secorvo
security consulting

BS 7799
Von „Best Practice“ zum Standard

Secorvo White Paper

Informationssicherheits-Management nach BS 7799 im Überblick

Version 1.3
Stand 27. September 2005

Jörg Völker

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

BS	British Standard
BSI	British Standard Institute
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCSC	DTI Commercial Computer Security Centre
DIT	Department of Trade and Industry
EA	European co-operation for Accreditation
EMS	Environmental Management Systems
GSHB	Grundschutzhandbuch
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO TR	ISO Technical Report
ITSEC	Information Technology Security Evaluation Criteria
NCC	National Computing Centre
OECD	Organisation for Economic Co-operation and Development
PD	Public Document
PDCA	Plan-Do-Check-Act Model
QMS	Quality Management Systems
SoA	Statement of Applicability
TGA	Trägergemeinschaft für Akkreditierung GmbH

Historie

Version	Datum	Änderung	Autor
1.0	06.10.2003	Erste Fassung	Jörg Völker
1.1	06.11.2003	Redaktionelle Änderungen	Jörg Völker
1.2	26.11.2004	Ergänzung um weitere Entwicklung des Standards	Jörg Völker
1.3	27.09.2005	Einarbeitung Änderungen ISO 17799:2005	Jörg Völker

1 Zusammenfassung

Der zweiteilige britische Standard BS 7799 zum Management von Informationssicherheit enthält eine umfassende Sammlung von Maßnahmen, die dem Best Practice-Ansatz in der Informationssicherheit genügen. Teil 1 des Standards hat die Aufgabe, diese Maßnahmen darzustellen; Teil 2 bildet eine Basis für die Beurteilung eines Informationssicherheits-Managementsystems, die für ein formales Verfahren zur Zertifizierung herangezogen werden kann.

Dieses White Paper beschreibt die Inhalte der beiden Teile von BS 7799. Ferner werden Hilfestellungen gegeben, wie BS 7799 in das Qualitätsmanagement einer Organisation integriert werden kann; abschließend werden die entsprechenden Prüf- und Zertifizierungsprozesse erläutert.

2 Entstehungsgeschichte

Der Ursprung von BS 7799/ISO 17799 reicht zurück zu den Tagen des britischen Department of Trade and Industry (DTI) Commercial Computer Security Centre (CCSC). Gegründet im Mai 1987, hatte das CCSC zwei Hauptaufgaben. Die eine bestand darin, Herstellern von IT-Sicherheitsprodukten dabei zu helfen, international anerkannte Kriterien zur Evaluierung von Sicherheitsprodukten und ein darauf basierendes Evaluierungs- und Zertifizierungsschema zu entwickeln. Diese Bemühungen flossen letztendlich in die Entwicklung der „Information Technology Security Evaluation Criteria“ (ITSEC) ein.

Der zweite Schwerpunkt des CCSC lag in der Entwicklung eines „code of good security practice“ und resultierte 1989 in der Veröffentlichung des „Users code of practice“. Diese Verhaltensrichtlinie wurde später vom National Computing Centre (NCC) und einer Gruppe von führenden Unternehmen und Organisationen weiterentwickelt; es sollte auf diesem Wege sichergestellt werden, dass der Code sinnvoll und aus Benutzersicht auch praktisch anwendbar war. Das Resultat wurde schließlich als Public Document (PD) 0003, *„A Code of Practice for Information Security Management“* veröffentlicht und mündete nach einiger Umgestaltung 1995 in den durch das British Standard Institute (BSI) herausgegebenen britischen Standard BS 7799 Teil 1.

Dieser "Leitfaden zum Management von Informationssicherheit", der Sicherheitsmaßnahmen und Hinweise für ein sinnvolles Vorgehen enthielt, sollte Industrie und Behörden bei der Umsetzung von Informationssicherheit unterstützen. Im Jahre 1998 wurde dann ein zweiter Teil, BS 7799 Teil 2 *„Information Security Management Systems – Specification with guidance for use“*, veröffentlicht, der den Prozess zur Entwicklung eines Information Security Management Systems (ISMS) beschreibt und als Grundlage für eine Zertifizierung dient.

Im Jahr 1998 wurde BS 7799 einer gründlichen Revision unterzogen. Ziel dieser Überarbeitung war, neue Entwicklungen (z.B. E-Commerce, mobiles Arbeiten) und entsprechende Maßnahmen hinzuzufügen, sowie die internationale Akzeptanz des Standards zu erhöhen, beispielsweise durch das Entfernen aller „UK-spezifischen Verweise“ innerhalb des Dokuments. Die neue Fassung des Standards wurde schließlich im März 1999 veröffentlicht.

Das internationale Interesse an BS 7799 führte schließlich im Dezember 2000 dazu, dass BS 7799 Teil 1 als sog. „Fast Track" in die ISO-Standardisierung (International Organization for Standardization) eingebracht wurde und unter der Bezeichnung ISO 17799:2000 als internationaler Standard veröffentlicht wurde. „Fast Track“ bedeutet, dass, mit Ausnahme einiger unbedeutender editorischer Änderungen, die ursprüngliche Fassung von BS 7799 Teil 1 ohne weitere inhaltliche Korrekturen übernommen wurde.

ISO 17799 umfasst jedoch nicht den zweiten Teil der BS 7799, der den Bereich der Umsetzung abdeckt und die Grundlage für die Auditierung und Zertifizierung bildet. Innerhalb von ISO wird ISO 17799 in der Working Group 1 des Informationssicherheitskomitees ISO/IEC JTC1 SC27 „IT Security Techniques" betreut. Schon bald nach der Veröffentlichung von ISO 17799:2000 hat man sich an dessen Überarbeitung begeben. Im Juni diesen Jahres wurde dann die neue Revision ISO 17799:2005 verabschiedet, die einige wesentliche Änderungen mit sich brachte.

