Edition <kes>

Heinrich Kersten
Jürgen Reuter
Klaus-Werner Schröder

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

4. Auflage

<kes>

Springer Vieweg

Edition <kes>

Herausgegeben von
P. Hohl, Ingelheim, Deutschland

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s.a. www.kes.info), die seit 1985 im Secu-Media Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

Secure ICT Service Provisioning for Cloud, Mobile and Beyond
Von Eberhard von Faber und Wolfgang Behnsen

Security Awareness
Von Michael Helisch und Dietmar Pokoyski

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

IT-Notfallmanagement mit System
Von Heinrich Kersten, Gerhard Klett und Klaus-Werner Schröder

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Information Security Risk Management
Von Sebastian Klipper

Konfliktmanagement für Sicherheitsprofis
Von Sebastian Klipper

IT-Risiko-Management mit System
Von Hans-Peter Königs

Rollen und Berechtigungskonzepte
Von Alexander Tsolkas und Klaus Schmidt

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Heinrich Kersten · Jürgen Reuter ·
Klaus-Werner Schröder

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

4., aktualisierte und erweiterte Auflage

Springer Vieweg

Dr. Heinrich Kersten
Meckenheim, Deutschland

Dipl.-Math. Klaus-Werner Schröder
Bornheim, Deutschland

Dipl.-Ing. Jürgen Reuter
Ober-Ramstadt, Deutschland

DIN-Normen wiedergegeben mit Erlaubnis des DIN Deutsches Institut für Normung e.V. Maßgebend für das Anwenden der DIN-Norm ist deren Fassung mit dem neuesten Ausgabedatum, die bei der Beuth Verlag GmbH, Burggrafenstr. 6, 10787 Berlin, erhältlich ist.

ISBN 978-3-658-01723-1
ISBN 978-3-658-01724-8 (eBook)
DOI 10.1007/978-3-658-01724-8

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Vorwort

Zum Inhalt

Die Sicherheit der Information und der informationsverarbeitenden Prozesse wird heute immer mehr zu einem Eckpfeiler der Unternehmensvorsorge.

Image, Geschäftserfolg und Unternehmensstabilität hängen in entscheidendem Maße von qualifizierten Management-Prozessen und Management-Systemen ab – sei es, dass solche

- von Aufsichtsbehörden gefordert,
- von Geschäftspartnern erwartet,
- von Kunden wohlwollend bei Kaufentscheidungen berücksichtigt,
- bei Ausschreibungen sogar verbindlich vorgeschrieben werden oder
- zur Bewertung von Kreditwürdigkeit und Versicherungsrisiken (Stichwörter Basel II/III, Solvency II) erforderlich sind.

Management-Standard

Die sich hieraus ergebenden Anforderungen wurden bereits in der Vergangenheit in Management-Standards zusammengefasst, z. B. die ISO 9000-Reihe für das Qualitätsmanagement, die ISO 14000-Reihe für das Umweltschutzmanagement und die ISO 20000 für das IT-Service-Management.

Im vorliegenden Buch wird das Management der *Informationssicherheit* auf der Basis der Normenreihe ISO 27000 erläutert. Informationssicherheit umfasst neben IT-Sicherheit und Datenschutz *alle* mit der Sicherheit von Informationen zusammenhängenden Aspekte einer Organisation.

Es richtet sich an Leser, die

- sich für die genannten Standards interessieren,
- mit der Einrichtung eines entsprechenden Management-Systems in einer Organisation beauftragt sind,
- IT-Sicherheitsbeauftragter (IT Security Manager) sind,
- zum IT-Sicherheitsmanagement in anderen Funktionen beitragen,
- in der Leitungsebene einer Organisation solche Management-Systeme überwachen,

- das Informationssicherheitsmanagement-System (ISMS) ihrer Organisation zertifizieren lassen wollen,
- Beratungen zu Management-Systemen durchführen,
- Management-Systeme prüfen und auditieren.

In diesem Buch werden vor allem die Inhalte des Standards ISO 27001 exemplarisch erläutert, weil nach dieser Norm zertifiziert werden kann. Der Leser wird Schritt für Schritt bei der Herstellung von Konformität zu diesem Standard angeleitet und begleitet. Bei der Darstellung werden auch wesentliche Inhalte der begleitenden Normen aus der ISO 27000-Reihe berücksichtigt, die wichtige Elemente eines ISMS vertiefen und beispielhafte Interpretationen der Normtexte liefern – etwa die ISO 27002 und die ISO 27003.

Mindest-anforderungen

Anforderungskataloge an Management-Systeme gewinnen in der Standardisierung immer mehr an Bedeutung. Sie werden darüber hinaus in Gesetzen und Ausschreibungstexten herangezogen, um Management-Strukturen und Prozess-Modelle in abstrakter Weise (unabhängig vom jeweiligen Kontext) festlegen zu können.

Ebenso wie im Umwelt-, Qualitäts- und IT-Service-Management wurden auch beim Management der Informationssicherheit keine standardisierten Management-Systeme festgelegt, sondern lediglich *Mindestanforderungen* aufgestellt.

Tailoring

Die Anwendung solcher Anforderungskataloge auf eine Organisation erfordert ein exaktes Maßnehmen, Zuschneiden und Verknüpfen (Tailoring) der Einzelaspekte zu einem auf die Organisation zugeschnittenen Management-System. Bei diesem Tailoring muss eine Organisation das Ziel verfolgen, die Anforderungen aus den verschiedenen Standards zweckentsprechend zu interpretieren und zu harmonisieren, um so effiziente und effektive Strukturen, Prozess-Modelle und Management-Aktivitäten festzulegen.

Ein derartiges Tailoring ist wegen seiner tief greifenden Implikationen nicht ohne ein hohes Maß an Engagement des Top Managements der Organisation durchführbar.

Kopiert man dagegen Management-Systeme anderer Organisationen oder beschränkt sich auf das formale Erfüllen von Zertifizierungsnormen, so wird einem die leidvolle Erfahrung (z. B. aus der Anwendung der ISO 9000-Reihe) nicht erspart bleiben, eine überbordende Bürokratisierung, aber eben keinen für die Organisation nutzbringenden Ansatz gewählt zu haben.

Risikoanalyse Die Risikobetrachtung ist ein wesentlicher Grundpfeiler der Informationssicherheit. Sie ist Gegenstand der ISO 27005 und wird in Kapitel 6 dieses Buches an Beispielen erläutert.

Darunter findet sich auch ein Abschnitt zur *monetären Einschätzung von Risiken*, um dieses in der Praxis oft auftauchende Thema zu unterfüttern.

Maßnahmen Einen erheblichen Umfang nimmt das Kapitel 7 *Maßnahmenziele und Maßnahmen bearbeiten* ein, in dem die einzelnen Controls aus dem Anhang der ISO 27001 kommentiert und mit Beispielen versehen sind.

