2 Einführung in die Informationssicherheit

Was ist Informationssicherheit?

Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer gespeichert sein. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Die klassischen Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender beziehen in ihre Betrachtungen weitere Grundwerte ein. Dies kann je nach den individuellen Anwendungsfällen auch sehr hilfreich sein. Weitere generische Oberbegriffe der Informationssicherheit sind beispielsweise Authentizität, Verbindlichkeit, Zuverlässigkeit, Resilienz und Nichtabstreitbarkeit.

Die Sicherheit von Informationen wird nicht nur durch vorsätzliche Handlungen bedroht (z. B. Schadsoftware, Abhören der Kommunikation, Diebstahl von Rechnern). Die folgenden Beispiele verdeutlichen dies:

- Durch höhere Gewalt (z. B. Feuer, Wasser, Sturm, Erdbeben) werden Datenträger und IT-Systeme in Mitleidenschaft gezogen oder der Zugang zum Rechenzentrum versperrt. Dokumente, IT-Systeme oder Dienste stehen nicht mehr wie gewünscht zur Verfügung.
- Nach einem missglückten Software-Update funktionieren Anwendungen nicht mehr oder Daten werden unbemerkt verändert.
- Ein wichtiger Geschäftsprozess verzögert sich, weil die einzigen Mitarbeiter, die mit der Anwendungssoftware vertraut sind, erkrankt sind.
- Vertrauliche Informationen werden versehentlich von einem Mitarbeiter an Unbefugte weitergegeben, weil Dokumente oder Dateien nicht als „vertraulich" gekennzeichnet waren.

Wortwahl: IT-Sicherheit versus Informationssicherheit und Cyber-Sicherheit

Da die elektronische Verarbeitung von Informationen in nahezu allen Lebensbereichen allgegenwärtig ist, scheint die Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, nicht mehr zeitgemäß. Der Begriff der Informationssicherheit statt IT-Sicherheit ist daher umfassender und besser geeignet. Es sollte jedoch beachtet werden, dass in der (Forschungs-)Literatur oftmals noch der Begriff „IT-Sicherheit" verwendet wird (unter anderem, weil dieser kürzer ist), auch wenn häufig „Informationssicherheit" gemeint ist. Das Aktionsfeld der klassischen IT-Sicherheit wird unter dem Begriff „Cyber-Sicherheit" auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

2.1 Überblick über Normen und Standards zur Informationssicherheit

Im Bereich der Informationssicherheit haben sich verschiedene Normen und Standards entwickelt, bei denen teilweise andere Zielgruppen oder Themenbereiche im Vordergrund stehen. Der Einsatz von Sicherheitsnormen und -standards in Unternehmen oder Behörden verbessert nicht nur das Sicherheitsniveau, er erleichtert auch die Abstimmung zwischen verschiedenen Institutionen darüber, wel-

che Sicherheitsmaßnahmen in welcher Form umzusetzen sind. Der folgende Überblick zeigt die Ausrichtungen der wichtigsten Normen und Standards.

2.1.1 ISO-Normen zur Informationssicherheit

Innerhalb der internationalen Normungsorganisationen ISO und IEC werden die Normen zur Informationssicherheit in der 2700x-Reihe zusammengeführt, die stetig wächst. International werden diese Normen als Standards bezeichnet. Ein Teil dieser internationalen Standards liegt auch in Übersetzungen als DIN-Normen vor.

Die wesentlichen Normen der ISO-/IEC-2700x-Reihe sind:

ISO/IEC 27000 *(Information security management systems – Overview and vocabulary)*
Diese Norm gibt einen Überblick über Managementsysteme für Informationssicherheit (ISMS) und über die Zusammenhänge der verschiedenen Normen der ISO-/IEC-2700x-Familie. Hier finden sich außerdem die grundlegenden Begriffe und Definitionen für ISMS.

ISO/IEC 27001 *(Information security management systems – Requirements)*
Die ISO-Norm 27001 ist eine internationale Norm zum Management von Informationssicherheit, die auch eine Zertifizierung ermöglicht. ISO/IEC 27001 gibt auf ca. neun Seiten normative Vorgaben zur Einführung, dem Betrieb und der Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems. In einem normativen Anhang werden mehr als 100 Maßnahmen (Controls) aufgeführt, die unter Berücksichtigung der relevanten Risiken ausgewählt werden sollten. Die Leser erhalten allerdings keine Hilfe im Hinblick auf die Umsetzung in der Praxis.

