Dauer nicht wirtschaftlich gearbeitet werden kann. Der konkrete Schutzbedarf hängt hierbei stark vom unternehmensindividuell eingeschätzten Schutzbedarf der jeweiligen Unternehmenswerte, wie z. B. die Kritikalität von Informationen oder Systemen, ab.

Ein hinreichender Informationsschutz ist für die meisten Werte mit normalem Schutzbedarf schon mit einer Standardabsicherung (siehe Abschnitt 1.2.4) der IT mit verhältnismäßig geringen Mitteln zu erreichen. In Bild 1.2 finden Sie eine Prinzip-Darstellung für die Festlegung des optimalen Sicherheitsniveaus. In der Abbildung werden die Maßnahmenkosten und das Sicherheitsbedürfnis gemessen über das Schadensausmaß in Abhängigkeit vom Restrisiko dargestellt. Zudem finden Sie eine grobe Zuordnung zu Fehlerklassen nach dem CRISAM®-Modell (siehe [Hen13]) dargestellt.

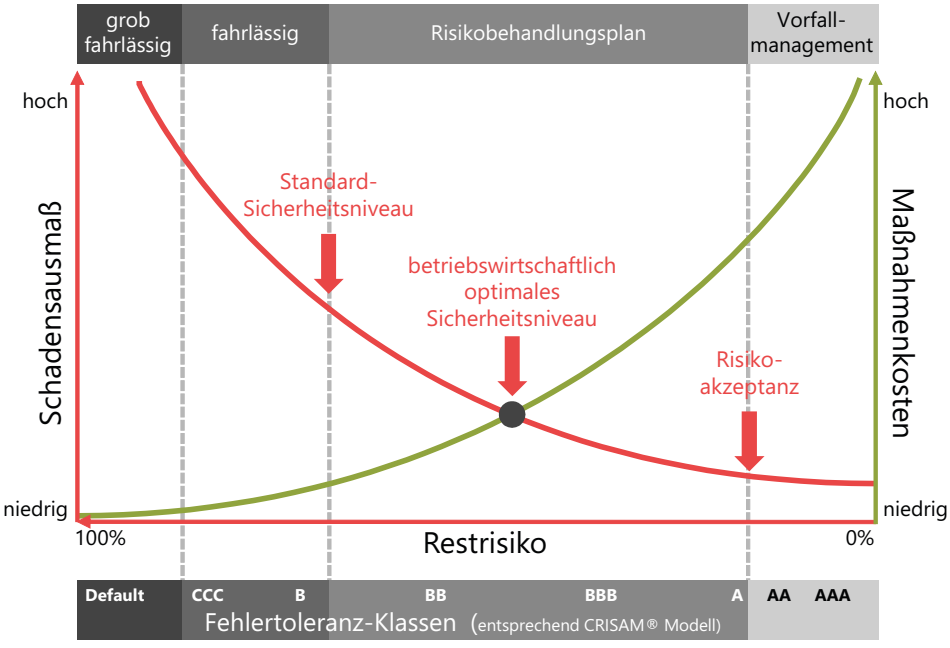

Bild 1.2 Optimales Sicherheitsniveau

Ohne Sicherheitsmaßnahmen und damit ohne Maßnahmenkosten wird ein extrem niedriges Schutzniveau erreicht und bestehende gesetzliche Anforderungen, wie z. B. aus der EU-DSGVO (siehe Abschnitt 1.2.5), werden nicht eingehalten. Die Organisation ist anfällig für Sicherheitsbedrohungen wie z. B. Kompromittierung von Webseiten, da entsprechende Vorkehrungen fehlen. Die Leitungsebene handelt grob fahrlässig und ist auch persönlich haftbar.

