DuD
Datenschutz und Datensicherheit

Neufassung IS 17799:2005

Oliver Weissmann

Im Rahmen der Überarbeitung durch die ISO wurde der 17799-Standard in vielen Punkten internationalisiert und korrigiert. Der Standard wurde dabei um einige Altlasten erleichtert und um Elemente ergänzt, die der aktuellen Situation von Organisationen im Hinblick auf die geforderte Sicherheit Genüge tun. Im vorliegenden Beitrag werden die Erweiterungen und Änderungen des Standards im Überblick beschrieben, so z. B. die Elemente und Anforderungen an eine Risikobewertung, die Ergänzungen bei den Sicherheitsmaßnahmen und die neue Struktur der „Controls". Zudem wird die derzeitige Situation und Zielsetzung innerhalb der ISO SC 27 / WG 1 beschrieben, besonders im Hinblick auf die Integration in ein von der ISO betreutes ISMS (Information Security Management) und einen Standard zur Messbarkeit.
Diese Struktur spiegelt sich bereits bei anderen Managementstandards wie z.B. IS 9000 (QM) und IS 14000 (Umwelt) wieder und wird innerhalb der ISO intensiv diskutiert.

Dr. Oliver Weissmann

Senior Security Consultant bei der atsec information security GmbH.
Tätigkeitsschwerpunkte: Security Management, Sicherheitsstandards und Sicherheitskonzepte. Derzeit einer der beiden Editoren für die Überarbeitung von IS 17799
E-Mail: o.weissmann@atsec.com

Einleitung

Der Erfolg von Management-Systemen wie ISO 9000 oder ISO 14000 vollzog sich auch im Umfeld der Informationssicherheit, d. h. dem organisationsweiten Schutz von Information ungeachtet ihrer Darstellungs- und Speicherform. Zwar gab es in Deutschland zwar bereits Standards wie das Grundschutzhandbuch (Bundesamt für Sicherheit in der Informationstechnik (BSI)) oder auf internationaler Ebene den Standard of Good Practice (Information Security Forum, ISF), doch erreichten beide nicht im Geringsten die Verbreitung des Britischen Standards BS 7799 (British Standards Institute, BSI). Dieser war 1999 schon international anerkannt, und eine Vielzahl von Ländern hatte nationale Versionen des Standards im Einsatz, wie z. B. ANZ 4444, gültig in Australien und Neuseeland. Der erste Versuch, den Teil eines „Code of Practice for Information Security Management" als internationalen Standard zu etablieren, scheiterte an der Ablehnung der Experten. Erst im zweiten Anlauf wurde der Teil 1 des britischen Standards BS 7799 im Rahmen eines beschleunigten Verfahrens als ISO Standard IS 17799:1999 etabliert.[1]

Aufgrund der kontroversen Diskussionen wurde beschlossen, den Standard sofort in Revision zu nehmen. So begann zeitgleich mit der Etablierung des Standards als ISO Standard IS 17799:1999 die Überarbeitung. Zu diesem Zeitpunkt wurde im Rahmen der ISO-Arbeit nur Teil 1 des britischen Standards BS 7799 betrachtet. Dieser Teil hat die besten Chancen, 2005 endgültig verabschiedet und durch die ISO veröffentlicht zu werden: Er befindet sich derzeit in der letzten Runde des Standardisierungsprozesses, der im April 2005 abgeschlossen werden soll.

[1] Zur Entstehungsgeschichte und Struktur des BS 7799 siehe Völker, DuD 2/2004, S. 102-108.

1 Ziele

Die Überarbeitung des Standards diente verschiedenen Zielen. Für einen internationalen Standard war es zunächst notwendig, eine Darstellung und Beschreibung der Schutzmaßnahmen (engl. „Controls") zu erreichen, die allgemein verständlich ist. Sprachliche Besonderheiten, Beschreibungsarten und andere nationale Eigenheiten sollten aus dem Standard entfernt werden, um so die allgemeine Lesbarkeit zu verbessern.