Bisher orientierten sich die Anforderungen der ISO/IEC 27001 an einem Lebenszyklusmodell, das nach der englischen Benennung der einzelnen Phasen („Plan", „Do", „Check", „Act") auch als PDCA-Zyklus bezeichnet wird. Um mit dem Annex SL (Leitfaden für die Entwicklung und Überarbeitung von ISO-Normen für Managementsysteme) kompatibel zu sein, ist bei der Überarbeitung der ISO/IEC 27001 auf eine explizite Nennung des PDCA-Zyklus verzichtet worden. Dadurch soll deutlich gemacht werden, dass die Reihenfolge der einzelnen Anforderungen in der Norm keinen Rückschluss auf deren jeweilige Wichtigkeit oder die Reihenfolge ihrer Umsetzung gibt. Alle Aktivitäten zum Aufbau und Betrieb eines ISMS lassen sich jedoch weiterhin nach dem PDCA-Zyklus durchführen.

ISO/IEC 27002 *(Code of practice for information security controls)*
Diese Norm unterstützt bei der Auswahl und Umsetzung der in der ISO/IEC 27001 beschriebenen Maßnahmen, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Institution zu verankern. Die dafür geeigneten Sicherheitsmaßnahmen werden auf den 90 Seiten der Norm ISO/IEC 27002 beschrieben. Die Empfehlungen sind in erster Linie für die Management-Ebene gedacht und enthalten daher kaum konkrete technische Hinweise. Die Umsetzung der Sicherheitsempfehlungen der ISO/IEC 27002 ist eine von vielen Möglichkeiten, die Anforderungen der ISO-Norm 27001 zu erfüllen.

ISO/IEC 27004 *(Monitoring, measurement, analysis and evaluation)*
Die ISO-Norm 27004 behandelt die Bewertung der Umsetzung und der Wirksamkeit eines ISMS anhand verschiedener Kenngrößen.

ISO/IEC 27005 *(Information security risk management)*
Diese Norm enthält Rahmenempfehlungen zum Risikomanagement für Informationssicherheit. Unter anderem unterstützt sie bei der Umsetzung der Anforderungen aus ISO/IEC 27001. Hierbei wird allerdings keine spezifische Methode für das Risikomanagement vorgegeben. Diese Norm basiert wiederum wesentlich auf der Norm ISO/IEC 31000 *Risk management – Principles and guidelines on im-*

plementation (siehe [31000]). In der unterstützenden Norm ISO/IEC 31010 *Risk assessment techniques* (siehe [31010]) wird beschrieben, wie die Risikobeurteilung in ein Risikomanagementsystem integriert werden kann und wie Risiken identifiziert, eingeschätzt, bewertet und behandelt werden können. Der Anhang B von ISO 31010 gibt einen ausführlichen Überblick über Methoden zur Risikobeurteilung; hier werden insgesamt 31 verschiedene Methoden aufgeführt.

ISO/IEC 27006 *(Requirements for bodies providing audit and certification of information security management systems)*
Die ISO-Norm 27006 spezifiziert Anforderungen an die Akkreditierung von Zertifizierungsstellen für ISMS und behandelt auch Spezifika der ISMS-Zertifizierungsprozesse.

ISO/IEC 27009 *(Sector-specific application of ISO/IEC 27001 – Requirements)*
Die ISO-Norm 27009 beschreibt, wie sektorspezifische Erweiterungen (z. B. aus den Bereichen Energie, Cloud Computing, Finanzen) zukünftig in ein ISMS nach ISO/IEC 27001 einfließen und dort als Anforderungen berücksichtigt werden können. Dazu sollen einzelne Maßnahmen aus dem Anhang der ISO/IEC 27001 erweitert bzw. ergänzt werden.

Sektorspezifische Normen *(ISO/IEC 27010 bis ISO/IEC 27019)*
Viele sektorspezifische Normen (z. B. ISO/IEC 27019 für den Energiesektor) werden basierend auf der ISO/IEC 27009 entwickelt.