Das andere Extrem ist das Ziel, das Restrisiko von Sicherheitspannen weitestgehend auszuschließen. Jedoch ist der Versuch, alle möglichen Sicherheitsvorfälle vorherzusehen, sehr teuer; sowohl einmalig in der Erstellung als auch im kontinuierlichen Betrieb des Datenschutz- und Informationssicherheitsinstrumentariums. Für alle möglichen Konstellationen müssen organisatorische Maßnahmen, wie z. B. Richtlinien und Verfahrensanweisungen, oder technische Maßnahmen, wie z. B. automatisierte Forcierung der Einhaltung der Passwort-Richtlinie, vorgesehen werden.

Jedes Unternehmen muss sein vorhandenes Sicherheitsniveau ermitteln und sein angestrebtes Sicherheitsniveau, den „Risikoappetit", festlegen. Durch eine GAP-Analyse (siehe Abschnitt 3.1) können entsprechende Maßnahmen zur Schließung der Lücke ermittelt werden.

Das angestrebte Sicherheitsniveau sollte sich idealerweise nahe an dem in Bild 1.2 dargestellten betriebswirtschaftlich optimalen Sicherheitsniveau befinden. Über Standard-Absicherungsmaßnahmen z. B. aus dem IT-Grundschutz (siehe Abschnitt 1.2.4) kann für die Werte mit normalem Schutzbedarf ein Standard-Sicherheitsniveau auf dem „Stand der Technik" erreicht werden. Für die darüberhinausgehenden Risiken, insbesondere für die Werte mit erhöhtem Schutzbedarf, sollte ein Risikobehandlungsplan erstellt und umgesetzt werden. Jedoch sollte hierbei eine Abwägung zwischen Schadensausmaß und Maßnahmenkosten durchgeführt werden. Wenn die Maßnahmenkosten in keinem Verhältnis zum Schadensausmaß stehen, dann muss die oberste Leitungsebene über die Risikoübernahme entscheiden. Akzeptierte Risiken müssen bei ihrem Auftreten schnell erkannt und über eine Vorfall- und Notfallmanagement-Organisation gemanagt werden. So können auch bei akzeptierten Risiken die Schadensauswirkungen reduziert werden.

Beispiele für akzeptierte Risiken aus der Praxis sind:

- **IT-System-bedingte Einschränkungen**
  Die Umsetzung von Sicherheitsanforderungen bedarf einer erheblichen Veränderung von IT-Systemen, die nur mit großem Aufwand mittelfristig umgesetzt werden können.
  Beispiel: „unverzichtbare" Standardlösungen, die auf veralteten Patch-Level aufsetzen.
- **„Daten" sind wesentlich für den Geschäftserfolg**
  Beispiel: (Personenbezogene) Daten, wie z. B. Kundeninteressen oder -vorlieben werden für Marketing- und Vertriebsaktionen benötigt. Hier werden diese Daten zum „berechtigten" Interesse erklärt und nur auf Einzelaufforderung hin gelöscht oder anonymisiert.

Ein Hilfsmittel für die Abwägung zwischen Schadensausmaß und Maßnahmenkosten sowie die Risikoübernahme sind Risikoportfolios mit den Dimensionen Schadensauswirkung und Eintrittswahrscheinlichkeit. Den Bereichen im Portfolio kann eine entsprechende Risikobehandlungsstrategie, wie z. B. Risikoübernahme, zugeordnet werden. In Abschnitt 4.2 finden Sie Best-Practices zum Risikomanagement.

Die Abwägung zwischen Schadensausmaß und Maßnahmenkosten sowie der Risikoappetit müssen unternehmensindividuell festgelegt werden.

