Heinrich Kersten
Jürgen Reuter
Klaus-Werner Schröder

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Edition <kes>

Herausgegeben von Peter Hohl

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 SecuMedia 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.

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

ITIL Security Management realisieren
Von Jochen Brunnstein

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

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

Praxis des IT-Rechts
Von Horst Speichert

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

www.vieweg.de

Heinrich Kersten
Jürgen Reuter
Klaus-Werner Schröder

IT-Sicherheits-management nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

Mit 2 Abbildungen

Herausgegeben von Heinrich Kersten
und Klaus-Dieter Wolfenstetter

vieweg

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.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2008

Lektorat: Günter Schulz / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.
www.vieweg.de

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de
Umschlagbild: Nina Faber de.sign, Wiesbaden
Druck- und buchbinderische Verarbeitung: MercedesDruck, Berlin
Printed in Germany

ISBN 978-3-8348-0178-4

Vorwort

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[1] von Kreditwürdigkeit und Versicherungsrisiken erforderlich sind.

Management-Standard

Die sich hieraus ergebenden Anforderungen wurden bereits in der Vergangenheit in Management-Standards zusammengefasst, z. B. die ISO 900x für das Qualitätsmanagement und die ISO 1400x für das Umweltschutz-Management.

Im vorliegenden Buch wird das Management der *Informationssicherheit*[2] auf der Basis des neuen Standards ISO 27001[3] erläutert. 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,

---

1 Stichwörter Basel II, Solvency II.

2 Informationssicherheit umfasst neben IT-Sicherheit und Datenschutz *alle* mit der Sicherheit von Informationen zusammenhängenden Aspekte einer Organisation.

3 Erster Bestandteil der Normenreihe ISO 2700x und hervorgegangen aus dem British Standard 7799-2.

- in der Leitungsebene einer Organisation solche Management-Systeme überwachen,
- Management-Systeme prüfen und auditieren,
- das Informationssicherheits-Management-System (ISMS) ihrer Organisation zertifizieren lassen wollen.

In diesem Buch werden die Inhalte des Standards exemplarisch erläutert. Der Leser wird Schritt für Schritt bei der Herstellung von Konformität zu diesem Standard angeleitet und begleitet.

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- und im Qualitätsmanagement 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 900x) nicht erspart bleiben, eine überbordende Bürokratisierung, aber eben keinen für die Organisation nutzbringenden Ansatz gewählt zu haben.

BS 7799

Der British Standard (BS) 7799 ist der Kern aller Standardisierungsaktivitäten der letzten Jahre zum Thema „Management der Informationssicherheit".

Er besteht 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, die letzte Fassung datiert von 2002.

Zum BS 7799 gehören weiterhin einige Guidelines zu speziellen Themen (etwa die Risikoanalyse oder die Vorbereitung auf eine Auditierung betreffend).

ISO 17799

BS7799-1 ist im Jahre 2000 in den Standard ISO 17799 eingeflossen, der inzwischen in der Version ISO 17799:2005 erschienen ist.

ISO 2700x

Mit dieser Migration war auch eine Übernahme von BS 7799-2 durch die ISO geplant. Nach längeren internationalen Abstimmungsprozessen hat man sich jedoch zu einem Re-Design entschieden und die Normenreihe ISO 2700x konzipiert. Die 2005 in englischer Sprache erschienene ISO 27001 basiert auf dem „Vorgänger" BS 7799-2. Inzwischen existiert der Entwurf einer deutschen Übersetzung der ISO 27001.

Aus BS 7799-1 bzw. ISO 17799 soll dann zukünftig der Standard ISO 27002 werden. Auch die Guidelines zu BS 7799 sind – nach entsprechender Überarbeitung – zur Aufnahme in die Normenreihe 2700x vorgesehen.

Wesentlicher Punkt ist, dass es auf Grundlage der ISO 27001 bereits jetzt möglich und sinnvoll ist, ein ISMS zu auditieren und zu zertifizieren.

