2.1 Erfüllung von gesetzlichen und Compliance-Anforderungen

Neben den zunehmenden Bedrohungen der Cyber-Security sind die steigenden Anforderungen aus Datenschutz und Informationssicherheit aufgrund der **EU-Datenschutz-Grundverordnung** (siehe [4]) und in der Informationssicherheit entsprechend der individuellen Anforderungen oder gesetzlichen Vorgaben zu bewältigen.

Wesentliche gesetzliche Vorschriften im Kontext Informationssicherheit und Datenschutz sind:

- **EU-DSGVO:** Die europäische Datenschutz-Grundverordnung (EU-DSGVO) zur Vereinheitlichung des Datenschutzrechtes in Europa. Siehe hierzu Abschnitt Abschn. 2.4.
- **IT-Grundschutz:** Der IT-Grundschutz ist eine Methodik für einen praktikablen und aufwandsarmen 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 (BSI) (weiter-)entwickelt und in regelmäßigen Abständen mit den internationalen Normen wie ISO/IEC 27001 abgeglichen. Siehe hierzu Abschn. 2.3.
- **IT-Sicherheitsgesetz:** Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme im Kontext von sogenannter „kritischer Infrastrukturen".
- **PCI DSS** (Payment Card Industry Data Security Standard) des PCI Security Standards Council: PCI DSS formuliert Sicherheitsanforderungen an die Abwicklung von Kreditkartentransaktionen.
- **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.
- **GoBD:** Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff durch die Finanzverwaltungen und Grundsätze ordnungsgemäßer DV gestützter Buchführungssysteme (GoBS) und Umsetzung dieser über ein internes Kontrollsystem (IKS).
- **HGB** (Handelsgesetzbuch): Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit. Dies umfasst auch bestimmte Aufbewahrungsfristen (Archivierungspflicht) für Geschäftsdokumente. Für die

Archivierung werden zudem gewisse Anforderungen gestellt, wie die unveränderte (originäre) und unveränderbare Speicherung, die Möglichkeit der Anzeige und Ausdrucks wie im Original, Filtermöglichkeiten zur zeitnahen Suche von Dokumenten (Indizierung, Tagging), Protokollierung aller Aktionen im Archiv zur Nachvollziehbarkeit sowie die Anforderung, dass Migrationen auf neue u. a. Plattformen, Medien ohne inhaltliche Informationsverluste erfolgen müssen.

Es ist davon auszugehen, dass sich Gesetze im Kontext Informationssicherheit aufgrund der zunehmenden Bedrohungslage weiter verschärfen oder neue hinzukommen.

Die Unternehmensführung steht bei den gesetzlichen und Compliance-Anforderungen in der Pflicht, für ausreichende Verfügbarkeit der IT und Daten, Datenschutz, Informationssicherheit und z. B. Einhaltung der Aufbewahrungspflichten zu sorgen. Eine Missachtung der Vorschriften kann zu empfindlichen Bußgeldern oder Strafen bis hin zur Existenzbedrohung führen. Daher muss sich jedes Unternehmen damit beschäftigen und sich folgende Fragen stellen:

- Welche Anforderungen aus welchen Normen und Gesetzen sind für das Unternehmen relevant? Welche sind verpflichtend?
- Welche Geschäftsprozesse sind betroffen und welche technischen und organisatorischen Maßnahmen sind notwendig, um IT-Compliance sicherzustellen? Welche sind bereits eingeführt? Welche müssen noch eingeführt werden?
- Gibt es bereits ein übergreifendes Risikomanagementsystem? Sind hier die Risiken aus Informationssicherheit und Datenschutz einbezogen?

Ein integriertes Managementsystem für Datenschutz und Informationssicherheit beantwortet alle diese Fragen und sichert die Unternehmensführung ab. Siehe hierzu Abschn. 2.4.

Im Folgenden schauen wir uns die ISO/IEC 27001, IT-Grundschutz und EU-DSGVO aufgrund deren großen Bedeutung für Unternehmen an.

2.2 ISO/IEC 27001

Die Norm ISO/IEC 27001 hat sich international als Standard für Informationssicherheit in Unternehmen und Behörden etabliert. Sie ist Teil der ISO/IEC 2700X-Normenreihe und wurde 2005 von den internationalen Normungsorganisationen ISO und IEC als ISO-Norm veröffentlicht. Sie basiert auf dem

britischen Standard BS 7799-2. Die letzte Revision dieser Norm wurde im Juni 2017 veröffentlicht. Die Norm ISO/IEC 27001 legt den internationalen Standard für ein Informationssicherheitsmanagementsystem *(ISMS)* fest.