Bei allen Aspekten wird auch die Verbindung zum Maßnahmenkatalog des IT-Grundschutzes (siehe unten) behandelt.

Validieren Das Kapitel 8 *Maßnahmen: Validieren und Freigeben* beschreibt, wie mögliche Maßnahmen-Alternativen nach verschiedenen Faktoren bewertet werden können, bevor eine Alternative ausgewählt und für die Umsetzung freigegeben wird.

Kennzahlen Für das Normerfordernis, die Leistungsfähigkeit bzw. Wirksamkeit der ergriffenen Sicherheitsmaßnahmen zu beurteilen, sind seit geraumer Zeit Ansätze für Metriken und Kennzahlen in der Diskussion. Dieses Thema wird Kapitel 9 dieses Buches behandelt und orientiert sich an ISO 27004.

Audits Die Normen ISO 27006, 27007 und 27008 befassen sich mit Audits und Zertifizierungen. Im vorliegenden Buch werden dazu in Kap. 10 umfangreiche praktische Hinweise gegeben, darunter ein Abschnitt mit Erfahrungen aus realen Audits.

Leitlinien Im *Anhang* dieses Buches wird ein kommentiertes Beispiel für eine Informationssicherheitsleitlinie wiedergegeben. Dieses Beispiel dient der Erläuterung der Sachverhalte an einem sehr einfach gestrickten Fall, kann aber durchaus als Ausgangspunkt für reale Leitlinien angesehen werden.

IT-Grundschutz In Deutschland bzw. im deutschsprachigen Raum ist die Anwendung des IT-Grundschutzes des BSI verbreitet. Inzwischen wurde dessen Vorgehensmodell ebenfalls nach der ISO 27000-Reihe ausgerichtet. Der IT-Grundschutz mit seinen Baustein- und Maßnahmenkatalogen kann sehr hilfreich sein, um die Anforderungen des Standards vor allem auf der Maßnahmenseite zu konkretisieren. Insofern wird in diesem Buch auch beschrieben, wie der IT-Grundschutz bei dem Bemühen um Konformität zu ISO 27001 helfen kann.

Änderungen in der 4. Auflage

In dieser 4. Auflage sind folgende Ergänzungen vorgenommen worden:

- Aktualisierung aller Angaben zu Gesetzen, Richtlinien und Normen.
- Informationen über den aktuellen Stand des Ausbaus der ISO 27000-Reihe.
- Das Thema *Datenschutz* (personenbezogener Daten) wird durch viele Hinweise vertieft.
- Die Erläuterungen zu den Controls aus Anhang A der ISO 27001 wurden aktualisiert und ergänzt.
- Die vom BSI herausgegebene *Auslagerungsrichtlinie* wird im Zusammenhang mit der Grundschutz-Zertifizierung näher behandelt; sie enthält u. a. Anforderungen an Auftragnehmer bei der Vergabe von Aufträgen (Outsourcing) durch öffentliche Stellen.

Wichtige Hinweise

Nicht zuletzt wegen der zunehmenden Berücksichtigung der ISO 27001 in der Unternehmenspraxis, die die Autoren in ihrer beruflichen Tätigkeit als Auditoren und Zertifizierer feststellen konnten, haben sich einige Checklisten als nützlich erwiesen, in denen wichtige Schritte im Sicherheitsprozess tabellarisch abgebildet worden sind. Die Checklisten sind über den Verlag erhältlich[1].

Das vorliegende Buch versteht sich *nicht* als Einführung in die Informationssicherheit. Grundbegriffe und Grundstrukturen in dem hier verstandenen Sinne findet man z. B. in dem Buch *Der IT Security Manager*[2]. Da die genannten Standards jedoch eigene Begrifflichkeiten verwenden, werden wir diese in einem einführenden Abschnitt behandeln und den klassischen Begriffen gegenüberstellen.

---

1 http://www.springer.com/springer+vieweg; nach dem vorliegenden Buch suchen und auf den Auswahlpunkt „ZUSÄTZLICHE INFORMATIONEN“ klicken!

2 3. Auflage erschienen 2012 im gleichen Verlag.

Danksagung

Allen Lesern herzlichen Dank für die vielen Anregungen zu den früheren Auflagen. Die vorliegende vierte Auflage des Buches entstand mit tatkräftiger Unterstützung des Verlags Springer Vieweg. Vielen Dank an Herrn Hansemann und das gesamte Lektorat IT/Informatik.

Im Februar 2013
Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder

Inhaltsverzeichnis

1 Gesetze und Standards im Umfeld der Informationssicherheit

In diesem Kapitel soll eine Einführung in das *rechtliche Umfeld* der Informationssicherheit und ein Abriss über verschiedene Standards zu Management-Systemen und zur Informationssicherheit gegeben werden.

Es sei aber darauf hingewiesen, dass dieses Kapitel keine Rechtsberatung im Einzelfall – etwa durch einen spezialisierten Anwalt – ersetzen kann.

Die Auseinandersetzung mit rechtlichen Aspekten ist im Rahmen der Einführung eines ISMS *unerlässlich:*

- Spätestens bei der Bearbeitung des Anhangs A der ISO 27001 – und hier der Gruppe A.15 „Compliance" – müssen klare Aussagen über die Erfüllung der geltenden rechtlichen Anforderungen getroffen werden.
- Es ist deshalb wichtig, die zu beachtenden (aktuellen) Regeln zusammenzustellen und auszuwerten.

Auf eine möglichst vollständige Erfassung aller Regelungen ist zu achten. Die einseitige Ausrichtung eines ISMS auf ein einzelnes Regelwerk führt in der Praxis zu suboptimalen Ergebnissen. Es kommt mitunter vor, dass konkurrierende Anforderungen aus unterschiedlichen Rechtsquellen oder anderen unternehmerischen Gesichtspunkten zu beachten und zu berücksichtigen sind. Letztendlich sind rechtliche Fragen ein wichtiger *Teilaspekt* der Informationssicherheit und des Datenschutzes. Hierbei ist zu bedenken, dass die Entscheidung über die praktisch zu realisierende Erfüllung der Anforderungen nicht aus einer einseitig juristischen sondern aus einer interdisziplinären Sicht getroffen werden muss.

1.1 Corporate Governance und Risikomanagement

Eine Vielzahl der in den letzten Jahren vorgenommenen Änderungen an rechtlichen Bestimmungen berührt die Informationssicherheit. Die haftungsrechtlichen Konsequenzen aus diesen Gesetzesänderungen sind für den flüchtigen Betrachter im Allgemeinen nicht ohne weiteres erkennbar. Schlagworte wie *Basel*

H. Kersten, J. Reuter, K.-W. Schröder,
IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Edition <kes>,
DOI 10.1007/978-3-658-01724-8_1, © Springer Fachmedien Wiesbaden 2013

II/III, Sarbanes-Oxley, Euro-SOX tragen hier zum Teil mehr zur Verwirrung als zur Aufklärung bei.