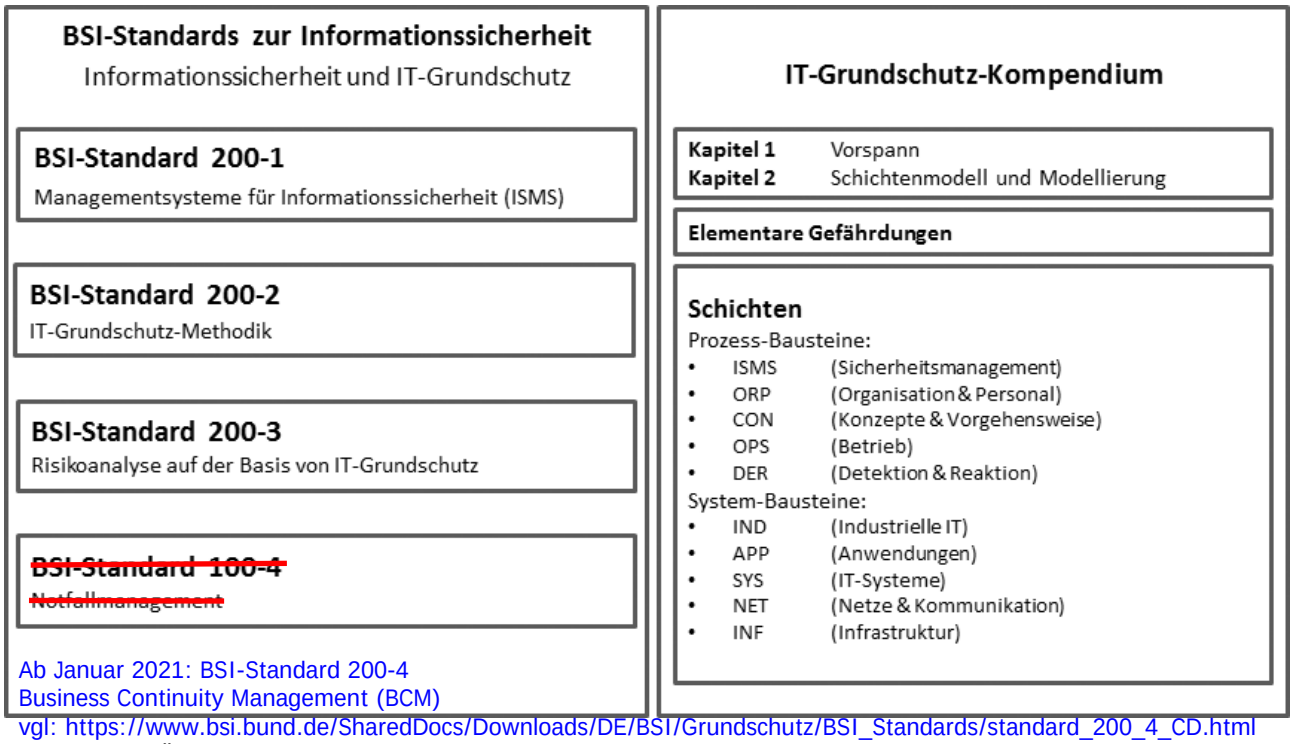
Weitere Normen der ISO-2700x-Reihe
Die Normenreihe ISO 2700 x wird voraussichtlich langfristig aus den ISO-Normen 27000 bis 271xx bestehen. Alle Normen dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO/IEC 27001. Die weiteren Normen sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO/IEC 27001 beitragen. Diese beschäftigen sich beispielsweise mit der Umsetzung der ISO/IEC 27001 in der Praxis und mit Methoden zur Kontinuität von Geschäftsprozessen.

2.1.2 Ausgewählte BSI-Publikationen und Standards zur Informationssicherheit

IT-Grundschutz

Die Methodik des BSI zur Informationssicherheit ist seit 1994 der IT-Grundschutz. Der IT-Grundschutz ist eine ganzheitliche Vorgehensweise, um für Institutionen aller Arten und Größen eine angemessene Informationssicherheit umzusetzen. Mit der Kombination aus den IT-Grundschutz-Vorgehensweisen zur Basis-, Standard- und Kern-Absicherung, die im BSI-Standard 200-2 *IT-Grundschutz-Methodik* beschrieben sind, und dem IT-Grundschutz-Kompendium, in dem für die verschiedensten Einsatzumgebungen Sicherheitsanforderungen enthalten sind, bietet der IT-Grundschutz ein effizientes und effektives Handwerkszeug, um adäquate Maßnahmen zum sicheren Umgang mit Informationen für eine Institution auszuwählen und anzupassen. Der IT-Grundschutz ist von Anfang an darauf ausgelegt worden, dass er von den Anwendern modular an verschiedene Einsatzumgebungen angepasst werden kann. Dazu wird er vom BSI auch kontinuierlich aktualisiert und erweitert.

