Universität Hamburg
Fachbereich Informatik

Bachelorarbeit

Geschichtliche Entwicklung des IT-Sicherheitsmanagements

vorgelegt von

Martin Hinsch
geb. am 23. März 1983 in Hamburg
Matrikelnummer 6142625
Studiengang Wirtschaftsinformatik

eingereicht am 28. Oktober 2013

Betreuer: M.A. Christoph Gerber
Erstgutachter: Prof. Dr.-Ing. Hannes Federrath
Zweitgutachter: PD Dr. Klaus-Dieter Heidtmann

Aufgabenstellung

IT-Sicherheitsmanagement beschäftigt sich mit der strukturierten Absicherung des Informationsverbundes eines Unternehmens oder einer Organisation gegen Bedrohungen der Informationssicherheit und des Datenschutzes. Anerkannte Standards auf diesem Gebiet (beispielsweise die *ISO/IEC 2700x*-Familie oder der *IT-Grundschutz*) helfen, Absicherungsaufgaben koordiniert und kontinuierlich anzugehen.

Im Rahmen dieser Abschlussarbeit sollen die Herkunft, Verbreitung und geschichtlichen Hintergründe von Basistechniken des IT-Sicherheitsmanagements identifiziert und herausgearbeitet werden. Besonderes Augenmerk soll dabei auf die Entstehung und Entwicklung der *IT-Grundschutz*-Vorgehensweise und die Standards *ISO/IEC 2700-1/2* gelegt werden. Hierbei sollen zum einen Vorläuferdokumente (wie etwa *BS 7799*) berücksichtigt werden. Zum anderen sollen auch gesetzliche Vorgaben im Zeitverlauf diskutiert werden.

Zusammenfassung

Diese Arbeit ordnet die *ISO/IEC 2700x*-Familie und den *IT-Grundschutz*, ihre Verbreitung und die gesetzlichen Rahmenbedingungen in den historischen Kontext ein.

Einzelne Staaten entwickelten in den 1980er Jahren jeweils eigene Regelwerke, anhand derer technische Komponenten auf ihre IT-Sicherheit bewertet wurden. Hierauf aufbauend, entstanden Anfang der 1990er Jahre der englische Standard *BS 7799* und der deutsche *IT-Grundschutz*. Beide Normen ermöglichen ein koordinierten Schutz der unternehmenseigenen IT. Durch eine Angleichung des *IT-Grundschutzes* an den *BS 7799*-Nachfolgestandard *ISO/IEC 27001* können beide Standards auch kombiniert in Unternehmen genutzt werden.

Indirekt üben gesetzliche Vorgaben wie der amerikanische *Sarbanes-Oxley-Act* einen Einfluss auf die Verbreitung von Standards des IT-Sicherheitsmanagement aus. Die Standards helfen zum Beispiel bei der Erfüllung der gesetzlichen Vorgabe, ein zuverlässig funktionierendes Risikomanagementsystem zu betreiben.

Weltweit am stärksten verbreitet ist die *ISO/IEC 27001*-Norm. Auffällig ist, dass insbesondere *Konzerne* die Methodiken des IT-Sicherheitsmanagements nutzen. *Kleinen und mittleren Unternehmen* fehlt hingegen das Bewusstsein für IT-Sicherheit und für die damit verbundenen Risiken. Oft ist ihnen das Thema IT-Sicherheit zu komplex. Diese Komplexität wird durch die fortschreitende technische, rechtliche und organisatorische Entwicklung stetig erhöht. Die Bewältigung der Komplexität zählt zu den Aufgaben von Standards des IT-Sicherheitsmanagements und ist entscheidend für ihre Verbreitung.

Inhaltsverzeichnis

Abbildungsverzeichnis **V**

Tabellenverzeichnis **VI**

Verwendete Abkürzungen **VII**

1 Einleitung **1**

2 Stand der Forschung **3**

3 Grundlagen der IT-Sicherheit **3**
3.1 Definitionen zum Themenbereich IT-Sicherheit 4
3.2 IT-Standards: Komplexität von soziotechnischen Systemen 5
3.3 IT-Sicherheitsmanagement 5

4 Die geschichtliche Entwicklung der IT-Sicherheitskriterien **7**
4.1 Erste Standardisierungsbemühungen 7
4.2 Das Orange Book 8
4.3 Fazit 10

5 IT-Standards **10**
5.1 Grundlegende Informationen zu ISMS 11
5.2 ISO/IEC 2700x 12
5.2.1 Geschichtliche Hintergründe 14
5.2.2 ISO/IEC 27001-Zertifikat 18
5.3 IT-Grundschutz 19
5.3.1 Geschichtliche Hintergründe 21
5.3.2 IT-Grundschutz-Zertifikat 29
5.3.3 ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz . . 29
5.4 Entwicklung beider Standards im Zeitverlauf 30

6 Bedeutung, Akzeptanz und Verbreitung **33**
6.1 Die Zeit vor IT-Sicherheitsmanagement-Standards 33
6.2 ISO/IEC 27001 34
6.2.1 Mengenmäßige und regionale Verteilung der Zertifikate . . . 34
6.2.2 Verbreitung, Bedeutung und Akzeptanz am Beispiel Großbritanniens 37
6.3 IT-Grundschutz 40
6.3.1 IT-Sicherheit in kleinen und mittleren Unternehmen in Deutschland 40

6.3.2 Mengenmäßige und regionale Verteilung 42
6.3.3 Zahlenmäßiger Vergleich zur ISO/IEC 27001 44
6.4 Akzeptanz von IT-Sicherheitsstandards 44
6.5 Fazit 48

7 Gesetzliche Rahmenbedingungen 48
7.1 Corporate Governance als Rahmen der IT-Sicherheit 48
7.2 Gesetze zur Corporate Governance 49
7.3 Datenschutzgesetze 52
7.4 Fazit und Ausblick 53

8 Schlussbetrachtungen 57

Literaturverzeichnis I

Erklärung XVII

Abbildungsverzeichnis

1 Evolution der *ISO/IEC 27001/2*-Standards. 13
2 Zusammenhänge in der *ISO/IEC 2700x*-Familie [II12]. 16
3 Evolution des *IT-Grundschutzes*. 20
4 Bundesamt für Sicherheit in der Informationstechnik (BSI)-Standardwerke zur IT-Sicherheit 1992 [Bun92]. 22
5 *IT-Grundschutzhandbuch (IT-GSHB)* 1994-2005. 24
6 Ergänzungslieferungen (EL) des *IT-GSHBs* bis 2005 [ARG01] [Bun02a] [Bun03]. Das Fragezeichen steht für ein nicht genau bekanntes Datum. 25
7 *IT-Grundschutz* seit 2006 (nach [Fed13, Folie 97]). 26
8 Ergänzungslieferungen (EL) der IT-Grundschutz-Kataloge seit 2005 [Mün07] [Mün08b, S. 215] [Mün08a, Folie 13 ff.] [Bun11c] [FG11, Folie 3]. Die Fragezeichen stehen für nicht genau bekannte Daten. . 28
9 Evolution der *ISO/IEC 27001/2*-Standards und des *IT-Grundschutzes*. 32
10 Anzahl Zertifikate 2006 bis 2011 nach [Int13c]. 35
11 Marktanteil nach Regionen 2006 bis 2011 nach [Int13c]. 36
12 Durchschnittlichen Kosten für den schwerwiegendsten Vorfall im UK 2002 bis 2013 [Dep02, S. 11] [Dep04, S. 25] [Dep06, S. 30] [Dep08, S. 31] [Dep10b, S. 18] [Dep12, S. 18] [Dep13a, S. 18]. 38
13 Anzahl registrierter, öffentlicher Anwender 1997 bis 2009 (nach [Bun97, Anhang] [Bun98, S. 1 u. Anhang] [Bun00, Anhang] [Bun09]). 42
14 Marktanteil nach Regionen 1997 bis 2000 (nach [Bun97, Anhang] [Bun98, S. 1 u. Anhang] [Bun00, Anhang] [Bun02a, Anhang]). . . . 43
15 Einordnung des IT-Sicherheitsmanagements in die IT-Governance und IT-Compliance (nach [Fal12, S. 32-37]). 55
16 Evolution gesetzlicher Rahmenbedingungen. Gestrichelte Linien zeigen einen Einfluss eines Gesetzes auf andere Gesetze. Eine durchgehende Linie zeigt direkte Nachfolgeregelungen. 56
17 Evolution der IT-Sicherheit (nach [Sol10] und in Anlehnung an [ISA13]). 57

Tabellenverzeichnis

1 Grundlegende Informationen über Standards des IT-Sicherheitsmanagements [ENI13b] [BF08, S. 10]. 11
2 Standards des IT-Sicherheitsmanagements [ENI13b] [BF08, S. 10]. . 33
3 Verwendung von IT-Sicherheitsrichtline und -standards im UK 2000 bis 2013 [Dep02, S. 15 u. 19] [Dep04, S. 8 u. 10] [Dep06, S. 7 u. 9] [Dep08, S. 7 u. 9] [Dep10b, S. 6] [Dep12, S. 6] [Dep13a, S. 6] [Int13c]. 39
4 Entscheidende Faktoren für die Verwendung eines Informationssicherheitsmanagement-System (ISMS) (nach [BF08, S. 10] [BF10, S. 69-84] [Dep02, S. 19]). 47

Verwendete Abkürzungen

AG	Aktiengesellschaft
AITP	Association of Information Technology Professionals
AktG	Aktiengesetz
Basel	Richtlinie über Eigenkapitalanforderungen
BDSG	Bundesdatenschutzgesetz
BERR	Department for Business, Enterprise and Regulatory Reform
BilMoG	Bilanzrechtsmodernisierungsgesetz
BIS	Department for Business, Innovation and Skills
BMI	Bundesministerium des Inneren
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes
CC	Common Information Technology Security Criteria
CCSC	Commercial Computer Security Center
CSC	Computer Security Center
CSI	Computer Security Institute
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DIN	Deutsches Institut für Normung
DIS	Draft International Standard
DMAIC	Define - Measure - Analyse - Improve - Control
DNSBL	DNS-basierte Schwarze Liste
DoD	Department of Defense
DPA	Data Protection Act
DPMA	Data Processing Management Association
DTI	Department of Trade and Industry

EA	European co-operation for Accreditation
EG	Europäische Gemeinschaft
EL	Ergänzungslieferung
EU	Europäische Union
EuroSOX	Abschlussprüfungs-Richtlinie
FDIS	Final Draft International Standard
GmbH	Gesellschaft mit beschränkter Haftung
HGB	Handelsgesetzbuch
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
ISBS	Information Security Breaches Survey
ISIT	Interministriellen Ausschuß für die Sicherheit in der IT
ISM	Industrial Security Manual for Safeguarding Classified Information
ISMS	Informationssicherheitsmanagement-System
ISO	International Organisation for Standardization
IT	Informationstechnologie
ITEHB	IT-Evaluationshandbuch
IT-GSHB	IT-Grundschutzhandbuch
ITK	Informations- und Kommunikationstechnologie
ITSEC	Information Technology Security Evaluation Criteria
ITSHB	IT-Sicherheitshandbuch
ITSK	IT-Sicherheitskriterien
ITU	International Telecommunication Union
IÜS	Internes Überwachungssystem
JTC	Joint Technical Committee
KMU	kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
MLS	Multilevel security
NBS	National Bureau of Standards

NCC	National Computing Centre
NCSC	National Computer Security Center
NISPOM	National Industry Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PDCA	Demingkreis
PwC	PricewaterhouseCoopers
RACF	Resource Access Control Facility
Solvency	Richtlinie für Basissolvenzkapitalanforderungen
SOX	Sarbanes-Oxley-Act
TCSEC	Trusted Computer System Evaluation Criteria
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UK	Vereinigte Königreich
WIK	Wissenschaftlichen Institut für Kommunikationsdienste
WSC	World Standards Cooperation
ZfCh	Zentralstelle für das Chiffrierwesen
ZSI	Zentralstelle für Sicherheit in der Informationstechnik

1 Einleitung

Mit der Zunahme der weltweiten Vernetzung durch das Internet steht die informationstechnische Sicherheit (IT-Sicherheit) zunehmend im Fokus der Öffentlichkeit und insbesondere der Unternehmen. Bedrohungen wie der von 2008 bis 2011 unentdeckten Cyberspionage bei verschiedenen US-amerikanischen Medien wie der *New York Times* und der *Washington Post* [hei13] lassen das Vertrauen der Mitarbeiter in die unternehmensinterne Sicherheit schwinden. DDoS-Angriffe auf Organisationen wie *Spamhaus*[1] im März 2013 haben mitunter so große Auswirkungen, dass es zu länderübergreifenden Beeinträchtigungen des Internets und damit auch vieler Dienste von Unternehmungen kommt [HM13].

Die Verschmelzung von privater und beruflicher Informationstechnologie (IT) (englisch: *Consumerization of IT*) zeichnet sich seit einigen Jahren als Trend ab. Private Smartphones, Laptops und Software werden auch beruflich von Arbeitnehmern am Arbeitsplatz genutzt. Arbeitgeber weltweit fördern diese Maßnahme, davon versprechen sie sich unter anderem eine höhere Produktivität ihrer Angestellten. Gleichzeitig bedeutet die Einbindung und Nutzung von benutzereigener Hard- und Software (*Bring Your Own (Device)*) eine größere Herausforderung für die IT-Infrastruktur. Die Arbeit mit neuen, den Firmenadministratoren teilweise noch nicht bekannten mobilen Geräten und Betriebssystemen (zum Beispiel Android, iOS, Blackberry 10, Windows Phone) muss ermöglicht sowie miteinander interagierende Dienste und Software für diese Geräte in die Geschäftsprozesse, Compliance-Richtlinien und die IT-Sicherheit des Unternehmens eingebunden werden [Pri13, ENI12, ENI13a].

Vor einigen Jahren traten eine Reihe von rechtlichen Bestimmungen (Gesetze und Richtlinien) in Kraft oder wurden verändert, welche alle das Gebiet der Informationssicherheit berühren. Dazu zählen in Deutschland das KonTraG[2] (1998), in den USA der Sarbanes-Oxley-Act (SOX) (2002), für den Banken- und Versicherungssektor Basel II (2007) und Solvency II (nationale Umsetzung steht in 2013 noch aus) sowie das Bundesdatenschutzgesetz (BDSG) [KRSW13, S. 1-6].

All diese Beispiele haben eine Gemeinsamkeit: sie zeigen den Zusammenhang des Einsatzes von IT und dessen Auswirkungen auf die unternehmerischen Prozesse (englisch: *business impact*), Strategien und Ziele. Durch einen Ausfall der IT käme es zu großen finanziellen Verlusten von Firmen, über einen längeren Zeitraum wäre der Ausfall existenzbedrohend (vgl. [HS04, S. 287 ff.]). Ebenso bedrohlich für die Existenz eines Unternehmens sind das (unbemerkte) Abgreifen von digitalen

[1] Diese Non-Profit-Organisation stellt eine DNS-basierte Schwarze Liste (DNSBL) über mögliche Spam-Versender für den Einsatz in Mailservern zur Verfügung [The13].

[2] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich.

Unternehmenswerten wie Kundendaten und Informationen über Produktionsverfahren durch Einbrüche in das Firmennetzwerk.

Die große Bedeutung des Schutzes der IT und damit der Informationen an sich bedingt ein auf die Bedürfnisse des Unternehmens ausgerichtetes IT-Sicherheitsmanagement. Die Informationssicherheit wird durch ein optimiertes Sicherheitsmanagement „effektiver und nachhaltiger“, ebenso sind „positive Nebeneffekte“ wie eine „erhöhte Arbeitsqualität“, ein gesteigertes Kundenvertrauen, verbesserte Organisationsabläufe und Kosteneinsparungen zu erwarten [Bun11a].

Den Unternehmen stehen für den Einsatz eines IT-Sicherheitsmanagements verschiedene Standards zur Verfügung. Die Standards erhöhen das Sicherheitsniveau und ermöglichen Institutionen einen einheitlichen Austausch über den Einsatz von Sicherheitsmaßnahmen. Die Bekanntesten sind die *International Organisation for Standardization (ISO)/International Electrotechnical Commission (IEC)*-Standards der *2700x*-Reihe und die *IT-Grundschutz*-Kataloge des BSI [Bun11a].

Diese Arbeit soll die verschiedenen Standards im IT-Sicherheitsmanagement in ihren historischen und rechtlichen Kontext einordnen, ihre Herkunft und Verbreitung untersuchen und miteinander vergleichen[3].

Methodisch orientiert sich diese Arbeit in ihrer wissenschaftlichen Forschungsmethodik an der Metanalyse nach Bortz und Döring [BD06]. Der aktuelle Forschungsstand zur geschichtlichen Entwicklung des IT-Sicherheitsmanagements wird in Kapitel 2 beschrieben. Im darauf folgenden Kapitel 3 werden dem Leser grundlegende Begriffe zum Thema IT-Sicherheitsmanagement erläutert. Mittels einer Analyse von Primär- und Sekundärquellen bereiten die Kapitel 4 und 5 die Herkunft und die geschichtlichen Hintergründe der *ISO/IEC 2700x*-Familie und des *IT-Grundschutzes* auf. Anschließend folgt eine Analyse der Zusammenhänge, der zahlenmäßigen Verbreitung und der Bedeutung der Standards für Unternehmen im Kapitel 6. Eine Analyse und Bewertung des Einflusses der gesetzlichen Grundlagen findet im Kapitel 7 statt. Abschließend fasst Kapitel 8 die Ergebnisse der Arbeit zusammen.

[3]Der vorliegende Text ist mithilfe von [Goc08] erstellt.

2 Stand der Forschung

Dieser Abschnitt erläutert, inwiefern sich die wissenschaftliche Forschung bereits mit der geschichtlichen Evolution des IT-Sicherheitsmanagements und der gesetzlichen Vorgaben auseinandergesetzt hat und liefert einen Überblick über das bisher Erforschte.

Der historische Hintergrund der IT-Sicherheit wurde bereits von vielen Autoren detailliert beschrieben (zum Beispiel [Kem02] [Ran98] [Rob93]). Eine umfassende Hintergrundanalyse der *Cyber Security* (Computersicherheit) für technische Produkte und Systeme bis zum Jahr 2002 bietet [Kem02] in der *Encyclopedia of Software Engineering* [Mar02]. Dabei wird unter anderem auf die Entwicklung verschiedener Konzepte und Architekturen wie der *security kernel architecture* in den 1970er Jahren für hochsichere Computersysteme eingegangen. Kemmerer beschreibt, wie 1983 das amerikanische Department of Defense (DoD) Computer Security Center (CSC) ihre ersten Bewertungskriterien Trusted Computer System Evaluation Criteria (TCSEC) veröffentlichte und wie Kanada, die Bundesrepublik Deutschland und Großbritannien Ende der 1980er Jahre mit eigenen Kriterien nachzogen. Allerdings beschreibt [Kem02] nur die historische Entwicklung der Evaluationskriterien für IT-Sicherheit (*Common Information Technology Security Criteria*), ohne jedoch auf ISMS einzugehen.

Die geschichtliche Entwicklung der IT-Sicherheitsstandards wurde unter anderem von [Völ04, S. 102-105] [Cal05, S. 80 ff.] [KRSW08, S. VII] [SA09, S. 18-21] beschrieben. Allerdings schreiben die Autoren entweder sehr detailliert über einen einzigen Standard wie die *ISO/IEC*-Familie oder gehen nur sehr vage und knapp auf die historische Entwicklung der jeweiligen Standards ein. Eine graphische Übersicht in Form eines Diagramms oder einer Zeitleiste zur besseren Einordnung der verschiedenen Standards fehlt in der Literatur.

Eine zusammenfassende Darstellung der historischen Kontexte der erwähnten Standards, der gesetzlichen Regelungen und deren Verbreitung ist bisher weder in schriftlicher, noch in graphischer Form erfolgt. Dieses Faktum bildet die Grundlage für die nachfolgende Arbeit.

3 Grundlagen der IT-Sicherheit

In diesem Kapitel werden grundlegende Begriffe der Informationssicherheit, Standards und gesetzliche Vorgaben erläutert und Grundsätzliches zum Themenbereich des IT-Sicherheitsmanagements ausgeführt.

3.1 Definitionen zum Themenbereich IT-Sicherheit

In Literatur und Praxis finden sich je nach Autor und sprachlichem Umfeld unterschiedliche Interpretationen der im Folgenden erläuterten Begrifflichkeiten.

Für die Abkürzung **IT** wird die Bezeichnung Informationstechnik synonym zu Informationstechnologie benutzt. Die technische Verarbeitung und Übertragung von Informationen steht bei der IT im Vordergrund.

Im Englischen hat der deutsche Begriff der **IT-Sicherheit** zwei verschiedene Ausprägungen. Die Eigenschaft der **Funktionssicherheit** (englisch: *safety)* stellt sicher, dass sich ein System konform zur erwarteten Funktionalität verhält. Es funktioniert so, wie es soll. **Informationssicherheit** (englisch: *security*) bezieht sich auf den Schutz der technischen Verarbeitung von Informationen und ist eine Eigenschaft eines funktionssicheren Systems. Sie soll verhindern, dass nicht-autorisierte Datenmanipulationen möglich sind oder die Preisgabe von Informationen stattfindet [Eck09, S. 4 f.].

Schutzziele werden zum Erreichen bzw. Einhalten der Informationssicherheit und damit zum Schutz der Daten vor beabsichtigten Angriffen von IT-Systemen definiert: **Vertraulichkeit** (englisch: *confidentiality*) ist gewährleistet, wenn kein unbefugter Informationsgewinn zum Beispiel durch Abhören einer Leitung möglich ist. Das Schutzziel der **Integrität** (englisch: *integrity*) der Daten ist erreicht, wenn die Daten vor unerlaubter und unbemerkter Modifikation geschützt sind. Funktioniert der autorisierte Zugriff auf ein System oder Dienst zuverlässig, wird dieser Zustand als **verfügbar** (englisch: *available*) angesehen. Inkludiert sind dabei geplante Beeinträchtigungen wie Ausführungsverzögerungen beim Zuweisen von Prozessorzeit für einzelne Prozesse [Eck09, S. 6-11].

Jedes noch so gut geplante und umgesetzte IT-System kann **Schwachstellen** besitzen. Sind bestimmte Angriffe zum Umgehen der vorhandenen Sicherheitsvorkehrungen möglich, ist das System **verwundbar**. Nutzt ein Angreifer eine Schwachstelle oder eine Verwundbarkeit zum Eindringen in ein IT-System, sind die Vertraulichkeit, Datenintegrität und Verfügbarkeit bedroht (englisch: *threat*). Angriffe auf die Schutzziele bedeuten für Unternehmen Angriffe auf reale Unternehmenswerte, im Regelfall das Abgreifen oder Verändern von unternehmensinternen Informationen. Jede mögliche Bedrohung ist ein **Risiko** (englisch: *risk*) für das Unternehmen. Unternehmungen versuchen durch die Verwendung eines **Risikomanagement**s (englisch: *risk management*) die Wahrscheinlichkeit des Eintretens eines Schadens und die daraus resultierende Schadenshöhe zu bestimmen [Eck09, S. 14-17].

Nach einer *Risikoanalyse* und *Bewertung* der unternehmensspezifischen IT-Systeme, können entsprechende *Schutzziele* definiert werden. Anschließend folgt die Auswahl von **IT-Sicherheitsmaßnahmen** für die jeweiligen

Geschäftsprozesse eines Unternehmens. Dieser Vorgang zählt zu den Tätigkeiten des **IT-Sicherheitsmanagements**. Eine normierte Vorgehensweise wird durch das Verwenden von **IT-Standards** ermöglicht. Gründe für die Verwendung von Standards werden im nächsten Abschnitt erläutert.

3.2 IT-Standards: Komplexität von soziotechnischen Systemen

Während Unternehmen grundsätzlich auf sozialer Interaktion von Individuen beruhen, kommunizieren technische Systeme mit Hilfe von formalen Methoden und mathematischer Logik miteinander. Diese beiden hochkomplexen „Welten" stehen in direkter Wechselwirkung zueinander. Ihr gemeinsamer Erfolg rührt aus der Kombination und dem Zusammenwirken von sozialer als auch technischer Leistung (englisch: *performance*). Das Zusammenwirken und -funktionieren dieser voneinander abhängigen Komponenten ist charakteristisch für die sogenannten **soziotechnischen Systeme** und erhöht deren Komplexität nochmals [Syl08, S. 3-7]. Zur Bewältigung der Komplexität benutzen viele Organisationen ab einer bestimmten Unternehmensgröße das Werkzeug der Standardisierung[4] als Koordinierungsmechanismus [Min79, S. 5-9, S. 249 ff., S. 261 f.]. Diese formelle Koordinierung von Tätigkeiten dient betriebswirtschaftlich der Senkung von Geschäftsprozesskosten[5]. Eine Normung, wie die Standardisierung auch genannt wird, kann im technischen Bereich verschiedene Ziele beinhalten: beispielsweise das Herbeiführen einer Systemkompatibilität, Interoperabilität zwischen unterschiedlichen Systemen oder die Sicherstellung eines geeigneten, dem Unternehmen angepassten Niveaus an Sicherheit.

3.3 IT-Sicherheitsmanagement

Im Rahmen des IT-Sicherheitsmanagements findet die Auswahl und Umsetzung entsprechender IT-Sicherheitsstandards statt [SA09, S. 5]. Zu diesem Zweck existieren im Bereich IT-Sicherheitsmanagement verschiedene Standards. Wie im vorherigen Abschnitt erläutert, besitzen soziotechnische Systeme von Grund auf eine hohe Komplexität. Mit Hilfe des *ISO/IEC 27001*- oder des *IT-Grundschutz*-Standards wird mit anerkannten Regeln versucht, diese Komplexität für den Bereich des IT-Sicherheitsmanagements zu reduzieren und ein geeignetes Maß an Informationssicherheit zu finden. Mit anderen Worten werden die relevanten IT-Prozesse

[4] zum Beispiel von Arbeitsprozessen, -ergebnissen und -fähigkeiten.