Ein weiteres Ziel der Überarbeitung war die Aktualisierung. So merkte man es dem Standard an, dass er seine Wurzeln in einer Zeit der mainframe-basierten Rechenzentren hatte. Heutige Sicherheitsrisiken, die durch die allgegenwärtige Verfügbarkeit von Rechenleistung in Form von „Personal Devices" entstehen, sowie die Dominanz paketvermittelnder Netze und der damit verbundenen Unvorhersagbarkeit des Kommunikationsflusses wurden durch den Standard nur wenig beachtet.

Die allgemeine Abgrenzung zwischen Managementaufgaben und technischen Anforderungen wurde ebenfalls intensiv überarbeitet. Die Zielgruppe ist nun der Sicherheitsmanager und keinesfalls mehr der technische Experte. Damit ergibt sich eine Abgrenzung gegenüber anderen ISO-Standards, die klarer ist und weniger Überschneidungen beinhaltet.

Daraus begründen sich auch die Aktivitäten der ISO, zusätzlich zum „Code of Practice for Information Security Management" einen Standard zu einem „Information Security Management System", angelehnt an den aktuellen britischen Standard BS 7799-2:2002, und einen Standard zur Messbarkeit von Security Management Systemen zu etablieren.

Abbildung 1 beschreibt ein mögliches Zusammenspiel der Standards, die derzeit in der ISO diskutiert werden und auf dem Markt verfügbar sind. Dabei wird deutlich, dass ein Zusammenspiel von Managementstandards und Systemen bis auf die technische Ebene möglich wird. Dabei soll an

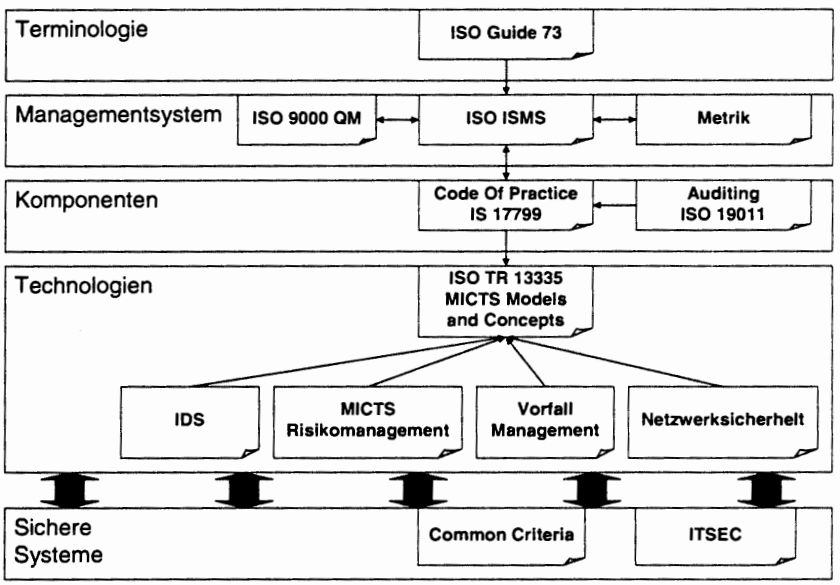

Abbildung 1: Zusammenhang der Komponenten

dieser Stelle betont werden, dass dies nur einen möglichen Weg beschreibt. Im Rahmen der Arbeitsgruppen werden derzeit noch viele weitere Optionen diskutiert.

Schlussendlich mussten auch noch die Anwender, die bereits eine Zertifizierung ihres ISMS nach BS 7799-2:2002 unter Verwendung von IS 17799 erworben hatten, eine Möglichkeit haben, diese Investition zu schützen und mit vernünftigem Aufwand auf den neuen Standard migrieren zu können.

Doch wie unterscheidet sich jetzt die neue Fassung des IS 17799:2005 von der Fassung des IS 17799:1999?

2 Änderungen

Im Rahmen der fast fünfjährigen Bearbeitung des Standards wurden mehr als 4.500 Kommentare aus nahezu allen an dem ISO-Prozess beteiligten Ländern eingearbeitet, um dem Wunsch nach einer Anwendbarkeit in allen Ländern und Industrien nachzukommen. Daraus resultiert jedoch auch, dass eigentlich alle Maßnahmen des „Code of Practice" mehr oder minder betroffen sind. Die Tabelle am Ende des Beitrags zeigt die Änderungen gegenüber der früheren Fassung. Im Folgenden werden einige Besonderheiten und ausgewählte Beispiele der vorgenommenen Änderungen dargestellt, an denen sich die Entwicklung des Standards gut nachvollziehen lässt.