Selbst bei näherer Beschäftigung mit den Gesetzestexten bleibt die Verpflichtung zur Absicherung der Informationssysteme in ihrer Qualität weitgehend im Verborgenen. Insofern lohnt es, die entsprechenden Gesetze und die einschlägigen Passagen an dieser Stelle kritisch zu beleuchten.

KonTraG

Im Jahre 1998 traten mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verschiedene Änderungen im *Aktiengesetz* und im *Handelsgesetzbuch* in Kraft. Diese Änderungen[3] betreffen die Ermittlung, die Aufnahme in die Berichterstattung sowie die Prüfung solcher Risiken, die für den Bestand der Unternehmen gefährlich sein können.

Die verbreitete Annahme, das KonTraG habe nur für Aktiengesellschaften oder Konzerne eine Bedeutung, wird durch die Ansiedlung der entsprechenden Paragrafen im 2. Abschnitt des 3. Buches des HGB widerlegt. Dieser Abschnitt gilt neben den Kapitalgesellschaften einschließlich der GmbH[4] auch für Personengesellschaften, bei denen die persönlich haftenden Gesellschafter keine natürlichen Personen sind.

Unabhängig davon gilt für alle Unternehmen der § 239(4) des HGB und damit die Bindung an die Grundsätze ordnungsgemäßer Buchführung.

BilMoG

Im Jahre 2009 wurden durch das Bilanzrechtsmodernisierungsgesetz (BilMoG) weitere relevante Präzisierungen in das Handelsgesetzbuch und das Aktiengesetz eingeführt. Die getroffenen Regelungen ähneln in ihrem Inhalt den Regelungen im weiter unten besprochenen Sarbanes-Oxley Act. Sie setzen die Anforderungen aus der 8.ten Kapitalmarktrichtlinie der EU (so genannte *Euro S-Ox Richtlinie*) um.

GDPdU, GoBS

Eine allgemeingültige, gleichwohl weniger bekannte Verpflichtung zur Vorsorge ergibt sich[5] aus den seit 1.1.2002 geltenden *Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* /GdPdU/ sowie den *Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme* /GoBS/.

Durch diese Vorschriften werden einerseits die Rechte der Finanzverwaltung beim Zugriff auf unternehmenseigene elektro-

---

3 Vgl. insbesondere AktG § 91 (2), HGB § 289 (1).

4 Siehe auch § 43 GmbH-Gesetz.

5 Aufgrund der Abgabenordnung (§ § 146 und 147 AO).

nisch gespeicherte Informationen geregelt und andererseits dem Unternehmen gewisse Sorgfaltspflichten bei der Verarbeitung, Vorhaltung und Bereitstellung dieser Informationen auferlegt. Diese Vorschriften, die unabhängig von der Rechtsform eines Unternehmens gelten, fordern von den Unternehmen die Einrichtung eines internen Kontrollsystems (IKS)[6]:

– „Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die die folgenden Aufgaben haben: Sicherung und Schutz des vorhandenen Vermögens und vorhandener Informationen vor Verlusten aller Art...".

Ein solches IKS schließt offensichtlich ein vollständiges Informationssicherheitsmanagement-System (ISMS) ein.

S-Ox

Für Aktiengesellschaften, die an einer US-Börse notiert sind oder für Töchter dieser Unternehmen, ergeben sich ähnliche Forderungen aus dem amerikanischen *Sarbanes-Oxley* Gesetz (S-Ox), das anlässlich der Finanzskandale im Zusammenhang mit Worldcom, Enron und der Wirtschaftsprüfungsgesellschaft Arthur Anderson auf den Weg gebracht wurde und 2002 in Kraft trat.

Dieses Gesetz zielt hauptsächlich auf eine Wiederherstellung des Vertrauens in die Finanzberichterstattung und die damit in Zusammenhang stehenden Testate von Wirtschaftsprüfern ab. Zur Wiederherstellung des Vertrauens in deren unabhängiges Urteil sind die Wirtschaftsprüfer für Unternehmen, die unter dieses Gesetz fallen, von bestimmten Beratungsfeldern ausgeschlossen (IT-Beratung) bzw. unterliegen diesbezüglich Einschränkungen (IT-Sicherheitsberatung).

Andere sinnvolle Bestimmungen dieses Gesetzes beziehen sich auf den Schutz der „Whistleblower" – Mitarbeiter, die rechtswidrige Manipulationen des Managements den unternehmensinternen oder staatlichen Kontrollinstanzen zur Kenntnis bringen. Artikel 404 verlangt ein ähnlich qualifiziertes Kontrollsystem wie das oben im Zusammenhang mit GoBS bzw. GdPdU erwähnte. Verstöße des Managements gegen dieses Gesetz werden erstmals mit sehr harten Strafen geahndet, wobei eine Versicherung (Enthaftung des Managements) gegen finanzielle Strafen nur eingeschränkt erlaubt ist.

Inhaltlich legt das Gesetz keine Anforderungen fest, die zu größeren Anstrengungen bei den unter dieses Gesetz fallenden Un-

6 Aus /GoBS/, Abschnitt IV.

ternehmen führen sollten. Es werden lediglich formale Anforderungen gestellt, die dazu geeignet sind, dem Management der betroffenen Firmen ihre Haftung deutlich werden zu lassen. Wer dagegen in dem Gesetz explizite Bestimmungen zur Absicherung der IT sucht, wird enttäuscht: Im Gesetz findet die IT-Sicherheit keine Erwähnung.

Gleichwohl gilt unzweifelhaft, dass Konformität mit Sarbanes-Oxley ohne systematische Absicherung der IT nicht vorstellbar ist. Eine verlässliche IT, ein verantwortungsvoller Umgang mit den unternehmenseigenen Informationen einschließlich ihres Schutzes sind für eine zuverlässige Unternehmensberichterstattung im Sinne dieses Gesetzes unerlässlich. In den Prüfvorschriften der amerikanischen Börsenaufsicht sowie in den einschlägigen Richtlinien für die Wirtschaftsprüfungsgesellschaften wird dies dann deutlicher.

COSO

Zur Definition der Anforderungen an die Finanzberichterstattung bzw. Buchführung und deren sichere Verwahrung wird im amerikanischen Raum im Allgemeinen auf die unter dem Kürzel *COSO* (Committee of the Sponsoring Organizations of the Treadway Commission) bekannten Grundsätze zurückgegriffen. COSO definiert quasi die US-amerikanischen Grundsätze ordnungsgemäßer Rechnungslegung einschließlich einiger Implikationen hinsichtlich der IT.

Aus den praktischen Erfahrungen mit der Umsetzung des Sarbanes-Oxley Gesetzes wird jedoch klar, dass hier einiges falsch läuft: Die betroffenen Unternehmen treiben in erheblichem Maße unnützen Aufwand bürokratischer Art.