Politische Rahmenbedingungen wie das IT-Sicherheitsgesetz, das sehr dynamische Themengebiet der Informationssicherheit sowie die zunehmend professionelleren Cyberangriffe haben den Ausschlag dafür gegeben, den IT-Grundschutz erneut grundlegend zu modernisieren. Mit den vorliegenden BSI-Standards 200-1 bis 200-3 sind hieraus weitere Vorgehensweisen hervorgegangen, die einen abgestuften Einstieg in ein Sicherheitsmanagement ermöglichen. Ergänzt werden diese durch IT-Grundschutz-Bausteine, die im IT-Grundschutz-Kompendium zusammengefasst sind. Die Abbildung 1 veranschaulicht die Gliederung der IT-Grundschutz-Dokumente.



vgl: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.html

Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Das IT-Grundschutz-Kompendium ist modular aufgebaut und enthält Prozess- und Systembausteine für typische Geschäftsprozesse, Anwendungen, Systeme, Kommunikationsverbindungen und Räume. Die auf die Rahmenbedingungen der eigenen Institution zutreffenden Bausteine können nach Bedarf eingesetzt werden. Im IT-Grundschutz werden alle Bereiche betrachtet, die in Institutionen vorzufinden sind. Dazu gehören neben Organisation und Personal auch IT-Betrieb, aber auch Produktion und Fertigung mit Industrial Control Systems (ICS) ebenso wie Komponenten aus dem Bereich Internet of Things (IoT).

Jeder Baustein enthält eine kurze Beschreibung der Thematik und des Ziels, das mit der Umsetzung des Bausteins erreicht werden soll, sowie eine Abgrenzung zu anderen Bausteinen, die einen ähnlichen thematischen Bezug haben. Des Weiteren gibt es einen Überblick über die spezifischen Gefährdungen des betrachteten Themengebietes. Die Sicherheitsanforderungen für die Basis-, Standard- und Kern-Absicherung bilden den Schwerpunkt eines jeden Bausteins.

Zusätzlich kann es zu den Bausteinen des IT-Grundschutz-Kompendiums Umsetzungshinweise geben. Diese beschreiben, wie die Anforderungen der Bausteine in der Praxis erfüllt werden können, und enthalten dafür passende Sicherheitsmaßnahmen mit detaillierten Beschreibungen, die auf dem Erfahrungsschatz und den Best Practices des BSI und von IT-Grundschutz-Anwendern basieren.

Die Bausteine des IT-Grundschutz-Kompendiums und die Umsetzungshinweise werden regelmäßig aktualisiert und erweitert. Daher werden sie als Printversion und zudem auch noch zusätzlich kostenfrei im Internet veröffentlicht.

BSI-Standardreihe zur Informationssicherheit: Thema IS-Management

200-1 Managementsysteme für Informationssicherheit (ISMS)

Der vorliegende Standard definiert allgemeine Anforderungen an ein ISMS. Darin wird beschrieben, mit welchen Methoden Informationssicherheit in einer Institution generell initiiert, gesteuert und überwacht werden kann. Der BSI-Standard 200-1 ist vollständig kompatibel mit der Norm ISO/IEC 27001 und berücksichtigt zudem die in der ISO-Norm ISO/IEC 27000 definierten Begriffe sowie die Empfehlungen der ISO-Norm ISO/IEC 27002. Er bietet den Lesern eine leicht verständliche und systematische Anleitung, unabhängig davon, mit welcher Methode eine Institution die Anforderungen an ein ISMS umsetzen möchte.

Das BSI stellt den Inhalt der oben genannten ISO-Normen in einem eigenen BSI-Standard dar, um einige Themen ausführlicher beschreiben zu können und so eine didaktisch bessere Darstellung der Inhalte zu ermöglichen. Zudem wurde die Gliederung so gestaltet, dass sie mit der IT-Grundschutz-Vorgehensweise kompatibel ist.