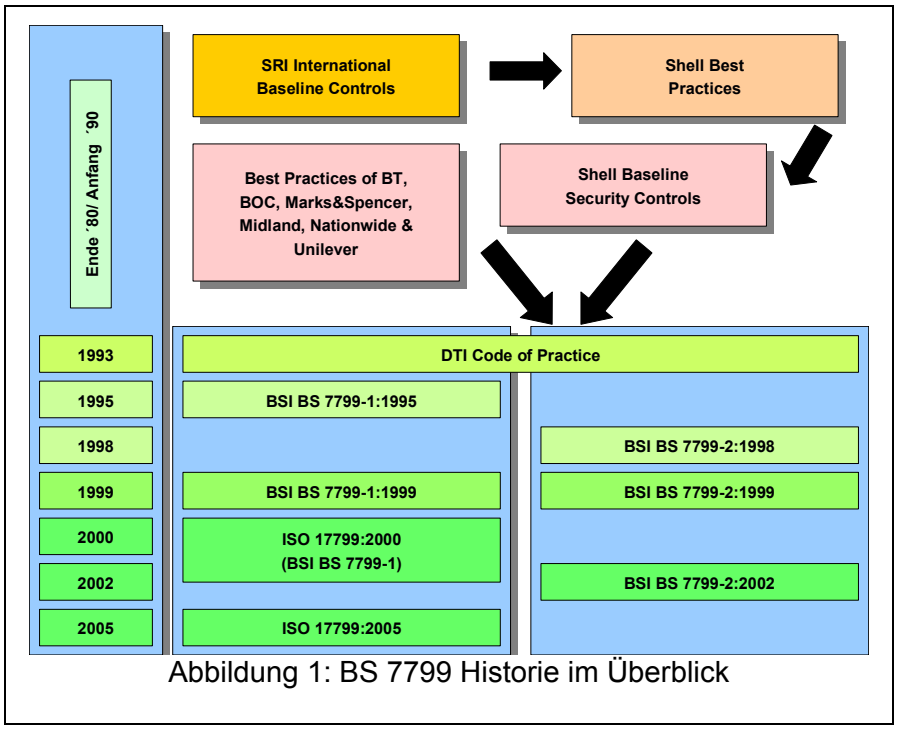

Abbildung 1: BS 7799 Historie im Überblick

Im Jahre 2002 wurde ferner eine überarbeitete Fassung von BS 7799 Teil 2 (BS 7779-2:2002) vorgelegt. Ziel dieser Revision war die Harmonisierung mit anderen Management-Standards, beispielsweise ISO 9001:2000 und ISO 14001.

3 BS 7799 / ISO 17799 im Überblick

3.1 ISO 17799:2000

3.1.1 Einführung

ISO 17799 „Code of Practice for Information Security Management“ ist ein heute international anerkannter Leitfaden zum Management von Informationssicherheit und umfasst eine Sammlung von Empfehlungen für Informationssicherheitsverfahren und -methoden, die sich in der Praxis bewährt haben („best practices“). Der Standard orientiert sich dabei an einem Top-Down-Ansatz mit generischen Standard-Sicherheitsmaßnahmen für annähernd alle relevanten Bereichen der Informationssicherheit (siehe Abbildung 2). Er enthält keine produktorientierten und nur allgemeine technologieorientierte Maßnahmen und empfiehlt bewusst keine konkreten Sicherheitslösungen.

ISO 17799 adressiert kein spezielles Sicherheitsniveau, wodurch eine individuelle Anpassung an ein höheres oder niedrigeres Sicherheitsniveau jederzeit möglich ist. Die

Auswahl der Maßnahmen orientiert sich dabei an den spezifischen Gegebenheiten des Unternehmens und ist so auch für kleinere Unternehmen problemlos anwendbar.

Eine konkrete Vorgehensweise gibt der Standard nicht vor, nennt aber kritische Erfolgsfaktoren, die für die Etablierung eines ISMS ausschlaggebend sind. Zu diesen Erfolgsfaktoren zählt insbesondere, dass:

- Sicherheitspolitik, Ziele und Aktivitäten an den Geschäftszielen ausgerichtet sind,
- das Vorgehen der Unternehmenskultur angepasst ist,
- Informationssicherheit der Unterstützung durch das (Top-)Management bedarf,
- ein gutes Verständnis der Sicherheitsanforderungen, von Risk Assessment und Risk Management vorliegt,
- zur Erhöhung der Sensibilisierung ein effektives Information Security Marketing existiert,
- alle Betroffenen die bestehenden Security Guidelines und Regeln kennen,
- ein Budget für Information Security Managemant zur Verfügung steht
- Trainings und Schulungen durchgeführt werden ,
- ein effektiver Incident Management Prozess etabliert wird und
- ein System zur Bemessung und Verbesserung des ISMS existiert.

Der Leitfaden sieht sich als Basis zur Entwicklung organisationsbezogener Sicherheits-normen und effektiver Managementpraktiken. Er eröffnet Unternehmen, Institutionen und Behörden den Weg zu einer formalen Zertifizierung des eigenen ISMS (nach BS7799-2) und definiert die Zielsetzung der Informationssicherheit hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit.

3.1.2 Gliederung

ISO 17799 gliedert sich in elf Managementgebiete und umfasst 39 Maßnahmenziele. Die Maßnahmenziele wiederum spezifizieren insgesamt 133 Maßnahmen („baseline controls“), die zur Zielerreichung umgesetzt werden können.

Die elf Managementgebiete umfassen dabei folgende Punkte:

1) Security Policy
2) Organization of information security
3) Asset Management
4) Human Resources Security
5) Physical and Environmental Security
6) Communications and Operations Management
7) Access Control
8) Information systems acquisition, development & maintance
9) Information security incident handling
10) Business Continuity Management
11) Compliance