[5] Anfang der 1990er Jahre begann sich eine prozessorientierte Sichtweise in den Organisationen durchzusetzen. Der Kunde und die Geschäftsprozesse stehen im Fokus. Die IT nimmt dabei eine wichtige Unterstützungsfunktion ein.

„transparent und somit beherrschbar“ gemacht und das IT-Gesamtrisiko reduziert [SA09, S. 4 f.]. Durch die „Nutzung vorhandener [...] Vorgehensmodelle“ [SA09, S. 4 f.] wird zudem eine Senkung der Kosten angestrebt. Die Unternehmen haben durch die „Zertifizierung des Unternehmens sowie von Produkten“ [SA09, S. 4 f.] einen Wettbewerbsvorteil. Sie zeigen externen Dritten durch die Zertifizierung, dass sie die vorgegebenen Anforderungen an die IT-Sicherheit erfüllt haben. Die IT-Sicherheit hat aus diesen Gründen enorm an Bedeutung gewonnen.

Der Begriff des IT-Sicherheitsmanagements taucht vor Veröffentlichung der *Green Books* des Department of Trade and Industry (DTI) im Jahre 1989 nicht auf (siehe Abschnitt 5.2.1). Die Terminologie existierte bis zu diesem Zeitpunkt schlichtweg nicht. Gleichwohl wurden bereits von amerikanischen Behörden in den 1970er Jahren Methoden für ein strukturiertes Vorgehen zur Absicherung gegen Bedrohungen der Informationssicherheit verwendet [RM77]. In den 1980er Jahren folgten im englischsprachigen Bereich einige Studien und Aufsätze zum Thema *computer abuse and security* und wie eine effektive Informationssicherheit durch organisatorische Maßnahmen in einem Unternehmen erreicht werden konnte [Str86, Dat87, Str88, FKB89, Str90]. Zu diesem Zeitpunkt war zumindest einigen Autoren klar, dass die Datensicherheit Aufgabe des Managements ist [Mou84]. Diese Einsicht setzte sich erst langsam in den Köpfen der Verantwortlichen in Unternehmen fest.

4 Die geschichtliche Entwicklung der IT-Sicherheitskriterien

Zur Zeit der ersten Computer standen Einzelarbeitssysteme in einem extra gesicherten Raum. Der Zutritt wurde nach Überprüfung der Identität durch Wachpersonal gewährt. Der Zugriff auf einen Computer war nur einem einzigen Benutzer zur Zeit möglich. Die Datensicherheit hing demnach in erster Linie von der physischen Sicherheit ab [Kem02, S. 1].

Seit dem Aufkommen des *Time-Sharing*-Ansatzes in den 1960er Jahren rückte die Datenzugriffskontrolle in den Fokus. Erstmals wurde mehreren Usern das gemeinsame Arbeiten auf einem (Groß)rechner ermöglicht. Dieser Mehrbenutzeransatz brachte das Problem der mehrstufigen Sicherheit (englisch: *Multilevel security (MLS)*[6]) mit sich. Zur Lösung dieses Problems wurden vom DoD mehrere Studien in Auftrag gegeben: Auf Basis von James P. Andersons *reference monitor*-Prinzip aus dem Jahr 1972 wurde die *secure kernel*-Architektur erforscht und in verschiedene Computersysteme wie dem *IBM 370* implementiert. Es gelang allerdings aufgrund von Desgin- und Implementierungsfehlern beinahe jedes System zu kompromittieren [Kem02, S. 1 f.].

4.1 Erste Standardisierungsbemühungen

Im Oktober 1967 begann eine Taskforce unter der Führung des *Defense Science Boards*[7] Maßnahmen zum Schutz von vertraulichen Informationen in Mehrbenutzer-Computersystemen mit Fernzugriff (englisch: *remote-access, resource-sharing computer systems*) zu entwickeln. Der *Security Controls for Computer Systems*-Report präsentierte die Ergebnisse der Taskforce im Februar 1970. Der Report sprach einige richtlinienbezogene und technische Empfehlungen aus [Dep85b, S. 7]. Die „Security Requirements for Automatic Data Processing (ADP) Systems“ (*DoD Directive 5200.28*) aus dem Jahr 1972 und das dazugehörige Handbuch *DoD 5200.28-M* führten einheitliche DoD-Richtlinien, Sicherheitsanforderungen, administrative Kontrollen und technische Maßnahmen ein. Diese dienten dem Schutz von vertraulichen Informationen, welche durch DoD-Computer verarbeitet wurden [Dep85b, S. 7].

In den siebziger Jahren wurde unter der Leitung des National Bureau of Standards (NBS) begonnen, „problems and solutions for building, evaluating, and au-

[6] Verwendung von nicht-vertrauenswürdigen und vertrauenswürdigen Komponenten oder unterschiedlichen Sicherheitsstufen.

[7] In diesem Board beraten zivile Experten das DoD bei technischen und wissenschaftlichen Fragestellungen.

diting secure computer systems“ [Dep85b, S. 7] zu definieren. Zwei Workshops fassten die verschiedenen bis dato existierenden Computer-Sicherheitsrichtlinien der amerikanischen Behörden unter den Titeln *Audit and Evaluation of Computer Security* (November 1977) und *Audit and Evaluation of Computer Security II* (April 1978) zusammen. Die verwendeten behördlichen Richtlinien beinhalteten unter anderem die Anweisung, Zuständigkeiten klar zu benennen, sowie Vorlagen und Leitfäden zum Ausfüllen von Reports und Checklisten (*DoD Regulation 5200.1-R* von 1982 und *DoD 5220.22-M* von 1987) [Depb, S. 2]. Das Industrial Security Manual for Safeguarding Classified Information (ISM)[8] führte einheitliche „security practices“ in industriellen Betrieben zum Schutz vertraulicher Informationen ein und ermutigte Manager zu erhöhter Aufmerksamkeit vor der Preisgabe von unternehmensinternen Informationen [Depb, S. 280]. Das Memorandum „Security of Federal Automated Information Systems“ (*OMB Circular No. A-71*) aus dem Jahr 1978 wies jede Behörde an, ein Computer-Sicherheitsprogramm einzuführen und zu unterhalten. Es machte den Leiter einer Abteilung oder Behörde dafür verantwortlich, ein angemessenes Sicherheitsniveau für alle behördlichen Daten zu gewährleisten. Das galt sowohl für die interne als auch für die externe, kommerzielle Datenverarbeitung. Der verantwortliche Beamte war darüber hinaus auch für den Aufbau von physischen, administrativen und technischen Schutzvorkehrungen verantwortlich. Diese Vorkehrungen sollten persönliche, behördeneigene oder andere sensitive Daten ausreichend schützen [Dep85b, S. 70].

Fites und seine Mitautoren [FKB89] zeigten, wie nordamerikanische Unternehmen in der Zeit vor der Existenz von IT-Sicherheitsmanagement-Standards ihre IT-Sicherheit überprüfen konnten. Zunächst wurden im Rahmen eines Risikomanagements die wichtigen Unternehmenswerte (englisch: *assets*) möglichen Bedrohungen gegenübergestellt. Anschließend entwarf und implementierte man organisatorische, administrative und technische Sicherheits- und Kontrollmaßnahmen. Eine wiederkehrende Überprüfung der Implementierung und ständige Reviews der Maßnahmen stellten im Ergebnis eine effektive Sicherheit und Kontrolle der IT dar. Allerdings fehlten anders als zum Beispiel beim Vorgehen nach *IT-Grundschutz* konkrete Vorschläge zur Maßnahmenumsetzung [FKB89, S. 5. f].

4.2 Das Orange Book

Auf dieser konzeptionellen Grundlage gründete 1981 das DoD das CSC[9] als eine Unterabteilung der National Security Agency (NSA), um eine Möglichkeit zur Eva-

[8] *DoD 5220.22-M* wurde in den 1990er Jahren in National Industry Security Program Operating Manual (NISPOM) umbenannt und beinhaltete ein Vorgehen auf Basis einer Bedrohungsanalyse und eines Risikomanagements [Depa, S. 2].

[9] Das heutige National Computer Security Center (NCSC).

luierung kommerzieller Computersysteme mit Bezug auf IT-Sicherheit zu schaffen. Weitere Aufgaben des CSC waren die Standardisierung der Evaluierung sowie das Forschen und Entwickeln im Bereich der IT-Sicherheit. Zwei Jahre später (1983) wurden mit dem sogenannten *Orange Book* (TCSEC)[10] weltweit die ersten IT-Sicherheitskriterien veröffentlicht und 1985 zum Standard [Dep85b] erklärt. Der Standard verfolgte zwar einen „Commercial Produce Evaluation Process", mit dem kommerzielle Unternehmen ihre Produkte auf die behördlichen Anforderungen abstimmen konnten. Allerdings stellten die *TCSEC* keine umfassende Evaluierung der Sicherheit von Computersystemen dar [Dep85b, S. 85]. Die Anforderungen an ein umfassendes IT-Sicherheits-Konzept wurden zu diesem Zeitpunkt folgendermaßen beschrieben:

> A complete study [...] must consider additional factors dealing with the system in its unique environment, such as it's proposed security mode of operation, specific users, applications, data sensitivity, physical and personnel security, administrative and procedural security, TEMPEST, and communications security. [Dep85b, S. 85]

Das DoD summiert in [Dep85b] auf Seite 59, dass Schutzmaßnahmen in Form von Sicherheitsrichtlinien in Abhängigkeit der wahrgenommen Gefahren, ihren Risiken und den Unternehmenszielen definiert werden müssen. Das *Yellow Book* (CSC-STD-003-85) definiert im Juni 1985 zu diesem Zweck einen Risikoindex[11] [Dep85a].

Durch den *Computer Security Act of 1987* wurden gesetzliche Vorgaben für ein Mindestmaß an Sicherheit für staatliche Computersysteme (militärisch und zivil) beschlossen [100], nach [Kem02, S. 2 f.].

Im Anschluss an die Veröffentlichung des *Orange Book*[12] zogen die Bundesrepublik Deutschland, Kanada und das britische *Commercial Computer Security Center (CCSC)* mit eigenen Kriterien für die Bewertung von IT-Sicherheit nach. Die Westdeutschen nannten ihren Standard *Deutsche IT-Sicherheitskriterien* (englisch: *IT-Security Criteria*)[13]. Er wurde im Januar 1989 veröffentlicht. Im Mai des selben Jahres stellten die Kanadier ihre *Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)* vor. Eine Besonderheit stellten die ebenfalls 1989 veröffentlichten britischen *Green Books*[14] des *DTI* dar (für eine grafische Übersicht

[10] Der Zweck des Orange Books wird folgendermaßen beschrieben: „Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28." [Dep85b, S. 2]

[11] Risikoindex „is defined as the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system." [Dep85a, S. 1]

[12] Den Spitznamen erhielt das Buch durch die Farbe der Titelseite bzw. des Covers.

[13] Die deutschen Kriterien wurden auch *Grünbuch* bzw. *Green Book* genannt.

[14] Leicht zu verwechseln mit dem deutschen *Green Book*.

siehe Abbildung 1). Sie ermöglichten Anbietern erstmals eine Bewertung von kommerziellen Produkten der IT-Sicherheit [Rob93, S. 154 f.] [Kem02, S. 3]. Aus ihnen ging die spätere *ISO/IEC 2700x*-Norm hervor. Eine detaillierte Auseinandersetzung mit der *ISO/IEC 2700x*-Norm folgt im Abschnitt 5.2.1.

1990 begannen Frankreich, Deutschland, die Niederlande und Großbritannien gemeinsam, international gültige Evaluationskriterien für die IT-Sicherheit zu entwickeln. Sie nannten das Projekt *Information Technology Security Evaluation Criteria (ITSEC)*. 1993 beschlossen die Vereinigten Staaten mit den Kanadiern und Europäern zusammenzuarbeiten. Die erste Version der *Common Information Technology Security Criteria (CC)* (oder auch Common Criteria) wurde im Januar 1996 veröffentlicht. Seit Dezember 1999 sind die Common Criteria der internationale Standard *ISO/IEC 15408* [Kem02, S. 3 f.]. Die aktuelle Fassung im September 2013 ist die vierte Revision der *CC* 3.1[15].

4.3 Fazit

Das Problem der Datenzugriffskontrolle entstand, sobald es mehreren Benutzern möglich war, die Kapazität eines Großrechners gemeinsam zu benutzen. Seit den 1960er Jahren versuchten die amerikanischen Behörden unter der Federführung des DoD, Maßnahmen zum Schutz von Informationen zu erforschen und umzusetzen. Dabei wurden bereits existierende Sicherheitsrichtlinien aufgegriffen und zu einem großen Teil 1985 im amerikanischen *Orange Book* vereinheitlicht. Dieser Standard führte Kriterien und eine Evaluierung technischer Komponenten aller Art ein. Die Weiterentwicklung des *Orange Book* stellen die international ausgerichteten *Common Criteria* dar. Die beiden Standards sind allerdings kein umfassendes IT-Sicherheitskonzept. Das nachfolgende Kapitel befasst sich mit umfassenden IT-Sicherheitskonzepten.

5 IT-Standards

In diesem Kapitel folgen detaillierte Analysen der geschichtlichen Hintergründe der beiden ISMS *ISO/IEC 2700x* und *IT-Grundschutz*. Die *ISO/IEC 2700x*-Familie und der *IT-Grundschutz* sind die bekanntesten Standards im Bereich IT-Sicherheit.

[15] Die *CC* 3.1 wurde im September 2012 veröffentlicht.

5.1 Grundlegende Informationen zu ISMS

Einleitend folgt eine vergleichende Übersicht allgemeiner Informationen von Standards des IT-Sicherheitsmanagements.

Tabelle 1: Grundlegende Informationen über Standards des IT-Sicherheitsmanagements [ENI13b] [BF08, S. 10].

	ISO/IEC 2700x	**IT-Grundschutz**
Vorgänger	BS 7799, ISO/IEC 17799	ITSHB, IT-GSHB
Kompatibel zu	ISO-Standards	ISO/IEC 27001
Erstpublikation	2005	2005
Anzahl Standards[a]	über 20	4
Prozessorientiertes Verbesserungskonzept	PDCA, DMAIC, u.a.[b]	PDCA
Audit	ja	ja
Zertifizierung	ja[c]	ja

[a] Alle Standards werden von zusätzlichen Leitfäden / Anleitungen unterstützt.
[b] Die Verwendung anderer Konzepte ist mit der *ISO/IEC 27001:2013*-Norm möglich.
[c] Zertifizierung nur nach der *ISO/IEC 27001*-Norm möglich.

Entwickelten sich viele Standards ursprünglich in sprachlicher, geographischer und institutioneller Hinsicht unabhängig voneinander, nähern sich die Normen immer mehr einander an. Seit Erscheinen der *ISO/IEC 17799*-Norm im Jahr 2000 hat besonders das Thema der *Kompatibilität* der Standards untereinander (siehe Tabelle 1) die Weiterentwicklung geprägt. So ist der *IT-Grundschutz* zur *ISO/IEC 27001*-Norm kompatibel. Seit 2012 werden alle ISO-Normen einer neuen Struktur für Managementstandards mit dem Namen *Annex SL* angepasst. Damit bezweckt die ISO eine bessere Verknüpfung der Standards untereinander. Die Einführung und Verwendung mehrerer ISO-Standards wie zum Beispiel der *ISO/IEC 27001* und der *ISO/IEC 27000* nebeneinander soll vereinfacht werden [TW12].

Jeder Standard besitzt grundsätzlich eine *Anzahl* für die Umsetzung unbedingt notwendiger Standardwerke (die sogenannten *Standards*). Im *ISO/IEC 2700x*-Jargon sind dies die *normativen Standards* (Anforderungen). Ergänzende Leitfäden (Anleitungen) können zum Beispiel technische Hilfestellungen oder die Terminologie erklärende Werke sein. Sie zählen zu den *informativen Standards*. Die Zahlen in der Tabelle 1 dienen nur als Richtwerte und unterscheiden sich je nach Autor und Interpretation des Wortes „Standard“.

Allen in der Tabelle 1 dargestellten Standards ist die Verwendung des Demingkreis-Zyklus gemeinsam. In vier sich wiederholenden Schritten (Plan - Do - Check - Act) wird ein *kontinuierlicher Prozess zur Qualitätsverbesserung* beschrieben[16].

Unabhängig durchgeführte *Audits* können jederzeit von dafür ausgebildeten Auditoren vorgenommen werden. Sie dienen zur unternehmensinternen Überprüfung der IT-Sicherheit. Die *Zertifizierung* hingegen kann nur von speziellen Zertifizierungsstellen vorgenommen werden und zeigt externen Firmen oder Personen, dass das Unternehmen die gesetzten Anforderungen an die IT-Sicherheit erfüllt hat.

5.2 ISO/IEC 2700x

Die *ISO* ist der größte Entwickler von internationalen Standards. Sie entstand 1947 aus einem Zusammenschluss von Normungsorganisationen aus 25 Ländern. Im Jahr 2013 zählen Mitglieder aus 163 Staaten zu der Organisation, das *Deutsches Institut für Normung (DIN)* trat 1951 bei. Bis dato hat die ISO über 19.500 Normen im industriellen Bereich publiziert [Int13b]. In den Bereichen der Elektrik und Elektrotechnik entwickelt die *IEC* als gleichberechtigte Organisation[17] neben der ISO ebenfalls Normen. In einigen Bereichen wie der IT-Sicherheit arbeiten beide Organisationen in gemeinsamen Komitees (englisch: *Joint Technical Committee (JTC)*) zusammen. Das ISO/IEC JTC 1 *Information technology* in dem Subkomitee SC 27 *IT Security techniques* befasst sich mit der Entwicklung der *ISO/IEC 2700x*-Standards [Int13a]. Das deutsche Pendant ist der *Normenausschuss Informationstechnik und Anwendungen* NA 043 NIA-01-27 *IT-Sicherheitsverfahren* [Deu10].

Nachdem die wichtigen Organisationen rund um die *ISO/IEC 2700x*-Familie erklärt wurden, wird nachfolgend geklärt, wie sich die Familie geschichtlich entwickelt hat. Die Abbildung 1 bereitet den folgenden Text in visueller Form zum einfachen Nachvollziehen der Ereignisse auf.

[16] Die für Oktober 2013 erwartete *ISO/IEC 27001:2013*-Norm löst sich erstmals von dem PDCA-Konzept als einzigem kontinuierlichem Verbesserungsprozess (siehe Kapitel 5.2.1).

[17] Die ISO, IEC und die *International Telecommunication Union (ITU)* gehören der *World Standards Cooperation (WSC)* an [Wor11].

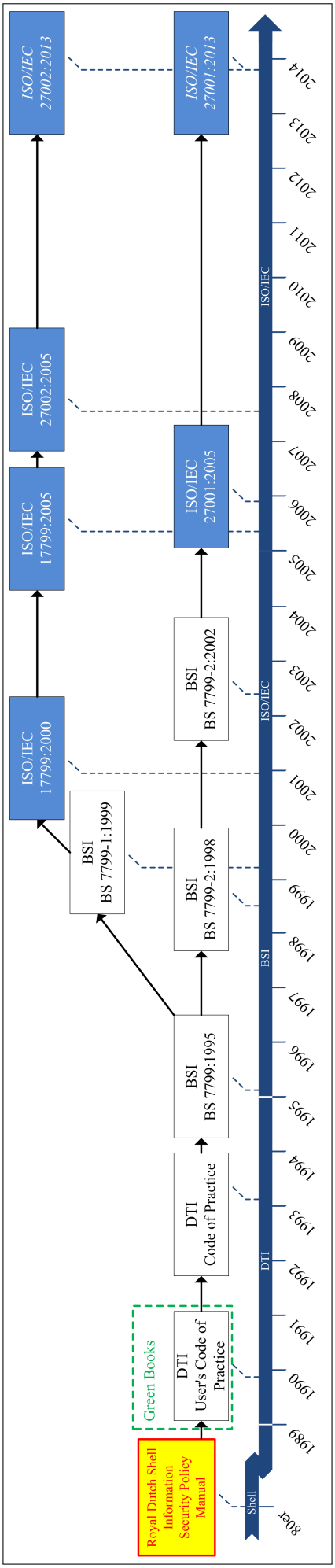

Abbildung 1: Evolution der *ISO/IEC 27001/2*-Standards.

5.2.1 Geschichtliche Hintergründe

Wie bereits im Kapitel 4.2 angedeutet, entwickelte die Abteilung CCSC der britische Behörde DTI[18] als Vorreiter im Bereich des IT-Sicherheitsmanagements die sogenannten *Green Books*. Sie enthielten zum einen den britischen Entwurf von Evaluationskriterien für die IT-Sicherheit und ein dazugehöriges Evaluierungs- und Zertifizierungs-Schema (siehe Abschnitt 4). Gleichzeitig wurde ein „code of good security practice“[19] [Völ04, S. 102] entwickelt, welcher im Ergebnis die Bücher *User's Code of Practice* (V11) und *Vendor's Code of Practice* (V31) hervorbrachte. Die englischen *Green Books* wurden von Februar bis November 1989 als Vorentwurf (englisch: *draft*) veröffentlicht und kamen nicht über diesen Status hinaus [Rob93, S. 154 f. und 160].

Auf Initiative des DTI wurde seit 1992 gemeinsam mit führenden britischen Firmen und Organisationen[20] und dem National Computing Centre (NCC) der bisherige Vorentwurf des *User's Code of Practice* weiterentwickelt. Das Resultat, *A code of practice for information security management* (Public Document 003), erschien 1993, wurde anschließend überarbeitet und im Februar 1995 der britische Standard *BS 7799:1995*[21]. Die Norm trug den Titel *Code of Practice for IT Security Management* und sollte der Industrie und den Behörden als Unterstützung bei der Umsetzung von Maßnahmen zur Informationssicherheit dienen [Völ04, S. 102]. Unternehmungen konnten ihre *Code of Practice*-kompatiblen ISMS nun von unabhängiger Seite überprüfen lassen, allerdings fehlte die Möglichkeit einer Zertifizierung.

Aufgrund einer steigenden Aufmerksamkeit auch außerhalb Großbritanniens entwickelte sich die Norm zu einer international verwendeten *best practice*. Im Jahr 1998 begann eine Revision des Standards. Maßnahmen für neue technische Entwicklungen wie E-Commerce wurden hinzugefügt und alle „UK-spezifischen Verweise“ entfernt. Die neue, international ausgerichtete Fassung *BS 7799-1:1999* (Teil 1) wurde im März 1999 veröffentlicht. Im gleichen Jahr entschied sich das englische ISO-Komitee, den Standard in einem beschleunigtem Verfahren (*Fast Track*[22]) bei der ISO einzureichen. In diesen Prozess wurde der ursprüngliche Text des

[18] Der Nachfolger des DTI wurde 2009 das *Department for Business, Innovation and Skills (BIS)* [Dep10a].

[19] In Teilen basierte dieser auf dem unternehmensinternen *Information Security Policy Manual* von Royal Dutch Shell [KM11, Kapitel 3.2].

[20] Dazu zählten Royal Dutch Shell, BT, BOC, Marks&Spencer, Midland Bank, Nationwide Building Society und Unilever [Völ04, S. 103].

[21] Herausgeber war das British Standards Institute (BSI).

[22] Dabei wird ein eingereichter Standard direkt als *Draft International Standard (DIS)* oder *Final Draft International Standard (FDIS)* eingestuft. Es bedarf nur noch der Freigabe der ISO-Komitee-Mitglieder.

BS 7799-1:1999 vom gemeinsamen Technischen Komitee ISO/IEC JTC 1/SC 27 ohne Korrektur in den Standard *ISO/IEC 17799:2000*[23] übernommen [Völ04, S. 102]. Im Rahmen des normalen ISO-Revisionszyklus folgte im Juni 2005 die zweite Fassung des Standards mit dem Namen *ISO/IEC 17799:2005*. Im Juli 2007 beschloss die ISO eine Namensänderung vom bisherigen *ISO/IEC 17799:2005* in *ISO/IEC 27002:2005* [Fri13b, Folie 4]. Abbildung 1 stellt die Zusammenhänge übersichtlich dar.

Der zweite Teil des britschen Standards, *BS 7799-2:1998* (Teil 2), mit dem Namen *Information Security Management Systems - Specification with Guidance for Use* ging aus der ursprünglichen *BS 7799:1995*-Norm hervor. Er erschien 1998 zum ersten Mal „und beschreibt in Form von Spezifikationen ein Modell eines ISMS“ [KRSW13, S. 12]. Firmen und Behörden waren erstmals anhand eines Standards in der Lage, ihre ISMS zu beurteilen und zertifizieren zu lassen. 2002 folgte eine Revision des Standards mit großen Veränderungen unter anderem im Anhang A. Ziel war „die Harmonisierung mit anderen Management- Standards, beispielsweise ISO 9001:2000 und ISO 14001“ [Völ04, S. 102]. Das Ergebnis war der *BS 7779-2:2002* [Cal05, S. 80 f.]. Im Jahr 2004 entschied sich das ISO-Komitee des Vereinigten Königreiches (UK) den Standard bei der ISO einzureichen. Nach dem Durchlaufen des *Fast Track*-Verfahrens folgte ein Jahr später die Freigabe der internationalen *ISO/IEC 27001:2005*-Norm innerhalb der neuen Normenreihe *ISO/IEC 2700x* [Fri13b, Folie 4]. Abbildung 1 visualisiert den bisherigen Verlauf.

Eine Übersetzung der Standards in die deutsche Sprache erfolgte durch den Normenausschuss NA 043 NIA-01-27 *IT-Sicherheitsverfahren*. Die englischsprachige *ISO/IEC 27001:2005* liegt als *DIN ISO/IEC 27001:2005* seit September 2008 in einer deutschen Fassung vor. Im selben Zeitraum erschien die deutsche Fassung *DIN ISO/IEC 27002:2005* der englischsprachigen *ISO/IEC 27002:2005* [Deu13].