200-2 IT-Grundschutz-Methodik

Die IT-Grundschutz-Methodik beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Organisationsstruktur für Informationssicherheit sind dabei wichtige Themen. Die IT-Grundschutz-Methodik geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt werden kann, wie angemessene Sicherheitsanforderungen ausgewählt werden können und was bei der Umsetzung des Sicherheitskonzepts zu beachten ist. Auch die Frage, wie die Informationssicherheit im laufenden Betrieb aufrechterhalten und kontinuierlich verbessert werden kann, wird ausführlich beantwortet.

Um einen abgestuften Einstieg in ein Sicherheitsmanagement zu ermöglichen, werden je nach angestrebtem Sicherheitsniveau und zu sichernden Informationen unterschiedliche Vorgehensweisen angeboten. Abhängig davon, welche Ansätze zur Informationssicherheit bereits innerhalb der Institution verfolgt werden, kann es zweckmäßig sein, zunächst von der „vollständigen" IT-Grundschutz-Vorgehensweise („Standard-Absicherung") abzuweichen. Beispielsweise kann sich eine Institution als Ziel setzen, zunächst möglichst flächendeckend alle Basis-Anforderungen umzusetzen („Basis-Absicherung"), um schnellstmöglich die größten Risiken zu senken, bevor die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Ein anderer denkbarer Ansatz ist, sich zunächst auf den Schutz der essenziellen Werte der Institution zu konzentrieren („Kern-Absicherung").

Der IT-Grundschutz interpretiert ausgehend vom BSI-Standard 200-2 die allgemein gehaltenen Anforderungen bzw. Sicherheitsmaßnahmen der zuvor genannten ISO-Normen 27001 sowie 27002 und hilft den Anwendern bei der Umsetzung in der Praxis mit ausführlichen Hinweisen, Hintergrundinformationen und Beispielen. Die Bausteine des IT-Grundschutz-Kompendiums erklären, was gemacht werden sollte, die Umsetzungshinweise geben sehr konkrete Hinweise, wie eine Anforderung (auch auf technischer Ebene) erfüllt werden kann. Ein Vorgehen nach IT-Grundschutz ist somit eine erprobte und effiziente Möglichkeit, allen Anforderungen der oben genannten ISO-Normen nachzukommen bzw. gerecht zu werden.

200-3 Risikoanalyse auf der Basis von IT-Grundschutz

Das BSI hat eine Methodik zur Risikoanalyse auf der Basis des IT-Grundschutzes erarbeitet. Der BSI-Standard 200-3 beschreibt, wie aufbauend auf der IT-Grundschutz-Vorgehensweise eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Diese basiert auf den elementaren Gefährdungen, die im IT-Grundschutz-Kompendium beschrieben sind und auf deren Basis auch die IT-Grundschutz-Bausteine erstellt werden. Diese

Vorgehensweise bietet sich an, wenn Unternehmen oder Behörden bereits erfolgreich mit dem IT-Grundschutz arbeiten und möglichst nahtlos eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten.

100-4 Notfallmanagement
Im BSI-Standard 100-4 wird eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten Notfallmanagements erläutert. Die hier beschriebene Methodik basiert dabei auf der in BSI-Standard 200-2 beschriebenen IT-Grundschutz-Vorgehensweise „Standard-Absicherung" und ergänzt diese sinnvoll.

Leitfaden für die IS-Revision auf Basis von IT-Grundschutz

Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus innerhalb einer Institution. Hierzu hat das BSI mit dem *Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* (siehe [BSIR]) ein Verfahren entwickelt, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können.