Normen, wie z. B. die ISO-2700X-Familie, geben sowohl Anforderungen als auch Empfehlungen für die umzusetzenden Sicherheitsmaßnahmen vor. Insbesondere der BSI-IT-Grundschutz (siehe Abschnitt 1.2.4) gibt zudem Umsetzungshinweise und Maßnahmenempfehlungen. Rund 80 % der bekannten Angriffe lassen sich mit den Standard-Schutzmaßnahmen des IT-Grundschutzes abwehren. Über technische und organisatorische Maßnahmen (TOMs) müssen sowohl die Sicherheit der für das Unternehmen schützenswerten Assets als auch insbesondere die personenbezogenen Daten abgedeckt werden. Die richtige Auswahl der Sicherheitsmaßnahmen für die hinreichende Absicherung und deren handhabbare Operationalisierung ist dabei erfolgsentscheidend.

Die Sicherheitsmaßnahmen zur Erreichung und Aufrechterhaltung einer störungsfreien Informationsverarbeitung müssen einerseits wirksam (effektiv) sein, um ein erforderliches Schutzniveau zu erreichen. Das Schutzniveau wird maßgeblich von der Kritikalität der zu schützenden Assets, wie z. B. Kundendaten, sowie von geltenden Gesetzen und Regularien bestimmt, die eingehalten werden müssen.

Andererseits müssen die Schutzmaßnahmen auch wirtschaftlich angemessen (effizient) sein und dürfen die Organisation nicht überfordern, d. h., die Möglichkeiten der Aufbau- und Ablauforganisation sowie weiterer Randbedingungen müssen berücksichtigt werden. Ein handhabbares und integriertes Instrumentarium ist notwendig, um sowohl die EU-Datenschutz-Grundverordnung (EU-DSGVO) als auch die Anforderungen der Informationssicherheit (u. a. BSI und ISO 27001) nachhaltig zu erfüllen.

Im Folgenden werden sowohl die Anforderungen der EU-Datenschutz-Grundverordnung als auch des Informationssicherheitsmanagements eingeführt.

1.2 Anforderungen an Informationssicherheit und Datenschutz

Zunehmende Cyber-Angriffe sowie gesetzliche und Compliance-Anforderungen, wie die EU-DSGVO, erfordern eine deutlich höhere Aufmerksamkeit in den Unternehmen für Informationssicherheits- und Datenschutzfragestellungen. Für die Festlegung eines integrierten Managementsystems für Informationssicherheit und Datenschutz müssen die Anforderungen verstanden und im Kontext des Unternehmens bewertet werden.

Die Anforderungen in der Informationssicherheit und im Datenschutz für Unternehmen sind vielfältig. Der Umgang mit Cyber-Security und die Erfüllung von gesetzlichen und Compliance-Anforderungen, wie die EU-DSGVO, sind hierfür Beispiele. Die immer weiter zunehmende Durchdringung von Informationstechnik in den Geschäftsprozessen, die steigende Bedrohungslage sowie gesetzliche und Compliance-Anforderungen führen zu Gefahren, wie

- Missbrauch oder Verlust von schützenswerten Daten,
- Verstöße gegen gesetzliche Bestimmungen oder unternehmensspezifische Richtlinien und Regeln mit zum Teil persönlicher Haftung und
- Behinderung oder sogar Unterbrechung der Geschäftstätigkeit durch z. B. nicht verfügbare Systeme.

Diese Bedrohungslage nimmt immer weiter zu. Gründe sind hierfür u. a.:

- Steigender Vernetzungsgrad: Menschen und IT-Systeme arbeiten zunehmend vernetzt (horizontal und vertikal siehe [Han18]) auch über Unternehmensgrenzen hinweg. Eine Sicherheitslücke kann nicht isoliert, sondern muss mit ihren Abhängigkeiten betrachtet werden.
- IT-Verbreitung und Durchdringung: Immer mehr Bereiche werden von der Informationstechnik durchdrungen. Beispiele sind Smart Home oder RFIDs zur Steuerung von Besucher- oder Warenströmen oder IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die verschiedenen IT-Komponenten kommunizieren miteinander zunehmend drahtlos und sind über das Internet lokalisierbar und steuerbar.
- Zunehmende und schnellere Ausnutzung von Schwachstellen: Die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen (z. B. Computerviren, Trojanische Pferde oder andere Angriffe) sinkt immer weiter. So muss zunehmend schneller die Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates, bekannt sein. Ein gut aufgestelltes Informationssicherheitsmanagement mit Warnsystem ist extrem wichtig, um schnell die richtigen Maßnahmen zu ergreifen.