IT-Grundschutz

In Deutschland wurde das vom BSI[4] 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 Maß-

[4] Bundesamt für Sicherheit in der Informationstechnik.

nahmen sind von einer Organisation unbedingt umzusetzen, wenn eine Konformität zum IT-Grundschutzhandbuch hergestellt werden soll.

Inzwischen hat sich der IT-Grundschutz insofern gewandelt, als das Sicherheitsmanagement an ISO 27001 ausgerichtet und die weitere Methode 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 existiert ein umfangreicher Gefährdungskatalog.

Beschreibungen der Methodik sind von diesen Katalogen getrennt und in so genannte BSI-Standards 100-1 (Managementsysteme für Informationssicherheit), 100-2 (IT-Grundschutz-Vorgehensweise) und 100-3 (Risikoanalyse auf der Basis von IT-Grundschutz) aufgenommen worden.

Diese Synthese von ISO-Standard und IT-Grundschutzhandbuch 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 seinen Anwendungsbereich konkrete Vorgehensweisen und Einzelmaßnahmen[5] zwingend vorgibt.

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.

Unabhängig davon wird in diesem Buch beschrieben, wie der des IT-Grundschutz bei dem Bemühen um Konformität zu ISO 27001 helfen kann.

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*

5 Zumindest für eine beschränkte Zahl von modellhaften Bausteinen.

IT Security Manager“[6]. Da die genannten Standards jedoch eigene Begrifflichkeiten verwenden, werden wir diese in einem einführenden Abschnitt behandeln und den klassischen Begriffen gegenüberstellen.

Wichtiger Hinweis

Die in diesem Buch wiedergegebenen Texte aus dem Anhang A des Standards ISO 27001 sind dem aktuellen Entwurf der deutschen Übersetzung entnommen worden (DIN ISO/IEC 27001:2007-02). Es kann nicht ausgeschlossen werden, dass diese Texte im Zuge der Konsolidierung der deutschen Fassung des Standards noch Änderungen erfahren. Die Kommentierungen und Erläuterungen zu diesen Texten sind jedoch davon nicht betroffen, da sie sich an dem Wortlaut des englischen Originals orientieren.

Danksagung

Herrn Günter Schulz und Herrn Dr. Klockenbusch, Programmleiter des Vieweg-Verlags, möchten die Autoren für die professionelle Unterstützung bei der Herstellung dieses Buches und die Bereitschaft danken, ein solches Spezialthema in diese Buchreihe aufzunehmen.

Dem Beuth-Verlag möchten wir für die Genehmigung danken, Passagen aus dem deutschen Entwurf des Standards ISO/IEC 27001 für dieses Buch verwenden zu dürfen.

Im Juli 2007

Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder.

6 Erschienen in der Edition KES im Vieweg-Verlag; das vorliegende Buch kann als eine Ergänzung jenes Werkes angesehen werden.

Inhaltsverzeichnis

1 Gesetze und Standards im Umfeld der Informationssicherheit

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

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 II", „Sarbanes-Oxley" 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[7] 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[8] auch für Personengesellschaften, bei denen die persönlich haftenden Gesellschafter keine natürlichen Personen sind. Unabhängig davon gilt für alle

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

8 Siehe auch § 43 GmbH-Gesetz.

Unternehmen der § 239(4) des HGB und damit die Bindung an die Grundsätze ordnungsgemäßer Buchführung.

GDPdU, GoBS

Eine allgemeingültige, gleichwohl weniger bekannte Verpflichtung zur Vorsorge ergibt sich[9] aus den seit 1.1.2002 geltenden *Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen* (GDPdU) sowie den *Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme* (GoBS) vom 7.11.1995.