2.1.3 Weitere Sicherheitsstandards

COBIT 5

COBIT 5 sieht die IT als wesentliche Grundlage einer Institution zur Erreichung der Geschäftsziele und fordert, dass die Ziele aus der Geschäftsstrategie in die Ziele der IT einfließen und die gelieferten Services den Qualitätsanforderungen der Geschäftsprozesse genügen. Ebenso wie ITIL setzt COBIT 5 auf zielgerichtete, optimierte IT-Prozesse. COBIT 5 führt den Aspekt des Prozesspotenzials ein, in dem eine Aussage darüber getroffen wird, inwieweit eine Institution dazu in der Lage ist, die geforderten Ziele verlässlich und nachhaltig zu erreichen. Aus der Gesamtbetrachtung der Reife aller 37 Prozessgebiete, die in fünf Domänen unterteilt sind, kann die Professionalität der unterstützenden IT-Prozesse abgeleitet werden. Die COBIT-Dokumente werden von der Information Systems Audit and Control Association (ISACA) herausgegeben. Bei der Entwicklung von COBIT orientierten sich die Autoren an bestehenden Normen und Standards zum Thema „Sicherheitsmanagement", insbesondere an der Norm ISO/IEC 27002.

ITIL

Die IT Infrastructure Library (ITIL) ist eine Ansammlung mehrerer Bücher zum Thema „IT-Service-Management". Sie wurde vom britischen Office of Government Commerce (OGC) entwickelt. Die ITIL befasst sich mit dem Management von IT Services aus Sicht des IT-Dienstleisters. Der IT-Dienstleister kann dabei sowohl eine interne IT-Abteilung als auch ein externer Service Provider sein. Das allgemeine Ziel ist die Optimierung beziehungsweise Verbesserung der Qualität von IT-Dienstleistungen und der Kosteneffizienz. Informationssicherheit wird im Rahmen der betrachteten Services aus der operativen Perspektive heraus begutachtet. Umgekehrt ist ein funktionierender IT-Betrieb ein wesentlicher Stützpfeiler für das ISMS, wodurch sich viele Disziplinen der ITIL in ähnlicher Art und Weise, aber mit einem eindeutigen Fokus auf der Informationssicherheit im IT-Grundschutz und anderen Sicherheitsstandards wiederfinden.

Auf der Basis der ITIL wurde die Norm ISO/IEC 20000 erarbeitet, auf deren Grundlage wiederum ein Service-Management-System zertifiziert werden kann.

PCI DSS

Der Payment Card Industry Data Security Standard (PCI DSS) wird von einem Konsortium führender Kreditkartenorganisationen herausgegeben. Er wurde vom PCI Security Standards Council erstellt und formuliert Sicherheitsanforderungen bezüglich der Abwicklung von Kreditkartentransaktionen. Die Anforderungen des PCI DSS müssen von allen Institutionen umgesetzt werden, die Karteninhaberdaten von Kreditkarten speichern, verarbeiten oder übertragen, also z. B. von Händlern, die Kreditkartenzahlungen akzeptieren, oder von Dienstleistern, die diese im Auftrag weiterverarbeiten.

NIST

Das US-amerikanische National Institute of Standards and Technology (NIST) ist eine Bundesbehörde, die unter anderem für die Entwicklung von Standards zuständig ist. Diese Standards sind für US-Behörden verpflichtend. In der Reihe *Special Publication 800* („NIST SP 800"-Serie) veröffentlicht das NIST regelmäßig Dokumente zu einzelnen Themen der Informationssicherheit (Kryptografie, Cloud-Computing usw.), die nicht nur wertvolle Informationen liefern, sondern auch international einen weitreichenden Einfluss auf die Gestaltung der Informationssicherheit haben.

Das Dokument NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* stellt dabei für den Bereich Sicherheitsmanagement eine große Zahl sogenannter „Controls" zusammen, die dazu eingesetzt werden können, Informationsverbünde zu schützen. Die Controls sind nach zusammengehörigen Themen in diverse Bereiche gegliedert (z. B. Schulung und Sensibilisierung, Berechtigungsmanagement, Infrastruktursicherheit).

ISF – The Standard of Good Practice

Das Information Security Forum (ISF) ist eine unabhängige und weltweit tätige Organisation für Informationssicherheit. Das ISF veröffentlicht mit dem *Standard of Good Practice* (SoGP) einen auf anerkannten Best Practices basierenden Leitfaden zur Informationssicherheit. Der praxisorientierte Leitfaden deckt nach eigenen Angaben die Anforderungen der Standards ISO/IEC 27002, COBIT 5, PCI DSS 3.1 und NIST Cybersecurity Framework ab. Der SoGP gliedert die verschiedenen Themen in diverse Bereiche (z. B. Security Governance, Information Risk Assessment usw.).