Neben den zunehmenden Bedrohungen der Cyber-Security sind die steigenden Anforderungen aus Datenschutz und Informationssicherheit aufgrund der EU-Datenschutz-Grundverordnung (siehe [Voi18]) und in der Informationssicherheit entsprechend der individuellen Anforderungen oder gesetzlichen Vorgaben zu bewältigen.

1.2.1 Wesentliche Normen und gesetzliche Vorschriften

ISO/IEC 2700X

ISO/IEC 2700X ist die De-facto-Normenreihe für die Informationssicherheit. Die Sicherheitsstandards der ISO/IEC-2700X-Normenreihe zielen darauf ab, das Sicherheitsniveau in Unternehmen zu verbessern. Die ISO/IEC 2700X enthält Anforderungen und Maßnahmen für den Aufbau, Betrieb und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Die Anforderungen der Norm sind durch die Implementierung von für das Unternehmen passenden Sicherheitsmechanismen zu erfüllen. Siehe hierzu Abschnitt 1.2.3.

In Abschnitt 1.2.3 unter der Zwischenüberschrift „TISAX“ finden Sie Informationen über TISAX, einen Standard für externe Zulieferer und Dienstleister der Automobilindustrie. Dieser erweitert die ISO/IEC 27001 um branchenspezifische Anforderungen.

IT-Grundschutz (IT-GS)

Der IT-Grundschutz ist eine Methodik für einen praktikablen und aufwandsarmen sowie angemessenen Schutz von Informationen, um das Informationssicherheitsniveau in Unternehmen zu erhöhen. Er liefert einen De-facto-Standard für IT-Sicherheit. Er wird vom Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) (weiter-)entwickelt und in regelmäßigen Abständen mit den internationalen Normen wie ISO/IEC 27001 abgeglichen. Siehe hierzu Abschnitt 1.2.4.

IT-Sicherheitsgesetz (ITSG)

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, um den Gefahren beim Ausfall von kritischen Infrastrukturen zu begegnen

Am 3. Mai 2016 ist der erste Teil der BSI-KRITIS-Verordnung (§ 10 BSI-Gesetz) in Kraft getreten. Hier werden neben dem BSI-Gesetz auch das **Energiewirtschaftsgesetz (EnWG)**, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze geändert und ergänzt.

Im Vordergrund stehen Betreiber sogenannter „kritischer Infrastrukturen".

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Diese müssen innerhalb von vorgegebenen Fristen (zwei Jahre) Mindeststandards für IT-Sicherheitsmaßnahmen in den kritischen Branchen wie Energie oder Gesundheit entwickeln und nachweislich umsetzen. Zudem besteht bei Ausfällen oder IT-Sicherheitsvorfällen Meldepflicht gegenüber dem BSI sowie Informationspflichten gegenüber betroffenen Nutzern.

EU-DSGVO

Die europäische Datenschutz-Grundverordnung (EU-DSGVO) zur Vereinheitlichung des Datenschutzrechts in Europa

Schwerpunkt der EU-DSGVO liegt auf der Stärkung der Rechte der Betroffenen (Auskunftsrecht und Recht auf Vergessen) sowie Rechenschaftspflicht der Verantwortlichen zum Nachweis der Grundsätze für die Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, zeitliche Beschränkung, Integrität und Vertraulichkeit der Datenverarbeitung. Siehe hierzu Abschnitt 1.2.5.