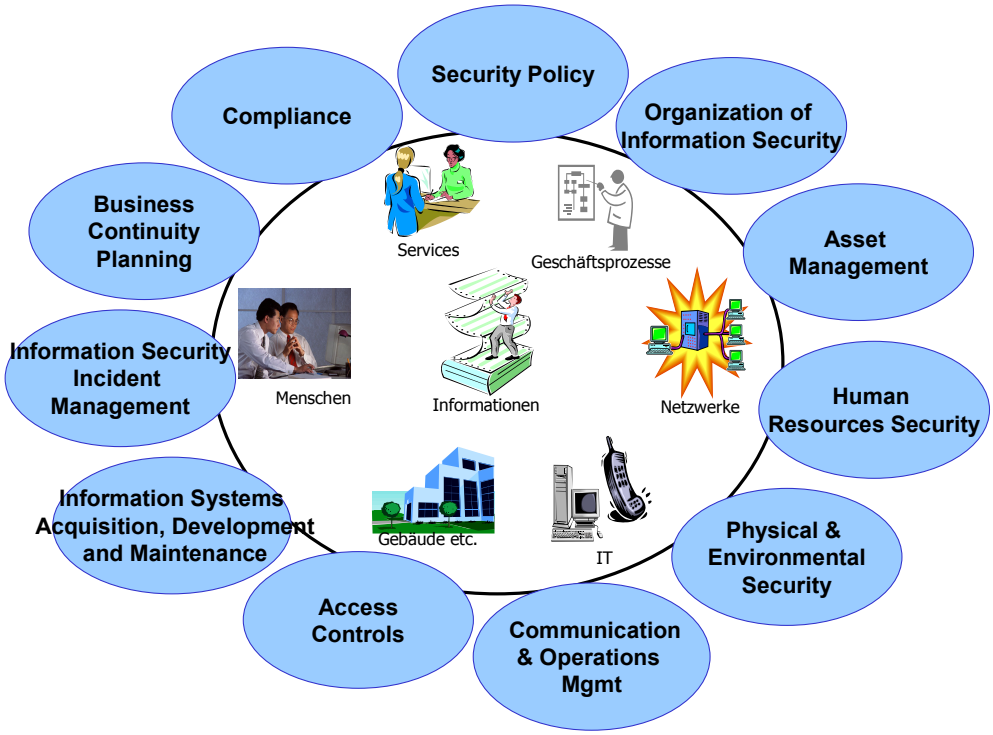

Abbildung 2: ISO 17799:2005 Managementgebiete

Die Inhalte und Ziele dieser Managementgebiete werden im Folgenden näher dargestellt.

Security Policy

Die Sicherheitspolitik dient der Festlegung der strategischen Ausrichtung und der Dokumentation der Unterstützung durch das Management hinsichtlich aller Belange der Informationssicherheit. Diese Richtungsvorgabe soll an alle Mitarbeiter kommuniziert werden; eine regelmäßige Überprüfung und Bewertung der Security Policy stellt die Aktualität und Angemessenheit der getroffenen Maßnahmen sicher.

Organization of information security

Es sollte ein entsprechendes Management Framework etabliert werden, das Methoden, Verfahren und Prozesse zur Initiierung, Implementierung und Kontrolle von Informationssicherheit im Unternehmen zur Verfügung stellt. Neben dem Aufbau einer entsprechenden internen organisatorischen Infrastruktur und der Klärung von Verantwortlichkeiten, werden hier auch grundlegende Sicherheitsaspekte bei Zugriff auf Informationen und IT-Systeme durch Dritte adressiert.

Asset Management

Um einen angemessenen Schutz der Unternehmenswerte erreichen zu können, bedarf es einer gründlichen und umfassenden Inventarisierung dieser Werte. Diese Werte sollten einen eindeutigen Eigentümer aufweisen. Um eine Einstufung und Zuordnung von Sicherheitsmaßnahmen durchführen zu können, sollte ein Klassifikationsschema erstellt und zur Kennzeichnung der Werte herangezogen werden.

Human Resources Security

Dieses Managementgebiet dient der Reduzierung von Risiken durch menschliche Fehler, Diebstahl, Betrug oder Missbrauch von Einrichtungen. Es umfasst sowohl Maßnahmen für interne und externe Mitarbeiter, als auch für sonstige Auftragnehmer. Unterschieden werden

hierbei grundlegende Maßnahmen, Maßnahmen während des Beschäftigungsverhältnisses als auch Maßnahmen, die bei der Beendigung des Beschäftigungsverhältnisses berücksichtigt werden sollten.

Physical and Environmental Security

Durch die Errichtung von Sicherheitszonen sollen vorbeugende Maßnahmen ergriffen werden, die der Vermeidung von unberechtigtem Zugang und Beschädigung von Geschäftsgebäuden und Informationen dienen. Des Weiteren werden Maßnahmen definiert, die vor Verlust, Beschädigung oder Kompromittierung von Wirtschaftsgütern und Unterbrechung der Geschäftstätigkeit schützen.

Communications and Operations Management

Dieser sehr umfassende Managementbereich adressiert folgende Maßnahmenziele:

a) Sicherstellung des sicheren und korrekten Betriebs

b) Service Management bei Bereitstellung von Leistungen durch Dritte

c) Risikominimierung bei Systemausfällen durch Systemplanung und Abnahmevon Systemen

d) Integrationsschutz von Informationen und Software, Schutz vor Malicious und Mobilen Code

e) Integrität und Verfügbarkeit von IT-Systemen & TK-Anlagen durch geeignete Backup Prodzeduren

f) Schutz von Informationen in Netzwerken und der Infrastruktur

g) Verhinderung von Beschädigungen von Wirtschaftsgütern u. Störung der Geschäftsaktivitäten beim Umgang mit Medien

h) Vermeidung von Verlust, Modifikation oder Missbrauch von ausgetauschten Informationen

i) Gewährleistung von Sicherheit von Electronic Commerce Services

j) Erkennung von unauthorisierten Aktivitäten

Access Control

Dieses Managementgebiet verweist auf die Bedeutung von Kontroll- und Überwachungsmaßnahmen für den Zugriff auf Informationen und Systemen zum Schutz vor unberechtigtem Missbrauch durch interne Mitarbeiter oder externe Angreifer. Die Maßnahmenziele fokussieren hier auf die Geschäftsanforderungen an Zugangs- und Zugriffskontrolle, das Benutzerzugriffsmanagement, die Verantwortung der Benutzer, der Netzwerkzugriffskontrolle, die Kontrolle des Betriebssystemszugriffs, die Zugriffskontrolle für Anwendungen, die Überwachung von Systemzugriffen und -nutzung sowie auf Sicherheitsaspekte bei Mobile Computing und Telearbeit.

Information systems acquisition, development & maintance

Vor der Entwicklung von informationsverarbeitenden Systemen müssen Sicherheitsforderungen identifiziert und vereinbart werden. Bei der Wartung von Systemen müssen diese Forderungen berücksichtigt werden. Hierzu sind

a) Sicherheitsanforderungen an Systeme bereits während der Entwicklung zu berücksichtigen,

b) der Verlust, die Änderung oder der Missbrauch von Benutzerdaten in Anwendungssystemen zu verhindern,

c) kryptographische Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität zu ergreifen,

d) der Schutz von Systemdateien sicher zu stellen,

e) Sicherheit bei Entwicklungs- und Supportprozessen zu integrieren, sowie

f) ein Technical Vulnerability Management zu etablieren.