Notwendig ist im Bereich der finanzbezogenen IT lediglich das Festlegen unternehmensindividuell angemessener Regeln, die nachgewiesene Überwachung von deren Befolgung und die Überprüfung von deren Zweckmäßigkeit. Die Darlegung erfolgt gegenüber einem Wirtschaftsprüfer nach den Regeln der ISAE[7] 3402 (vormals SAS 70). Inwiefern der Wirtschaftsprüfer hierbei Zertifikate berücksichtigt, steht in seinem Ermessen. Die für die Zertifizierung nach ISO 27001 bzw. nach Grundschutz erstellte Dokumentation sollte jedoch hierfür geeignet sein.

Nach dem amerikanischen Gesetz ist dies in der bislang beobachteten Form weder erforderlich noch allein ausreichend, um ein angemessenes Sicherheits- und Vertrauensniveau herzustellen. Die sehr abstrakt gehaltenen Anforderungen des S-Ox Gesetzes verdienen eine intelligentere Umsetzung als die gängige

7 International Standard on Assurance Engagements.

Praxis mit möglichst vielen bürokratischen Einzelmaßnahmen, die durch Kontrolle und die Kontrolle von der Kontrolle gekennzeichnet ist. Das führt nicht zu einem Mehr an Sicherheit und rechtfertigt auch keinen erhöhten Vertrauensvorschuss, sondern stellt eine unnötige Wertvernichtung in hohem Ausmaß dar.

Basel II/III, Solvency II

Wenig Konkretes zu IT- und Informationssicherheit findet sich auch in anderen Vorgaben. Die *Kapitaladäquanzrichtlinie* für Banken (*Basel II*) gilt zunächst einmal nur für Banken. Das Pendant für Versicherungen ist unter dem Namen *Solvency II* bekannt und wird über eine EU-Richtlinie, nach der die EU-Staaten jeweils ihre Gesetze auszurichten haben, für die betroffenen Unternehmen verbindlich. Die Baseler Richtlinien befinden sich in einer ständigen Fortentwicklung; aktuell soll Basel III in Kraft treten – wobei Basel IV bereits in der Diskussion ist.

Allgemein wird im Zusammenhang mit solchen Vorgaben die Berücksichtigung der operativen Risiken gefordert, zu denen auch die IT-Risiken zählen. Da Banken und Versicherungen auch die Risiken im Zusammenhang mit ihren Kunden zu berücksichtigen haben, wirken die Forderungen dieser Gesetze mittelbar auf die Kreditnehmer, Versicherungsnehmer und die Dienstleister für diese Zielgruppen.

Kreditwesengesetz

Ähnlich allgemein gehaltene Regelungen finden sich im Kreditwesengesetz bzw. den Mindestanforderungen an das Risikomanagement (MARisk)[8]. Von Bedeutung ist, dass die Banken und Versicherungen nicht mehr wie bisher einen einheitlichen Prozentsatz Ihrer Eigenkapitalunterlegung für die Absicherung der getätigten Risiken unterstellen dürfen. Vielmehr müssen diese Institute in Zukunft eine filigranere interne Risikoermittlung durchführen. An Hand des ermittelten Risikos wird dann der verlangte Eigenkapitalanteil festgemacht. Hierbei wird auch eine Betrachtung der operativen Risiken verlangt.

Zu diesen operativen Risiken gehören auch die Risiken, die mit dem Einsatz von Informationssystemen verbunden sind. Da die Banken auch die Kreditausfallrisiken ihrer Schuldner (Adressenausfall) zu berücksichtigen haben, wirken diese rechtlichen Anforderungen mittelbar auf sämtliche Unternehmen, die am Kapitalmarkt Kredite aufnehmen möchten. Ein Unternehmen mit einer relativ schlechten Risikoeinstufung wird, wenn es kreditwürdig ist, einen relativ hohen Kreditzins zu entrichten haben.

---

8 Die MARisk werden in Form von Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht in ihrer jeweils aktuellen Fassung auf der Webseite der BAFIN veröffentlicht.

Derartige Ratingsysteme, die Banken und Versicherungen in Folge von Basel II/III und Solvency II auf ihre Kunden anwenden, sind nicht standardisiert und von Institut zu Institut unterschiedlich. Bei der Vielzahl der Ratingkriterien ist nach derzeitigem Erkenntnisstand davon auszugehen, dass ein ISMS zwar einen bemerkenswerten, aber in der Mehrzahl der Fälle nicht den *entscheidenden* Einfluss auf die Höhe der Kreditzinsen haben wird.

BDSG

Beim Bundesdatenschutzgesetz leitet sich die Verpflichtung zur Einrichtung eines ISMS aus dem § 9 einschließlich seiner Anlage ab. Demnach sind alle Stellen, die in irgendeiner Form für den Schutz personenbezogener Daten sorgen müssen, dazu verpflichtet, die erforderlichen organisatorischen und technischen Vorkehrungen zu treffen. Welcher Art diese Vorkehrungen sind, ergibt sich aus der Berücksichtigung der Anlage zum § 9 BDSG, in der die Grundsätze des Datenschutzes dargelegt sind. Der bei der Realisierung dieser Grundsätze zu treibende Aufwand ist anhand des Schutzzweckes abzuwägen. Der Nachweis der Erfüllung dieser Erfordernisse sollte sinnvollerweise im Rahmen eines ISMS durch das Risikomanagement erfolgen.

Sonstige

Neben den genannten Vorschriften existieren für den Bereich der Informationssicherheit eine ganze Reihe weiterer Spezialvorschriften, die im Grunde ein ISMS fordern, auf die an dieser Stelle jedoch nicht näher eingegangen werden soll:

- Produkthaftungsgesetz bzw. § 823 BGB (z.B. bei Software-Kauf).
- Teledienstegesetz (TDG).
- DeMail-Gesetz (bei Nutzung von DeMail-Diensten).
- Teledienstedatenschutzgesetz (TDDSG).
- Wassenar-Abkommen (europäische Kryptoregulierung) und zu berücksichtigende länderspezifische Gesetze, die Einschränkungen hinsichtlich der einsetzbaren Verschlüsselungstechnik vorschreiben.
- Grundgesetz Art. 10 und G10-Gesetz.
- Urheberrechtsgesetz (UrhG).
- Signaturgesetz (SigG).
- Umsatzsteuergesetz (§14, Echtheitsanforderungen an elektronische Rechnungen).
- Strafgesetzbuch, insbesondere § 203, was den Schutz von Berufsgeheimnisträgerdaten betrifft.
- Sicherheitsüberprüfungsgesetz (SüG).

Im Rahmen der Umsetzung eines ISMS wird es jedoch erforderlich sein, sich mit *allen* im konkreten Einzelfall anzuwendenden Gesetzen näher auseinander zu setzen.

Insgesamt existiert also eine Vielzahl von Gesetzen, die den Unternehmen und anderen Organisationen auferlegen, Vorkehrungen zu treffen, die einem ISMS vergleichbar sind oder die im Rahmen eines ISMS abzuhandeln sind.