Seit dem Jahr 2005 wuchs die Anzahl neuer Standards innerhalb der *ISO/IEC 2700x*-Familie auf über 20 Normen an (Stand: Juni 2013). Zu diesem Zeitpunkt war eine Gesamtzahl von mindestens 31 Standards geplant [Fri13b, Folie 7 ff.]. Eine Übersicht über die Beziehungen und Abhängigkeiten innerhalb der Normenfamilie gibt Abbildung 2.

Anhand der Abbildung 2 zeigt sich die mengenmäßige Entwicklung der *ISO/IEC 2700x*-Familie. 2005 beziehungsweise 2007 bestand sie nur aus den „ISMS-Anforderungen“ (*ISO/IEC 27001:2005*) und dem „Leitfaden zur Umsetzung“ (*ISO/IEC 27002:2005*). Anschließend folgte 2007 die „Anforderungen an Stellen, die Audits und Zertifizierungen durchführen“ (*ISO/IEC 27006:2007*). In den darauf folgenden Jahren wurden weitere allgemeine normative Leitfäden

[23] Erschien im Dezember 2000.

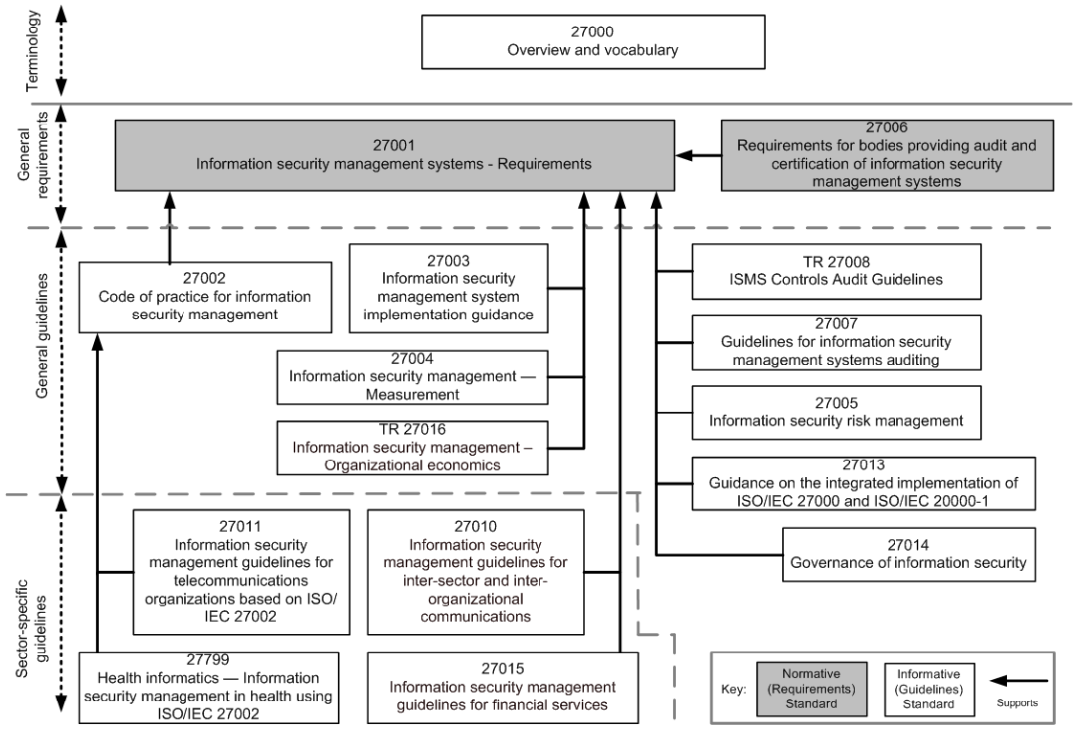

Abbildung 2: Zusammenhänge in der *ISO/IEC 2700x*-Familie [II12].

wie die *ISO/IEC 27005:2008* (Risikomanagement), *ISO/IEC 27004:2009* (Metriken und Kennzahlensysteme) und *ISO/IEC 27003:2010* (Implementierung eines ISMS) veröffentlicht. Diverse weitere Standards sind branchenspezifisch ausgerichtet (zum Beispiel *ISO/IEC 27011:2008* für Telekommunikationsunternehmen) oder decken spezielle Themengebiete wie die *Cybersecurity* ab (*ISO/IEC 27032:2012*) [KRSW13, S. 13]. Der zunehmenden Menge an Standards zum Trotz benötigen Unternehmen für eine ISMS-Zertifizierung lediglich den Standard *ISO/IEC 27001* und als Hilfestellung für Anbieter von Audits und Zertifizierungen die *ISO/IEC 27006*-Norm. Dies verdeutlicht Abbildung 2. Mehr zur Zertifizierung findet sich im Kapitel 5.2.2.

Nach jahrelanger Revision verabschiedete im Januar 2013 das ISO/IEC JTC 1/SC 27-Gremium die DIS-Version *ISO/IEC DIS 27001:2013*. Sie war bis März 2013 öffentlich einseh- und kommentierbar. Im April 2013 fand ein ISO-Komitee-Meeting zur Diskussion des Feedbacks der nationalen ISO-Mitglieder statt. Im Rahmen des Treffens folgte die Freigabe (englisch: *approval*) der DIS-Version durch die nationalen ISO-Komitee-Mitglieder. Im Juli 2013 wurde die FDIS-Version herausgegeben. Bis Anfang September 2013 konnte über die neue Version abgestimmt werden [BSI13d, BSI13b, BSI13c, Fri13b, Fri13a].

Der endgültige Standard erschien am 25. September 2013 [BSI13a]. Inhaltlich wird in der *ISO/IEC 27001:2013*-Norm eine Angleichung an den Risikomanagementprozess der *ISO 31000:2008 Risk management - Principles and guidelines* vorgenommen. Der bisher verwendete, verbindliche PDCA-Zyklus kann durch andere (kontinuierliche) Verbesserungsprozesse wie zum Beispiel die DMAIC-Methode des Prozess-Verbesserungskonzepts *Six Sigma (6σ)*[24] ersetzt werden. Für die Risikobewertung (englisch: *risk assessment*) entfallen als Grundlage zur Bewertung *Werte*, *Bedrohungen* und *Schwachstellen* (englisch: *assets, vulnerabilities und threats*). Die neue Version der Norm konzentriert sich auf den allgemeineren Ansatz „Identifizierung der Auswirkungen, die der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit auf die Werte haben könnte“ [II05, S. 5]. Die Rolle des Top-Managements im ISMS erhält durch spezifische Anforderungen eine höhere Bedeutung. Die Anzahl an *Maßnahmenzielen* (englisch: *control objectives*) im Anhang A wurde von 11 auf 14 erhöht. Gleichzeitig sinkt die Anzahl der *Maßnahmen* (englisch: *controls*) von 133 auf 113. Die Begriffe und Definitionen sind entfernt und in den informativen Standard *ISO/IEC 27000* verschoben worden [Fri13b, Fri13a, IT 13]. Ein Blick auf Abbildung 1 lässt die gesamte Entwicklung der ISO/IEC-Standards in einfacher visueller Form nachvollziehen.

5.2.2 ISO/IEC 27001-Zertifikat

Amerikanische Behörden hatten bereits in den 1970er Jahren interne Sicherheitsrichtlinien für ihre IT, nutzten *best practices* und führten interne Audits durch (siehe Kapitel 4.1). Der vorherige Abschnitt 5.2.1 erwähnt, dass in vielen britischen Großunternehmen in den 1980er Jahren eigene Sicherheitsrichtlinien in Bezug auf die IT-Sicherheit gebräuchlich waren. Durch eine interne Begutachtung (auch **Audit** genannt) konnten sie ihr korrektes Vorgehen im Abgleich mit ihren Vorgaben überprüfen. Unternehmungen konnten allerdings ihre Kompetenzen im Bereich der IT-Sicherheit nicht öffentlichkeitswirksam gegenüber (möglichen) Kunden aufzeigen.

Die Veröffentlichung des *British Standard (BS) 7799* im Jahr 1995 ermöglichte es, ISMS von unabhängiger Seite begutachten[25] zu lassen. Eine Zertifizierung des

[24] Das Prozessmanagementsystem Six Sigma entstand Ende der 1980er Jahre bei Motorola. Die dem System zugrundeliegende DMAIC-Methodik ähnelt dem Demingkreis [Chi12, S. 37-39].

[25] Ein von einer unabhängigen Zertifizierungsstelle anerkannter Auditor kann zunächst ein internes Audit durchführen. Das Ergebnis der Überprüfung ist ein sogenannter Auditbericht. Eine Veröffentlichung dieses Bericht wäre aufgrund der verwendeten Interna nicht wünschenswert. Bei Weitergabe des Auditberichts an eine vertrauenswürdige Zertifizierungsstelle prüft diese den Bericht und stellt bei festgestellter Konformität zum Standard ein Zertifikat aus. Das Zertifikat weist gegenüber Dritten die Erfüllung von z.B. gesetzlichen Vorgaben nach [KRSW13,

unternehmenseigenen ISMS auf Basis des *BS 7799* war zu diesem Zeitpunkt nicht möglich.

Der *BS 7799-2 Information Security Management Systems - Specification with Guidance for Use* ermöglichte es Unternehmen seit 1998, ihre ISMS zertifizieren zu lassen. Die Möglichkeit der Zertifizierung blieb in der dem *BS 7799-2* nachfolgenden Norm *ISO/IEC 27001* aus dem Jahr 2005 erhalten. Vergleiche dazu Kapitel 5.2.1.

Innerhalb der *ISO/IEC 2700x*-Familie kann man mit Hilfe des *ISO/IEC 27001*-Standards den Erfüllungsgrad der Konformität nachvollziehen. Wie ein Audit durchgeführt wird, beantwortet seit November 2011 der Standard *ISO/IEC 27007 Management-Audit eines ISMS* [KRSW13, S. 296].

Mit der *ISO/IEC 27006*-Norm *Anforderungen an Stellen, die Audits und Zertifizierungen durchführen* wurde 2007 der bisherige Prozess der akkreditierten Zertifizierung und damit das European co-operation for Accreditation (EA)-Dokument *EA7/03 EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems* ersetzt [Ise13].

Begleitet werden die vorher genannten Standards seit November 2011 durch den „Technischen Report“ *ISO/IEC TR 27008*. Er betrifft technische Audits von IT-Systemen und bezieht sich direkt auf Maßnahmen (englisch: *controls*) aus dem Anhang A der *ISO/IEC 27001*-Norm [Ise13] [KRSW13, S. 296].

Es ist zu beachten, dass die ISO selbst keine Zertifizierungen durchführt. Eine Organisation hat vielmehr drei Möglichkeiten, die Konformität zu einem Standard zu zeigen:

1. sie kann ihre Konformität von sich aus verkünden,
2. sie kann ihre Kunden bitten, die Konformität zu bestätigen und
3. ein unabhängiger externer Auditor kann die Konformität verifizieren [Int13d].

Auskunft über die mengenmäßige Verbreitung der *ISO/IEC 27001*-Norm gibt das Kapitel 6.2.1.

5.3 IT-Grundschutz

Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* ist eine Bundesoberbehörde der Bundesrepublik Deutschland. Sie ist dem Bundesministerium des

S. 296 f.]. Die Konformität muss nach Ablauf der Gültigkeit eines Zertifikats erneut bestätigt werden.

Inneren (BMI) untergeordnet. Die Behörde wurde am 1. Januar 1991 gegründet (vgl. *BSI-Errichtungsgesetz*[26] [Bunb]) und hat ihren Hauptsitz in Bonn. Sie ist der zentrale Dienstleister der Bundesregierung in Bezug auf die IT-Sicherheit und beschäftigte 2012 ungefähr 550 Mitarbeiter. Neben den öffentlichen Verwaltungen des Bundes, der Ländern und Kommunen zählen auch privatwirtschaftliche Unternehmen und Privatpersonen zu den Kunden des BSI. Das Ziel des BSI ist die präventive Förderung der IT-Sicherheit, damit der sichere Einsatz von Informations- und Kommunikationstechnologie (ITK) in der Gesellschaft möglich wird [Bun12a, S. 4 f.] [Bun13f]. Zu den Aufgaben zählen unter anderem der Schutz der IT-Systeme des Bundes, die Entwicklung von Mindeststandards im Bereich der IT-Sicherheit, eine Sicherheitsberatung für die Behörden und andere Kunden, Entwicklung von Kryptosystemen und die „Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen“ [Bun13e].

Kapitel 5.2 setzte sich mit den geschichtlichen Hintergründen der *ISO/IEC 2700x*-Familie textuell und anhand der Grafik 1 auseinander. In gleicher Vorgehensweise wird nachfolgend geklärt, wie sich der *IT-Grundschutz* historisch entwickelt hat. Die Abbildung 3 visualisiert die folgenden textuellen Erläuterungen zur besseren Orientierung des Lesers.

[26] Das BSI-Errichtungsgesetz wurde im August 2009 durch das *Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes* vom 14. August 2009 (BGBl. I S. 2821) ersetzt.

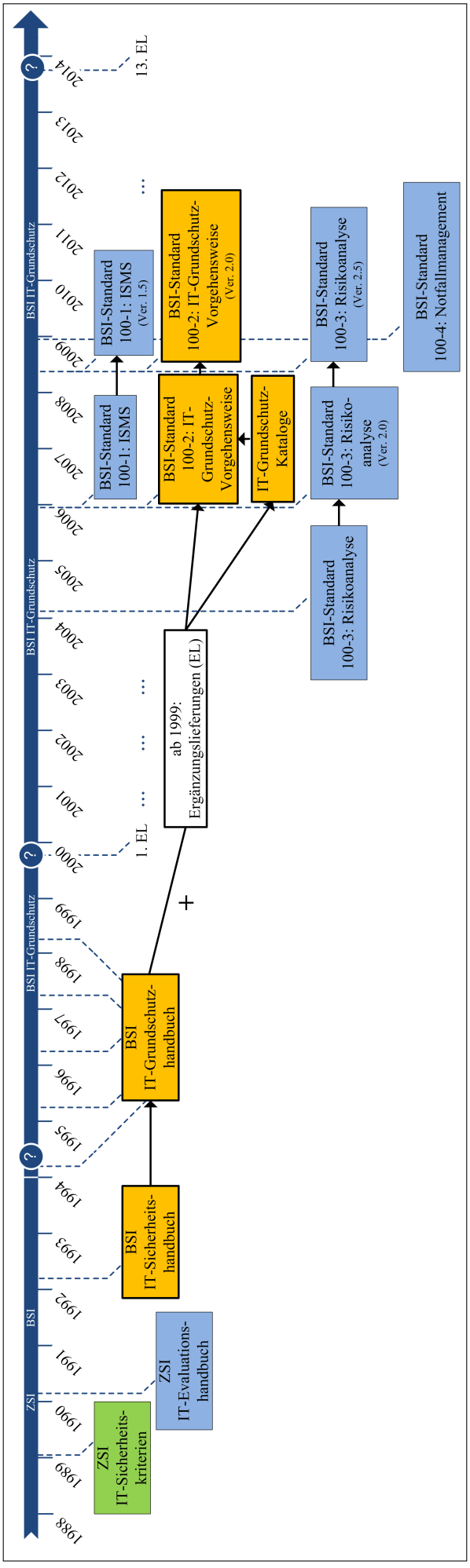

Abbildung 3: Evolution des *IT-Grundschutzes*.

5.3.1 Geschichtliche Hintergründe

Seine Wurzel hat das BSI in der *Zentralstelle für das Chiffrierwesen (ZfCh)*[27], einer Unterabteilung für Kryptoanalyse des Bundesnachrichtendienstes (BND). Deren zentrale Aufgabe konzentrierte sich auf die Kommunikationssicherheit. 1986 wurde innerhalb der ZfCh eine Arbeitsgruppe mit dem Aufgabenbereich *Computersicherheit* aufgebaut. Die Mitarbeiteranzahl wuchs auf 70 an, wobei sich die Arbeitsgruppe insbesondere „mit der Evaluierung und Zertifizierung von IT-Produkten und -systemen“ [Bun04, S. 15] beschäftige. 1987 folgte die Bildung des Interministriellen Ausschuß für die Sicherheit in der IT (ISIT) durch das BMI, im Januar 1989 wurde die ZfCh in die *Zentralstelle für Sicherheit in der Informationstechnik (ZSI)* umgewandelt. Diese Umwandlung geschah aufgrund des erweiterten Aufgabenbereiches rund um das Thema der *Zertifizierung*. Im gleichen Jahr erschienen mit dem *Grünbuch* die deutschen *IT-Sicherheitskriterien (ITSK)* (siehe Kapitel 4.2 und Abbildung 3) [Bun04, S. 15 ff.].

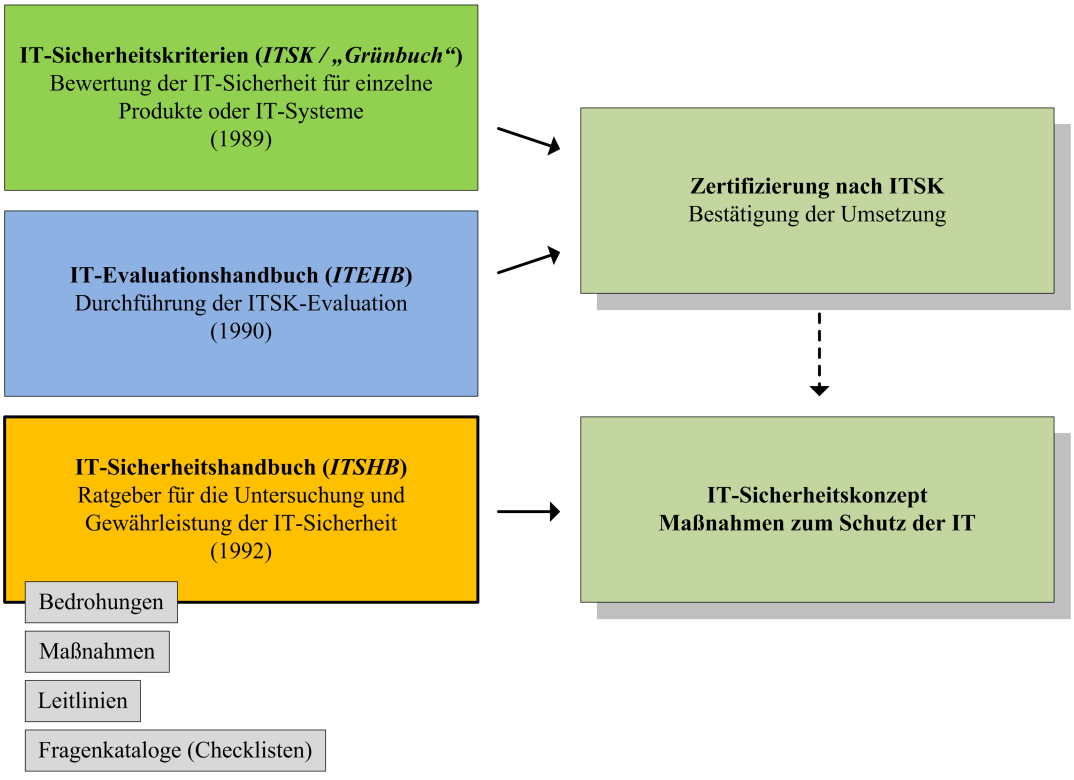

Abbildung 4: BSI-Standardwerke zur IT-Sicherheit 1992 [Bun92].

[27] Die Abteilung entstand 1953 in Bad Godesberg unter dem Decknamen *Bundesstelle für Fernmeldestatistik* [Bau00, S. 33].

Die *IT-Sicherheitskriterien* bildeten zusammen mit dem im Februar 1990 erschienenen *IT-Evaluationshandbuch (ITEHB)* und dem *IT-Sicherheitshandbuch (ITSHB)* (Erstveröffentlichung März 1992) die grundlegenden, vom ZSI und ab 1991 vom BSI publizierten Werke zur IT-Sicherheit [Zen90, S. i f.] [Bun92] [PR93, S. 1]. Die in Zusammenarbeit mit Beteiligten aus Privatwirtschaft und Wissenschaft entwickelten *IT-Sicherheitskriterien* widmeten sich Kriterien für die Bewertung von IT-Sicherheit von einzelnen Produkten oder ganzen IT-Systemen. Das *ITEHB* baute auf den *IT-Sicherheitskriterien* auf. Es beschreibt, wie eine Prüfung von IT-Systemen oder einzelner Komponenten nach den *IT-Sicherheitskriterien* durchgeführt wird. Das Ziel der Evaluation ist die Zertifizierung des IT-Systems bzw. Produkts (siehe Abbildung 4).

Das *Handbuch für sichere Anwendung der Informationstechnik* oder auch *IT-Sicherheitshandbuch (ITSHB)* war hingegen eine Anleitung für ein praxisnahes Erstellen eines **IT-Sicherheitskonzepts**, wie Abbildung 4 zeigt. Das *ITSHB* beschrieb ein „Verfahren zur Untersuchung und Gewährleistung der IT-Sicherheit“. Es sah vier aufeinander aufbauende Stufen vor (1. Ermittlung der Schutzbedürftigkeit, 2. Bedrohungsanalyse, 3. Risikoanalyse und 4. Erstellung des Sicherheitskonzepts). Innerhalb dieser Stufen mussten insgesamt zwölf Schritte nacheinander durchgeführt werden, um den Prozess abzuschließen [Bun92, Kapitel 4]. Es setzte sich intensiv mit möglichen Bedrohungen und Maßnahmen gegen diese Bedrohungen auseinander.

Das Handbuch gab weiterhin Empfehlungen für die Auswahl von – gegebenenfalls *ITSK*-zertifizierten – IT-Systemen und erwähnte generelle Fehler bei der Einführung eines Sicherheitskonzepts. Diese *Best Practice*-Ratschläge sollten bereits von anderen Organisationen gemachte Fehler verhindern. Das finale Kapitel 11 „Allgemeine Leitlinien und Fragenkataloge für die Praxis“ stellte Leitlinien und Checklisten zur IT-Sicherheit zur Verfügung. Wenn Unternehmen aus zeitlichen oder personellen Gründen eine aufwendige Analyse ihrer IT-Sicherheit nicht durchführen konnten oder wollten, konnte auf eine spezifische Bedrohungs- und Risikoanalyse verzichtet werden. Der aus diesem Vorgehen resultierende ***Grundschutz*** sollte die unternehmenseigene IT vor größeren Schäden schützen. Die *Leitlinien für einen Grundschutz* legten für IT-Anwendungen eine standardisierte Ansichts- und Herangehensweise zugrunde [Bun92, Kapitel 11].

Allerdings wurde das ITSHB unter anderem von [PR93] kritisch gesehen und in seiner damaligen Version als verwendungsuntauglich beschrieben. 1992 wurde begonnen, an dem *IT-Grundschutzhandbuch (IT-GSHB)* zu arbeiten. 1994 veröffentlichte das BSI die erste Version des *IT-GSHBs* in Eigendruck. Das Buch widmete sich ausführlich der **IT-Sicherheitskonzeption** und beinhaltete detaillierte technische, infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen. Die empfohlenen Maßnahmenpakete sollten beim Erreichen eines mitt-

leren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme (dem Ziel des *IT-Grundschutzes*) helfen [Bun98, Kapitel 1]. Einen visuellen Überblick liefert Abbildung 5.

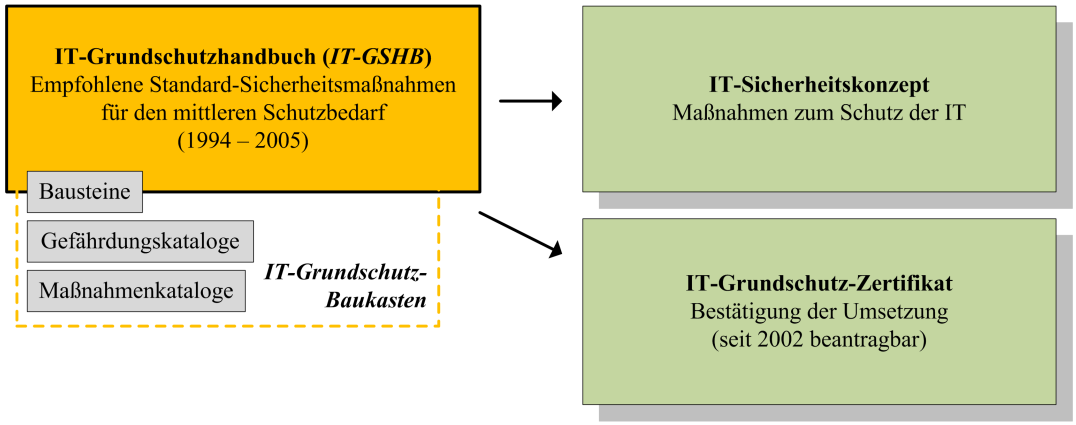

Abbildung 5: *IT-GSHB* 1994-2005.

Für eine angemessene und ausreichende IT-Sicherheit schlug das BSI einen kontinuierlichen IT-Sicherheitsprozess in Form eines Aktionsplans vor. Dieser bestand aus den drei Aktionen *Planung*, *Realisierung* und *Aufrechterhaltung*. Zum erfolgreichen Durchlaufen des Prozesses mussten innerhalb der drei Aktionen fünf wesentliche Schritte durchgeführt werden (vgl. [Bun98, Kapitel 1.1]).

Bei der Erstellung eines IT-Sicherheitskonzepts sind sowohl der *IT-Grundschutz* als auch eine aufwendige Risikoanalyse je nach Anwendungsfall korrekte Vorgehensweisen. Nach einer notwendigen Identifizierung der schutzwürdigen IT-Systeme (*Schutzbedarfsfeststellung*) wird mit Hilfe des *IT-GSHB* das vorhandene IT-System mit Bausteinen möglichst genau abgebildet. Jeder Baustein enthält spezifische Maßnahmen und Gefährdungen, welche in Katalogform zusammengestellt sind. Anhand dieser Maßnahmen wird ein SOLL-IST-Vergleich durchgeführt. Das Ergebnis ist eine Liste noch umzusetzender Maßnahmen, um den *IT-Grundschutz* zu erreichen.