Information security incident management

Information Security Incident Management wurde mit dem Release 2005 als einziges neues Managementgebiet mit in den Standard aufgenommen und somit der Wichtigkeit und Bedeutung des Themas explizit Rechnung getragen. Das Information Security Incident Management soll geeignete Prozesse zur Meldung, Behebung, Weiterverfolgung von Sicherheitsvorfällen sowie zur Sicherung von Beweismaterial beinhalten.

Business Continuity Management

Es sind präventive und reaktive Maßnahmen gegen Unterbrechungen der Geschäftsaktivitäten zu treffen und kritische Geschäftsprozesse vor den Auswirkungen von Ausfällen und Katastrophen zu schützen.

Compliance

Dieses Managementgebiet widmet sich der Einhaltung gesetzlicher Verpflichtungen, der Überprüfung der Sicherheitspolitik und Einhaltung technischer Normen, sowie Überlegungen zum Systemaudit. Die hier getroffenen Empfehlungen dienen

- der Vermeidung von Verletzungen jeglicher Gesetze des Straf- oder Zivilrechts, gesetzlicher, behördlicher oder vertraglicher Verpflichtungen an die Informationssicherheit,
- der Sicherstellung der Erfüllung unternehmenseigener Sicherheitspolicies und –standards, und
- der Maximierung der Effektivität und Minimierung der Störungen beim System-Auditprozess.

3.2 BS 7799-2:2002

3.2.1 Einführung

Während ISO 17799 die Managementgebiete, Maßnahmenziele und Maßnahmen zum Management von Informationssicherheit benennt, beschäftigt sich BS 7799-2:2002 „Information Security Management System – Specification with guidance for use" mit der Fragestellung des zugrundeliegenden Managementsystems selbst und liefert ein Modell zum Aufsetzen und Managen eines effizienten ISMS. BS 7799-2 beschreibt hierzu die Prozesse zur Implementierung, Überwachung, Prüfung, Instandhaltung und Verbesserung eines ISMS, die in den vier zentralen Themenkomplexen

- Information Security Management System (Kapitel 4)
- Verantwortung des Managements (Kapitel 5)
- Management Review des ISMS (Kapitel 6)

- ISMS Verbesserungen (Kapitel 7)

erläutert werden. Des Weiteren umfasst der Standard vier Anhänge:

- A: Kontrollziele und Maßnahmen
- B: Anleitung zur Benutzung des Standards
- C: Vergleich mit ISO 9001 und ISO 14001
- D: Vergleich mit BS 7799-2:1999

Schwerpunkt bei der Überarbeitung von BS 7799-2:1999 zur 2002-Edition war die Harmonisierung des Standards mit anderen Management-Standards. So wurde beispielsweise die Gliederung analog zu ISO 9000 (Quality Management Systems, QMS) und ISO 14000 (Environmental Management Systems, EMS) strukturiert und das in diesen Standards referenzierte Plan-Do-Check-Act (PDCA) Model übernommen.

Zur Vereinheitlichung des Sprachgebrauchs orientiert sich BS 7779-2 bei der Definition der Begriffe des Risk Managements an ISO Guide 73 (Risk management - Vocabulary - Guidelines for use in standards). Ebenfalls in die 2002-Edition Eingang gefunden haben die „OECD Guidelines for the Security of Information Systems and Networks“ (2002), die neun (sehr abstrakt gehaltene) Leitsätze zu den folgenden Themengebieten benennt:

- Awareness
- Responsibility
- Response
- Ethics
- Democracy
- Risk assessment
- Security design and Implementation
- Security management und
- Reassessment.

Durch die Anwendung von BS7799-2:2002 demonstrieren Unternehmen, dass sie auch diese Richtlinien beachten.

3.2.2 Information Security Management System – Plan-Do-Check-Act

Das PDCA-Modell, als Teil des Management-System Ansatzes zur Entwicklung, Umsetzung und kontinuierlichen Verbesserung des ISMS, stellt wohl die fundamentalste Änderung in der überarbeiteten Fassung von BS 7799-2 dar.

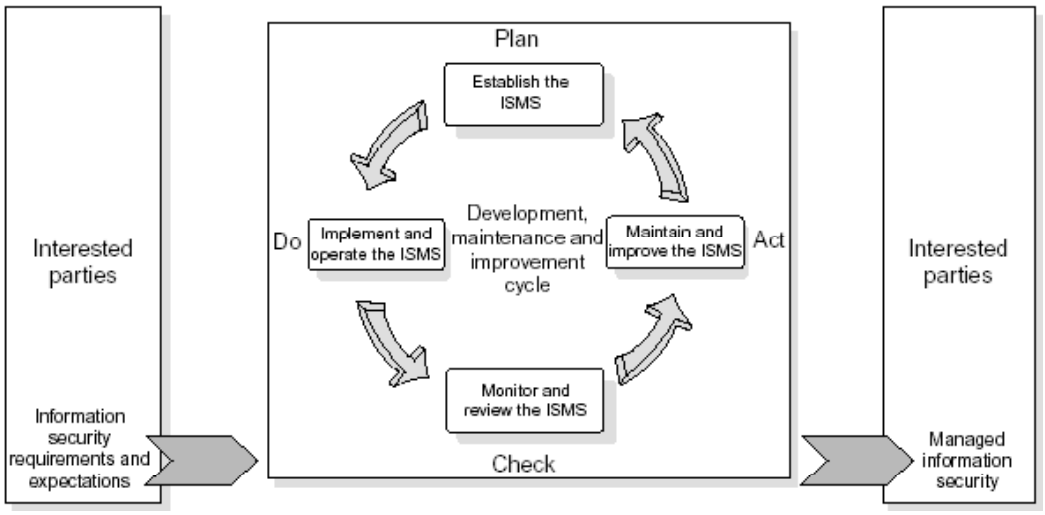

Abbildung 3: PDCA-Modell

Plan

Schwerpunkte der ISMS-Planungsphase bilden die Etablierung der Sicherheitspolitik, die Bestimmung der strategischen Sicherheitsziele sowie die Einführung von Prozessen und Abläufen, die für das Risikomanagement relevant sind.