Letztlich dienen Normen wie ISO 27001 auch der nationalen und internationalen Rechtsprechung als Maßstab, um die Erfüllung normaler Sorgfaltspflichten durch Unternehmen prüfen zu können, die in den Gesetzen meist nur abstrakt vorgegeben sind.

1.2 Die Bedeutung des öffentlichen Beschaffungsrechts

Eine nicht zu unterschätzende Bedeutung für die Durchsetzung von Zertifizierungsmodellen kommt dem öffentlichen Beschaffungsrecht und hier insbesondere den für diesen Bereich gültigen europäischen Richtlinien zu.

Zur Wahrung der Chancengleichheit der Bieter und zur Vermeidung der Diskriminierung ausländischer Bieter sind hinsichtlich der Spezifikation der technischen Anforderungen an Management-Systeme bestimmte Normen bevorzugt zu berücksichtigen. Hierbei handelt es sich primär um solche nationale Standards, die ihrerseits eine europäische Norm umsetzen[9].

ISO 27001

Von der Vielzahl der bestehenden Modelle wird für den Bereich des Managements der Informationssicherheit nur ISO 27001 (nach Übernahme als EN und DIN) diesen Anforderungen genügen.

Gleichwertige Nachweise

Die Anforderungen an ein ISMS, die ein öffentlicher Auftraggeber im Rahmen von Ausschreibungen vorschreiben darf, sind grundsätzlich auf die ISO 27001 beschränkt.

Nachweise für ein vorhandenes Management der Informationssicherheit sind in diesem Zusammenhang in Form von Zertifikaten zu erbringen, wie sie bereits im Zusammenhang mit ISO 9001 und ISO 14001 bekannt sind.

---

9 Vgl. Richtlinie 2004/18/EG v. 31.3.2004, *Koordinierung der Verfahren zur Vergabe öffentlicher Bauaufträge, Lieferaufträge und Dienstleistungsaufträge*, hier insbesondere Art. 23 *Technische Spezifikationen*, Artikel 49 f. zu Qualitätssicherungs- und Umweltmanagementnormen sowie Artikel 52 zur Zertifizierung durch öffentlich-rechtliche und privatrechtliche Stellen.

Auch wenn das Beschaffungsrecht die Erfüllung der Anforderungen durch andere gleichwertige Nachweise zulässt, wird die praktische Relevanz anderer Nachweise als einer Zertifizierung nach ISO 27001 recht gering sein, weil damit ein erhöhter bzw. komplizierter Erklärungsaufwand verbunden sein dürfte.

Erstellt werden diese Zertifikate entweder durch dafür bestimmte (notifizierte) öffentlich-rechtliche Stellen, die hierzu einen gesetzlichen Auftrag haben, oder gleichwertig durch privatrechtliche Stellen, bei denen eine entsprechende Akkreditierung vorhanden sein muss.

Zertifikate anderer Aussteller müssen von öffentlichen Auftraggebern nicht anerkannt werden.

IT-Grundschutz

In der Bundesrepublik Deutschland steht neben einigen für ISO 27001 akkreditierten privaten Stellen auch das Bundesamt für Sicherheit in der Informationstechnik für den Erwerb der benötigten Zertifikate zur Verfügung. Die entsprechenden BSI-Zertifikate sind überschrieben mit *ISO 27001-Zertifikat auf der Basis von IT-Grundschutz* und gehen in dem Detaillierungsgrad der Anforderungen über die ISO 27001 vielfach hinaus.

CobiT

Obwohl in einzelnen EU-Richtlinien neben dem *Code of Practice* in ISO 27002 bzw. dem Vorläufer ISO 17799 auch Modelle wie CobiT oder das *frühere* Grundschutzmodell des BSI Erwähnung finden, kann hinsichtlich des öffentlichen Beschaffungsrechts nicht von einer Gleichwertigkeit dieser Modelle ausgegangen werden.

CobiT *(Control Objectives for Information and Related Technology)* ist ein Verfahren zur *IT Governance* und gliedert die Aufgaben der IT in Prozesse und Control Objectives (Regelziele). CobiT verfolgt ähnlich ISO 27001 einen Top-Down Ansatz, bei dem ausgehend von den Geschäftszielen IT-Ziele festgelegt werden, welche wiederum die IT-Architektur beeinflussen. CobiT nimmt für sich in Anspruch, ein integrierendes Modell zu sein, welches die Anforderungen sämtlicher verbreiteter Modelle für die IT-Organisation in einem Reifegradmodell integriert.

Würde ein öffentlicher Auftraggeber in einer internationalen Ausschreibung z. B. den Grundschutznachweis alter Form des BSI einfordern, so würde er damit ein so genanntes nicht-tarifäres Handelshindernis etablieren und ausländische Bieter diskriminieren. Die Verwendung von CobiT würde im Widerspruch zur vorgegeben Normenhierarchie stehen, nach der *europäische Normen* für die Formulierung technischer Anforderungen zu präferieren sind.

Wenn also mit der Einführung bzw. Zertifizierung eines ISMS der Nebenzweck erfüllt werden soll, die Zulassungskriterien für internationale Ausschreibungen zu erfüllen, ist eine Konzentration auf ISO 27001 ratsam.

1.3 Standards zu Management-Systemen

ISO 9000

Die ISO 9000-Serie gilt in Normungskreisen als die wohl erfolgreichste Norm aller Zeiten. Die Norm fordert von den anwendenden Organisationen, sich bereichsübergreifend so zu organisieren, dass ihre Prozesse stets Produkte und Dienstleistungen hervorbringen, die den Anforderungen der Kunden gerecht werden.

So erfolgreich die Norm für die Normungsinstitute und Zertifizierungsstellen ist, so umstritten ist die Norm in der Praxis.

Historisch und von den Ansätzen her geht die Norm auf Anforderungskataloge militärischer Beschaffungsämter zurück. Mitte der 70er Jahre wurde hieraus eine britische Norm, in den 80er Jahren kam dann die ISO 9000-Reihe auf.

Ihre Vorbilder, nämlich die hauptsächlich aus dem militärischen Bereich stammenden Checklisten, waren hinsichtlich des damals *elementeorientierten* Aufbaus noch recht klar erkennbar. Inzwischen hat hier ein Paradigmenwechsel zugunsten eines *prozessorientierten* Aufbaus stattgefunden, der sich aber hinsichtlich der praktischen Auswirkungen auf die Organisation inhaltlich nicht nennenswert von den ursprünglichen Modellen unterscheidet.

Der eigentlich gute Grundgedanke der Überwachung von Geschäftsprozessen hinsichtlich der Parameter, die für das Produzieren erfolgreicher Produkte erforderlich sind, degeneriert in der Praxis nur allzu häufig zu einem eher hinderlichen Übermaß an Formalismen und Bürokratie. Das Resultat der Prozesse, nämlich das Produkt selbst, ist zunehmend aus dem Blickfeld der qualitätsbezogenen Aktivitäten vieler Organisationen geraten.