Das *IT-Grundschutzhandbuch (IT-GSHB)* erschien ab 1995 im Bundesanzeiger-Verlag. Es enthielt 18 Bausteine, 200 Maßnahmen und war 150 Seiten stark [Mün11, Folie 12] [Mül10, Folie 5]. Es folgten bis einschließlich 1998 jährlich neue Ausgaben, welche einige strukturelle Anpassungen und viele neue Bausteine einführten. Von Anbeginn entwickelt das BSI mit Hilfe von Anwendern aus Behörden und Privatwirtschaft die Bausteine bedarfsorientiert weiter. Ab 1999 stellte das BSI das *IT-GSHB* in Form einer Loseblatt-Sammlung zur Verfügung. Jährliche erscheinende Ergänzungslieferungen (EL) sorgten für eine inhaltliche An-

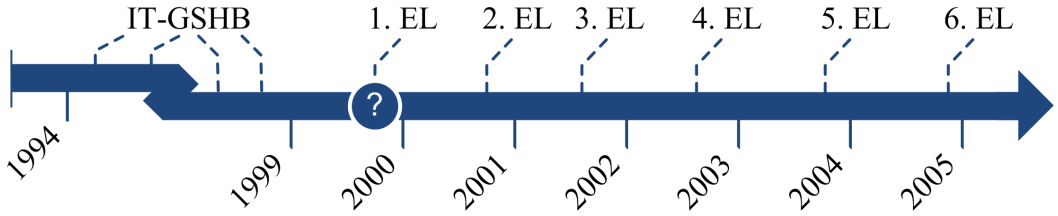

Abbildung 6: Ergänzungslieferungen (EL) des *IT-GSHBs* bis 2005 [ARG01] [Bun02a] [Bun03]. Das Fragezeichen steht für ein nicht genau bekanntes Datum.

passung der Bausteine des *IT-GSHB*s an technische Neuerungen. Die Neustrukturierung visualisiert Abbildung 6. 2004 umfasste das Handbuch auf 2.550 Seiten 58 Bausteine und 720 Maßnahmen [Mül10, Folie 5]. Im gleichen Jahr endete mit der 6. EL die Zeit des *IT-Grundschutzhandbuch*s.

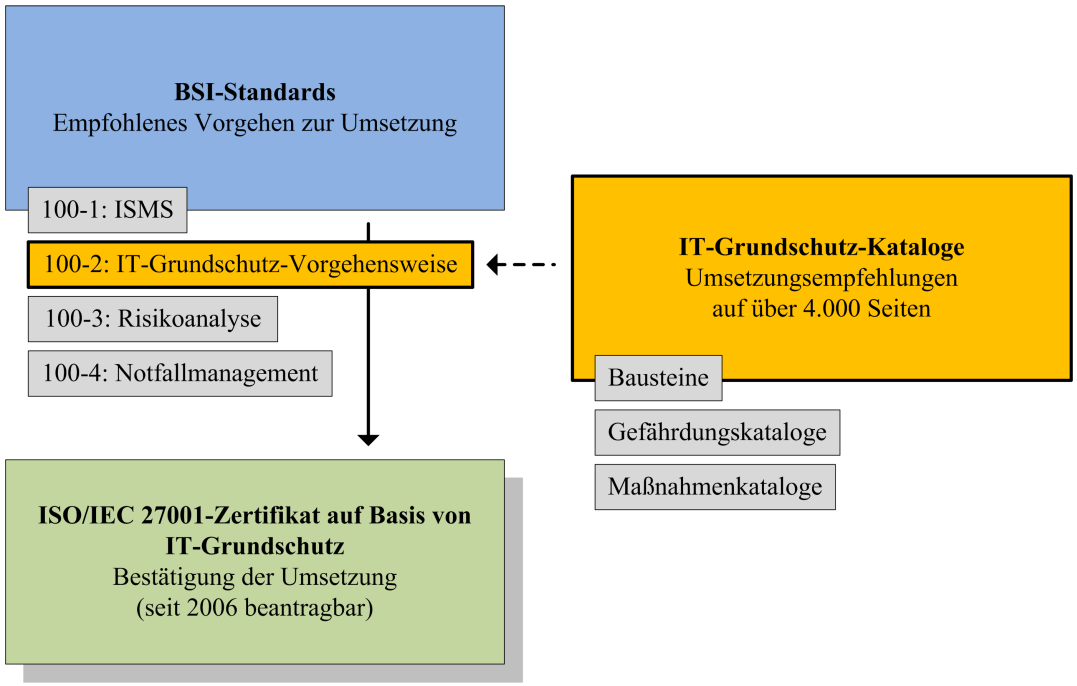

Abbildung 7: *IT-Grundschutz* seit 2006 (nach [Fed13, Folie 97]).

Im Februar 2004 wurde mit dem BSI-Standard *100-3 Risikoanalyse auf der Basis von IT-Grundschutz* ein neues Dokument veröffentlicht. Es deutete bereits eine strukturelle Änderungen im Aufbau der BSI-Werke zur IT-Sicherheit an. Das BSI publizierte im Dezember 2005 eine an das *IT-GSHB* angelehnte, aktualisier-

te und neu strukturierte Fassung des *IT-Grundschutzes* (siehe Abbildung 7). Die *Vorgehensweise* und die *IT-Grundschutz-Kataloge* mit den empfohlenen Bausteinen wurden voneinander getrennt. Ein empfohlenes Vorgehen zur Umsetzung des IT-Grundschutzes wurde in drei „BSI-Standards zur Informationssicherheit“ beschrieben: allgemeine Anforderungen an ein ISMS (*100-1 Managementsysteme für Informationssicherheit (ISMS)*, den schrittweisen Aufbau und Betrieb eines ISMS nach *IT-Grundschutz* in der Praxis (*100-2 IT-Grundschutz-Vorgehensweise*) und eine zum *BSI-Standard 100-2* passende Risikoanalyse (eine aktualisierte Fassung des BSI-Standards *100-3*). Im Mai 2008 wurden neue, besser an die ISO/IEC-Standards angepasste Versionen der BSI-Standards veröffentlicht. Die Zahl der Standards erhöhte sich im November 2008 durch den BSI-Standard *100-4 Notfallmanagement* auf vier. Die neue Version des *IT-Grundschutzes* erfuhr zudem eine Anpassung an die kurz zuvor erschienene *ISO/IEC 27001*-Norm (siehe Kapitel 5.2.1). Den historischen Verlauf und die Zusammenhänge bereitet Abbildung 3 auf.

Konkrete Umsetzungsempfehlungen für ein ISMS werden seit Januar 2006 in dem *BSI-Standard 100-2* in Verbindung mit den *IT-Grundschutz-Katalogen* gegeben. Diese beinhalten die aus dem *IT-GSHB* bekannten Bausteine, Gefährdungen und Sicherheitsmaßnahmen. Im Jahr 2012 umfasste der Katalog von Handlungsempfehlungen 79 Bausteine und 1.200 Maßnahmen auf über 4.500 Seiten [Bun12b, S. 15].

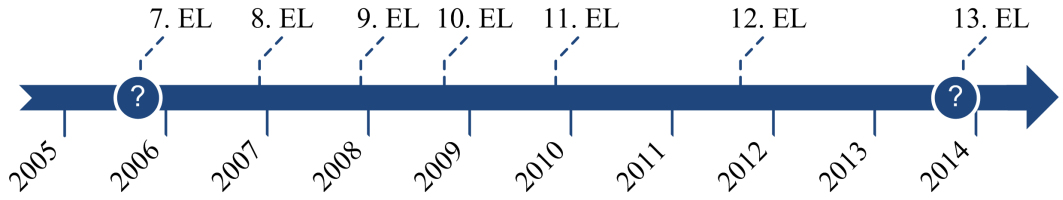

Abbildung 8: Ergänzungslieferungen (EL) der IT-Grundschutz-Kataloge seit 2005 [Mün07] [Mün08b, S. 215] [Mün08a, Folie 13 ff.] [Bun11c] [FG11, Folie 3]. Die Fragezeichen stehen für nicht genau bekannte Daten.

Eine jährliche Aktualisierung der Inhalte und insbesondere eine Ergänzung der Bausteine findet seit der 7. EL (erschien 2005) im Rahmen der IT-Grundschutzkataloge statt. Das Veröffentlichungsdatum der Online-Version liegt in der Regel ein bis drei Monate nach den Druckausgaben. Daher können sich Angaben zu den Veröffentlichungszeitpunkten der EL um einige Monate unterscheiden (vgl. zum Beispiel bei [FG11, Folie 3]. Mit der 12. Ergänzungslieferung aus dem September 2011 änderte sich erstmals der jährliche Erscheinungsrhythmus. Abbildung 8 zeigt die Ergänzungslieferungen seit 2005.

Eine neue, 13. EL wird für Oktober 2013 erwartet und soll ab November 2013 online verfügbar sein. Es sollen neue Bausteine für „Windows Server 2008“, „Windows 7“ und von Anwendern aus der Wirtschaft entwickelte Bausteine rund um das Thema „Cloud Computing“ bereitgestellt werden [Wel13]. Ob dabei auch bereits auf die im Oktober 2013 veröffentlichte, neue Version des *ISO/IEC 27001*-Standards Bezug genommen wird, ist unklar. Eine weitere Anpassung des *IT-Grundschutzes* an den *ISO/IEC*-Standard will das BSI mit den Anwendern des *IT-Grundschutzes* erläutern. Besonders im Fokus der Anwender steht im Jahre 2013 das Thema *Cloud Computing*, wie das Thema „Cloud Management und Zertifizierung von Cloud-Computing nach IT-Grundschutz“ des 3. IT-Grundschutz-Tages 2013 zeigt [Bun13c]. Die beschriebenen geschichtlichen Zusammenhänge werden in Abbildung 3 visualisiert.

5.3.2 IT-Grundschutz-Zertifikat

Ein Zertifizierungsschema für IT-Produkte und -Systeme existiert seit der Veröffentlichung der *IT-Sicherheitskriterien* (1989) und des *IT-Evaluationshandbuch* (1990) (vgl. Kapitel 5.3.1). Die Einführung des *ITSHBs* im März 1992 brachte ebenso wie die Veröffentlichung des *IT-GSHBs* (1994) keine Möglichkeit das unternehmenseigene ISMS anhand des *IT-Grundschutz*-Schemas von unabhängiger Seite zertifizieren zu lassen. Vielmehr konnten sich Firmen durch interne Audits über die Konformität zum *IT-Grundschutz* bzw. den Fortschritt bei der Umsetzung des *IT-Grundschutzes* berichten lassen.

Seit der Veröffentlichung des *IT-GSHBs* beteiligten sich die Benutzer unter anderem durch die Teilnahme an Umfragen, das Abgeben von Verbesserungsempfehlungen sowie Bereitstellung von Bausteinen an der Fortentwicklung des *IT-Grundschutzes*. Die Nutzer trugen auch den Wunsch nach einer Möglichkeit der Zertifizierung ihrer ISMS an das BSI heran [Bun13a]. Durch eine Änderung des *Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik* und einem Erlass des BMI vom 6. Februar 2001 wurde ein Qualifizierungs- und Zertifizierungsschema für den *IT-Grundschutz* eingeführt (nach [Bun02b, Seite 4] [Bun02c]). Am 16. Oktober 2002 wurde das erste *IT-Grundschutz*-Zertifikat an die Firma *memIQ AG* erteilt [Bun03].

5.3.3 ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz

Nach der Veröffentlichung des *ISO/IEC 27001*-Standards im Jahr 2005 (vgl. Kapitel 5.2.1) wurde neben der *IT-Grundschutz-Vorgehensweise* und den *IT-Grundschutz-Katalogen* (vgl. Kapitel 5.3.1) auch das *Zertifizierungsschema*

der *ISO/IEC*-Norm angepasst. Ein *ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz* kann seit Anfang des Jahres 2006 beim BSI beantragt werden. Dieses neue, beide ISMS-Standards kombinierende Zertifikat löste das bis 2006 verwendete *IT-Grundschutz*-Zertifikat vollständig ab. Nur ein vom BSI zertifizierter ISO/IEC 27001-Grundschutz-Auditor kann eine Evaluierung vornehmen [Bun13a].

Wie viele Anwender die Möglichkeit der Zertifizierung nutzen, zeigt das Kapitel 6.3.2.

5.4 Entwicklung beider Standards im Zeitverlauf

Sowohl die *ISO/IEC 2700x*-Familie als auch der *IT-Grundschutz* haben ihre Wurzeln in Kriterien für eine Evaluierung technischer Komponenten, den britischen *Green Books* und den IT-Sicherheitskriterien (vgl. Kapitel 5.2.1 und 5.3.1). Beide entstanden etwa zeitgleich Ende der 1980er Jahre und näherten sich durch die Internationalisierung der *BS 7799*-Norm im Jahre 2000 und die 2005 erfolgte Angleichung des *IT-Grundschutzes* an die *ISO/IEC 2700x*-Familie stark einander an. Eine grafische Gegenüberstellung der Entwicklung beider Standards im Zeitverlauf stellt Abbildung 9 dar.

Anhand der Abbildung 9 fällt eine unterschiedliche Herangehensweise bei der Aktualisierung der jeweiligen Standards auf. Aus dem DTI *Code of Practice* von 1989 wurde 1995 die *BS 7799*-Norm. Anschließend folgte die Teilung in die Standards *BS 7799-2* (1998) und *BS 7799-1* (1999). Im gleichen Zeitraum veröffentlichte das BSI zunächst im Jahr 1992 das ITSHB und 1994 das IT-GSHB. Es folgte bis 1998 eine jährliche Aktualisierung des Handbuches. Die britischen Standards *BS 7799-2/1* erhielten ab 1998 bzw. 1999 in einem Rhythmus von drei bis fünf Jahren eine Aktualisierung. Zuletzt brauchte die ISO/IEC acht Jahre (*ISO/IEC 27002*) bzw. elf Jahre[28] (*ISO/IEC 27001*) für eine Aktualisierung ihrer ISMS-Standards. Auf Seiten des BSIs änderte sich die Struktur des IT-GSHB von 1994 bis Ende 2005 nicht. Mit Erscheinen der BSI-Standards 100-1 und 100-2 (2005) wurde erstmals seit elf Jahren eine grundlegende Überarbeitung und Neustrukturierung des *IT-Grundschutzes* vorgenommen. Das BSI behielt eine jährliche Aktualisierung ihrer Maßnahmen-Kataloge zum *IT-Grundschutz* in Form der Ergänzungslieferung von 1999 bis 2010 bei. Danach erhöhte sich der Rhythmus der EL-Veröffentlichung auf zwei Jahre. Mit der fortschreitenden technischen Entwicklung wächst die Komplexität der beiden Standards weiter. Das zeigt sich anhand der länger werdenden zeitlichen Abstände, in welchen überarbeitete Versionen der Standards erscheinen.

[28] Gerechnet ab der Veröffentlichung der *BS 7799-2:2002*-Norm. Die *ISO/IEC 27001:2005* entspricht inhaltlich der *BS 7799-2:2002*.

Es ist davon auszugehen, dass der Trend der Harmonisierung des *IT-Grundschutzes* mit der *ISO/IEC 2700x*-Familie weiter anhalten wird.

Allerdings unterscheiden sich die jeweiligen Herangehensweisen der beiden Normen bezüglich der Erreichung eines gewissen Maßes an IT-Sicherheit sehr. Das *ISO/IEC 2700x*-Konzept erfordert seit ihren Anfängen eine Risikoanalyse der vorhandenen IT zur Erreichung der gesetzten Ziele und gegebenenfalls einer Zertifizierung. Anders ist die deutsche Verfahrensweise: das IT-Sicherheitshandbuch sah eine Bedrohungs- und Risikoanalyse zur Erstellung eines IT-Sicherheitskonzepts zwar explizit vor. Allerdings wurde Behörden und Unternehmen mit dem Weglassen der Bedrohungs- und Risikoanalyse der vereinfachte, mit weniger Zeit- und Ressourcenaufwand zu betreibende Weg des *Grundschutzes* aufgezeigt. Der *IT-Grundschutz* bietet auch 2013 noch eine für viele Unternehmen weniger aufwendige Vorgehensweise zur Erreichung eines Mindestmaß an IT-Sicherheit. Zudem bietet das BSI mit dem *ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz* die Möglichkeit, in nur einem Zertifizierungsprozess einen in Deutschland angesehenen und gleichzeitig einen international anerkannten IT-Sicherheitsstandard zu erfüllen.

Anhand der geschichtlichen Zusammenhänge der ISMS-Standards kann man nicht unbedingt auf deren Erfolg oder deren Verbreitung schließen. Im nächsten Kapitel 6 wird daher auf die Bedeutung, die Akzeptanz und die Verbreitung der Standards eingegangen.

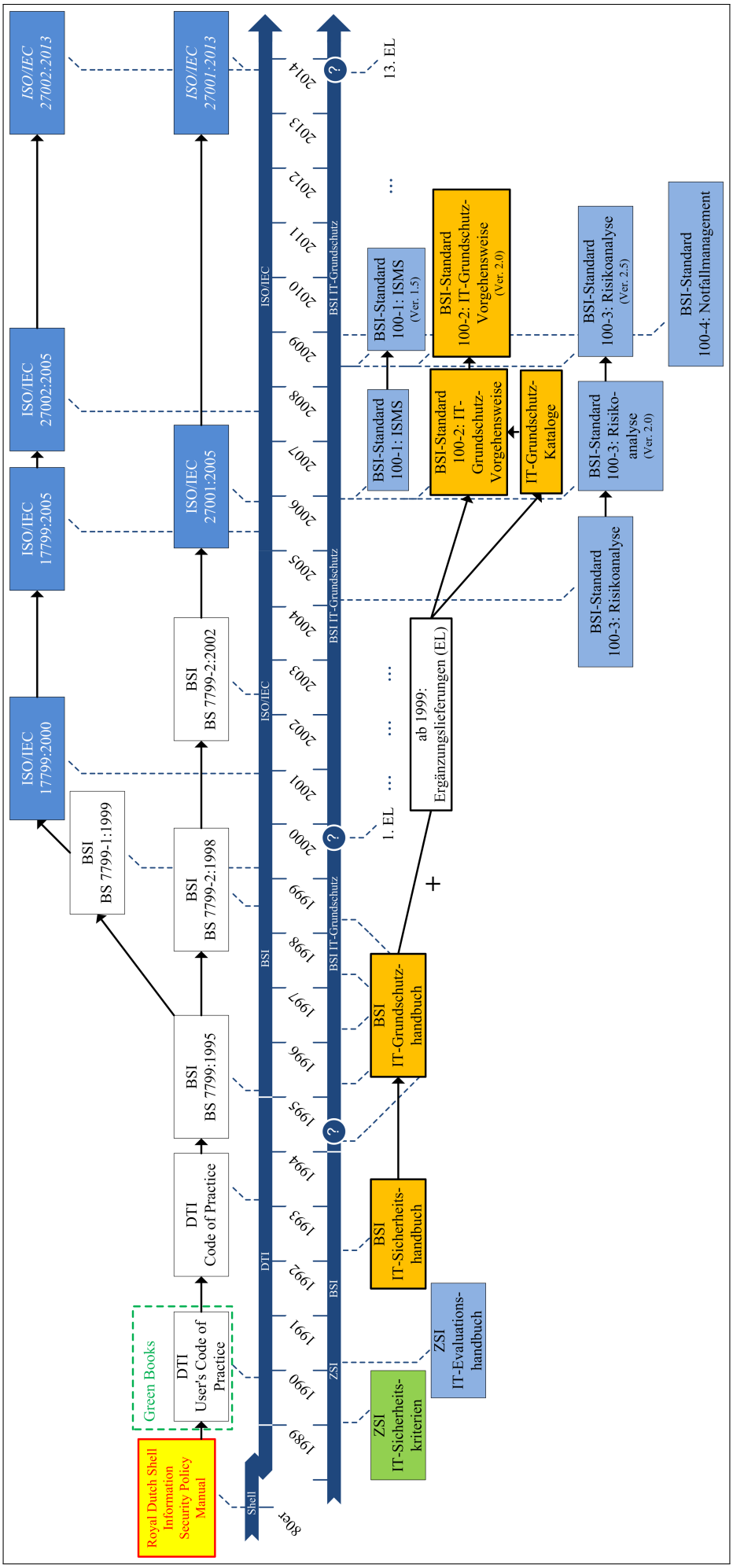

Abbildung 9: Evolution der *ISO/IEC 27001/2*-Standards und des *IT-Grundschutzes*.

6 Bedeutung, Akzeptanz und Verbreitung

Welche Bedeutung die ISMS weltweit und in einigen regionalen Gebieten wie Großbritannien oder Deutschland haben, lässt sich nicht alleine anhand der mengenmäßigen Verteilung der Zertifikate erklären. Faktoren wie der Einsatz der Unternehmensführung bei der Implementation von ISMS, die Berücksichtigung der Unternehmenskultur und das Bewusstsein für IT-Sicherheit der Mitarbeiter sind für die Akzeptanz und damit auch für die Verbreitung der IT-Sicherheitsmanagement-Standards entscheidend.

Tabelle 2: Standards des IT-Sicherheitsmanagements [ENI13b] [BF08, S. 10].

	ISO/IEC 27001	**ISO/IEC 27002**	**IT-Grundschutz**
Vorgänger	*BS 7799, ISO/IEC 17799*		*IT-GSHB*
Erstpublikation	2005	2005	2005
Audit	ja	ja	ja
Zertifizierung	ja	nein	ja
Kosten[a]	130 Euro	80 Euro	-
Sprachen	englisch, französisch, deutsch, spanisch, portugiesisch, russisch[b]		deutsch, englisch, schwedisch, estnisch[c]

[a]Einmalige Kosten für den Erwerb der Standard-Publikation.
[b]Laut dem Beuth Verlag [Beu13]. Die Auflistung erhebt nicht den Anspruch der Vollständigkeit.
[c]Laut der BSI-Homepage [Bun13d]. Die Auflistung erhebt nicht den Anspruch der Vollständigkeit.

Tabelle 2 zeigt eine Übersicht gängiger ISMS. Sie dient der groben Einordnung der im folgenden beschriebenen Bedeutung und Verbreitung von ISMS.

6.1 Die Zeit vor IT-Sicherheitsmanagement-Standards

Die 1989 erschienene amerikanische Studie *Staffing Dedication to Security Redcues Computer Abuse New Study Discovers* der Data Processing Management Association (DPMA)[29] sagte aus, dass die Anzahl an Stunden und Mitarbeiter für den Bereich der IT-Sicherheit entscheidende Faktoren sind. Unternehmen,

[29]Die DPMA benannte sich 1996 in die Association of Information Technology Professionals (AITP) um.

die Software mit Auditing-Funktion wie IBMs *Resource Access Control Facility (RACF)*[30] verwendeten, hätten bedeutend weniger Probleme als Unternehmen ohne solche Software. Gleichzeitig verwendeten 41 % aller Firmen gar keine IT-Sicherheitsvorkehrungen [FKB89, S. 289].

6.2 ISO/IEC 27001

Dieser Abschnitt gibt Auskunft über die Bedeutung und Verbreitung des *ISO/IEC 27001*-Standards. Zunächst geht die ISO-Studie *The ISO Survey of Management System Standard Certifications (2006-2011)* auf die mengenmäßige und regionale Verteilung des Standards weltweit ein. Anschließend wird der UK-spezifische Report *Information Security Breaches Survey* des *BIS* die Verbreitung, Bedeutung und Akzeptanz der Norm in den Jahren 2002 und 2013 miteinander verglichen.

6.2.1 Mengenmäßige und regionale Verteilung der Zertifikate

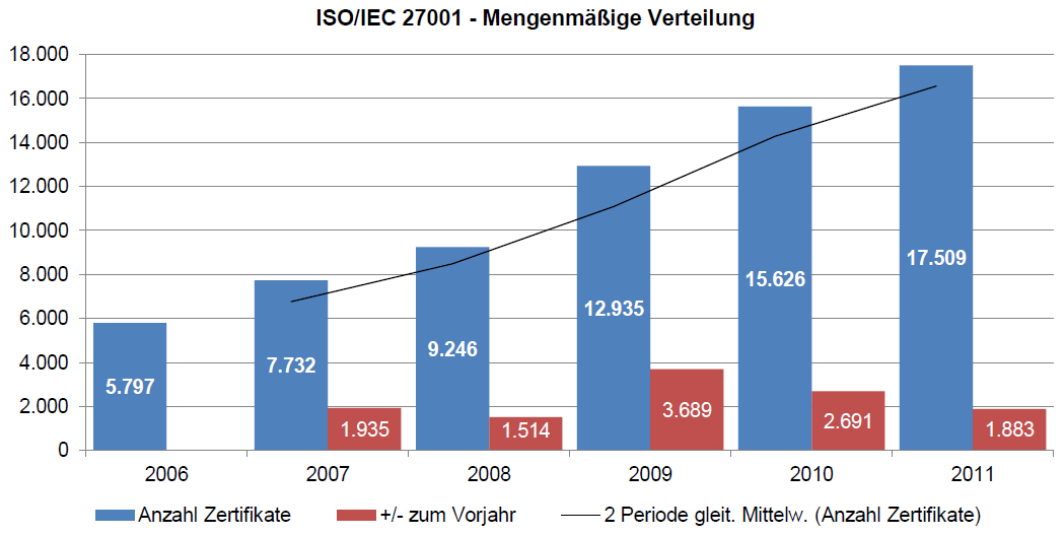

Abbildung 10: Anzahl Zertifikate 2006 bis 2011 nach [Int13c].

Die ISO-Studie *The ISO Survey of Management System Standard Certifications (2006-2011)* [Int13c] stellt die Anzahl der vergebenen Zertifikate und deren

[30] RACF wurde 1976 eingeführt und ist ein Sicherheitssystem zum Regeln der Zugriffsrechte inklusive Auditing-Funktion für die Betriebssysteme z/OS und z/VM [IBM06].

regionale und weltweite Verteilung der Jahre 2006 bis 2011 dar. Die Erhebung der Zahlen findet jährlich statt.