2.1 Struktur

Die Struktur des Standards hat sich, was die Kapitelüberschriften angeht, wenig geändert. Es wurde ein eigenes Kapitel zur Risikobetrachtung eingefügt, da diese die Grundlage für ein sinnvolles ISMS darstellt. Der Standard selber hat jetzt die in Abb. 2 dargestellte Struktur – ISO Präambeln, Definitionen und Ähnliches sind hier nicht aufgeführt.

Neu eingeführt wurde das Kapitel über Risikobewertung, in dem allerdings nicht eine Methodik für eine Risikobewertung beschrieben wird. Dafür gibt es, wie bereits beschrieben, andere Anwendungen. Das Kapitel beschreibt vielmehr, welche Anforderungen an eine Risikobewertung, insbesondere im Hinblick auf ihre Nachvollziehbarkeit gestellt werden müssen. Gleiches gilt auch für die dann notwendige Behandlung und die Behandlungsmöglichkeiten solcher Risiken im Sinne von

- Reduktion des Risikos
- Vermeidung des Risikos
- Übertragung des Risikos
- Akzeptanz des Risikos

Dabei wird in dem Standard davon ausgegangen, dass nur bekannte Risiken akzeptiert werden können. Dies ist im Hinblick auf den ISO Guide 73 wesentlich, da es dort weitere Risikotypen gibt.

Darauf folgen die Klassen von Schutzmaßnahmen, von denen die meisten schon aus der Fassung von 1999 bekannt sind. Dabei ist besonders zu beachten, dass die Reihenfolge keine Priorisierung bedeutet und die Klassen mehr oder minder gleichberechtigt nebeneinander stehen. Neu sind dabei die drei in Abbildung 2 eingefärbten Klassen. Jede Klasse beginnt mit der Darstellung des Ziels der Klasse, die einer starken Überarbeitung unterzogen wurden.

Die Schutzmaßnahmen („Controls") selber unterliegen jetzt einer fixen Struktur die sich wie in Abbildung 3 darstellt:

- Das **Control Statement** beschreibt, nach Möglichkeit in einem Satz, das Ziel und die Idee einer Schutzmaßnahme.
- Die **Implementation Guidance** stellt dem Anwender des Standards dann zusätzliche Informationen bereit, die bei der tatsächlichen Umsetzung helfen sollen. Hier werden auch sehr viele Beispiele in Form von Aufzählungen angeboten. Diese sind jedoch nicht als Checklisten zu verstehen, sondern dienen der Unterstützung.
- Die Beschreibung einer Schutzmaßnahme wird dann von dem Abschnitt **Other Information** abgeschlossen. Hier ver-