Dabei ist zu betonen, dass die inhaltlichen Forderungen der Norm keinesfalls für die oben angedeuteten Fehlentwicklungen verantwortlich zu machen sind. Vielmehr ist die gängige Art der Beantwortung der Normanforderungen durch die anwendenden Organisationen zu beanstanden.

Festzustellen ist, dass hierzu immer wieder auf Praktiken zurückgegriffen wird, die sich z. B. im Behördenalltag als hervorragend ineffizient erwiesen haben. Anstatt beispielsweise eine sinnvolle Vertragsüberprüfung durchzuführen, bei der sich alle an der beabsichtigten Leistungserbringung Beteiligten miteinander verständigen, wird die bekannte Abzeichnungspraxis angewandt.

Pro Forma wird die Normforderung auf diese Weise natürlich erfüllt. Von der Zertifizierungsstelle gibt es folgerichtig auch kaum eine Beanstandung. Die Auswirkungen auf die Vitalität der Unternehmen sind jedoch verheerend.

Aus Gesprächen mit Zertifizierern und eigener Praxis ist den Verfassern bekannt, dass 60-90% der Beanstandungen bei Zertifizierungsaudits im Bereich der *Dokumentation* liegen. Glaubt man wirklich, dass man durch immer mehr Dokumentation besser wird? Die Norm fordert eine *angemessene* Dokumentation der Prozesse, mehr nicht.

In vielen der gängigen Qualitätshandbücher findet sich zu Beginn eine ansprechende Sammlung von Grundsätzen der Qualitätspolitik. Den Satz, der die praktizierte Qualitätspolitik am besten kennzeichnet, findet man dort nie, in allen Amtsstuben ist er bestens bekannt: „Wer schreibt, der bleibt!"

Bei einer anstehenden Einführung der ISO 27001 wird dringend angeraten, diese Vorüberlegungen beim Aufbau des Sicherheitsmanagements zu berücksichtigen. Einige Normforderungen der ISO 9001 sind fast wortgleich auch in ISO 27001 enthalten. Es handelt sich im Wesentlichen um Forderungen nach

- einer gelenkten Dokumentation,
- Sicherung beweiserheblicher Aufzeichnungen,
- der Organisation interner Audits und
- Verbesserung der installierten Prozesse.

Unternehmen können sich Aufwand und leidvolle Erfahrungen bei der Einführung redundanter Verfahren ersparen, wenn sie sich für sinnvoll integrierte und effiziente Verfahren entscheiden.

ISO 14000

Die ISO 14000-Serie betreffend Umweltschutzmanagement-Systeme wurde nicht unter dem gleichen Druck wie ISO 9000 eingeführt. Vielmehr geschah dies häufig aus intrinsischer Motivation der Unternehmen. Aus diesen Gründen ist auch die Verbreitung dieser Normenreihe in der Unternehmenspraxis im Vergleich zu ISO 9000 recht gering.

Auch hier empfiehlt sich der Integrationsansatz bezüglich ISO 27001. Die Themen Notfallplanung und Notfallkommunikation sind hier besonders zu erwähnen.

ISO 20000

ISO 20000 ist ein verbreiteter Standard, der sich mit dem IT Service Management beschäftigt. Der Standard rührt aus den umfangreichen Büchern der *Information Technology Information*

Library (ITIL)[10] her. Sie wurden aufgrund einer Auswertung der Ereignisse beim Versagen von militärischen IT-Systemen im Falkland-Krieg von britischen Behörden zusammengestellt.

Der Standard betrifft im Wesentlichen die Organisation der IT-Abteilungen. Er sorgt für eine klare Aufgabenabgrenzung und für die Definition eindeutiger Ansprechstellen bei IT-Problemen sowie geeignete Eskalationsstufen.

Der auf ISO 20000 bzw. ITIL abgestimmte Standard zur Informationssicherheit ist ISO 27001. Hier finden sich im Detail vielfältige Überschneidungen. So wird beispielsweise das Kapazitätsmanagement in beiden Standards behandelt. Einen wichtigen Aspekt stellt das Incident Management nach ISO 20000 dar, welches das Security Incident Management nach ISO 27001 sinnvollerweise einschließen muss. Die Aufzählung weiterer Details würde den Rahmen des vorliegenden Buches sprengen.

Unsere Empfehlung ist auch hier, koordiniert und integrierend vorzugehen – wobei wir diese Empfehlung mit etwas weniger Nachdruck als hinsichtlich ISO 9000 und ISO 27001 aussprechen möchten. Bei gleichzeitiger Einführung von IT-Grundschutz ist das Bedürfnis der Integration mit ITIL hingegen ein erfolgskritischer Faktor.

Bei Anwendung von ISO 20000 ist eine sehr genaue Interpretation und Anwendung der Normerfordernisse auf die Organisation notwendig. Nur so kann der Gefahr der Überbewertung von Formalien – eine in der bisherigen Praxis beobachtbare Tendenz – begegnet werden. Dies gilt vor allem für kleinere IT-Abteilungen, in denen die von der Norm in filigraner Weise geforderten Aufgaben nur auf wenige Mitarbeiter verteilt werden können.

PCI-DSS

Wir gehen noch kurz auf PCI-DSS ein: Das Kürzel steht für *Payment Card Industry Data Security Standard*. Hierbei handelt es ich um einen amerikanischen Standard /PCI-DSS/, der auf die am elektronischen Zahlungsverkehr mit Kreditkarten beteiligten Unternehmen anzuwenden ist. PCI-DSS gilt somit nicht nur für die Banken, sondern für jedes Unternehmen, welches als Händler oder Dienstleister an der Verarbeitung von Kreditkartendaten beteiligt ist.

Die enthaltenen Anforderungen sind technisch nicht außergewöhnlich anspruchsvoll, jedoch sind sie sehr detailliiert und lassen vergleichsweise wenig Spielraum für individuell zugeschnittene Sicherheitsmaßnahmen.

---

10 British Standard BS 15000.

Bei der Anwendung ist das *Scoping* von Bedeutung, der Anwender sollte die betroffenen Systeme möglichst isoliert von anderen Systemen betreiben und die Maßnahmen soweit zweckmäßig nur auf die PCI-DSS-relevanten Systeme beschränken.

Eine Integration des Anforderungskatalogs von PCI-DSS in eine Systematik der risikoabhängigen Auswahl von Sicherheitsmaßnahmen, wie es ISO 27001 fordert, ist aus unserer Sicht anzuraten.

Bei größeren Anwendungsfällen ist die Erbringung eines Nachweises durch einen zugelassenen Penetrationstester (Approved Scanning Vendor) erforderlich. In derartigen Fällen sollte ein Zertifizierer gewählt werden, bei dem sowohl die Auditierung als auch der Penetrationstest bezogen werden kann. Zur Zeit ist den Autoren jedoch kein Anbieter bekannt, der dahingehend akkreditiert ist, Zertifizierungen sowohl hinsichtlich PCI-Konformität als auch gemäß ISO 27001 anbieten zu können.