Laut der Abbildung 10 waren Ende Dezember 2011 weltweit 17.509 *ISO/IEC 27001*-Zertifikate ausgestellt. Im Vergleich zum Jahr 2006 mit 5.797 vergebenen Zertifikaten bedeutet dies eine Steigerung von rund 302 % in fünf Jahren. Mit Blick auf den *absoluten Zuwachs* stieg die Anzahl der Zertifikate durchschnittlich von 2006 bis 2011 um 2.342 jährlich. Der Standard scheint von immer mehr Unternehmen weltweit genutzt zu werden und an Bedeutung zu gewinnen. Der Trend eines verlangsamten Wachstums der Anzahl der ausgestellten Zertifikate ist aus der Grafik nicht ersichtlich.

Abbildung 11 zeigt eine deutliche Verschiebung der *Marktanteile nach Regionen* (englisch: *regional share*) der vergebenen *ISO/IEC 27001*-Zertifikate. Die Norm gewann in den letzten sechs Jahren besonders in Europa stark an Bedeutung. Europäische Firmen stellten 2011 rund ein Drittel aller ausgestellten Zertifikate. Die Region „Ostasien und Pazifik“ war gemessen an der Anzahl der Zertifikate weiterhin die bedeutendste Region für die *ISO/IEC 27001*-Norm [Int13c].

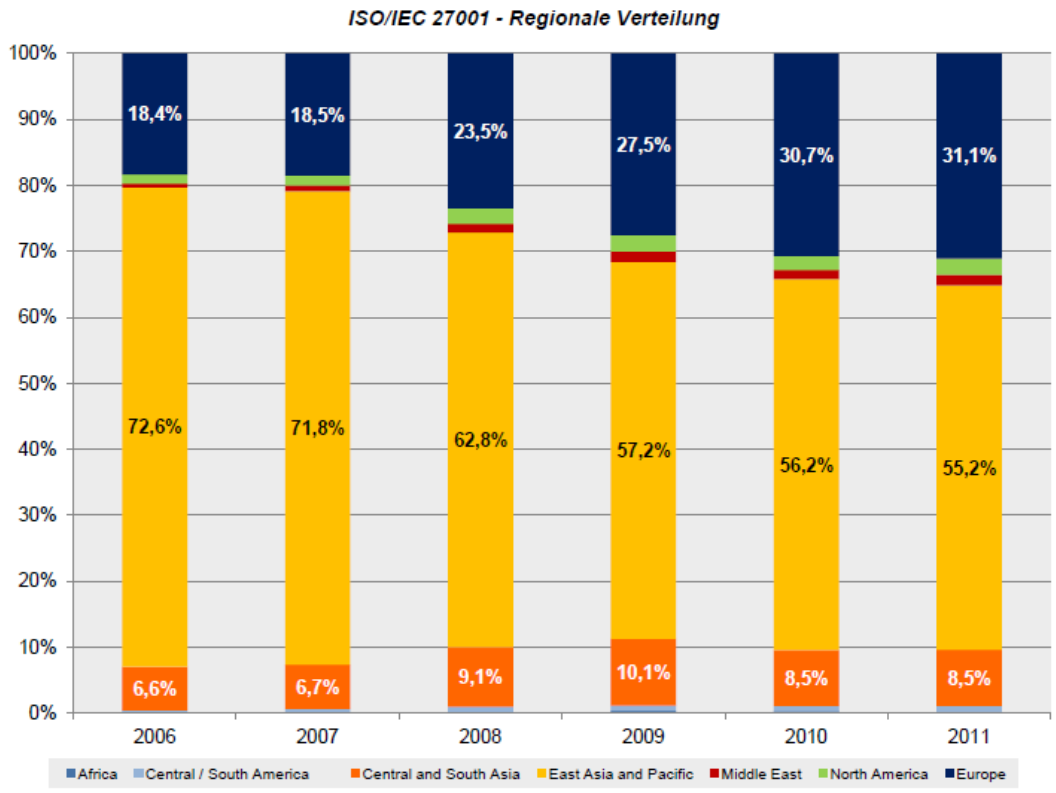

Abbildung 11: Marktanteil nach Regionen 2006 bis 2011 nach [Int13c].

Allerdings muss die ISO-Studie auch kritisch betrachtet werden: Es lässt sich von der Anzahl der Zertifikate nicht auf eine Anzahl zertifizierter Unternehmen schließen. Eine Unternehmung kann mehrere *ISO/IEC 27001*-Zertifikate besitzen. Die Zertifizierung eines großen Unternehmens oder einer staatlichen Behörde kann so sehr schnell zu einer Zunahme der Zertifikatsanzahl führen. Die Anzahl der zertifizierten Unternehmen bleibt bis auf Weiteres unbekannt. Eine genaue Analyse der Marktdurchdringung oder Akzeptanz des Standards ist damit nicht möglich.

6.2.2 Verbreitung, Bedeutung und Akzeptanz am Beispiel Großbritanniens

Im Auftrag des BIS und seiner Vorgänger DTI und Department for Business, Enterprise and Regulatory Reform (BERR) untersucht seit 1991 das Beratungsunternehmen PricewaterhouseCoopers (PwC) den Status der IT-Sicherheit in Unternehmen Großbritanniens und liefert Informationen über IT-Sicherheitsvorfälle (englisch: *information about cyber security breaches*). Die Ergebnisse der alle ein bis zwei Jahre stattfindenden Umfragen fasst jeweils der Bericht *Information Security Breaches Survey (ISBS)*[31] zusammen. Seit 2011 ist der Bericht ein Schlüsselelement in der *UK Cyber Security Strategy*[32] [Dep13a, S. 1]. Das Ziel des ISBS ist, Unternehmen Großbritanniens zu helfen, die Risiken im Bereich der IT-Sicherheit zu verstehen [Dep02, S. 1]. Wie sich das Vereinigte Königreich (UK) im Hinblick auf seine besondere Rolle als Vorreiter bei der Gestaltung des ISMS-Standards *BS 7799* und deren Nachfolger entwickelt hat, zeigt folgender Text.

Laut den ISBS verzeichneten britische Unternehmen einen starken *Anstieg der Bedrohungen* im Bereich der Informationstechnologie. Durchschnittlich 50 % aller Unternehmungen berichteten 2013 von mehr IT-Sicherheitsvorfällen (englisch: *security incidents*) als im Vorjahr. Große Unternehmen mit über 250 Mitarbeitern beklagten im Schnitt 113, kleinere Unternehmen mit bis zu 50 Mitarbeitern[33] 17 Vorfälle.

Mit der Zunahme der Sicherheitsvorfälle stiegen auch die *Kosten für* die *Auswirkungen von Sicherheitsvorfällen*. Zu den Auswirkungen zählten unter anderem der Ausfall eines angebotenen Dienstes, dessen Wiederherstellungszeit und der mit dem Ausfall einhergehende Ansehensverlust. Beispielhaft für die Kostensteigerung

[31] Ähnliche Berichte sind der *Information Security Survey* von KPMG, *The Business Information Security Survey* (BISS) vom NCC, der *Computer Crime and Security Survey* vom Computer Security Institute (CSI) oder die Studie *2nd Annual Global Information Security Survey* von Ernst&Young [Poo03, S. 12].

[32] Mehr zur *UK Cyber Security Strategy* findet sich unter [Cab11].

[33] Unterschieden sich die Ergebnisse für die mittleren Unternehmen mit 50 bis 250 Mitarbeitern, wurden diese im Text des ISBS erwähnt [Dep13a, S. 1].

zeigt die Abbildung 12 eine Steigerung der durchschnittlichen Kosten des schwerwiegendsten Sicherheitsvorfalls. Ein kleines Unternehmen hatte im Jahr 2002 Kosten von ungefähr £ 30.000. Diese stiegen auf £ 35.000 bis 65.000 im Jahre 2013. Sehr viel größer sind die Kostensprünge für Großfirmen: gaben sie 2004 noch zwischen 65.000 bis £ 190.000 aus, wuchsen die Kosten 2013 auf 450.000 bis £ 850.000 für den schwerwiegendsten Sicherheitsvorfall.

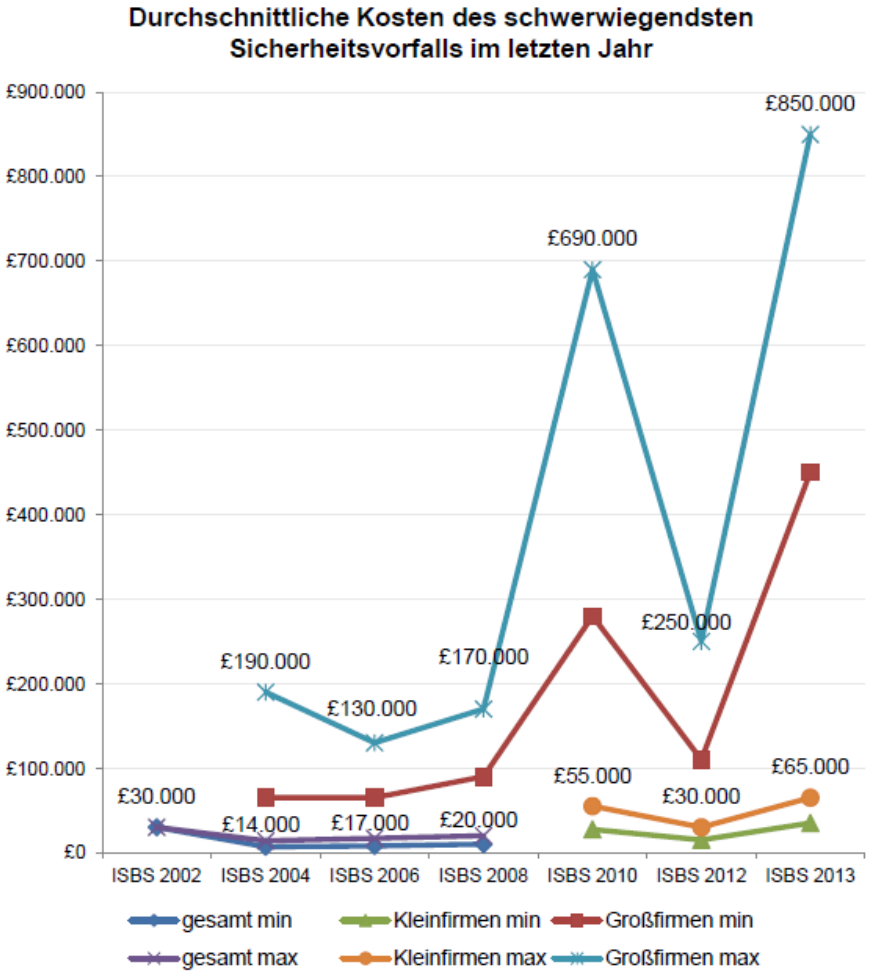

Abbildung 12: Durchschnittlichen Kosten für den schwerwiegendsten Vorfall im UK 2002 bis 2013 [Dep02, S. 11] [Dep04, S. 25] [Dep06, S. 30] [Dep08, S. 31] [Dep10b, S. 18] [Dep12, S. 18] [Dep13a, S. 18].

Eine Maßnahme, um die Anzahl und die (finanziellen) Auswirkungen der Sicherheitsvorfälle einzudämmen, stellen die Verwendung einer IT-Sicherheitsrichtlinie und die Einführung eines ISMS zum Beispiel nach der *ISO/IEC 27001*-Norm dar.

Tabelle 3 zeigt eine starke Vorreiterrolle der großen Unternehmen. Beinahe alle Großunternehmen hatten 2013 eine Richtlinie vorzuweisen. Sie waren sich der Gefahren im Bereich der IT-Sicherheit bewusst und $\frac{3}{4}$ waren mit der *ISO/IEC 27001*-Norm konform. Bei den kleineren und damit dem Großteil aller Unternehmen im UK schien das Interesse an IT-Sicherheit seit 2010 wieder abgenommen zu haben. Nur gut die Hälfte dieser Unternehmungen hatten eine IT-Sicherheitsrichtline implementiert und nur ungefähr $\frac{1}{3}$ waren mit dem *ISO/IEC 27001*-Standard konform. Die steigende Anzahl der *ISO/IEC 27001*-Zertifikate lässt sich auf einen vermehrten Einsatz in Großfirmen zurückführen.

Tabelle 3: Verwendung von IT-Sicherheitsrichtline und -standards im UK 2000 bis 2013 [Dep02, S. 15 u. 19] [Dep04, S. 8 u. 10] [Dep06, S. 7 u. 9] [Dep08, S. 7 u. 9] [Dep10b, S. 6] [Dep12, S. 6] [Dep13a, S. 6] [Int13c].

Jahr	IT-Sicherheitsrichtline gesamt[a] (Großfirmen)	BS 7799 & ISO/IEC 27001[b] gesamt[a] (Großfirmen)		ISO/IEC 27001 zertifiziert Anzahl
		bekannt	bekannt & konform[c]	
2000	14 %	25 %		
2002	27 % (59 %)	14 % (42 %)	38 %[d]	
2004	34 % (65 %)	12 % (39 %)	59 %	
2006	40 % (73 %)	10 % (38 %)	67 % (75 %)	486
2008	45 % (88 %)	21 % (46 %)	51 % (65 %)	738
2010	67 % (90 %)	[e]	51 % (68 %)	1.157
2012	63 % (95 %)	[e]	39 % (74 %)	
2013	54 % (99 %)	[e]	36 % (76 %)	

[a] Die *gesamt*-Werte sind nahezu identisch mit *kleinen* Unternehmen (vgl. [Dep13a, S. 1]).
[b] gefragt wurde bis 2008 nach der *BS 7799*, ab 2010 nach der *ISO/IEC 27001*-Norm.
[c] *vollständig* und *teilweise* konform.
[d] 2002: 48 % der konformen Unternehmen waren durch ein Sicherheitsaudit auch akkreditiert.
[e] ab 2010 wurde die Frage gestrichen.

Alle ISBS seit 1991 zeigen, dass sich insbesondere kleinere Unternehmen mit der Umsetzung von IT-Sicherheitsmaßnahmen schwer tun. Aus diesem Grund gibt das BIS in Großbritannien unter anderem den kompakten Ratgeber *Cyber security: what small businesses need to know.* [Dep13b] auf 12 Seiten heraus. Dieser Ratgeber soll die Verantwortlichen auf Problemstellungen im Bereich *cyber security* aufmerksam machen. Dies geschieht mit sehr verständlichen, allgemein gehaltenen Beschreibungen (ähnlich der Beschreibungen in der *ISO/IEC 2700x*-Serie). Schlagwörter wie „manage the risks“, „planning, implementing and reviewing your

cyber security“ führen den Leser grob an die Thematik heran. Wie groß der Aufwand für die einzelne Unternehmung sein wird, lässt sich jedoch nicht absehen.

6.3 IT-Grundschutz

Das folgende Kapitel befasst sich mit der IT-Sicherheit in mittelständischen Unternehmen in Deutschland. Anschließend wird auf die mengenmäßige und regionale Verteilung der Vorgehensweise nach *IT-Grundschutz* inklusive erteilter Zertifikate eingegangen.

6.3.1 IT-Sicherheit in kleinen und mittleren Unternehmen in Deutschland

Über 99 % aller Unternehmen in Deutschland werden aufgrund definierter Grenzen ihrer Beschäftigtenzahl, ihres Umsatzes oder ihrer Bilanzsumme dem Bereich kleine und mittlere Unternehmen (KMU) zugeordnet [Bun12c, S. 8]. Das Bundesministerium für Wirtschaft und Technologie (BMWi) und das BSI versuchen durch Initiativen insbesondere die Verantwortlichen von KMU für die Sicherheit ihrer IT zu sensibilisieren. Verschiedenen Studien (zum Beispiel [HBDK97], [Bun11b], [Bun12c] und [Bun13h]) untersuchten, wie es um die IT-Sicherheit in mittelständischen Unternehmen in Deutschland bestellt ist.

Die Studien *Informations- und Telekommunikationssicherheit in kleinen und mittleren Unternehmen* [HBDK97] und *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen* [Bun12c] aus den Jahren 1997 und 2012 befassten sich mit dem Niveau der der IT-Sicherheit in KMU in Deutschland. Beiden Studien ist gleich, dass sie von Annette Hillebrand und Franz Büllingen vom *Wissenschaftlichen Institut für Kommunikationsdienste (WIK)* mitverfasst wurden.

Die Datenerhebung erfolgte 1997 durch persönliche Interviews bei 73 Unternehmen aus verschiedenen Branchen [HBDK97, S. 12]. Die 15 Jahre später durchgeführte Studie aus 2012 gewichtete die Branchen anhand der tatsächlichen Firmenstruktur in Deutschland und erhielt ihre Ergebnisse durch computergestützte Telefonumfragen unter 955 bzw. 922 Teilnehmern. Die Fragebögen der späteren Studie wurden an den *IT-Grundschutz* angelehnt [Bun12c, S. 10]. Beide Studien sind als repräsentative Erhebungen anzusehen.

In dem Zeitraum von 15 Jahren hat die IT eine enorme Bedeutungssteigerung erfahren. Über 99 % aller Unternehmen verwendeten 2012 für ihre Geschäftsprozesse IT [Bun12c, S. 1]. 1997 taten dies 25-30 % [HBDK97, S. 17]. Mit der erhöhten Verwendung von IT im Unternehmen stieg auch das Bewusstsein für die Bedeutung der IT-Sicherheit an. Dazu beigetragen haben unter anderem den Unternehmen widerfahrende Schäden durch IT-Sicherheitsvorfälle.

Gleichzeitig überschätzten KMU ihre eigene Fertigkeiten und ihr eigenes Wissen in Bezug auf IT-Sicherheit und unterschätzten häufig die eigene Risikosituation. Eine angemessene Risikoeinschätzung fand meistens nur aufgrund bereits erlebter Vorfälle statt. Waren schnelle Gegenmaßnahmen in Form von technischen Lösungen möglich, wurden diese auch zügig umgesetzt [HBDK97, S. 78 f.] [Bun12c, S. 1 f.].

Ein möglicher finanzieller Grund für die fehlende Umsetzung weitergehender Maßnahmen zur IT-Sicherheit war nicht ersichtlich, es mangelte vor allem an fachlichem Personal und Wissen im Bereich der IT-Sicherheit. Folglich waren eine detaillierte Strategieplanung und definierte (Gegen)maßnahmen wie zum Beispiel Notfallpläne nicht vorhanden. IT-Sicherheit wurde als ein kurzfristiger, einmaliger Vorgang zur Behebung eines aufgetretenen Problems denn als ein kontinuierlicher Prozess angesehen. Fehlendes Wissen oder Personal im Bereich der IT-Sicherheit war den Teilnehmern der Studie nicht unbedingt bewusst. Die Unternehmen waren mit der Informationsflut überfordert, hielten Beratungsbedarf allerdings für unnötig oder konnten mit dem Informationsangebot nichts anfangen. Eine gering ausgeprägte Bereitschaft Mitarbeiterschulungen durchzuführen, passte zu diesem Bewusstseinsmangel [HBDK97, S. 78 ff.] [Bun12c, S. 2 f.].

Gerade die fehlenden Ressourcen bzw. die Höhe der Kosten (Zeit, Geld, organisatorischer Aufwand) stellten die *größte Barriere* für eine Erhöhung des Risikobewusstseins und die damit verbundenen Investitionen in Maßnahmen zur IT-Sicherheit dar (vergleiche hierzu auch Kapitel 6.4) [Bun12c, S. 4]. Allerdings stieg das Bewusstsein für IT-Sicherheit und für das einhergehende Risiko mit zunehmender Nutzung von IT-Anwendungen und -Diensten an. In den KMU mit Mitarbeiterzahl über 50 stieg zugleich auch die Bereitschaft, höhere finanzielle Investitionen in die IT-Sicherheit zu tätigen [HBDK97, S. 78 ff.] [Bun12c, S. 1].

Die Studie aus 2012 weist darauf hin, dass sich die Unternehmen ihrer eigenen Unternehmenswerte (englisch: *assets*) nicht bewusst sind. Kundendaten, Produkte und Verfahren wurden in ihrem Wert für das Unternehmen falsch oder gar nicht als Wert eingeschätzt. Als Konsequenz sollen die KMU verstärkt auf ihre schützenswerten Assets aufmerksam gemacht werden [Bun12c, S. 3 f.].

Folgende Voraussetzungen sind für die Teilnehmer in 2012 ausschlaggebend für eine zukünftige Umsetzung von mehr IT-Sicherheitsmaßnahmen [Bun12c, S. 3 f.]:

- Aktivitäten zur Informationsbereitstellung,
- Aufklärung über Risiken und
- Sensibilisierung der Mitarbeiter.

Genau diese Maßnahmen wurden bereits in der Studie von 1997 als wichtigste Handlungsempfehlungen für Verbände, Wirtschaft und Politik empfohlen

[HBDK97, S. 80] und werden seit Jahren von diesen Akteuren durchgeführt [Bun12c, S. 4].

6.3.2 Mengenmäßige und regionale Verteilung

Zur Veröffentlichung der dritten Ausgabe des IT-GSHB im Jahr 1996 hatten sich bereits über 200 Anwender freiwillig beim BSI registriert[34] [Bun96, S. 1]. Wie die Zahl der registrierten und mit einer Veröffentlichung ihrer Namen einverstandenen Anwender von 1997 bis 2009 stieg, zeigt Abbildung 13.

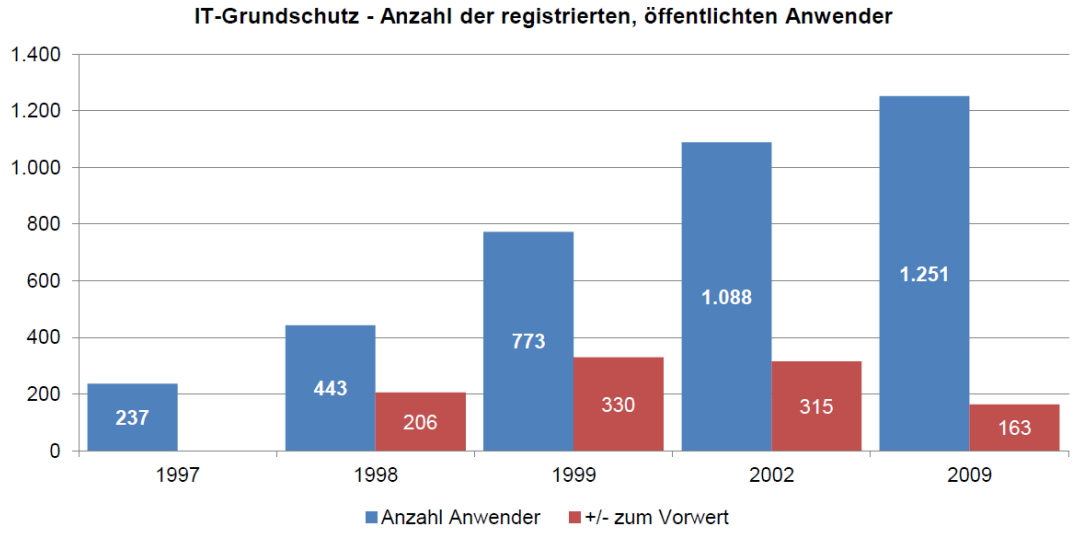

Abbildung 13: Anzahl registrierter, öffentlicher Anwender 1997 bis 2009 (nach [Bun97, Anhang] [Bun98, S. 1 u. Anhang] [Bun00, Anhang] [Bun09]).

Nach [Bun97, Anhang] [Bun98, S. 1 u. Anhang] [Bun00, Anhang] stimmen im Mittel 22,6 % aller registrierten Anwender einer Namensveröffentlichung zu. Die eigentliche Anzahl an registrierten Anwender liegt daher höher als in Abbildung 13 angegeben.

Laut Abbildung 14 stammte ein großer Teil der Anwender des *IT-Grundschutzes* in den Jahren 1997 bis 2000 aus Deutschland. Es zeigt sich ein langsamer, stetiger Trend zu mehr Anwendern in den restlichen Staaten Europas und der Welt.

Problematisch sind die angegebenen Daten der Abbildungen 13 und 14 im Hinblick auf ihre Aussagekraft und die fehlenden Jahrgänge insbesondere zwischen

[34] Die registrierten Benutzer erhalten aktuelle Informationen zum Thema *IT-Grundschutz*.

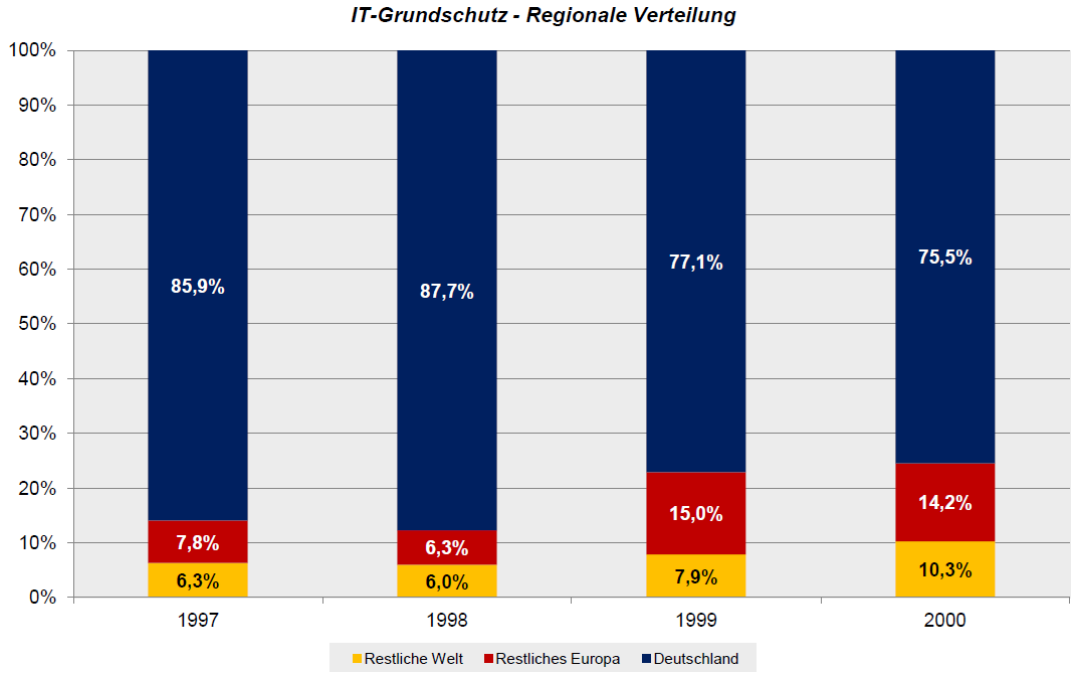

Abbildung 14: Marktanteil nach Regionen 1997 bis 2000 (nach [Bun97, Anhang] [Bun98, S. 1 u. Anhang] [Bun00, Anhang] [Bun02a, Anhang]).

den Jahren 2002 und 2009 sowie ab 2009. Wie sich die Situation bis zum heutigen Zeitpunkt im Jahr 2013 geändert hat, kann aus Mangel an Quellen nicht nachvollzogen werden. Insofern können im Rahmen dieser Arbeit die Anzahl der Anwender und die regionale Verteilung des *IT-Grundschutzes* in der aktuellen Entwicklung nicht eingeschätzt und bewertet werden.