DIN EN ISO 14001, Umweltmanagement für Umweltschutz

Die Bedeutung des Umweltmanagements wächst sowohl im öffentlichen Interesse als auch auf strategischer Ebene im Unternehmen zusehends. Eine Zertifizierung nach DIN EN ISO 14001 erfordert zwar ein Umweltmanagementsystem, hat aber das Potenzial für Ressourceneinsparungen und stärkt die Wettbewerbsfähigkeit des Unternehmens.

Jedoch gibt es natürlich gerade bei Verfahrens- und Arbeitsanweisungen Überlappungen zu einem ISMS. Diese sollten durch ein integriertes Managementsystem eliminiert werden.

ISO 20000 auf Basis der ITIL (siehe [Buc07])

Die Norm ISO/IEC 20000 wurde auf Basis der IT Infrastructure Library (ITIL) erarbeitet. Auf dieser Grundlage kann ein Service-Management-System zertifiziert werden. ITIL, vom britischen Office of Government Commerce (OGC) entwickelt, ist eine Ansammlung mehrerer Bücher zum Thema „IT-Service-Management". Das allgemeine Ziel von ITIL ist die Verbesserung der Qualität von IT-Dienstleistungen, der Kosteneffizienz und ein funktionierender IT-Betrieb. Informationssicherheit wird aus der operativen Perspektive der verschiedenen Services, wie Service Support und Service Delivery, heraus betrachtet. Service Support stellt alle operativen Prozesse bereit, die zur Behandlung von Service-Unterbrechungen und zur Durchführung von Änderungen dienen. Somit wird die Aufrechterhaltung der IT-Services garantiert.

Service Delivery stellt sicher, dass verbindliche Rahmenbedingungen für die operativen Prozesse bestehen. Es regelt die planerischen, vertraglichen und finanziellen Themen.

NIST (National Institute of Standards and Technology)

Die US-amerikanische Bundesbehörde NIST ist u. a. für die Entwicklung von Standards zuständig. Diese Standards sind für US-Behörden verpflichtend. Zudem veröffentlicht das NIST in der Reihe Special Publication 800 („NIST SP 800"-Serie) regelmäßig Dokumente zu Informationssicherheit-Themen, wie Kryptografie oder Cloud-Computing. Die Standards und die Dokumente haben international einen weitreichenden Einfluss auf die Gestaltung der Informationssicherheit. Insbesondere das Dokument „NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations" stellt für den Bereich Sicherheitsmanagement eine große Zahl an Kontrollen für den Schutz von Informationsverbünden zusammen. Die Kontrollen sind nach zusammengehörigen Bereichen, wie z. B. Schulung und Sensibilisierung, Berechtigungsmanagement oder Infrastruktursicherheit, gegliedert.

PCI DSS (Payment Card Industry Data Security Standard) des PCI Security Standards Council

PCI DSS formuliert Sicherheitsanforderungen an die Abwicklung von Kreditkartentransaktionen, d. h. wenn eine Zahlungskartennummer, eine PAN (Primary Account Number), gespeichert, verarbeitet oder übermittelt wird. PCI DSS bezieht sich hierbei auf Karteninhaberdaten, die in Verbindung mit der PAN gespeichert werden. Dies sind laut PCI DSS der Name des Karteninhabers, der Servicecode und das Ablaufdatum der Karte.

Vertrauliche Authentisierungsdaten, wie z. B. die Daten des Magnetstreifens einer Debit- oder Kreditkarte, PINs und Kartenprüfwerte wie z. B. der CVC2 (Card Validation Code Version 2), haben einen sehr hohen Schutzbedarf. Diese dürfen nach der Authentisierung nicht in den Händlersystemen gespeichert werden.

Die Anforderungen von PCI DSS müssen von allen Unternehmen umgesetzt werden, die Karteninhaberdaten von Kreditkarten speichern, verarbeiten oder übertragen. Beispiele sind Händler, die Kreditkartenzahlungen akzeptieren, Hosting-Anbieter oder Dienstleister, die diese im Auftrag weiterverarbeiten, sowie alle Dienstanbieter, die auf Karteninhaberdaten zugreifen können.