Bei Anwendung des PCI-DSS ist zu beachten, dass dieser Standard einseitig an den Sicherheitsbedürfnissen der Kreditkartenanbieter ausgerichtet ist. Hinsichtlich der Zertifizierungsbedingungen ist nur der Schutz der eng definierten *Kreditkartendaten* gefordert. Das sind im Wesentlichen die Nummerncodes, die auf den Karten gespeichert sind. Der Datenschutz wird in den Standards zwar erwähnt – aber nicht automatisch sichergestellt. Insofern bedeutet PCI-Compliance nicht unbedingt Sicherheit oder umfassende Compliance zur Sicherheit.

ISO 27000

Man muss feststellen, dass der Ausgangspunkt für ein standardisiertes Sicherheitsmanagement bei der Informationsverarbeitung zweifelsohne im angelsächsischen Raum angesiedelt ist.

Der seinerzeit herausgegebene British Standard (BS) 7799 bestand aus zwei Teilen: Teil 1 (BS 7799-1) stellt einen so genannten *Code of Practice* dar, der eine Sammlung von Hinweisen, Maßnahmen und bewährten Praktiken für die Informationssicherheit enthält und erstmalig 1995 erschienen ist. Der Teil 2 (BS 7799-2) trägt den Titel *Specification with Guidance for Use* und beschreibt in Form von Spezifikationen ein Modell eines ISMS. Er ist erstmalig 1998 erschienen.

Weiterhin gehören zu dieser Normenreihe einige Guidelines zu speziellen Themen (etwa die Risikoanalyse oder die Vorbereitung auf eine Auditierung betreffend). Als Zwischenschritt ist BS 7799-1 im Jahre 2000 in den Standard ISO 17799 eingeflossen, bevor dieser dann in die ISO 27002 überführt wurde. BS 7799-2 ging auf direktem Wege in der ISO 27001 auf.

Hinsichtlich der uns primär interessierenden Normenreihe ISO 27000 haben wir folgenden aktuellen Stand. *Erschienen* sind[11]:

Allgemeine Normen

- ISO 27000[D] (Definitionen und Begriffe der Normenreihe)
- ISO 27001[D] (ISMS Anforderungen)
- ISO 27002[D] (Leitfaden zur Umsetzung, aus ISO 17799)
- ISO 27003 (Implementierung eines ISMS)
- ISO 27004 Measurement (Metriken / Kennzahlensysteme)
- ISO 27005 (Risikomanagement)
- ISO 27006 (Anforderungen an Stellen, die Audits und Zertifizierungen durchführen)
- ISO 27007 (ISMS Audits)
- ISO TR 27008 (Technische Audits)
- ISO 27010 (Austausch von Sicherheitsinformationen, z. B. in kritischen Infrastrukturen)

Spezielle Branchen

- ISO 27011 (Telekommunikation)
- ISO 27015 (Finanzdienstleistungen)
- ISO 27799 (Gesundheitswesen)

Spezialthemen

- ISO/IEC 27013 (Integration ISO 27001 und ISO 20000)
- ISO/IEC 27031 (Business Continuity)
- ISO/IEC 27032 (Cybersecurity)
- ISO/IEC 27033 (Network Security), teilweise vorhanden
- ISO/IEC 27034 (Application Security), teilweise vorhanden
- ISO/IEC 27035 (Incident Management)
- ISO/IEC 27037 (Digital Evidence)

Wenn man das Gefühl hat, bei der Vielzahl dieser Normen den Überblick zu verlieren, mag folgende Übersicht helfen:

---

11 Stand Februar 2013; das hochgestellte „D“ hinter der Nummer der Norm deutet an, dass diese in deutscher Sprache verfügbar ist.

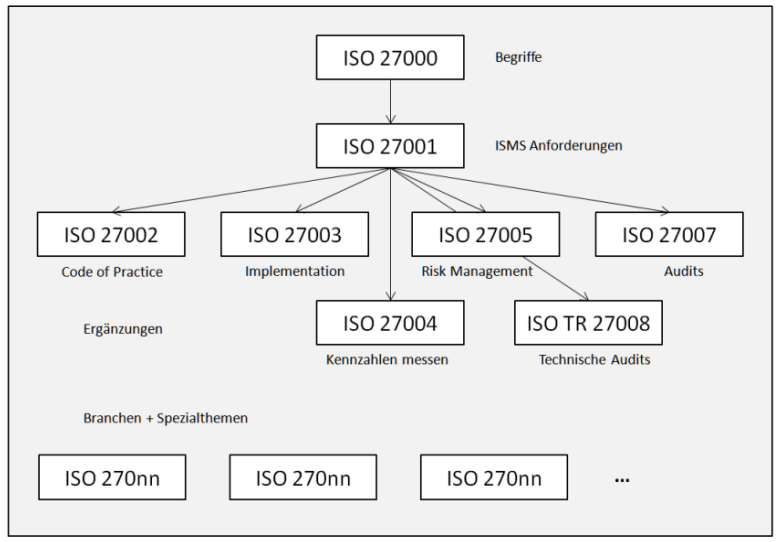

Abbildung 1: Übersicht über ISO 27000-Normenreihe

Gute Informationen zum jeweils aktuellen Stand aller Normen dieser Reihe liefert www.iso27001security.com. Dort findet man auch eine Reihe von White Papers, ein FAQ, Checklisten und Materialien und viele weitere Detail-Informationen – allerdings überwiegend in englischer Sprache.

Welche dieser Standards sollte man sich beschaffen?

Die Begriffsdefinitionen aus ISO 27000 werden in allen anderen Standards dieser Reihe – soweit dort benötigt – wiederholt; ein Erwerb dieser Norm ist im Grunde obsolet. Die englische Fassung ist allerdings kostenfrei downloadbar.

Für den Aufbau eines ISMS bis hin zu einer Zertifizierung benötigt man zumindest ISO 27001. Zur Unterstützung bei der Interpretation der Controls des Anhangs A dieses Standards kann zusätzlich die Beschaffung des ISO 27002 sinnvoll sein.

Die weiteren Standards in der Mitte der Abbildung 1 kann man bei Bedarf ergänzend zu Rate ziehen; ihre Verwendung ist jedoch nicht zwingend vorgeschrieben.

Inhaltlich bieten die weiteren Normen („Spezielle Branchen“ und „Spezialthemen“) keine wesentlich neuen Erkenntnisse, insofern ist ihre Beschaffung von geringerer Priorität.