Hierzu ist erforderlich,

- den ISMS-Geltungsbereich und dessen Umfang festzulegen (ISMS-Scope),
- eine ISMS Policy zu erstellen, aus der die Geschäftstätigkeit des Unternehmens, die Organisationsstruktur, Standorte, Wirtschaftsgüter, Technologie, usw. hervorgehen, sowie
- einen systematischen Ansatz zur Risikoabschätzung zu definieren, dessen Vorgehensmodell der Geschäftstätigkeit des Unternehmens angepasst ist und Politik und Ziele für das ISMS enthält, um die Risiken auf ein akzeptables Niveau zu senken, sowie Kriterien für die Akzeptanz von Risiken benennt.

Dem Risk Assessment kommt innerhalb von BS 7799-2 eine zentrale und entscheidende Bedeutung zu. Das ganze Information Security Management System basiert letztlich auf der Anwendung geeigneter Risk Management Methoden, die der Identifizierung von Bedrohungen und Schwachstellen, der Auswahl angemessener Maßnahmen und somit der Reduzierung der Gefährdungen auf ein akzeptables Restrisiko dienen. Welche Risk Management Methoden angewendet werden sollen, schreibt der Standard nicht vor, sondern verweist hier auf andere Dokumente, wie beispielsweise ISO TR 13335 Teil 3 oder BSI-DISC Guide PD 3002.

BS 7799 nennt allerdings sechs Prozessschritte, die im Rahmen des Risk Management durchzuführen sind:

1. Identifikation der Risiken

   In diesem Schritt sind die zu betrachtenden (Unternehmens-) Werte innerhalb des ISMS-Scope sowie deren Eigentümer (Owner) zu identifizieren. Im weiteren Verlauf sind dann die Bedrohungen festzulegen, denen die Werte ausgesetzt sind, die daraus entstehenden Schwachstellen aufzuzeigen, sowie die Auswirkungen bei Verlust von Vertraulichkeit, Integrität und Verfügbarkeit dieser Werte zu identifizieren.

2. Bewertung der Risiken

   Im zweiten Schritt werden Schadenshöhen, Eintrittswahrscheinlichkeiten, Risikolevel, akzeptables/inakzeptables Risiko für diese Werte festgelegt.

3. Identifikation und Bewertung der Möglichkeiten, mit den Risiken umzugehen

   In einem dritten Schritt werden Aktionen zum Umgang mit diesen Risiken bestimmt. Dies kann Maßnahmen zur Risikoreduktion, -vermeidung, -akzeptanz oder zum Risikotransfer beinhalten.

4. Auswahl von Maßnahmenzielen und Maßnahmen

   Zur Behandlung der Risiken können Maßnahmenziele und Maßnahmen aus Anhang A von BS 7799-2 herangezogen werden. Diese Maßnahmenziele und Maßnahmen sind dabei aus ISO 17799 entnommen. Auch hier erfolgt ein Hinweis, dass die in Anhang A aufgeführten „Controls“ unter Umständen nicht ausreichend sein können und zusätzliche Maßnahmen ergriffen werden müssen, so wie sie beispielsweise im Grundschutzhandbuch (GSHB) des Bundesamts für Sicherheit in der Informationstechnik oder in ISO TR 13335 Teil 4 aufgeführt sind.

5. Erstellen eines Eignungsberichts

   Die Maßnahmenziele und Maßnahmen, sowie die Gründe für deren Auswahl oder deren Ausschluss muss in einem sogenannten „Statement of Applicability“ (SoA) dokumentiert werden.

6. Zustimmung des Managements

   Im letzten Schritt muss das Management seine Zustimmung zu den identifizierten (Rest-) Risiken sowie die Autorisierung zur Umsetzung und zum Betrieb des ISMS geben.

Do

Ziel dieser Phase ist die Umsetzung der Planung; sie beinhaltet die Implementierung der Sicherheitspolitik, die Umsetzung von Kontrollmechanismen, die Integration von Prozessen und Abläufen zur Steuerung des ISMS und umfasst dabei folgende Tätigkeiten:

- formulieren eines Plans zur Behandlung der Risiken (Risk Treatment Plan)
- umsetzen des Risk Treatment Plan
- etablieren von Managementprozessen, festlegen von Verantwortlichkeiten und Prioritäten
- umsetzen der Maßnahmen aus der „Plan“-Phase
- umsetzen von Trainings- und Awareness-Maßnahmen
- operatives Controlling
- Controlling der Ressourcen
- schnelles Erkennen von Sicherheitsvorfälle und Reagieren

Check

Die Check-Phase dient der Bewertung und ggf. Messung der Prozessperformance gegenüber der Sicherheitspolitik, den Zielen und gesammelten praktischen Erfahrung. Sie umfasst:

- die Durchführung von Monitorprozessen zur Erkennung von Prozessfehlern, Sicherheitslücken und Sicherheitsverletzungen
- ein regelmäßiges Review der Wirksamkeit des ISMS
- ein Regelmäßiges Review der akzeptierten/restlichen Risiken
- die Durchführung interner ISMS Audits zu festen Terminen
- ein regelmäßiges (z. B. jährliches) Management-Review des ISMS
- die Dokumentation von Aktivitäten und Vorfällen, die eine Auswirkung auf die Wirksamkeit des ISMS haben können

Act

Die Act-Phase dient der kontinuierlichen Verbesserung des ISMS und beinhaltet die Ergreifung von Korrektur- und vorbeugenden Maßnahmen basierend auf den Ergebnissen des Management-Reviews. Hierzu sind:

- die identifizierten Verbesserungen des ISMS umzusetzen
- geeignete korrigierende und präventive Maßnahmen zu ergreifen
- die Ergebnisse und notwendigen Schritte mit allen beteiligten Parteien abzustimmen und an diese zu kommunizieren
- die Verbesserungen hinsichtlich der erwarteten Ziele zu überprüfen

3.2.3 Verantwortung des Managements

Der Verantwortung des Managements für Etablierung, Implementierung, Betrieb, sowie für Monitoring, Review und die Verbesserung des ISMS wird ein hoher Stellenwert beigemessen. Die Verantwortung des Managements erstreckt sich auf die drei Bereiche:

- Management Commitments
- Ressourcenmanagement
- Schulung, Sensibilisierung und Kompetenzen

Im Rahmen des Management Commitments hat das Management:

- die Verantwortung, dass die Information Security Policy eingeführt wird,
- zu gewährleisten, dass Ziele und Pläne definiert werden,
- dafür Sorge zu tragen, dass die notwendigen Rollen und Verantwortlichkeiten etabliert werden,
- die Bedeutung von Informationssicherheit für das Unternehmen an alle Beteiligte zu kommunizieren,
- hinreichend Ressourcen für die Entwicklung, Umsetzung, den Betrieb und die Wartung des ISMS bereitzustellen,
- Entscheidungen über tragbare Risiken zu treffen, und
- den Review des ISMS zu leiten.