Die ISO/IEC 27001 enthält Anforderungen und Maßnahmen für den Aufbau, Betrieb und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS), das an die Gegebenheiten der jeweiligen Organisation angepasst werden kann, um individuelle Besonderheiten zu berücksichtigen. Die Anforderungen der Norm sind durch die Implementierung für das Unternehmen adäquate Sicherheitsmechanismen zu erfüllen.

Die ISO/IEC 27001 ist Teil der ISO/IEC 2700X-Normenreihe (siehe Abb. 2.1). Die Sicherheitsstandards zielen darauf ab, in anwendenden Unternehmen oder Behörden das Sicherheitsniveau zu verbessern. Wesentliche Bestandteile der ISO/IEC 2700X-Normenreihe sind:

- **ISO/IEC 27000** gibt einen allgemeinen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Standards der ISO-2700x-Familie. Hier finden Sie außerdem die grundlegenden Prinzipien, Konzepte, Begriffe und Definitionen für ISMS.
- **ISO/IEC 27001** ist der zentrale und einzige zertifizierbare Standard der ISO 27000-Normenreihe. Er besteht aus 11 Abschnitten und dem Anhang A. Die Abschnitte 0 bis 3 sind allgemeine Empfehlungen zur Einführung, dem Betrieb und der Verbesserung des ISMS. Die Abschnitte 4 bis 10 sind

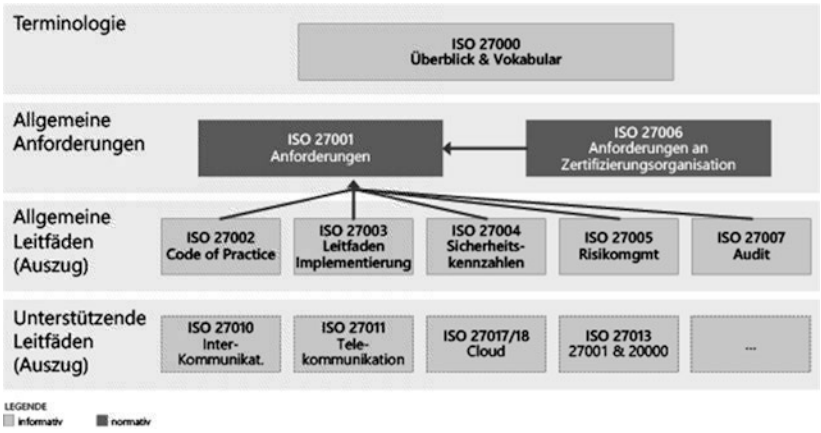

Abb. 2.1 ISO/IEC 2700X Normen-Familie (siehe [6])

obligatorisch (siehe Abb. 2.2), d. h. alle darin enthaltenen Anforderungen müssen umgesetzt werden. Der Anhang A enthält eine Auflistung von 114 Kontrollen, geordnet in 14 Abschnitten (Abschn. A.5 bis A.18) (siehe [16]) ohne Hilfe für die praktische Umsetzung. Welche Kontrollen relevant und anwendbar sind, wird in der Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) festgelegt. Die Abschnitte in Anhang A sind in Abb. 3.2 dargestellt.

- **ISO/IEC 27002 (Code of practice)** ist ein Rahmenwerk für Informationssicherheitsmanagement und beinhaltet Informationssicherheitsleitfäden.
- **ISO/IEC 27003** enthält Anleitungen zur Umsetzung eines ISMS entsprechend ISO/IEC 27001.
- **ISO/IEC 27004** beinhaltet Messmethoden und Metriken der Informationssicherheit.
- **ISO/IEC 27005** enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Hierbei wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben.
- **ISO/IEC 27006** spezifiziert Anforderungen an die Akkreditierung von Zertifizierungsstellen für ISMS und behandelt auch Spezifika der ISMS-Zertifizierungsprozesse.