IT-Grundschutz

In Deutschland wurde das vom BSI[12] Anfang der 90er Jahre herausgegebene IT-Grundschutzhandbuch vor allem in Behörden angewendet. Dieses Werk, das in einem etwas engeren Sinne die *IT-Sicherheit* einschließlich Datenschutz behandelt, hatte eine Maßnahmen-orientierte Sichtweise und stellte Standard-Maßnahmen vorwiegend für den normalen Schutzbedarf vor. Diese detaillierten Maßnahmen sind von einer Organisation grundsätzlich umzusetzen, wenn eine Konformität zum IT-Grundschutzhandbuch hergestellt werden soll.

Inzwischen hat sich der IT-Grundschutz insofern gewandelt, als die Ausführungen zum Sicherheitsmanagement an ISO 27001 ausgerichtet und die Methodik insgesamt der ISO 27001 angenähert wurde:

- Bei der Maßnahmen-Auswahl im technischen, organisatorischen und infrastrukturellen Bereich sind weiterhin die Baustein- und Maßnahmenkataloge anzuwenden.
- Für die Gefährdungsanalysen existieren umfangreiche Gefährdungskataloge.
- Beschreibungen der Methodik sind von diesen Katalogen getrennt und in so genannte BSI-Standards aufgenommen worden:
  - 100-1: Managementsysteme für Informationssicherheit,
  - 100-2: IT-Grundschutz-Vorgehensweise,
  - 100-3: Risikoanalyse auf der Basis von IT-Grundschutz.

Diese Synthese von ISO-Standard und IT-Grundschutz ist für viele Anwender ein wichtiges Kriterium. Man kann es so ausdrücken:

- ISO 27001 spezifiziert, welche Elemente ein ISMS enthalten muss und welche Anforderungen an das Management der IT-Sicherheit zu stellen sind – überlässt jedoch dem Anwender, detaillierte Prozesse und Einzelmaßnahmen auszuwählen, um die gestellten Mindestkriterien zu erfüllen.
- Der IT-Grundschutz hilft, diese Lücke zu schließen, indem er für seine Anwendungsbereiche konkrete Vorgehensweisen und Einzelmaßnahmen zwingend vorgibt – und zwar unter Nutzung von so genannten Bausteinen, die modellhaft bestimmte Einsatzszenarien und technische Komponenten beschreiben.

---

12 Bundesamt für Sicherheit in der Informationstechnik.

Die Möglichkeiten individueller Anpassungen sind beim IT-Grundschutz natürlich geringer als bei einer Vorgehensweise nach ISO 27001. Zudem ist der Anwendungsbereich des IT-Grundschutzes stark auf Aspekte der klassischen IT-Sicherheit eingeschränkt.

1.4 Zertifizierfähige Modelle

Die Anzahl der Modelle, nach denen Informationssicherheit bzw. IT-Sicherheit zertifiziert werden kann, ist groß. Sie unterscheiden sich hinsichtlich ihrer Verbreitung, Reputation, der Anwendungsgebiete und der Kosten. Zertifikate (deutsch: Bescheinigungen) kann grundsätzlich jeder erteilen, jedoch bieten erst *akkreditierte Stellen* die nötige Vertrauensbasis und die internationale Akzeptanz der Zertifikate.

Wegen des mit einer Zertifizierung verbundenen Aufwandes sollte vorher genau überlegt werden, welches Ziel man erreichen möchte, ob man dieses Ziel mit einem *bestimmten* Zertifikat erreichen kann und ob die Anstrengungen und Kosten dieses Ziel rechtfertigen. Im Folgenden gehen wir nur auf solche Zertifikatsmodelle ein, die nach Auffassung der Autoren ein Mindestmaß an Seriosität und Bekanntheit aufweisen.

Tabelle 1: Übersicht über Zertifizierungsmodelle

ISO 27001	
Anwendung	Z. B. vollständiges Unternehmen – unabhängig von seiner Ausrichtung bzw. Branche, aber auch Einschränkungen auf Teile (z. B. einzelne Geschäftsprozesse) möglich.
Aufwand	Einführung eines ISMS mit angemessenem Risikomanagement-System und daraus je nach Sachlage abzuleitender Sicherheitsmaßnahmen.
Reputation	International auf hohem Niveau.
Zertifizierer	Darauf achten, dass die Zertifizierungsprogramme unter die jeweilige Akkreditierung fallen.
Nutzen	Erfüllung der Forderungen aus S-Ox, Basel II/III, Solvency II. Zugang als Anbieter zu öffentlichen Beschaffungsmärkten. Vertrauensbildung beim Kunden. Hoher interner Nutzen für die Informationssicherheit.
Externe Kosten	Abhängig vom Zertifizierungsprogramm und der Unternehmensgröße; typischerweise in der Größenordnung von 10.000-50.000 €.

ISO 27001 auf Basis von IT-Grundschutz	
Anwendung	Vollständiges Unternehmen mit allen IT-Anwendungen theoretisch möglich – praktisch aber eher Einschränkung auf einzelne IT-Anwendungen oder kleine IT-Verbünde.
Aufwand	Hoher formaler Aufwand für Modellierung und Schutzbedarfsanalyse. Es empfiehlt sich wegen der komplexen Struktur und des Umfangs des Regelwerks auf erfahrene externe Beratung zurückzugreifen. Hierfür sollte kein zu geringer Betrag veranschlagt werden.
Reputation	Hohe Anerkennung in der Bundesrepublik, in europäischen Richtlinien als Referenzmodell erwähnt.
Zertifizierer	Bundesamt für Sicherheit in der Informationstechnik.
Nutzen	s. ISO 27001, aber international eingeschränkte Akzeptanz.
Externe Kosten	ca. 20.000-100.000 Euro (Zertifizierung).
Common Criteria	
Anwendung	Begrenzt auf (überschaubare) technische Produkte und Systeme: Betriebssysteme, Chipkarten, Firewallsysteme, Signatur- und Kryptoanwendungen usw. Unterschiedliche Evaluierungsstufen festgelegt. Die Anforderung sollte nur gezielt gestellt werden, da die Ausrüstung eines kompletten IT-Verbundes mit zertifizierten Komponenten aufgrund des Marktangebots – vor allem beim Einsatz moderner Technologien unrealistisch ist.
Aufwand	Hoher formaler und zeitlicher Aufwand.
Reputation	Anwendung wird inzwischen von vielen Seiten gefordert; in Europa auch im Zusammenhang mit elektronischer Signatur; internationale Anerkennung bei unteren Sicherheitsstufen gegeben, jedoch Restriktionen bei höheren Sicherheitsstufen.
Zertifizierer	Auf Akkreditierung achten.
Nutzen	Zugang als Anbieter zu öffentlichen Beschaffungsmärkten. Wenn das der Zertifizierung zugrunde liegende Schutzprofil mit der jeweiligen Anwendung übereinstimmt, erspart sich der Anwender individuellen analytischen Aufwand.
Externe Kosten	Evaluierungskosten ab ca. 20.000 €, je nach Sicherheitsstufe und Produkt bis in Höhe einiger hunderttausend Euro, zusätzlich Zertifizierungskosten ca. 10-20%.