Im Rahmen des Ressourcenmanagement ist durch das Management Vorsorge zu treffen, dass:

- ausreichend Ressourcen für die Etablierung, Implementierung, den Betrieb und die Erhaltung des ISMS zur Verfügung gestellt werden,
- Prozesse und Verfahren des ISMS den Geschäftsanforderungen entsprechen,
- Gesetze und vertragliche Verpflichtungen eingehalten werden,
- eine angemessene Sicherheit durch die korrekte Anwendung der implementierten Maßnahmen aufrecht erhalten wird,
- falls notwendig, Überprüfungen erfolgen und entsprechend der Ergebnisse der Überprüfungen reagiert wird, und
- falls notwendig, die Effektivität des ISMS verbessert wird.

Im Rahmen von Schulung, Sensibilisierung und Kompetenzen soll sichergestellt werden, dass:

- das für das ISMS verantwortliche Personal die entsprechenden fachlichen Kompetenzen besitzt,
- diese Kompetenzen durch entsprechende Schulungen oder die Einstellung von Personal aufgebaut werden,
- die Effektivität der Schulungen überprüft wird,
- eine Aufzeichnung über Schulungen, Fähigkeiten, Erfahrungen und Qualifikationen erfolgt.

3.2.4 Management Review des ISMS

Es muss ein regelmäßiges Review erfolgen, um die Tauglichkeit, Angemessenheit und Effizienz des ISMS sicherzustellen. Als Basis für dieses Review dienen:

- Resultate der ISMS Audits und Reviews
- Feedback, Status der Maßnahmen
- Bedrohungen oder Schwachstellen, die bisher nicht ausreichend behandelt wurden
- Internes ISMS Audit
- Überprüfung der Konformität zum BS 7799-2 sowie zur aktuellen Gesetzgebung oder anderen Regulierungsvorgaben
- Konformität zu Anforderungen an die Informationssicherheit
- Stand der Umsetzung und Wartung
- Wirksamkeit der Maßnahmen.

Das Ergebnis des Management-Reviews fließt ein in:

- Verbesserungsvorschläge hinsichtlich der Effizienz des ISMS,
- Änderungen an bestehenden Abläufen,
- die Bereitstellung notwendiger Ressourcen.

3.2.5 ISMS Verbesserungen

Die kontinuierliche Verbesserung des ISMS ist ein wesentliches Qualitätsmerkmal von BS 7799 und soll durch die konsequente Umsetzung der Security Policy, der Maßnahmen,

der Resultate aus Audits, der Analyse der Monitoring-Ereignisse sowie der Ergebnisse aus dem Management Review erreicht werden.

Hierbei wird unterschieden zwischen

- korrigierenden Maßnahmen, die zur Beseitigung von Schwachstellen im Zusammenhang mit der Umsetzung und dem Betrieb des ISMS auftreten, um ihr wiederholtes Auftreten zu vermeiden, sowie
- vorbeugenden Maßnahmen, um sich vor zukünftigen Schwachstellen zu schützen.

4 Einbindung in das Qualitätsmanagement

Primäres Ziel von BS 7799 ist die Etablierung eines ***dokumentierten*** Information Security Management Systems, in dem alle relevanten Strukturen, Prozesse und Abläufe für Planung, Steuerung und Kontrolle des ISMS beschrieben und schriftlich fixiert sind.

Benötigte Dokumente

Der Standard nennt eine Reihe von Dokumenten, deren Erstellung im Rahmen der Etablierung des ISMS notwendig ist:

- Security Policy
- ISMS-Scope
- Risk Assessment Report
- Risk Treatment Plan
- Dokumentierte Prozesse zur Sicherstellung einer effektiven Planung, Steuerung und Kontrolle der Information Security Prozesse
- Aufzeichnungen
- Statement of Applicability.

Zu Art, Umfang, Ausgestaltung und Form der Dokumentation macht BS 7799 keine Vorschriften. Diese Merkmale orientieren sich in der Praxis einzig an den Gegebenheiten und Notwendigkeiten der Sicherheitsanforderungen für den betrachteten Anwendungsbereich.

Dokumenten-Management (Lenkung von Dokumenten nach ISO 9001)

Allerdings gibt der Standard Hinweise zum Umgang mit dieser Dokumentation, welche geschützt und kontrolliert werden muss. Es muss ein dokumentierter Prozess etabliert werden zur Festlegung der folgenden (Dokumenten-) Managementtätigkeiten:

- Überprüfung der Dokumente bezüglich ihrer Angemessenheit vor Herausgabe
- Überprüfung und Aktualisierung der Dokumente und deren erneute Genehmigung
- Sicherstellung einer Versions- und Änderungskontrolle
- Bereitstellung der aktuellen Dokumente
- Sicherstellung der Lesbarkeit und Identifizierbarkeit der Dokumente
- Kennzeichnung externer Dokumente
- Kontrolle der Verteilung der Dokumente
- Entfernung obsoleter Dokumente

- Identifikation obsoleter Dokumente, falls sie aus irgendeinem Grund aufbewahrt werden.

Umgang mit Aufzeichnungen (Lenkung von Aufzeichnungen nach ISO 9001)

Dem ordnungsgemäßen Umgang mit Aufzeichnungen wird ein besonderer Abschnitt gewidmet. Die Erstellung und Pflege von Aufzeichnungen dient dem Nachweis der Konformität an die Anforderungen an Informationssicherheit und dem wirkungsvollen Betrieb des ISMS. Die Aufzeichnungen müssen einer Kontrolle unterworfen sein, alle relevanten gesetzlichen Anforderungen sind hierbei zu beachten. Aufzeichnungen müssen lesbar, leicht identifizierbar und wiederauffindbar sein. Die Prozesse zum Umgang mit Aufzeichnungen müssen dokumentiert sein und die Anforderungen an die Kennzeichnung, den Schutz, die Wiederherstellung, die Aufbewahrungsfristen und die Ablage von Aufzeichnungen festlegen.