Das BSI stellt auf seiner Homepage unter [Bun13b] und in [Sch13, Folie 19] Angaben über die *Anzahl an ausgestellten Zertifikaten* nach *ISO/IEC 27001 auf Basis von IT-Grundschutz* zur Verfügung. Aus den Unterlagen geht hervor, dass zwischen 2010 und einschließlich 2013 insgesamt 71 Zertifikate erteilt wurden. 22 Verfahren zur Zertifizierung waren 2013 noch am Laufen. Aus den Angaben lässt sich nicht entnehmen, wie viele Zertifikate aufgrund der begrenzten Gültigkeitsdauer von drei Jahren nicht mehr verwendet werden können oder bei wie vielen Unternehmen eine Re-Zertifizierung vorgenommen wurde.

6.3.3 Zahlenmäßiger Vergleich zur ISO/IEC 27001

Ein Vergleich zu den *ISO/IEC 27001*-Angaben aus Kapitel 6.2.1 lässt sich nur schwer vornehmen. Zum einen liegt die jeweilige Datenbasis unterschiedlichen Jahrgängen zugrunde. Zum anderen fehlen Daten der regionalen Verteilung beim

IT-Grundschutz nach 2000 völlig. Interessant ist ein Vergleich der Anzahl der öffentlichen Zertifikate des *IT-Grundschutzes* unter [Bun13b] zu den Zahlen der erteilten *ISO/IEC 27001*-Zertifikate aus der ISO-Umfrage [Int12]: Im Jahr 2010 wurden insgesamt 19 *ISO/IEC 27001-Zertifikate auf Basis von IT-Grundschutz* erteilt. Ein Jahr später waren es 16 Zertifikate. Die ISO verzeichnete in 2010 für Deutschland 357 erteilte *ISO/IEC 27001*-Zertifikate. 2011 waren es 424, wobei die BSI-Zertifikate mit in die Statistik der ISO zu zählen sind. Eine Ursachenforschung, wo dieser enorme Unterschied in der Anzahl der erteilten Zertifikate herrührt, würde im Rahmen dieser Arbeit zu weit führen.

Im nachfolgenden Abschnitt wird über wissenschaftliche Forschungen aus den Jahren 2008 und 2010 berichtet, die mögliche Gründe für eine geringe Akzeptanz der *ISO/IEC 27001*-Norm und anderer Standards sowie Maßnahmen zur Akzeptanzsteigerung untersuchten.

6.4 Akzeptanz von IT-Sicherheitsstandards

Auf wissenschaftlicher Basis beschäftigten sich Fomin und Barlette in ihren Untersuchungen [BF08], [FdB08] und [BF10] mit der Akzeptanz bzw. Verwendungsrate (englisch: *adoption*) des *ISO/IEC 27001*-Standards und IT-Sicherheitsstandards allgemein.

Die Einführung von Methoden oder Standards der Informationssicherheit ist eine *direkte* Maßnahme gegen die Gefährdungen von Informationssystemen. Ein *indirekter* Aspekt der Einführung eines IT-Sicherheitsstandards ist die Erzeugung von Bewusstsein für mögliche IS-Gefährdungen und kritische Prozesse [BF08, S. 1].

Warum entscheiden oder sollten sich Unternehmen für die Verwendung eines IT-Sicherheitsmanagementstandards entscheiden? Folgende Faktoren motivieren der Studie nach die Einführung eines ISMS:

- Steigende Zahl der IT-Bedrohungen,
- Anfragen von Geschäftspartnern,
- Anfragen von Versicherungen,
- Geschäftliche Anforderungen (z.B. Outsourcing),
- Gesetzliche Vorgaben,
- Vorhandene Leitfäden und umfangreiche Checklisten und
- Vergleichbarkeit der zertifizierten Unternehmen.

Die Autoren Fomin und Barlette arbeiteten in ihren Aufsätzen *Barrieren und Erfolgsfaktoren* für die Verwendung eines ISMS heraus. Diese sind in Tabelle 4 in aggregierter Form dargestellt.

Hinsichtlich der jährlich steigenden Zahl an Bedrohungen im Bereich der IT erwarteten die Autoren eine steigende Anzahl an ISMS-zertifizierten Unternehmungen. Leitfäden und umfangreiche Checklisten dienten bei der Einführung als *Motivation*, ebenso die Anfragen von Geschäftspartnern und Versicherungen nach einer ISMS-Konformität. Letztere stellten geringere Versicherungsbeiträge bei erfolgreicher Zertifizierung in Aussicht. Gesetzliche Vorgaben wie in Japan und geschäftliche Anforderungen an Unternehmen im Outsourcing- beziehungsweise Offshoring-Bereich (Taiwan, Singapur und Indien) führten ebenfalls zu einer hohen Zahl an Zertifikaten [FdB08, S. 9].

Die Autoren fanden heraus, dass weniger als ein Fünftel der kleineren und mittleren Unternehmen (KMU) (Unternehmen mit weniger als 250 Mitarbeitern)[35] ein Krisen- oder Kontinuitätsmanagement (englisch: *business continuity management*) besaßen [BF08, S. 1]. Gerade die KMU hatten Probleme, qualifiziertes IT-Personal zu finden und hatten Schwierigkeiten, IT-bezogene Risiken zu bewerten. Ihnen fehlte es zudem an Bewusstsein für IT-Sicherheit. Im Ergebnis waren die KMU gezwungen, ihre Kompetenzen in der IT und damit auch IT-Sicherheit an Dritte auszulagern. Weder die Zeit für die Einführung eines IT-Sicherheitsmanagements noch die Kosten waren die kleineren und mittleren Firmen bereit zu investieren beziehungsweise zu zahlen (vergleiche hierzu Kapitel 6.3.1) [BF08, BF10, S. 4, S. 78 f.]. Ein möglicher Ausweg wäre die Herausgabe von zwei Versionen eines ISMS-Standards: eine Version für große Unternehmen und eine auf KMU zugeschnittene Version [BF08, S. 8]. Eine sprachlich auf den Einsatzmarkt angepasste Version, z.B. eine französische Version (siehe Tabelle 2) des *ISO/IEC 27001*-Standards, könnte die Zahl der Zertifizierungen insgesamt steigern [FdB08, S. 7].

Die ISMS-Standards müssen der Unternehmenskultur und ihren Mitarbeitern angepasst werden. Vor der Einführung eines ISMS muss die Unternehmensführung dafür sorgen, dass sich ihre Mitarbeiter über die Ziele der neuen Richtlinien bewusst sind. Nur wenn dies der Fall ist, kann die Einführung eines ISMS-Standards auch den gewünschten Erfolg bringen. Zu diesem Zweck sind Mitarbeiterschulungen für den richtigen Umgang mit Software und alltäglichen Prozessen notwendig [BF08, S. 3].

Die Zahl der *ISO/IEC 27001*-Zertifizierungen steigt weniger stark als in der Vergangenheit. Mögliche Gründe sehen Fomin und Barlette in der speziellen Ausrichtung des Standards auf IT-Unternehmen[36] und in einer gewissen Übersättigung des

[35] KMU im Englischen gleichbedeutend mit SME (Small and Medium-sized Enterprises).

[36] Rund 40 % aller britischen Unternehmen der Branchen *IT* und *Telekommunikation* waren 2012

Tabelle 4: Entscheidende Faktoren für die Verwendung eines ISMS (nach [BF08, S. 10] [BF10, S. 69-84] [Dep02, S. 19]).

Barrieren für die Verwendung		**Erfolgsfaktoren für die Implementation**
Schwierige Durchsetzung der Richtlinien durch Unternehmensführung	→	Commitment der Unternehmensführung
Fehlerhafte Anpassung der Richtlinien	→	Anpassung der Standards an Unternehmenskultur
Fehlendes Bewusstsein der Mitarbeiter/ Führung für Bedrohungen[a]	→	Workshops und Schulungen für mehr Commitment der Mitarbeiter
Fehlende Ressourcen (Zeit, Geld, organisatorischer Aufwand)[a]	→	Aufzeigen des Informations-/Wertverlustes durch Sicherheitsvorfall
Komplexität der Standards[a]	→	Einführung eines zusätzlichen Standards für KMUs sowie Veröffentlichung einer sprachlich dem Einsatzmarkt angepassten Version
Nutzen schwer quantifizierbar	→	Gesteigertes Bewusstsein für IT-Sicherheit (langfristige Verbesserung von Prozessen und Systemen)
Branchenspezifische Ausrichtung der Standards	→	Unterstützung durch staatlichen Einfluss und Gesetzgebung sowie Industriegremien
Fehlende Kenntnisse der gesetzlichen Vorgaben[a]	→	Unterstützung durch staatlichen Einfluss (z.B. Infokampagnen) und Gesetzgebung (z.B. Meldepflicht für Sicherheitsvorfälle)
Fehlende konkrete Anleitungen zur Umsetzung[a]	→	Anleitungen zur Implementation (z.B. ISO/IEC 27003)
Kostenpflichtige Verbreitung einiger Standards	→	Kostenlose Standards zur Verfügung stellen

[a] insbesondere für/bei KMUs.

Marktes. Zertifizierte Unternehmen haben keinen großen Wettbewerbsvorsprung gegenüber nicht-zertifizierten Firmen und das allgemein Interesse an einer Zertifizierung sinkt. Gleichzeitig tun sich KMUs schwer, Anforderungen von Standards

mit der *ISO/IEC 27001*-Norm vollständig konform [Dep12, S. 6]. Weltweit waren 2011 rund 57 % aller Zertifikate auf IT-Unternehmen ausgestellt [Int13c].

zu erfüllen. Es fehlt an Engagement der Mitarbeiter und des Managements sowie an Zeit für die Erfüllung der Anforderungen [BF08, S. 5]. Zudem ist es schwierig, den entstandenen Nutzen durch einen eingeführten ISMS-Standard mit Zahlen zu belegen. Der eigentliche Nutzen liegt in dem gestiegenen Bewusstsein des Unternehmens für IT-Sicherheit und steigert allmählich die Verbesserungen im Bereich der Sicherheit. Nur wenn das (Top-)Management die Zertifizierung als Antrieb für die Verbesserung von internen Prozessen und Systemen ansieht, wird sich die Zertifizierung auch auszahlen [BF08, S. 6]. Ein weiteres Argument für die Zertifizierung ist, dass sich zwei oder mehr Unternehmen mit dem gleichen Zertifizierungsschema in ihrem Level an IT-Sicherheit untereinander vergleichen können [BF10, S. 75].

Bestehende Gesetze im Bereich des Datenschutzes haben teilweise harte Konsequenzen mit möglichen Gefängnis- und hohen Geldstrafen bei Verstoß gegen diese Regularien zur Folge. Trotzdem kennen viele Manager – insbesondere KMU-Manager – die gesetzlichen Vorgaben nicht. Für eine höhere Sensibilisierung müssen die jeweiligen Gesetzgeber mehr Wege finden, die notwendigen Informationen über gesetzliche IT-Sicherheitsvorgaben an Unternehmen zu geben [BF08, S. 7 f.]. Die Autoren gehen davon aus, dass sich mit den neu eingeführten Standards wie der *ISO/IEC 27003* (*Implementierung eines ISMS*) die Zahl der Implementierung eines ISMS-Einführungen nebst Zertifizierung steigt. Das Problem fehlender konkreter Anleitungen zur Umsetzung wird dadurch angegangen [BF10, S. 83].

6.5 Fazit

Insgesamt zeigt sich, dass insbesondere der Standard *ISO/IEC 27001* weltweit und in nahezu allen Wirtschaftszweigen akzeptiert wird [Int12, S. 2]. Der *IT-Grundschutz* wird trotz einer englischen Ausgabe hauptsächlich im deutschsprachigen Raum verwendet und orientiert sich zwecks Kompatibilität am Aufbau der *ISO/IEC 27001*-Norm. Beide Standards schließen sich allerdings nicht aus, sondern ergänzen sich und können parallel genutzt werden. Die Frage, warum das *ISO/IEC 27001-Zertifikat auf Basis von IT-Grundschutz* im Vergleich zum *ISO/IEC 27001-Zertifikat* weniger häufig im deutschsprachigem Raum genutzt wird, konnte nicht geklärt werden. Eine Antwortfindung ist weiteren Untersuchungen vorbehalten.

Verschiedene Studien zeigen, dass das Risikobewusstsein für IT-Sicherheit mit zunehmender Größe des Unternehmens steigt. Insbesondere Großunternehmen investieren Zeit, Geld und Personal zur Verbesserung ihrer IT-Sicherheit. Bei KMU besteht ein großer Nachholbedarf in Bezug auf Wissen über und Umsetzung von IT-Sicherheitsmaßnahmen.

7 Gesetzliche Rahmenbedingungen

Das folgende Kapitel ordnet eingangs das IT-Sicherheitsmanagement in den Kontext der gesetzlichen Rahmenbedingungen ein. Abbildung 15 visualisiert die Zusammenhänge. Anschließend werden einige für das Management der IT-Sicherheit relevante Gesetze in ihrem historischen Kontext beschrieben.

7.1 Corporate Governance als Rahmen der IT-Sicherheit

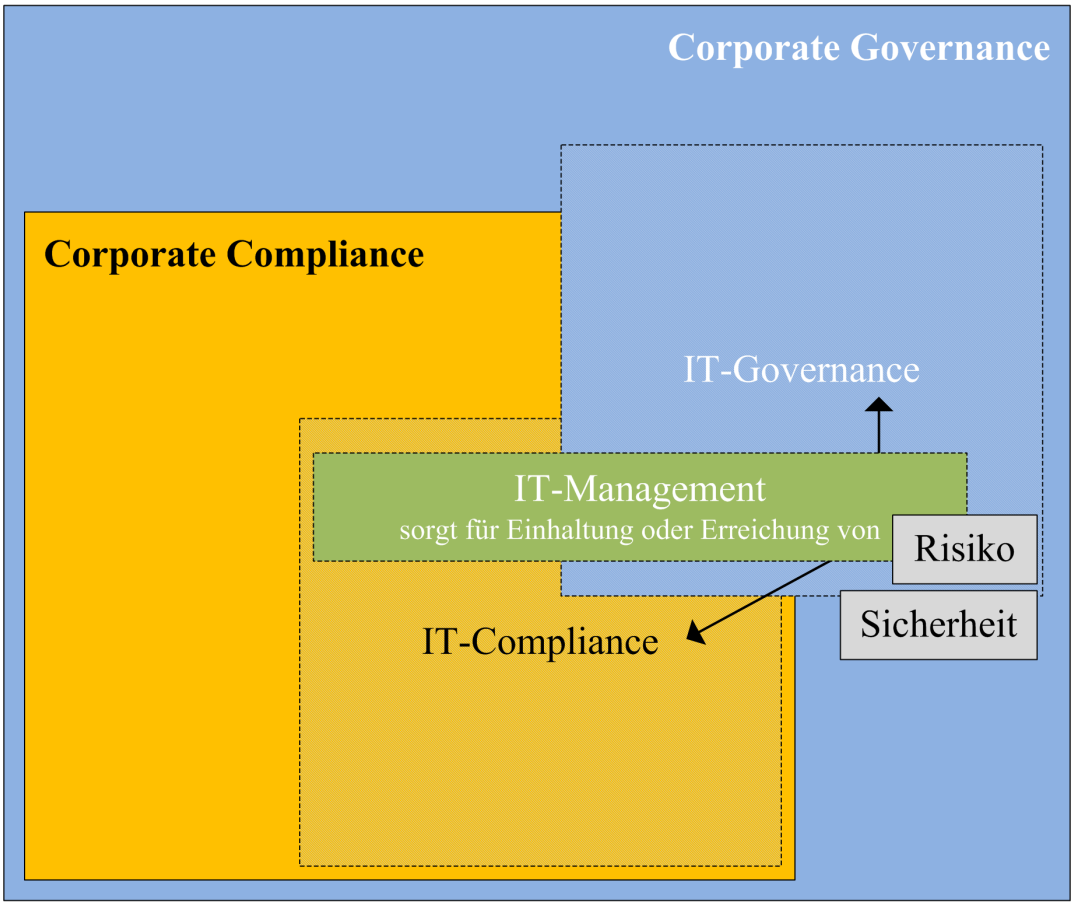

Abbildung 15: Einordnung des IT-Sicherheitsmanagements in die IT-Governance und IT-Compliance (nach [Fal12, S. 32-37]).

Coporate Governance wird von vielen Autoren unterschiedlich beschrieben. Die nachfolgende Definition wird für den Kontext dieser Arbeit verwendet. Der Begriff Coporate Governance ist aus dem strategischen Management und bezeichnet einen

Prozess zur Steuerung eines privatwirtschaftlichen Unternehmens. Durch Regeln und Kontrollmechanismen wird ein Ausgleich zwischen den verschiedenen Interessengruppen (Stakeholdern und Shareholdern) angestrebt. Der Prozess dient dem Erhalt des Unternehmens und unterliegt einer regelmäßigen externen Überprüfung [Fal12, S. 32 f.].

Ein Ziel der Corporate Governance ist die Einhaltung der für ein Unternehmen relevanten gesetzlichen, vertraglichen und organisatorischen Rahmenbedingungen. Erfüllt das Unternehmen die jeweils gestellten Anforderungen, so wird der Zustand als konform (englisch: *compliant*) bezeichnet. Im Fachjargon lautet die unternehmerische Konformität daher **Corporate Compliance** [Fal12, S. 35]. **IT-Governance** und **IT-Compliance** sind IT-bezogene Spezialisierungen der gesamt-unternehmerischen Governance und Compliance. IT-Governance ist ein Prozess zur Steuerung der IT. Regeln und Kontrollmechanismen stellen eine optimale Unterstützung der Unternehmensziele und -strategie durch IT sicher. Als Teildisziplin der Corporate Compliance bezeichnet IT-Compliance den Zustand der Konformität bezüglich der gestellten Anforderungen und die IT-gestützte Verwirklichung der Konformität mit den gesetzten Rahmenbedingungen [Fal12, S. 35 ff.].

Zu den Aufgaben des **IT-Managements** zählt, für die Einhaltung und Erreichung der *IT-Governance* und *IT-Compliance* zu sorgen. Innerhalb des IT-Managements werden für die Erreichung dieser Ziele unter anderem Methoden des **IT-Risiko- und Sicherheitsmanagements** genutzt.

Gesetzliche Regelungen wie das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)*, der amerikanische *Sarbanes-Oxley-Act (SOX)*, die *Abschlussprüfungs-Richtlinie (EuroSOX)*, das *Bilanzrechtsmodernisierungsgesetz (BilMoG)* und das *Bundesdatenschutzgesetz (BDSG)* beeinflussen das IT-Sicherheitsmanagement. Die Gesetze unterliegen einer regelmäßigen Überprüfung, werden gegebenenfalls überarbeitet und erscheinen in einer veränderten Version. Parallel zur folgenden textuellen Beschreibung bietet Abbildung 16 eine graphische Übersicht über die historische Entwicklung der Gesetze.

7.2 Gesetze zur Corporate Governance

Die Zahl der Unternehmenspleiten in Deutschland stieg in den 1990er Jahren kontinuierlich an. Die Gründe waren und sind vielfältig. Persönliches Fehlverhalten, globalisierte Märkte sowie steigende Komplexität des Unternehmen und ihrer Umwelt zählen zu den Gründen von Unternehmensinsolvenzen. Wesentlich bedeutsamer sind jedoch interne Ursachen. Ein fehlendes Risikomanagement, fehlende oder unzureichende Überwachung der Finanzbuchhaltung oder des Rechnungswesens ließen bereits zahlreiche Unternehmen zahlungsunfähig werden: Großunternehmen

wie der Baukonzern *Phillip Holzmann AG*, der Computerhändler *Escom* oder die Großwerft *Bremer Vulkan* wurden zwischen 1996 und 2002 insolvent [MB02, S. 1-6].

Mit dem Ziel einer besseren Überwachung der Unternehmensführung (Corporate Governance) und ausländischen Investoren den Zugang zu Informationen über die Unternehmen zu erleichtern (Transparenz), trat im Mai 1998 das **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)** in Kraft. Das Kernthema der weitreichenden Änderungen im Handelsgesetzbuch (HGB) und im Aktiengesetz (AktG) war die Einführung eines Risikofrüherkennungssystems zur Erkennung von bestandsgefährdenden Risiken. Jedes am Kapitalmarkt orientierte Unternehmen musste ein solches System einrichten und Risiken des Unternehmens im Lagebericht des Jahresabschlusses veröffentlichen [MB02, S. 37 f.].

Im Dezember 2001 meldete der amerikanische Großkonzern *Enron* Insolvenz an. Im Juli 2002 beantragte der Telekommunikationskonzern *WorldCom* Gläubigerschutz. Beide Unternehmen hatten im großen Umfang ihre Bilanzen gefälscht. Die Wirtschaftsprüfungsgesellschaft *Arthur Andersen*[37] war für die Durchführung von Audits bei Enron zuständig und löste sich nach einem Schuldspruch wegen Behinderung der Justiz größtenteils auf. Der im Juli 2002 in Kraft getretene **Sarbanes-Oxley-Act (SOX)** hatte das Ziel, verlorengegangenes Vertrauen der Anleger in die veröffentlichten Bilanzdaten von amerikanischen Unternehmen wiederherzustellen. Tochterunternehmen amerikanischer Gesellschaften im Ausland und nichtamerikanische Firmen, die an amerikanischen Börsen gehandelt werden, unterliegen ebenfalls dieser Regelung [HS10, S. 295 f.].

Die 61 Sections (zu deutsch: *Paragraph* oder *Artikel*) des Bundesgesetzes führen zu weitreichenden Veränderungen der Corporate Governance. Section 404 schreibt beispielsweise vor, dass jedes Unternehmen ein Internes Kontrollsystem (IKS) für die Rechnungslegung einführen, die nötigen Prozesse dokumentieren und jährlich durch einen Wirtschaftsprüfer die Wirksamkeit des IKS bestätigt werden muss. Der Finanzvorstand und der Vorstandsvorsitzende des jeweiligen Unternehmens haften für die Richtigkeit von Abschlüssen. Eine Enthaftung des Managements in Form einer Versicherung gegen finanzielle Strafzahlungen ist nur eingeschränkt möglich [KRSW13, S. 3 f.]. Infolgedessen bemüht sich die Unternehmensleitung durch geeignete organisatorische Maßnahmen Haftungsrisiken vorzubeugen und Ansprüche auf Schadensersatz zu vermeiden [Fal12, S. 10].

Das Gesetz schreibt Vorkehrungen im Bereich der IT-Sicherheit wie die Einführung eines ISMS nicht explizit vor. Eine einwandfreie Berichterstattung über die internen Unternehmensdaten ist nur durch zuverlässige IT-Prozesse und einen ange-

[37] Arthur Andersen zählte 2001 zu den *Big Five* der Wirtschaftsprüfungsgesellschaften.

messenen Schutz der verwendeten Daten möglich. Eine Konformität mit dem SOX ist daher nur mit Hilfe von Maßnahmen zur IT-Sicherheit möglich [HS10, S. 295 f.] [KRSW13, S. 3 f.].

Die europäische *Achte Richtlinie 2006/43/EG* (auch **Abschlussprüfungs-Richtlinie (EuroSOX)** genannt) entstand in Anlehnung an das amerikanische SOX-Gesetz und trat im Juni 2006 in Kraft. Sie beschreibt die Mindestanforderungen an Unternehmen für ein Risikomanagement und legt die Pflichten der Abschlussprüfer fest [HS10, S. 296]. Die Regelung änderte die *Vierte Richtlinie 78/660/EWG* aus dem Juli 1978 über die externe Prüfung des Jahresabschlusses und die *Siebente Richtlinie 83/349/EWG* aus dem Juni 1983 über den konsolidierten Abschluss ab. Gleichzeitig wurde die bisherige *Achte Richtlinie 84/253/EWG* vom 10. April 1984 aufgehoben [Eura, S. 87]. Im März 2008 wurde mit der *Richtlinie 2008/30/EG* die vorherige Regelung aus dem Jahr 2006 geändert. Zuletzt erfolgte eine minimale Änderung durch die *Richtlinie 2013/34/EU* im Juni 2013. Beide Änderungen beziehen sich ausschließlich auf technische Anpassungen des Ausschussverfahrens des EU-Parlaments und müssen daher nicht in nationales Recht umgesetzt werden [Eurb, S. 54].