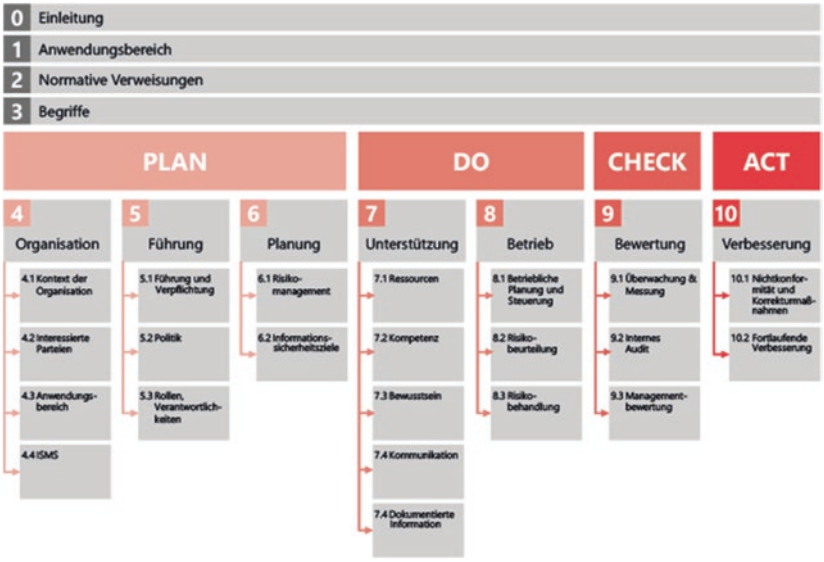

Abb. 2.2 ISO/IEC 27001 Abschnitte (siehe [6])

- **ISO/IEC 27010** dient als Leitfaden für die intersektionale und interorganisatorische Kommunikation.
- **ISO/IEC 27011** liefert einen Leitfaden für ISMS im Telekommunikationsbereich.
- **ISO/IEC 27013** dient als Leitfaden für die integrierte Implementierung eines ISMS nach ISO/IEC 27001 und eines IT-Servicemanagements nach ISO 20000-1.
- **ISO/IEC 27017** erweitert ISO/IEC 27002 um eine Reihe von „Good Practices" für eine sichere Nutzung bzw. Implementierung von Cloud-Diensten und gibt Anforderungen für das Themenfeld „Cloud-Computing" vor.
- **ISO/IEC 27018** beschreibt Umsetzungsempfehlungen für die sichere Verarbeitung von personenbezogenen Daten durch Cloud-Dienste.

Darüber hinaus gibt es weitere Bestandteile, wie z. B. ISO/IEC 22301, die Anforderungen für das betriebliche Kontinuitätsmanagement definiert. Für weitere Informationen sei auf die offizielle Seite der ISO/IEC (siehe https://www.iso.org/standard) hingewiesen.

Wichtig ist insbesondere die **Informationssicherheitsleitlinie** und die Definition des **Anwendungsbereiches** (auch Geltungsbereich genannt), um den Umfang und die Grenzen des ISMS festzulegen. Dabei sind das Geschäftsmodell, die Unternehmensorganisation und Unternehmenskultur sowie das Business Eco-System (mit u. a. Partnern auf den horizontalen und vertikalen Wertschöpfungsketten im und außerhalb des Unternehmens) zu berücksichtigen.

Alle relevanten Assets im Geltungsbereich einer Organisation müssen inventarisiert werden. Wesentliche Aspekte sind hier neben dem Namen, die Lage bzw. der Standort, der festgelegte Wert sowie der Asset-Owner. Der Asset-Owner ist der primäre Ansprechpartner für alle Sicherheitsaspekte der zugeordneten Assets. Gleichartige Assets sollten als Eintrag in der Inventarliste zusammengefasst werden, um den Aufwand für das Asset-Management zu beschränken. Beispiele hierfür sind Grundstücke, Gebäude oder Datenkategorien, wie z. B. Bewerberdaten.

Ausgangspunkt für die Inventarisierung bilden vorhandene Listen, wie z. B. Listen der Anlagenbuchhaltung, der Einkaufsabteilung oder aber eine Unternehmensarchitektur-Datenbasis beziehungsweise eine Change Management Datenbank (CMDB) für IT-Assets und die Verknüpfungen mit dem Business (siehe Kap. 4). Parallel zur Inventarisierung müssen Pflegeprozesse festgelegt und in der Organisation verankert werden, sodass die Inventarliste nicht veraltet.