Die Sicherstellung der Umsetzung der Anforderungen an das Dokumenten-Management sowie den Umgang mit Aufzeichnungen, die Gewährleistung der Aktualität und Konsistenz der Dokumente stellt im operativen Betrieb des ISMS eine große Herausforderung dar. Von Vorteil ist sicherlich, wenn bereits ausgereifte und etablierte Prozesse zum Umgang mit Dokumenten vorhanden sind. BS 7799-2:2002 orientiert sich mit seinen Anforderungen an das Dokumenten-Management klar an ISO 9000-2000. Unternehmen, die bereits ein ISO 9000 entsprechendes Qualitätsmanagementsystem aufgebaut haben, erfüllen somit bereits wesentliche Voraussetzungen für die Etablierung eines ISMS. Des Weiteren ergibt sich durch diese Synergien zwischen ISO 9000:2000 und BS 7799-2:2002 die Möglichkeit, die Zertifizierung beider Managementsysteme zu kombinieren und so erhebliche zeitliche und monetäre Ressourceneinsparungen zu erzielen.

5 Prüfungs- und Zertifizierungsprozess

Das Zertifizierungsschema zur Erlangung einer BS 7799-2:2002 Zertifizierung ist streng reglementiert. Die Zertifizierung darf nur durch speziell akkreditierte, sogenannte „Certification bodies“ erfolgen. Die Akkreditierung dieser „Certification bodies“ obliegt den nationalen Akkreditierungsstellen, in Deutschland ist dies die Trägergemeinschaft für Akkreditierung GmbH (TGA) in Frankfurt. Die nationalen Akkreditierungsstellen treffen gegenseitige Anerkennungsvereinbarungen, so dass die in einem Land ausgestellten Zertifikate auch in anderen Ländern Anerkennung finden. Die Akkreditierung der „Certification bodies“ erfolgt dabei gemäß der Richtlinie EA 7/03 der „European co-operation for Accreditation“. Zurzeit gibt es in Deutschland drei Unternehmen, die eine entsprechende Akkreditierung zur Durchführung von Zertifizierungen nach BS 7799-2 erhalten haben.

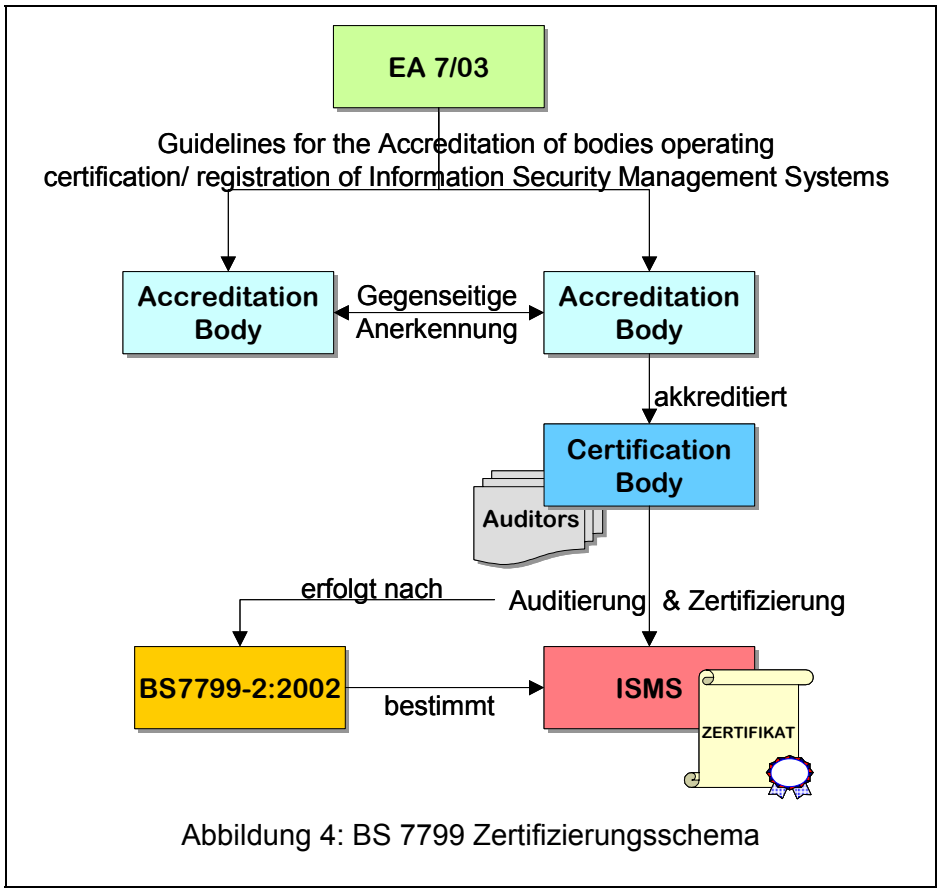

Abbildung 4: BS 7799 Zertifizierungsschema

Die eigentliche Zertifizierung erfolgt dann prinzipiell nach folgendem Ablaufschema:

- Das zu zertifizierende Unternehmen beauftragt ein akkreditiertes Unternehmen mit der Überprüfung des Information Security Management Systems.
- Das Audit-Team wird zusammengestellt.
- In einer ersten Phase erfolgt die Überprüfung und Beurteilung der Dokumentation.
- In einer zweiten Phase werden Vor-Ort-Audits durchgeführt.
- Es wird ein Audit-Bericht erstellt.
- Sofern der Audit-Bericht positiv ausfällt, wird das Zertifikat ausgestellt.

Das Zertifikat besitzt eine Gültigkeit von 3 Jahren, anschließend ist eine Wiederholungszertifizierung erforderlich, wodurch die Gültigkeit um weitere 3 Jahre verlängert wird.