Durch diese Vorschriften werden einerseits die Rechte der Finanzverwaltung beim Zugriff auf unternehmenseigene elektronisch 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)[10]:

– „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 Informationssicherheits-Management-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 Wirtschaftprüfern ab. Zur Wiederherstellung des Vertrauens in deren unabhängiges Urteil sind die Wirtschaftsprüfer für Unternehmen, die unter dieses Gesetz fallen, von bestimmten Beratungsfeldern ausgeschlossen

---

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

10 Aus GoBS, Absatz 4, Anlage zum Schreiben des Bundesministers der Finanzen vom 7.11.1995, AZ: IVA8-S0316-52/95-BStBl 1995 I S. 738.

(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 / 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 Unternehmen 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.

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 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, 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 – nach gegenwärtigem Diskussionsstand frühestens 2010.

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. 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.

Derartige Ratingsysteme, die Banken und Versicherungen in Folge von Basel II 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 Einfluss, 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 Softwarekauf),
- Teledienstegesetz (TDG),
- 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),
- 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 Managementsysteme bestimmte Normen bevorzugt zu berücksichtigen. Hierbei handelt es sich primär um solche nationale Standards, die ihrerseits eine europäische Norm umsetzen[11].

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

Zukünftig dürften die Anforderungen an ein ISMS, die ein öffentlicher Auftraggeber für Ausschreibungen vorschreiben darf, praktisch auf die ISO 27001 beschränkt sein.

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.

Auch wenn das Beschaffungsrecht die Erfüllung der Anforderungen durch andere „gleichwertige“ Nachweise zulässt, wird die

11 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.

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 den wenigen für ISO 27001 akkreditierten privaten Stellen 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*[12] zur ISO 27001 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.

Würde ein öffentlicher Auftraggeber in einer internationalen Ausschreibung 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 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 Managementsystemen

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 organi-

12 Aus ISO / IEC 17799.

sieren, 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 militärischen Checklisten, waren hinsichtlich des damals e*lementeorientierten* 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 bewiesen 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 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 kürzlich verabschiedeter Standard, der sich mit dem IT-Service-Management beschäftigt. Der Standard rührt aus den umfangreichen Büchern der *Information Technology Information Library* (ITIL)[13] 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

13 British Standard BS 15000.

die Definition eindeutiger Ansprechstellen bei IT-Problemen sowie geeignete Eskalationsstufen.

Der auf ISO 20000 bzw. ITIL abgestimmte Standard zur Informationssicherheit ist ISO 27001. Trotzdem finden sich im Detail in vielfältiger Weise Überschneidungen. So wird beispielsweise das Kapazitätsmanagement in beiden Standards behandelt. 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.

1.4 Zertifizierfähige Modelle

Die Vielzahl der Modelle, nach denen IT-Sicherheit zertifiziert wird, ist groß. Die Modelle 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 angemessenen Risikomanagementsystems 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, Solvency II. Zugang als Anbieter zu öffentlichen Beschaffungsmärkten. Vertrauensbildung beim Kunden. Hoher interner Nutzen für die Informationssicherheit.
Externe Kosten	Abhängig vom Zertifizierungsprogramm, in der Größenordnung von 10.000 €.
ISO 27001 auf Basis von Grundschutz	
Anwendung	Vollständiges Unternehmen mit allen IT-Anwendungen theoretisch möglich – praktisch aber eher Einschränkung auf einzelne IT-Anwendungen.
Aufwand	Hoher formaler Aufwand für Modellierung und Schutzbedarfsanalyse.
Reputation	Hohe Anerkennung in der Bundesrepublik, in europäischen Richtlinien als Referenzmodell erwähnt.
Zertifizierer	Bundesamt für Sicherheit in der Informationstechnik.
Nutzen	s. ISO 27001.
Externe Kosten	ca. 10.000 Euro.