Die erfolgreiche Umsetzung muss überprüft und das Ergebnis registriert werden. Je nach Art und Größe der Institution, der Anzahl der Transaktionen und der Führung der Karteninhaberdaten, gibt es hierzu verschiedene Möglichkeiten von Zertifizierungen oder Selbstzertifizierungen. Wenn eine Zertifizierung nicht zwingend notwendig ist, kann durch jährlich auszufüllende Selbstbeurteilungsfragebögen die Konformität zum PCI-Regelwerk mitgeteilt werden.

Anforderungen des PCI DSS sind hierbei insbesondere:

- Erstellung und Wartung eines sicheren Netzwerks mit Sicherheitszonen (Firewall) sowie regelmäßige Überwachung und regelmäßiges Testen von Netzwerken inklusive Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- Ändern der vom Anbieter festgelegten Standardeinstellung für Systemkennwörter und andere Sicherheitsparameter

- Schutz von Karteninhaberdaten sowie Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
- Verwendung und regelmäßige Aktualisierung von Antivirussoftware
- Vorgabe und Einhaltung von Richtlinien für eine sichere Systementwicklung (siehe Abschnitt 2.2)
- Implementierung starker Zugriffsschutz- und Kontrollmaßnahmen mit u. a. Zuweisung einer eindeutigen ID für jede Person mit Zugriff sowie Beschränkung des physischen Zugriffs auf Karteninhaberdaten

KonTraG, das Gesetz zur Kontrolle und Transparenz im Unternehmen

Wesentlich sind hier insbesondere die Verpflichtung zur Einrichtung eines Kontrollsystems mit verbindlichen Regeln im Unternehmen und ein unternehmensweites Risikomanagement, um für den Fortbestand des Unternehmens gefährdende Entwicklungen früh zu erkennen und gegenzusteuern.

MaRisk/BAIT

In den bankaufsichtlichen Anforderungen an die IT (BAIT) werden die in MaRisk enthaltenen Anforderungen an die IT in wesentlichen Punkten – auch im Kontext der Informationssicherheit – konkretisiert. Dies beinhaltet auch die Forderung nach einem Informationssicherheitsbeauftragten.

Die Anforderungen der BAIT bestehen aus folgenden Kapiteln:

- IT-Strategie: Wesentliche Anforderungen an die Nachhaltigkeit der IT-Strategie in Konsistenz mit der Geschäftsstrategie (Business-Alignment), strategische Entwicklung der IT inkl. der Auslagerungsstrategie, Verankerung der Informationssicherheit in der IT, Entwicklung einer IT-Architektur, Notfallmanagement, Umgang mit individualer, fachbezogener IT (IDV)

  Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.
- IT-Governance: Steuerung und Überwachung des IT-Betriebs und der Weiterentwicklung der Systeme, qualitative und angemessene Personalausstattung der IT, Trennung von Betrieb und Entwicklung
- Informationsrisikomanagement: Einrichtung eines Informationsrisikomanagements und Einbindung aller relevanten Bereiche, Festlegung der Methodik für Schutzbedarfsermittlung
- Informationssicherheitsmanagement: Etablierung eines Informationssicherheitsmanagements analog ISO27001 mit ISB/CISO-Rolle und u. a. Berichterstattung und Incident- und Vorfallmanagement
- Benutzerberechtigungsmanagement: Berechtigungskonzept mit Sicherstellung des Minimalprinzips und Funktionstrennung sowie SoD (Segregation of Duties), Umgang mit technischen Berechtigungen und Accounts, Steuerungs- und Überprüfungsprozesse zu Berechtigungen (Re-Zertifizierung, Attestierung, Reconciliation), Umgang mit und Kontrolle von privilegierten Benutzern sowie technische und organisatorische Maßnahmen zum Schutz des Umgehungstatbestands