Die deutsche Umsetzung der europäischen Abschlussprüfungs-Richtlinie (EuroSOX) erfolgte im **Bilanzrechtsmodernisierungsgesetz (BilMoG)**. Es trat im Mai 2009 in Kraft. Das Gesetz änderte zum Zwecke der Harmonisierung mit Europarecht einige Gesetze wie das HGB und das AktG. Unter anderem sind Kapitalgesellschaften[38] laut § 289 HGB Abs. 5 aufgefordert, wesentliche Eigenschaften ihres IKS im Lagebericht des Jahresabschlusses darzulegen [HS10, S. 296]. Das BilMoG geht über die Anforderungen des KonTraG aus dem Jahr 1998 hinaus. Ein bestehendes Risikofrüherkennnungssystem muss für eine ganzheitliche Risikoerkennung und -behandlung ausgelegt sein. Zusätzlich sollen ein Internes Überwachungssystem (IÜS) und Controlling die interne Kontrolle, Steuerung und Revision des Unternehmens ermöglichen. Zusammen bilden diese drei Komponenten das Risikomanagementsystem des Unternehmens[39] (nach [Det08, Anhang V]).

In den europäischen Regelungen *Richtlinie über Eigenkapitalanforderungen* (*Basel I*) aus dem Jahr 1988 und *Richtlinie für Basissolvenzkapitalanforderungen* (*Solvency I*) aus dem Jahr 1973 (2002 aktualisiert) wurden viele einzelne Gesetze unter einem Oberbegriff zusammengefasst [Rat]. Diese für Kreditinstitute und Versicherungsunternehmen bedeutsamen Regelungen enthielten viele Schwächen. Die neuen Regelungen **Basel II** (gilt seit Januar 2007 EU-weit) und

[38] Neben einer Aktiengesellschaft (AG) zählt dazu auch die Gesellschaft mit beschränkter Haftung (GmbH).

[39] Der Gesetzgeber spricht in § 91 Abs. 2 AktG nur von einem "Überwachungssystem". Eine detaillierte Ausgestaltung der Kontrollsysteme ist den Unternehmen überlassen.

die **Solvency II**[40] (Umsetzung steht in 2013 noch aus) enthalten unter anderem modernere Regelungen für ein Risikomanagement [HS10, S. 296 f.]. Die Nachfolgeregelung *Basel III* wird ab 2013 eingeführt und bis 2019 komplett implementiert sein. Beide Regelungen werden aufgrund ihres branchenspezifischen Charakters in dieser Arbeit nicht weiter besprochen.

7.3 Datenschutzgesetze

Die erste Fassung des **Bundesdatenschutzgesetzes (BDSG)** mit dem Namen *Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung* wurde im Februar 1977 im Bundesanzeiger verkündet. Unter dem Eindruck des sogenannten *Volkszählungsurteils* von 1983 trat durch das *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes* vom 20. Dezember 1990 am 1. Juni 1991 eine Neufassung des BDSG in Kraft[41]. Durch die Regelung der Verwendung von personenbezogenen Daten wurde eine Einschränkung des Rechts auf informationelle Selbstbestimmung auf eine gesetzliche Grundlage gestellt. Gleichzeitig beinhaltete das Gesetz Änderungen bzw. Neufassungen verschiedener Geheimdienstgesetze[42] und beschrieb unter anderem deren Aufgaben, Befugnisse, Regelungen zur Datenerhebung und Umgang mit personenbezogenen Daten [Bund]. Abbildung 16 veranschaulicht die im Text beschriebene zeitliche Entwicklung.

Eine der zahlreichen[43] Änderungen des Gesetzes trat im August 2002 in Kraft. Sie diente der Anpassung des Gesetzes an die **EG-Richtlinie 95/46/EG**[44] (Datenschutzrichtlinie). In dieser Neubekanntmachung wurde das deutsche Recht mit den europäischen Vorgaben harmonisiert [Buna]. Die letzte Änderung des Gesetzes datiert vom 14. August 2009: Durch das *Gesetz zur Änderung datenschutzrechtlicher Vorschriften* erhielt das BDSG den neuen § 42a *Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.* Nichtöffentliche Stellen müssen ihrer zuständigen Datenschutzbehörde melden, wenn personenbezogene Daten unrechtmäßig übermittelt oder ein Dritter auf eine andere Art und Weise un-

[40] Das Gesetz wurde 2009 von EU-Parlament und der -Kommission verabschiedet.

[41] Die neue Fassung des BDSG setzte außerdem das *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung* vom 27. Januar 1977, die *Datenschutzveröffentlichungsordnung* vom 3. August 1977, die *Datenschutzgebührenordnung* vom 22. Dezember 1977 und die *Datenschutzregisterordnung* vom 9. Februar 1978 außer Kraft [Bund, S. 2981].

[42] Bundesverfassungsschutzgesetz (BVerfSchG), Gesetz über den militärischen Abschirmdienst (MADG) und Gesetz über den Bundesnachrichtendienst (BNDG).

[43] Zwischen 1990 und 2002 wurde das Gesetz mindestens 11 Mal geändert [Buna, S. 66].

[44] Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

rechtmäßig Kenntnis von diesen erlangt und die Rechte und Interessen der Betroffenen drohen schwerwiegend beeinträchtigt zu werden [Bunc, S. 2818].

Neben dem BDSG existieren in Deutschland **weitere gesetzliche Vorschriften**, die die Einführung und das Betreiben eines ISMS erfordern. Dazu zählen das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG)[45].

Der Schutz der Privatsphäre wird in Großbritannien seit 1984 durch den **Data Protection Act (DPA)** geregelt. Dieser bot in seiner ursprünglichen Version einen minimalen Datenschutz. Die Verarbeitung personenbezogener Daten wurde 1998 durch eine neue Fassung des DPA ersetzt. Diese trat 2000 in Kraft und glich britisches Recht an die *EG-Richtlinie 95/46/EG* an. In Großbritannien verpflichtete die britische Regierung 2001 alle Ministerien mit dem *BS 7799* konform zu werden. Die Implementierung eines ISMS erleichtert es britischen Unternehmen eine Konformität zum DPA nachzuweisen [Ken01, S. 135 f.].

Die **Datenschutz-Grundverordnung** ist eine geplante EU-Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“. Sie soll die Richtlinie 95/46/EG ersetzen. Ein erster Entwurf wurde im Januar 2012 veröffentlicht [Eur12]. Die Verordnung würde bei Veröffentlichung sofort in allen europäischen Staaten gelten. Die bisherigen nationalen Regelungen wie der englische DPA und das deutsche BDSG würden abgelöst. Vor dem Hintergrund der NSA-Überwachungsaffäre drängen seit Juli 2013 einige europäische Staaten auf strenge Auflagen für den Umgang mit den Daten von EU-Bürgern [Bun13g]. Am 21. Oktober 2013 einigte sich der Rechtsausschuss des EU-Parlaments auf neue Regelungen für den Datenschutz. Damit das Gesetz in Kraft tritt, müssen die 28 Mitgliedsstaaten der Europäische Union (EU) noch zustimmen.

7.4 Fazit und Ausblick

Eine Gemeinsamkeit der in diesem Kapitel vorgestellten gesetzlichen Rahmenbedingungen ist ihr großer, wenn auch indirekter Einfluss auf die IT-Sicherheit. Keines der diskutierten Gesetze schreibt explizit die Einrichtung eines Informationssicherheitsmanagement-Systems vor. Zugleich schreibt der Gesetzgeber durch SOX (2002) oder EuroSOX (2006) für jedes kapitalmarktorientierte Unternehmen in den Vereinigten Staaten oder Europa ein Risikomanagementsystem

[45] Telemedien bezeichnet elektronische Informations- und Kommunikationsdienste. Das TMG legt unter anderem Vorschriften zum Impressum für Telemediendienste und zum Datenschutz bei Betreibern von Telemediendiensten fest. Das TKG reguliert den Wettbewerb im Bereich der Telekommunikationsleistungen. Es verbietet das unbefugte Abhören von Nachrichten und soll eine Überwachung der Telekommunikation durch Strafverfolgungsbehörden (sogenannte Vorratsdatenspeicherung) ermöglichen.

zwingend vor. Mit einem ISMS-Zertifikat wie dem *ISO/IEC 27001* zeigt die Unternehmensführung, dass ihr Risikomanagement geeignet ist, vollständig gesetzeskonform zu sein [Wec07, S. 3].

Abbildung 16 fasst das Kapitel 7 über die gesetzlichen Rahmenbedingungen in einer Graphik zusammen. Es zeigt sich, dass gesetzliche Regelungen (z.B. BDSG, DPA, Solvency I und Basel I) in den 1970er/1980er Jahren zunächst auf nationaler Ebene ausgearbeitet wurden. Danach trafen die EG bzw. dieEU eigene, supranational geltende Regelungen, die von den Mitgliedsstaaten in nationales Recht umgesetzt werden mussten bzw. müssen. Insbesondere die amerikanische SOX-Regelung aus dem Jahr 2002 zur Corporate Governance und die Basel- und Solvency-Regelungen zeigen eine stetige Entwicklung: Nationale gesetzlichen Regelungen reichen in Zeiten der global agierenden Unternehmen nicht mehr alleine aus. Dementsprechend müssen supranationale oder sogar weltweit geltende Regelungen folgen.

Zeitgleich zum Verfassen dieser Arbeit wurde der Entwurf eines deutschen *IT-Sicherheitsgesetzes* veröffentlicht. Der Gesetzgeber sieht umfangreiche Änderungen im Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSIG), im TKG und im TMG vor. Unter anderem wird eine Meldepflicht für Unternehmen bei Hackerangriffen diskutiert [Kau13, S. 172]. Es ist davon auszugehen, dass weitere Gesetze als Folgeerscheinungen der Finanzkrise von 2008 geändert werden und die gesetzlichen Anforderungen an die Unternehmen und ihre IT-Sicherheit noch vervielfältigen.

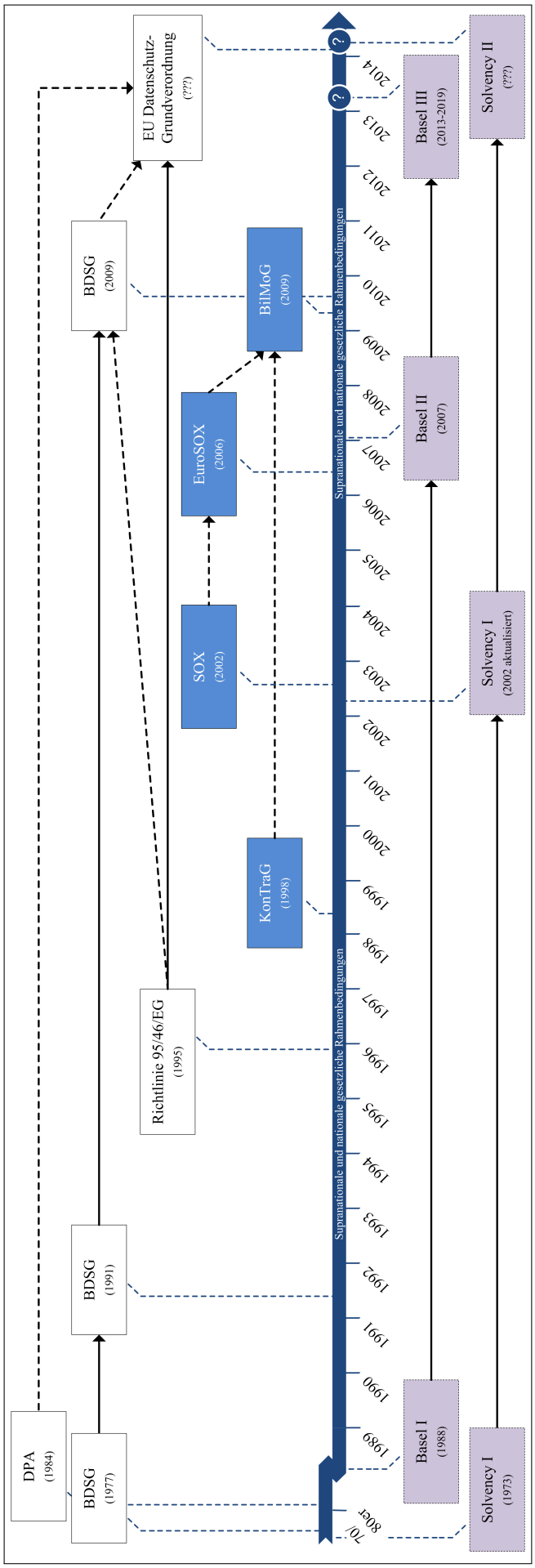

Abbildung 16: Evolution gesetzlicher Rahmenbedingungen. Gestrichelte Linien zeigen einen Einfluss eines Gesetzes auf andere Gesetze. Eine durchgehende Linie zeigt direkte Nachfolgeregelungen.

8 Schlussbetrachtungen

Nahezu jedes Unternehmen benutzt mittlerweile Informationstechnologie zum Erstellen und Verwalten ihrer Geschäftsprozesse sowie zur Kommunikation mit internen und externen Gesprächspartnern. Eine vor Ausfällen und unbefugten Eingriffen geschützte Kommunikationsinfrastruktur und das aufeinander abgestimmte Zusammenwirken von Organisation und IT sind heutzutage ein Muss für ein gesundes und auf Erfolg ausgerichtetes Unternehmen. Für diese Zwecke bietet sich der Einsatz eines ISMS nach *ISO/IEC 27001* oder *IT-Grundschutz* an.

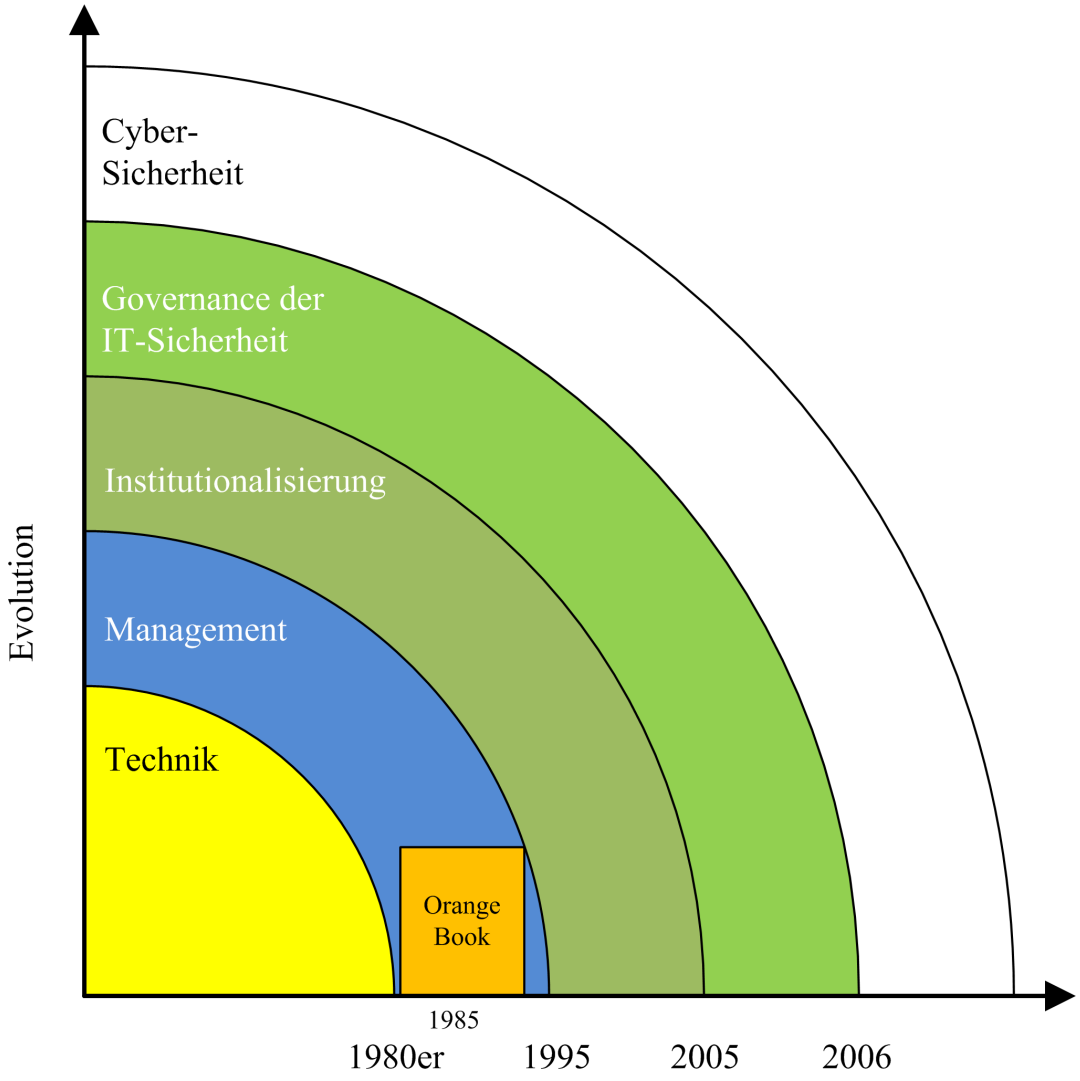

Abbildung 17: Evolution der IT-Sicherheit (nach [Sol10] und in Anlehnung an [ISA13]).

Die *geschichtliche Entwicklung* des IT-Sicherheitsmanagements wurde anhand diverser Primär- und Sekundärquellen detailliert beschrieben. Gleichzeitig wurden die *zeitlichen Verläufe und Zusammenhänge* in graphischer Form aufgearbeitet. Die Abbildung 17 fasst die wellenartige Entwicklung der IT-Sicherheit zusammen: IT-Sicherheit wurde bis Anfang der 1980er Jahre als ein rein **technisches Problem** angesehen. Während der zweiten Welle bis Mitte der 1990er Jahre rückte die IT-Sicherheit zunehmend in den Fokus des **Managements** bzw. der Unternehmensführung. Sicherheitsrichtlinien und andere Maßnahmen wurden innerhalb von Behörden (*Orange Book*) und Unternehmen entwickelt. Best practices und erste Standards wie der *BS 7799* hielten Einzug. Die Standarisierung der IT-Sicherheit (dritte Welle der **Institutionalisierung**) brachte ab Mitte der 1990er Jahre Methoden für eine Überprüfung der umgesetzten IT-Sicherheitsmaßnahmen mit sich. Gleichzeitig nahmen gesetzliche Regelungen mehr Einfluss auf unternehmerische Entscheidungen. Wie in Abbildung 17 zu sehen, standen und stehen Risikomanagement und IT-Governance im Fokus der vierten Welle **Governance der IT-Sicherheit** [Sol10, S. 1-4].

Großfirmen haben im Laufe der Jahrzehnte gegen IT-Sicherheitsvorfälle durch entsprechende Maßnahmen ein sehr hohes Absicherungslevel erreicht. Die *Verbreitung* von ISMS ist bei solchen Unternehmen am weitesten fortgeschritten. Immer mehr Unternehmen bieten heutzutage ihre Dienste weltweit über das Internet an. Mit der zunehmenden Vernetzung greifen viele Millionen Nutzer auf diese Dienste zu. Vor diesem Hintergrund sind für Kriminelle besonders kleine und mittlere Unternehmen und Privatanwender aufgrund ihres mangelnden Bewusstseins für und fehlenden Wissens über IT-Sicherheit lukrative Ziele geworden. Die Welle der **Cyber-Sicherheit** stellt IT-Experten vor neue Herausforderungen, entsprechende Maßnahmen und Lösungen für die Absicherung der Endbenutzer zu entwickeln [Sol10, S. 4 f.].

Seit Anfang Juni 2013 wurden die zukünftigen Herausforderungen im Bereich der IT-Sicherheit durch den NSA-Überwachungsskandal um eine Dimension erweitert. Die *Five Eyes*[46] zapfen Internetknoten und Unterwasserglasfaserkabel an, extrahieren Nutzerdaten von Internetfirmen und speichern große Mengen an Informationen zu Auswertungszwecken auf Vorrat [Bar13]. In den National Institute of Standards and Technology (NIST)-Standard SP 800-90A für einen Pseudo-Zufallszahlengenerator wurde gezielt eine Schwachstelle implementiert [Lar13].

Gegen die Manipulation von publizierten (technischen) Standards oder die Überwachung der Internetkommunikation durch staatliche Stellen mit ihren riesigen finanziellen, technischen und personellen Ressourcen ist es schwierig, geeignete und bezahlbare Maßnahmen zu finden und zu implementieren. Das Ausspähen

[46]Die Geheimdienste der USA, Großbritanniens, Neuseelands, Kanadas und Australiens.

von Informationen kann durch Maßnahmen der IT-Sicherheit (zum Beispiel der Verwendung einer starken Verschlüsselung der Daten und Kommunikationswege) zumindest erschwert werden. Für die Erreichung eines angemessenen Niveaus der unternehmenseigenen IT ist und bleibt IT-Sicherheitsmanagement damit ein geeignetes Mittel.

Literaturverzeichnis

[100] 100th United States Congress: *Computer Security Act of 1987: Public Law 100-235.* http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf

[ARG01] ARGE DATEN - Österreichische Gesellschaft für Datenschutz: *Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch, Standard-Sicherheitsmaßnahmen.* http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=08167tjz. Version: 2001

[Bar13] Barton Gellman and Laura Poitras ; The Washington Post (Hrsg.): *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program.* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Version: 06.06.2013

[Bau00] Bauer, Friedrich L.: *Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie.* 3., überarbeitete und erweiterte Auflage. Berlin : Springer, 2000. – ISBN 3–540–67931–6

[BD06] Bortz, Jürgen ; Döring, Nicola: *Forschungsmethoden und Evaluation: Für Human- und Sozialwissenschaftler.* 4., überarbeitete Auflage. Heidelberg : Springer, 2006 (Springer-Lehrbuch). – ISBN 3540333061

[Beu13] Beuth Verlag ; Beuth Verlag (Hrsg.): *Suchergebnis ISO/IEC 27001.* http://www.beuth.de/cn/d29ya2Zsb3duYW1lPWV4YUJhc2ljU2VhcmNoJmxhbmd1YWdlaWQ9ZGU*.html. Version: 16.09.2013

[BF08] Barlette, Yves ; Fomin, Vladislav V.: Exploring the Suitability of IS Security Management Standards for SMEs. In: Sprague, Ralph H. (Hrsg.): *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, IEEE Computer Society, 2008. – ISBN 978–0–7695–3075–8, 1–10

[BF10] Barlette, Yves ; Fomin, Vladislav V.: The Adoption of Information Security Management Standards: A Literature Review. Version: 2010. http://books.google.de/books?hl=de&lr=&id=zIdVXq5BLOMC&oi=

fnd&pg=PA69. In: Information Resources Management Association (Hrsg.): *Information Resources Management*. Hershey and Pa : IGI Global, 2010. – ISBN 9781615209668, 69–90

[BSI13a] BSI Group: *Upcoming revision of the ISO/IEC 27001 standard: The new version of ISO/IEC 27001:2013 is here*. http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/. Version: 01.10.2013

[BSI13b] BSI Group: *Standard in development: BS ISO/IEC 27001 Information technology - Security techniques - Information security mana gement systems - Requirements*. http://standardsdevelopment.bsigroup.com/Home/Project/200803528. Version: 2013

[BSI13c] BSI Group: *Standard in development: BS ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security controls*. http://standardsdevelopment.bsigroup.com/Home/Project/200802366. Version: 2013

[BSI13d] BSI Group: *Upcoming revision of the ISO/IEC 27001 standard*. http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/. Version: 2013

[Buna] Bundesminister des Inneren Schily: *Bekanntmachung der Neufassung des Bundesdatenschutzgesetzes*. http://emedien.sub.uni-hamburg.de/han/Juris/www.juris.de/jportal/portal/t/1gks/page/jurisw.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=BGBL1-2003-66&doc.part=F&doc.price=0.0#focuspoint

[Bunb] Bundespräsident und Bundesregierung: *Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik: BSI-Errichtungsgesetz (BSIG)*. http://www.bgbl.de/Xaver/text.xav?bk=Bundesanzeiger_BGBl&start=%2F%2F*[%40attr_id%3D%27bgbl111s2834.pdf%27]&wc=1&skin=WC#__Bundesanzeiger_BGBl__%2F%2F*[%40attr_id%3D%27bgbl190s2834.pdf%27]__1378734537517

[Bunc] Bundespräsident und Bundesregierung: *Gesetz zur Änderung datenschutzrechtlicher Vorschriften*. http://emedien.sub.uni-hamburg.de/han/Juris/www.juris.de/jportal/portal/t/1ikw/page/jurisw.psml?

pid=Dokumentanzeige&showdoccase=1&js_peid=
Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=
yes&doc.id=BGBL1-2009-2814&doc.part=E&doc.price=0.0#
focuspoint

[Bund] Bundespräsident und Bundesregierung: *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes*. http://www.bgbl.de/Xaver/text.xav?bk=Bundesanzeiger_BGBl&start=%2F%2F*[%40attr_id%3D%27bgbl111s2834.pdf%27]&wc=1&skin=WC#__Bundesanzeiger_BGBl__%2F%2F*[%40attr_id%3D%27bgbl190s2954.pdf%27]__1379931056769

[Bun92] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Sicherheitshandbuch: Handbuch für die sichere Anwendung der Informationstechnik: BSI 7105*. Version: 1.0, März 1992. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sicherheitshandbuch/sichhandbuch_zip.zip?__blob=publicationFile

[Bun96] Bundesamt für Sicherheit in der Informationstechnik: *Schriftenreihe zur IT-Sicherheit*. Bd. 3: *IT-Grundschutzhandbuch 1996: Maßnahmenempfehlungen für den mittleren Schutzbedarf*. Stand: 1996. Köln : Bundesanzeiger, 1996

[Bun97] Bundesamt für Sicherheit in der Informationstechnik: *Schriftenreihe zur IT-Sicherheit*. Bd. 3: *IT-Grundschutzhandbuch 1997: Maßnahmenempfehlungen für den mittleren Schutzbedarf*. Stand: 1997. Köln : Bundesanzeiger, 1997 http://www.worldcat.org/oclc/441590694. – ISBN 3–88784–760–1

[Bun98] Bundesamt für Sicherheit in der Informationstechnik: *Schriftenreihe zur IT-Sicherheit*. Bd. 3: *IT-Grundschutzhandbuch 1998: Maßnahmenempfehlungen für den mittleren Schutzbedarf*. Stand: 1998. Köln : Bundesanzeiger, 1998 http://www.ntua.gr/nmc/bsi/deutsch/menue.htm