Kombination ISO 27001 und Technik	
Anwendung	Services und Produkte eines Unternehmens, einschließlich des ISMS und der infrastrukturellen und technischen Gegebenheiten.
Aufwand	ISMS Einrichtung, Sicherheitsanalysen und Penetrationstests für die relevanten Services.
Reputation	Akkreditiertes Verfahren
Zertifizierer	Zertifizierungsstelle der T-Systems
Nutzen	Neben der Qualifizierung des ISMS zusätzlich Zertifizierung relevanter Services und Produkte.
Externe Kosten	Größenordnung ca. 30.000 Euro.
Common Criteria	
Anwendung	Begrenzt auf überschaubare Geräte, Betriebssysteme, Chipkarten, Firewallsysteme und dgl.
Aufwand	Hoher formaler Aufwand.
Reputation	Anwendung wird inzwischen von vielen Seiten gefordert; in den USA werden europäische Zertifikate bei hohen Sicherheitsanforderungen nicht anerkannt.
Zertifizierer	Auf Akkreditierung achten.
Nutzen	Zugang als Anbieter zu öffentlichen Beschaffungsmärkten.
Externe Kosten	Zertifikatskosten ab ca. 20.000 €, je nach Sicherheitsstufe und Produkt bis in Höhe einiger hunderttausend Euro.
Trusted Site	
Anwendung	Kommerzielle Webseiten.
Aufwand	Absicherung der Webseite und deren Management nach vorgegebenen Kriterien.
Reputation	In der Bundesrepublik hoch. Keine Referenzierung in Gesetzen.
Zertifizierer	TÜV-IT.
Nutzen	Vertrauensbildung beim Kunden.
Externe Kosten	Zertifikat kostet mehr als 10.000 Euro.

Webtrust	
Anwendung	IT-Bereich ist abzugrenzen.
Aufwand	Anwendung eines Kriterienkataloges auf einen IT-Bereich.
Reputation	Hohes Niveau.
Zertifizierer	Nur Wirtschaftsprüfer.
Nutzen	Vertrauensbildung beim Kunden.
Externe Kosten	Zertifikat kostet ca. ab 100.000 Euro.
ISO 20000 (ITIL)	
Anwendung	IT-Service-Bereich eines Betriebes.
Aufwand	Einführung eines angemessenen IT-Service-Managements einschließlich ISO 27001 für den begrenzten Bereich der IT-Services.
Reputation	Internationale Anerkennung, hohes Niveau.
Zertifizierer	Auf Akkreditierung achten.
Nutzen	Zugang als Anbieter zu öffentlichen Beschaffungsmärkten. Vertrauensbildung beim Kunden. Verbesserung des eigenen IT-Services.
Externe Kosten	Zertifikat kostet ca. 10.000 Euro

PCI-DSS

Wir gehen noch kurz ein auf PCI-DSS: 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. 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.

1.5 Konkrete Standards zur IT-Sicherheit

Eine wachsende Zahl von ISO-Normen beschäftigt sich mit Fragen der IT-Sicherheit. Die überwiegende Zahl beschäftigt sich mit Themen, die für den Adressatenkreis dieses Buches von geringerer Bedeutung sein dürften.

Hiervon zu unterscheiden sind eine Reihe von weiteren ISO-Standards, die eine echte Hilfe bei der Konkretisierung der Umsetzung der Normerfordernisse an die Informationssicherheit bieten. Um dem Leser einen Einblick zu gewähren und ihm die Möglichkeit zu verschaffen, sich gezielt um die wirklich benötigten Normen zu bemühen, geben wir an dieser Stelle einen knappen inhaltlichen Überblick anhand der Hauptnummern, ohne nach Teilnormen zu differenzieren.

Dort, wo ein besonderer Bezug zu konkreten Normerfordernissen der ISO 27001 besteht, geht die Erläuterung ein wenig über den ansonsten stichwortartig gehaltenen Charakter hinaus, insbesondere geben wir den entsprechenden Bezug zum Anhang A des Standards an.