6 Bewertung und Ausblick

Nach einer langen und steinigen Phase hat sich BS 7799/ISO 17799 mittlerweile zu einem weltweit anerkannten Leitfaden zum Management von Informationssicherheit entwickelt. Die internationale Ausrichtung sowie die große Flexibilität in der Handhabung dieser Standards machen die Anwendung für Unternehmen aller Größe und Branchen gleichermaßen attraktiv. Insbesondere für international ausgerichtete Unternehmen mit Niederlassungen in verschiedenen Ländern bietet ISO 17799 ein einheitliches Rahmenwerk zur strukturierten Organisation einer unternehmensweiten Informationssicherheit. Darüber hinaus erlaubt

BS 7799-2 die Zertifizierung des etablierten ISMS und damit verbunden die Möglichkeit ein messbares und effizientes Sicherheitsniveau zu erreichen.

Berücksichtigt werden sollte dabei aber, dass BS 7799/ISO 17799 ein sehr stark am Risk-Management orientierter Ansatz ist. Im Gegensatz beispielsweise zum Grundschutzhandbuch, das im Prinzip die Risikoanalyse für die Anwender bereits durchgeführt und entsprechend umzusetzenden Maßnahmen definiert hat, obliegt die Durchführung dieser Risikoanalyse bei BS 7799/ISO 17799 gänzlich dem Anwender. Letztendlich wird durch die Qualität des Risiko-Managements die Qualität des gesamten Information Security Management Systems bestimmt. Die Durchführung und Anwendung einer detaillierten Risikoanalyse erfordert dabei neben sehr viel Erfahrung auch ein Großmaß an Ressourcen, beispielsweise zur:

- Erfassung aller relevanten Unternehmenswerte,
- Abstimmung von Begrifflichkeiten,
- Einigung auf ein einheitliches und abgestimmtes Klassifikationsschema,
- Identifizierung von Schwachstellen und Bedrohungen, sowie zur
- Bewertung von Auswirkungen und Eintrittswahrscheinlichkeiten.

Erfahrungsgemäß bergen diese Punkte immer wieder ausreichend Potenzial zur kontroversen Diskussion.

Die Entwicklung von BS 7799/ISO 17799 geht derweil weiter. Zurzeit wird die BS7799-2 in einen ISO Standard überführt. Die Veröffentlichung des Standards, der bei ISO mit der Nummer ISO/IEC 27001 geführt wird, ist für Ende 2005 geplant.

Daneben befindet sich momentan auch noch mit ISO/IEC 27004 „Information security management metrics and measurement“ ein Standard in der Entwicklung, der das Thema „Messbarkeit von Informationssicherheit“ adressiert.

Des Weiteren bereitet das Informationssicherheitskomitee ISO/IEC JTC1 SC27 noch weitere Themen vor, bspw. ISMS Risikomanagement und Implementierungshilfen für ISMS, doch hierfür wurden bislang noch keine Nummern vergeben.

Über die Aufnahme von ISO/IEC 17799:2005 in die 27000 Serie soll wohl im Frühjahr 2007 entschieden werden, dann könnte ISO/IEC 17799:2005 als ISO/IEC 27002 weitergeführt werden.

Die weitere Entwicklung von ISO 17799 und BS 7799-2 bleibt vielversprechend. Die Überführung von BS 7799-2 in einen ISO Standard, die Harmonisierung der Standards in einer einheitlichen ISO 27000 Serie, die starke internationale Ausrichtung und die flexible Anwendbarkeit machen diese Standards für viele Unternehmen interessant, wie auch die zunehmende Anzahl ausgestellter Zertifikate zeigt.

Aufgrund der angestrebten Abwärtskompatibilität revidierter Fassungen mit älteren Versionen scheint hier auch die Sicherung bereits getätigter und geplanter Investitionen gewährleistet zu sein - ein weiterer positiver Aspekt, der durchaus entsprechend gewürdigt werden sollte.

7 Literatur

BS 7799-2:2002, Information security management — Part 2: Specification for information security management systems

ISO/IEC TR 13335-1:1996 , Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security, http://www.iso.ch

ISO/IEC TR 13335-2:1997, Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security, http://www.iso.ch

ISO/IEC TR 13335-3:1998, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security, http://www.iso.ch

ISO/IEC TR 13335-4:2000, Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards, http://www.iso.ch

ISO/IEC TR 13335-5:2001, Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security, http://www.iso.ch

EA 7/03, Guidelines for the Accreditation of bodies operating certification/ registration of Information Security Management Systems, http://www.european-accreditation.org/documents.html

ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems, http://www.iso.ch

ISO/IEC 17799:2005, Information technology -- Code of practice for information security management, http://www.iso.ch

ISO 9000:2000, Quality management systems -- Fundamentals and vocabulary, http://www.iso.ch

ISO 9000-3:1997, Quality management and quality assurance standards -- Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software, http://www.iso.ch

ISO 9000-4:1993, Quality management and quality assurance standards -- Part 4: Guide to dependability programme management, http://www.iso.ch

ISO 9001:2000, Quality management systems – Requirements, http://www.iso.ch

ISO 9004:2000, Quality management systems -- Guidelines for performance improvements, http://www.iso.ch

ISO 14001:1996, Environmental management systems — Specification with guidance for use, http://www.iso.ch

IT-Grundschutzhandbuch 2004, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/gshb/

Neundorf, Dörte; Petersen, Holger: Information Security Management. Datenschutz und Datensicherheit (DuD), 4/2003, S. 193-199.

OECD, OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. http://www.oecd.org

Anhang

Anhang A) Struktur Version 2000 und Version 2005

ISO 17799:2000	ISO 17799:2005
Security Policy	Security Policy
Organizational Security	Organization of information security
Asset Classification & Control	Asset Management
Personnel Security	Human Resources Security
Physical & Environmental Security	Physical & Environmental Security
Communications & Operations Manamgement	Communications & Operations Mgmt
Access Control	Access Control
Systems Development & Maintenance	Information systems acquisition, development & maintance
	Information security incident management
Business Continuity	Business Continuity
Compliance	Compliance

Anhang B) Verteilung Managementgebiet, Maßnahmenziele, Maßnahmen

Managementgebiet	Maßnahmenziele	Maßnahme
Security Policy	1	2
Organization of information security	2	11
Asset Management	2	5
Human Resources Security	3	9
Physical & Environmental Security	2	13
Communications & Operations Mgmt	10	32
Access Control	7	25
Information systems acquisition, development & maintance	6	16
Information security incident management	2	5
Business Continuity	1	5
Compliance	3	10