[Bun00] Bundesamt für Sicherheit in der Informationstechnik: *Schriftenreihe zur IT-Sicherheit*. Bd. 3: *IT-Grundschutzhandbuch 2000: Maßnahmenempfehlungen für den mittleren Schutzbedarf: Management-Report zur Anwendung des IT-Grundschutzes*. Stand: 2000. Köln : Bundesanzeiger, 2000 http://mata.gia.rwth-aachen.de/Vortraege/itgswbt/gsschul/gshb/deutsch/aktuell/manager.pdf

[Bun02a] Bundesamt für Sicherheit in der Informationstechnik: *Schriftenreihe zur IT-Sicherheit*. Bd. 3: *IT-Grundschutzhandbuch 2002: Maßnahmenempfehlungen für den mittleren Schutzbedarf*. Stand: 2002. Köln : Bundesanzeiger, 2002

[Bun02b] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Zertifizierung nach IT-Grundschutz: Aufgaben des Zertifizierers*. Version: 1, 24.04.2002. http://mata.gia.rwth-aachen.de/Vortraege/itgswbt/gsschul/gshb/zert/zertifi.pdf

[Bun02c] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Qualifizierung/Zertifizierung nach IT-Grundschutz: Prüfschema für Auditoren*. Version: 2, 25.06.2002. http://mata.gia.rwth-aachen.de/Vortraege/itgswbt/gsschul/gshb/zert/pruef.pdf

[Bun03] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Aktuelles zum IT-Grundschutzhandbuch*. http://mata.gia.rwth-aachen.de/Vortraege/itgswbt/gsschul/gshb/deutsch/aktuell/aktuell.htm. Version: 2003

[Bun04] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Jahresbericht 2003: Meilensteine von der Gründung bis heute*. Version: 2004. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Jahresberichte/BSI-Jahresbericht_2003_pdf.pdf?__blob=publicationFile

[Bun09] Bundesamt für Sicherheit in der Informationstechnik: *Management-Report zur Anwendung des IT-Grundschutzes 2009*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/RegistrierungNewsletter/newsletter_registriert.html. Version: 2009

[Bun11a] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile. Version: 15.08.2011

[Bun11b] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen: Grad der Sensibilisierung des Mittelstandes in Deutschland*. Version: 2011.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf;jsessionid=1DD1754A160024CEAD5CD7C51D655155.2_cid286?__blob=publicationFile

[Bun11c] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz-Kataloge: 12. Ergänzungslieferung.* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html. Version: September 2011

[Bun12a] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Leitfaden Informationssicherheit: IT-Grundschutz kompakt.* Version: 2012. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

[Bun12b] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Überblick IT-Grundschutz: Entscheidungshilfe für Manager.* Version: 24.10.2012. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/UberblickGrundschutz.pdf?__blob=publicationFile

[Bun12c] Bundesministerium für Wirtschaft und Technologie (Hrsg.): *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen.* Version: 01.09.2012. http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Redaktion/PDF/it-sicherheit-studie-publikation,property=pdf,bereich=itsicherheit,sprache=de,rwb=true.pdf

[Bun13a] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz-Zertifikat: Allgemeine Informationen.* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/itgrundschutzzertifikat_node.html. Version: 11.09.2013

[Bun13b] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz-Zertifikat: ISO 27001-Zertifikate auf der Basis von IT-Grundschutz.* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Zertifikate/iso27001zertifikate_node.html. Version: 11.09.2013

[Bun13c] Bundesamt für Sicherheit in der Informationstechnik: *3. IT-Grundschutz-Tag 2013: Programm für den IT-Grundschutz-Tag am 12.09.2013*. https://www.bsi.bund.de/SharedDocs/Termine/DE/2013/3_IT_Grundschutztag_2013.html. Version: 12.09.2013

[Bun13d] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz: IT-Grundschutz International*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html. Version: 2013

[Bun13e] Bundesamt für Sicherheit in der Informationstechnik ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Fragen und Antworten zu Aufgaben und Themen des BSI: Was sind die Aufgaben des BSI?* https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html#faq4139842. Version: 26.08.2013

[Bun13f] Bundesamt für Sicherheit in der Informationstechnik: *Historie*. https://www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html. Version: 26.08.2013

[Bun13g] Bundesministerium der Justiz: *Neuer Schwung für Datenschutzgrundverordnung*. http://www.bmj.de/SharedDocs/Kurzmeldungen/DE/2013/20132207_JI-Rat.html. Version: 22.07.2013

[Bun13h] Bundesministerium für Wirtschaft und Technologie ; Bundesministerium für Wirtschaft und Technologie (Hrsg.): *Mittelstand Digital des BMWi: IT-Sicherheit für KMU*. http://www.mittelstand-digital.de/DE/Wissenspool/it-sicherheit-kmu.html. Version: 2013

[Cab11] Cabinet Office ; Cabinet Office (Hrsg.): *Cyber Security Strategy*. https://www.gov.uk/government/publications/cyber-security-strategy. Version: 25.11.2011

[Cal05] Calder, Alan: *The case for ISO 27001*. Ely and U.K : IT Governance Pub., 2005 http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10496554. – ISBN 9781905356133

[Chi12] Chiarini, Andrea: *From Total Quality Control to Lean Six Sigma: Evolution of the most important management systems for the*

excellence. Milan and New York : Springer, 2012 (SpringerBriefs in business). – ISBN 884702658X

[Dat87] Data Processing Management Association (Hrsg.): *Staffing Dedication to Security Redcues Computer Abuse New Study Discovers*. 1987 (Inside DPMA)

[Depa] Department of Defense: *DoD 5220.22-M - National Industrial Security Program Operating Manual*. http://transition.usaid.gov/policy/ads/500/d522022m.pdf

[Depb] Department of Defense: *DoD 5220.22-R - Industrial Security Regulation*. http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf

[Dep85a] Department of Defense: *Technical Rational Behind CSC-STD-003-85: Computer Security Requirements - Guidance for Applying the DoD TCSEC in Specific Environments*. https://www.fas.org/irp/nsa/rainbow/std004.htm. Version: 25.06.1985

[Dep85b] Department of Defense: *Trusted Computer System Evaluation Criteria*. http://csrc.nist.gov/publications/history/dod85.pdf. Version: 26.12.1985

[Dep02] Department of Trade and Industry (Hrsg.): *Information security breaches survey 2002: technical report*. Version: 2002. http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/industry_files/pdf/sbsreport_2002.pdf

[Dep04] Department of Trade and Industry (Hrsg.): *Information security breaches survey 2004: technical report*. Version: 2004. http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf

[Dep06] Department of Trade and Industry (Hrsg.): *Information security breaches survey 2006: technical report*. Version: 2006. http://webarchive.nationalarchives.gov.uk/+/http://www.dti.gov.uk/files/file28343.pdf

[Dep08] Department for Business Enterprise and Regulatory Reform (Hrsg.): *Information security breaches survey 2008: technical report*. Version: 2008. http://www.eurim.org.uk/activities/ig/voi/DBERR.pdf

[Dep10a] Department for Business, Innovation and Skills: *History of BERR and DTI*. http://webarchive.nationalarchives.gov.uk/+/http://www.berr.gov.uk/aboutus/corporate/history/index.html. Version: 04.03.2010

[Dep10b] Department for Business, Innovation and Skills (Hrsg.): *Information security breaches survey 2010: technical report*. Version: 2010. http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1723

[Dep12] Department for Business, Innovation and Skills (Hrsg.): *Information security breaches survey 2012: technical report*. Version: 2012. http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf

[Dep13a] Department for Business, Innovation and Skills (Hrsg.): *Information security breaches survey 2013: technical report*. Version: 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

[Dep13b] Department for Business, Innovation and Skills (Hrsg.): *Small businesses: what you need to know about cyber security*. Version: 23.04.2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197177/bis-13-780-small-business-cyber-security-guidance.pdf

[Det08] Detlefsen, Wiebke: *Der Risikomanagementbericht nach dem BilMoG*. http://www.uni-hamburg.de/fachbereiche-einrichtungen/fb03/iwp/rut/Arbeit73.pdf. Version: 2008

[Deu10] Deutsches Institut für Normung e. V.: *NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA): NA 043-01-27 AA Homepage*. http://www.nia.din.de/cmd?level=tpl-artikel&languageid=de&cmstextid=sicherheitsverfahren. Version: 04.03.2010

[Deu13] Deutsches Institut für Normung e. V.: *NA 043 Normenausschuss Informationstechnik und Anwendungen (NIA): Alle gültigen Normen von NA 043-01-27 AA*. http://www.nia.din.de/cmd?search_grem_akt=54770248&level=tpl-suchergebnis&searchDisplay=-tabelle&committeeid=54738935&SEARCHACCESSKEY=

NORMS&languageid=de&subcommitteeid=54770248&search_level=d|i&workflowname=committeeNormSearch. Version: 2013

[Eck09] Eckert, Claudia: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. 6., aktualisierte und erweiterte Auflage. München : Oldenbourg, 2009. – ISBN 978–3–486–58999–3

[ENI12] ENISA: *Consumerization of IT: Top Risks and Opportunities: Responding to the Evolving Threat Environment [Deliverable – 2012-09-28]*. Version: 18.10.2012. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities

[ENI13a] ENISA: *Consumerization of IT: Risk Mitigation Strategies and Good Practices: Responding to the Evolving Threat Environment [Deliverable – 2012-12-19]*. Version: 17.04.2013. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report

[ENI13b] ENISA: *Inventory of Risk Management - Risk Assessment methods and tools: Inventory of Risk Management / Risk Assessment Methods*. http://rm-inv.enisa.europa.eu/methods. Version: 2013

[Eura] Europäisches Parlament und Rat der europäischen Union: *Richtlinie 2006/43/EG: Abschlussprüfungs-Richtlinie (EuroSOX)*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:0107:DE:PDF

[Eurb] Europäisches Parlament und Rat der europäischen Union: *Richtlinie 2008/30/EG: Abschlussprüfungs-Richtlinie (EuroSOX)*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:081:0053:0056:DE:PDF

[Eur12] Europäische Kommission: *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr: Datenschutz-Grundverordnung*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF. Version: 25.01.2012

[Fal12] Falk, Michael: *IT-Compliance in der Corporate Governance: Anforderungen und Umsetzung*. Wiesbaden : Gabler Verlag, 2012 (SpringerLink : Bücher). – ISBN 3834939889

[FdB08] Fomin, Vladislav V. ; de Vries, Henk J. ; Barlette, Yves: *ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption.* Version: 2008. http://pdf.aminer.org/000/249/641/an_empirical_exploration_of_how_process_standardization_reduces_outsourcing_risks.pdf

[Fed13] Federrath, Hannes: *Vorlesung Management von Informationssicherheit.* https://www.informatik.uni-hamburg.de/svs/teaching/folien/SMT-30secmgmt.pdf. Version: 08.04.2013

[FG11] Federrath, Hannes ; Gerber, Christoph: *Kollaboratives IT-Sicherheitsmanagement auf Basis von BSI-Grundschutz.* http://svs.informatik.uni-hamburg.de/publications/2011/2011-10-04_KollabITSM.pdf. Version: 05.10.2011 (INFORMATIK 2011)

[FKB89] Fites, Philip E. ; Kratz, Martin P. J ; Brebner, Alan F.: *Control and security of computer information systems.* Rockville and MD : Computer Science Press, 1989. – ISBN 9780716781912

[Fri13a] Fribbins, Suzanne: *Introducing the new ISO/IEC 27001: Based on the Final Draft International Standard (FDIS): ISO/IEC 27001 revision webinar.* https://bsiedge.bsi-global.com/iso27001fdis/. Version: 2013

[Fri13b] Fribbins, Suzanne: *What you can expect from the new ISO 27001: Based on the Draft International Standard (DIS): ISO 27001 revision webinar.* http://bsiedge.bsi-global.com/iso27001dis/. Version: 2013

[Goc08] Gockel, Tilo: *Form der wissenschaftlichen Ausarbeitung: Studienarbeit, Diplomarbeit, Dissertation, Konferenzbeitrag: Begleitende Materialien unter http://www.formbuch.de.* Berlin and Heidelberg : Springer-Verlag Berlin Heidelberg, 2008. – ISBN 364213906X

[HBDK97] Hillebrand, Annette ; Buellingen, Franz ; Dickoph, Olaf ; Klinge, Carsten ; Wissenschaftliches Institut für Kommunikationsdienste (Hrsg.): *Informations- und Telekommunikationssicherheit in kleinen und mittleren Unternehmen.* Version: Juni 1997. http://www.wik.org/index.php?id=diskussionsbeitraegedetails&tx_ttnews[cat]=4&tx_ttnews[year]=1997&tx_ttnews[tt_news]=263&tx_ttnews[backPid]=93&cHash=39935389fbf4d6cf323496c86121b0cf (Diskussionsbeitrag 175)

[hei13] HEISE ONLINE: *Auch Washington Post gehackt*. http://www.heise.de/newsticker/meldung/Auch-Washington-Post-gehackt-1796535.html. Version: 02.02.2013

[HM13] HAEBERLEN, Thomas ; MATTIOLI, Rossella: *Can Recent Attacks Really Threaten Internet Availability?* Version: 12.04.2013. http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability (Flash Note FN/02/2013)

[HS04] HOFMANN, J. ; SCHMIDT, W.: *Kompaktkurs IT-Management*. Vieweg, Friedr., & Sohn Verlagsgesellschaft mbH, 2004 http://books.google.de/books?id=RzgD3nvI4ygC. – ISBN 9783528058814

[HS10] HOFMANN, J. ; SCHMIDT, W.: *Masterkurs IT-Management: Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker*. 2., akt. und erw. Vieweg+Teubner, 2010. – ISBN 9783834808424

[IBM06] IBM CORPORATION: *IBM Resource Access Control Facility (RACF)*. http://www-03.ibm.com/systems/z/os/zos/features/racf/index.html. Version: 24.05.2006

[II05] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ; INTERNATIONAL ELECTROTECHNICAL COMMISSION: *ISO/IEC 27001 - Information technology. Security techniques. Information security management systems. Requirements*. 18.10.2005

[II12] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ; INTERNATIONAL ELECTROTECHNICAL COMMISSION: *ISO/IEC 27000 - Information technology. Security techniques. Information security management systems. Overview and vocabulary*. Second Edition. 01.12.2012

[Int12] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *The ISO Survey of Management System Standard Certifications 2011: Executive summary*. http://www.iso.org/iso/iso_survey2011_executive-summary.pdf. Version: 07.12.12

[Int13a] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *Standards catalogue: JTC 1/SC 27 - IT Security techniques: Standards and*

projects under the direct responsibility of ISO/IEC JTC 1/SC 27 Secretariat. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306. Version: 16.04.2013

[Int13b] International Organization for Standardization: *About ISO*. http://www.iso.org/iso/home/about.htm. Version: 19.06.2013

[Int13c] International Organization for Standardization: *The ISO Survey of Management System Standard Certifications (2006-2011)*. http://www.iso.org/iso/database_iso_27001_iso_survey_2011.xls. Version: 19.06.2013

[Int13d] International Organization for Standardization: *Management system standards*. http://www.iso.org/iso/home/standards/management-standards.htm. Version: 27.09.2013

[ISA13] ISACA Austria: *COBIT 5: Das Framework für Governance und Management der Unternehmens-IT: Die Entwicklung von COBIT*. http://www.isaca.org/chapters6/austria/Benefits/Pages/Page1.aspx. Version: 2013

[Ise13] IsecT Ltd ; IsecT Ltd (Hrsg.): *ISO27k Information Security Standards*. http://www.iso27001security.com/index.html. Version: 23.06.2013

[IT 13] IT Governance Ltd: *BS ISO/IEC DIS 27001 (Draft ISO27001:2013): What's different in the new draft of ISO27001?* http://www.itgovernance.co.uk/shop/p-1274-bs-isoiec-dis-27001-draft-iso27001-2013.aspx. Version: 2013

[Kau13] Kaufmann, Noogie C.: Schotten dicht im Cyberraum: Regierungsentwurf für IT-Sicherheitsgesetz lässt viele Fragen offen. In: *c't* (2013), Nr. 11, S. 172

[Kem02] Kemmerer, Richard A.: Computer Security. Version: 2002. https://www.cs.ucsb.edu/~kemm/courses/cs177/ency.pdf. In: Marciniak, John J. (Hrsg.): *Encyclopedia of Software Engineering*. New York : John Wiley, 2002. – ISBN 0471028959, 1–24

[Ken01] Kenning, M. J.: Security Management Standard: ISO 17799/BS 7799. In: *BT Technology Journal* 19 (2001), Nr. 3, 132–136. http://link.springer.com/content/pdf/10.1023%2FA%3A1011954702780.pdf

[KM11] Kouns, Jake ; Minoli, Daniel: *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Wiley, 2011 http://books.google.de/books?id=0D2eM4GQCqgC. – ISBN 9781118211618

[KRSW08] Kersten, Heinrich ; Reuter, Jürgen ; Schröder, Klaus-Werner ; Wolfenstetter, Klaus-Dieter: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung*. 1. Wiesbaden : Friedr. Vieweg & Sohn Verlag, 2008 (Edition Kes). – ISBN 978–3–8348–0178–4

[KRSW13] Kersten, Heinrich ; Reuter, Jürgen ; Schröder, Klaus-Werner ; Wolfenstetter, Klaus-Dieter: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung*. 4., akt. u. erw. Aufl. 2013. Wiesbaden : Springer, 2013 (Edition Kes). http://dx.doi.org/10.1007/978-3-658-01724-8. – ISBN 9783658017231

[Lar13] Larson, Jeff ; ProPublica (Hrsg.): *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*. http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption. Version: 05.09.2013

[Mar02] Marciniak, John J. (Hrsg.): *Encyclopedia of Software Engineering*. 2nd ed. New York : John Wiley, 2002. – ISBN 0471028959

[MB02] Martin, Thomas A. ; Bär, Thomas: *Grundzüge des Risikomanagements nach KonTraG: Das Risikomanagementsystem zur Krisenfrüherkennung nach [section] 91 Abs. 2 AktG*. München [u.a.] : Oldenbourg, 2002 (Managementwissen für Studium und Praxis). – ISBN 9783486258769

[Min79] Mintzberg, Henry: *The structuring of organizations: A synthesis of the research*. London : Prentice-Hall, 1979. – ISBN 0–13–853771–2

[Mou84] Moulton, Rolf: Data security is a management responsibility. In: *Computers & Security* 3 (1984), Nr. 1, S. 3–7

[Mül10] Müller, Jürgen: *Zertifizierung-IT-Sicherheitsbeauftragter: IT-Sicherheitsmanagement nach IT-Grundschutz*. http://www.ba-gera.de/Downloads/it-sibe/01_SiBe_IT-Grundschutz_Sicherheitsmanagement.pdf. Version: 29.01.2010

[Mün07] Münch, Isabel ; IHK Magdeburg (Hrsg.): *Informationssicherheit mit IT-Grundschutz*. http://www.magdeburg.ihk.de/servicemarken/presse/IHK_Zeitschrift/Archiv/Der_Markt_in_Mitteldeutschland_2007/September_2007/Titelthema/933658/Informationssicherheit_mit_IT_Grundschutz.html. Version: 2007

[Mün08a] Münch, Isabel ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz - der direkte Weg zur Informationssicherheit*. Version: 08.10.2008. http://www.security-forum.de/fileadmin/security_files/Handouts/2008/ForumI_Mi_12_45_Muench.pdf?PHPSESSID=

[Mün08b] Münch, Isabel: IT-Grundschutz-Kataloge 2007. In: *IT-Sicherheit & Datenschutz* (2008), Nr. 03, 215. http://link.springer.com/content/pdf/10.1007%2Fs11623-008-0034-7.pdf

[Mün11] Münch, Isabel ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz: Informationssicherheit ohne Risiken und Nebenwirkungen*. Version: 25.10.2011. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag_25102011/02_ITGSohneRisikenundNebenwirkungen.pdf?__blob=publicationFile

[Poo03] Poole, Owen: *Network security: A practical guide*. Oxford : Butterworth-Heinemann, 2003 http://books.google.de/books?id=gpTOgdBHL_IC. – ISBN 0750650338

[PR93] Pfitzmann, Andreas ; Rannenberg, Kai: Staatliche Initiativen und Dokumente zur IT-Sicherheit: eine kritische Würdigung. In: *Computer und Recht (CR)* 9 (1993), Nr. 3, 170–179. http://www.web-portal-system.de/wps/wse/dl/showfile/rannenberg/5708/StaatlicheInitiativenundDokume.pdf

[Pri13] PricewaterhouseCoopers: *The consumerization of IT: The next-generation CIO*. Version: 18.04.2013. http://www.pwc.com/us/en/technology-innovation-center/consumerization-information-technology-transforming-cio-role.jhtml

[Ran98] Rannenberg, Kai: Kriterien und Zertifizierung mehrseitiger IT-Sicherheit. In: Fiedler, Herbert (Hrsg.): *Ausgezeichnete*

Informatikdissertationen 1997. Stuttgart [u.a.] : Teubner, 1998. – ISBN 9783519026471, S. 98–117

[Rat] Rat der Europäischen Gemeinschaften: *Erste Richtlinie 73/239/EWG*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31973L0239:de:HTML

[RM77] Ruthberg, Zella G. (Hrsg.) ; McKenzie, Robert G. (Hrsg.): *NBS special publication*. Bd. 500-19: *Audit and evaluation of computer security: Proceedings of the NBS invitational workshop, held at Miami Beach, Florida, March 22-24, 1977*. [Gaithersburg and Md.] and Washington : U.S. Dept. of Commerce, National Bureau of Standards and for sale by the Supt. of Docs., U.S. Govt. Print. Off., 1977

[Rob93] Roberts, D. W.: Evaluation criteria for it security. In: Goos, Gerhard (Hrsg.) ; Hartmanis, Juris (Hrsg.) ; Preneel, Bart (Hrsg.) ; Govaerts, René (Hrsg.) ; Vandewalle, Joos (Hrsg.): *Computer Security and Industrial Cryptography* Bd. 741. Berlin and Heidelberg : Springer Berlin Heidelberg, 1993. – ISBN 978–3–540–57341–8, S. 149–161

[SA09] Sicherheitsmanagement, AK (Hrsg.) ; Arbeitsauschuss NIA-27 (Hrsg.): *Kompass der IT-Sicherheitsstandards: Leitfaden und Nachschlagewerk*. Version: 4, August 2009. http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_web.pdf

[Sch13] Schildt, Holger ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Neues aus dem IT-Grundschutz: Ausblick und Diskussion: Grundlagen der Informationssicherheit und IT-Grundschutz*. Version: 13.06.2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/2GS_Tag_2013/2_IT-Grund_2013_Schildt.pdf?__blob=publicationFile (IT-Grundschutz-Tag 2013 2)

[Sol10] Solms, S. H.: The 5 Waves of Information Security: From Kristian Beckman to the Present. In: Rannenberg, Kai (Hrsg.) ; Varadharajan, Vijay (Hrsg.) ; Weber, Christian (Hrsg.): *Security and Privacy – Silver Linings in the Cloud* Bd. 330. Berlin and Heidelberg : Springer Berlin Heidelberg, 2010. – ISBN 978–3–642–15256–6, S. 1–8

[Str86] Straub, Detmar W.: Computer abuse and security: Update on an empirical pilot study. In: *ACM SIGSAC Review* 4 (1986), Nr. 2, S. 21–31

[Str88] Straub, Detmar W.: Organizational structuring of the computer security function. In: *Computers & Security* 7 (1988), Nr. 2, S. 185–195

[Str90] Straub, Detmar W.: Effective IS Security: An Empirical Study. In: *Information Systems Research* 1 (1990), Nr. 3, S. 255–276

[Syl08] Sylvester, Axel: *Visualisierung soziotechnischer Prozesse unter Verwendung der Konzepte des Mikropolis-Modells*. Hamburg, Universität Hamburg, Diss., 29.07.2008. http://agis-www.informatik.uni-hamburg.de/fileadmin/asi/Diplomarbeiten/DiplA_Axel_Sylvester.pdf

[The13] The Spamhaus Project Webteam: *The Spamhaus Project*. http://www.spamhaus.org/. Version: 07.05.2013

[TW12] Tangen, Stefan ; Warris, Anne-Marie: *New format for future ISO management system standards*. http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1621. Version: 18.07.2012

[Völ04] Völker, Jörg: BS 7799: Von "Best Practice" zum Standard. In: *Datenschutz und Datensicherheit (DuD)* (2004), Nr. 28, 102–108. http://www.secorvo.de/publikationen/bs7799-voelker-2004.pdf

[Wec07] Weck, Gerhard: Messbare IT-Sicherheit. In: *Datenschutz und Datensicherheit (DuD)* (2007), Nr. 31, 84–86. http://link.springer.com/content/pdf/10.1007%2Fs11623-007-0044-x.pdf

[Wel13] Welsch, Günther ; Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Neues aus dem IT-Grundschutz: Ausblick und Diskussion: Grundlagen der Informationssicherheit und IT-Grundschutz*. Version: 12.09.2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag_2013/08_3_IT-Grund_2013_Welsch.pdf;jsessionid=4AAF3B2B95D74C523229DCB8316B0009.2_cid359?__blob=publicationFile (IT-Grundschutz-Tag 2013 3)

[Wor11] World Standards Cooperation: *About WSC: Established in 2001*. http://www.worldstandardscooperation.org/about.html. Version: 2011

[Zen90] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): *IT-Evaluationshandbuch: Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT): 1. Fassung.* Version: 22.02.1990. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/EHB0222_pdf.pdf?__blob=publicationFile

Erklärung

Ich versichere, dass ich die Bachelorarbeit im Studiengang Wirtschaftsinformatik selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen – benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht. Ich versichere weiterhin, dass ich die Arbeit vorher nicht in einem anderen Prüfungsverfahren eingereicht habe und die eingereichte schriftliche Fassung der auf dem elektronischen Speichermedium entspricht.

Ich bin mit der Einstellung der Arbeit in den Bestand der Bibliothek des Departments Informatik einverstanden.

Hamburg, den 28. Oktober 2013

Martin Hinsch