Tabelle 2: Normen mit Bezug zum Anhang A der ISO 27001

Themengebiet	ISO-Standard	Bezug zu Anhang A der ISO 27001 Stand und Empfehlungen
Kryptografie, Verschlüsselung, Digitale Signaturen, Hash-Funktionen, Datenauthentisierung, Authentisierung von Kommunikationspartnern, Key-Management	9979, 10116, 18033 9796, 14888, 10118, 15946, 9797, 9798 11770, 15946, 18031, 18032	Kaum Bezug! In Ausnahmefällen kann für IT- Spezialisten die Berücksichtigung dieser Normen im Rahmen der Realisierung von A.12.3 eine Rolle spielen, bei dem es um den Schutz der Informationen durch kryptografische Methoden geht.

Themengebiet	ISO-Standard	Bezug zu ISO 27001 bzw. Stand und Empfehlungen
Non-repudiation[14], Zeitstempeldienste Public Key Infrastructure	13888 15945, 18014 14516	Kaum Bezug! Die Standards können für Experten von Belang sein bei der Realisierung von: A.12.2.3 Nachrichtenintegrität A.10.9.x Schutz von E-Commerce-Diensten und deren Nutzung (mittelbar)
Guidelines for the Management of IT Security	13335	Starker Bezug! Für die praktische Arbeit sind die technischen Reporte aber entbehrlich.
Code of Practice for Information Security	17799	Als Interpretationshilfe für den Anhang des Standards zu empfehlen. Enthält Anregungen für einige hundert Sicherheitsmaßnamen.
Evaluation und IT Security Assurance	15408[15], 15292, 15446 15443	Weniger relevant: Sehr ambitionierte Standards, die mittels sehr stark formalisierter Verfahren Sicherheitsklassifizierungen erlauben. Enthalten zahlreiche interessante methodische Ansätze. Praktische Bedeutung nur für die Beurteilung der Sicherheit von technischen, meist sehr eng abgegrenzten Systemen wie Firewalls, Mailguards, Kartenanwendungen.
Netzwerksicherheit	18028	Sehr hilfreich bei der Identifizierung des Handlungsbedarfs hinsichtlich der netzwerkbezogenen Vorgaben aus A.10, A.11 und A.12 des Standards.
Einsatz von Intrusion Detection Systemen	18043	Nur sinnvoll, wenn der Einsatz derartiger Systeme im Rahmen der Auseinandersetzung mit dem Standard erwogen wird.

14 Nachweisverfahren für erfolgte elektronische Kommunikation (in Analogie zum Einschreibebrief).

15 Auch "Common Criteria" /CC/ genannt; Nachfolger der /ITSEC/.

Themengebiet	ISO-Standard	Bezug zu ISO 27001 bzw. Stand und Empfehlungen
Security Incident Management	18044	Klarer Bezug zu A.13: Der technische Report enthält zahlreiche Anregungen zur unterschiedlichen Ausgestaltung des Managements von Sicherheitsvorfällen.
IT Security Evaluation	18045	Der technische Report ist für die praktische Umsetzung des Standards eher entbehrlich.
Reifegradmodell CMM / CMMI für die Prozesse des System Security Engineering[16]	21827	Zahlreiche inhaltliche Überschneidungen mit dem Standard. Der nicht uninteressante Modellansatz birgt die Gefahr aller Reifegradmodelle, die Dokumentationsflut stark anwachsen zu lassen. Für die Umsetzung des Standards vor allem in der Anfangszeit eher hinderlich.
Begriffsdefinitionen zum ISMS	27000	In Arbeit
Code of Practice for Information Security Management	27002	In Arbeit
Einführungshilfe für ein ISMS	27003	In Arbeit
Metriken bzw. Performanzindikatoren für ein ISMS	27004	Die bisher bekannten Ansätze des Entwurfs der Norm erscheinen nicht sehr viel versprechend.

16 CMM = Capability Maturity Model, Software Engineering Institute der Carnegie Mellon University. CMMI = Capability Maturity Model Integration.