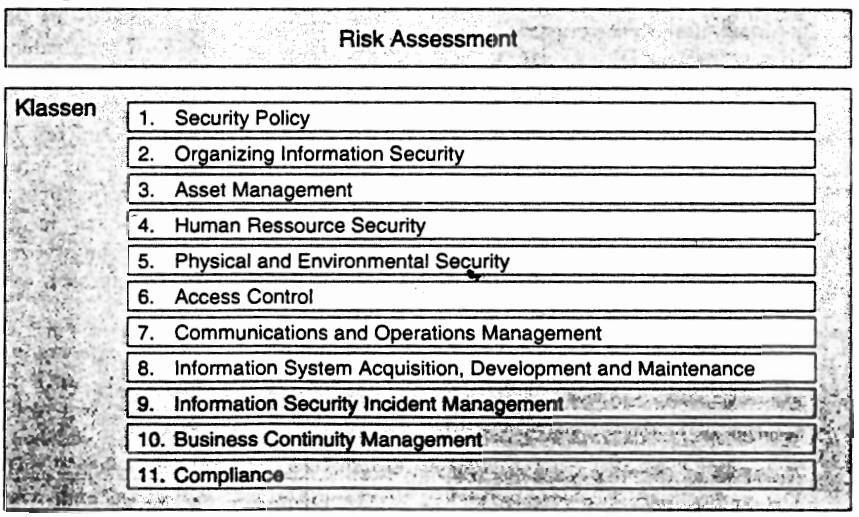

Abbildung 2: Struktur des Standards

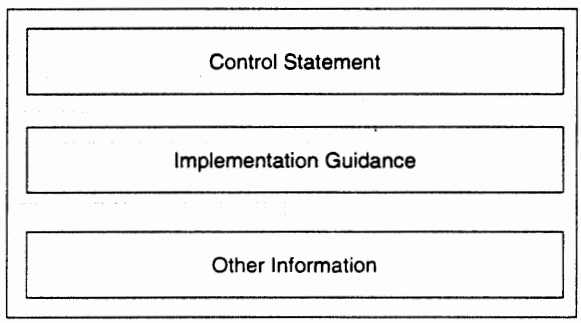

Abbildung 3: Struktur der Schutzmaßnahmen (Controls)

bergen sich zusätzliche Informationen, die in Betracht gezogen werden müssen.

Doch es hat sich nicht nur in der Struktur der Schutzmaßnahmen einiges geändert.

2.2 Risikobewertung

Der Standard beinhaltet, wie bereits erwähnt, einige klare Anforderungen an die Risikobewertung. Dabei verweist er auf die Technical Reports für das „Management of Information and Communication Technology Security (MICTS)" TR 13335. Die Referenzierung erfolgt jedoch nicht normativ, d. h. es dürfen auch andere Methoden zur Risikoermittlung eingesetzt werden. Grundsätzlich wird jedoch gefordert, dass die Bewertung transparent und nachvollziehbar ist.

Es werden auch die Methoden der Risikobehandlung angesprochen sowie eine Verbindung der Sicherheitsziele der Schutzmaßnahmen zu den Risiken hergestellt.

2.3 Maßnahmen

Auch wenn sich nicht alle Änderungen in den Maßnahmen beschreiben lassen, so werden hier einige Besonderheiten aufgeführt, die im Wesentlichen die Unterschiede zum vorigen Standard beschreiben.

First, Second and Third Parties

Wurden bisher im Standard eine Vielzahl verschiedener Begriffe für die unterschiedlichen Parteien verwendet, so wurden diese während der Überarbeitung zu den folgenden Bezeichnungen zusammengefasst:

- External Parties
  Alles, was nicht direkt zur Organisation gehört, z. B. Berater
- Third Parties
  Von den direkt Beteiligten unabhängige Partei, z. B. ISPs
- Customers
  Der Kunde bzw. die Organisationseinheit für die eine Dienstleistung erbracht wird.
- Employees
  Alle „Mitglieder" der Organisation

Diese Überarbeitung ist an den ISO Guide 2 angelehnt, um sicherzustellen, dass die verwendeten Begriffe sich auch in anderen Standards in gleicher Verwendung wiederfinden.

Human Resource Security

Dieses Control wurde jetzt an den tatsächlichen „Lebenszyklus" eines Mitarbeiters angepasst. Dieser beginnt nun beim Preemployment, also bei der Bewerbung des Mitarbeiters für eine bestimmte Position und endet mit dem Ausscheiden aus dieser Position. Es wird also der folgende Zyklus betrachtet:

- *Prior to employment* // Vor der Beschäftigung
  Diese Schutzmaßnahme beinhaltet die meisten der bereits bekannten Schutzmaßnahmen zu diesem Thema: Anforderungen an die Rollen und Verantwortungen, Verträge und die keineswegs unumstrittene Überprüfung des Mitarbeiters. Hier gilt, wie für jede Umsetzung des Standards, die Anforderung der lokalen Gesetzgebung, so dass der Mitarbeiter durch die geltenden Datenschutzbestimmungen geschützt ist.
- *During employment* // Während der Beschäftigung
  Die Schutzmaßnahme beschäftigt sich im Wesentlichen mit der Managementverantwortung, der Weiterbildung des Mitarbeiters und möglichen Disziplinarmaßnahmen. Ziel ist es, den Mitarbeiter in die Lage zu versetzen, ein Sicherheitsmanagement erfolgreich zu unterstützen und in seinen Tätigkeiten ausreichend sicher zu sein.
- *Termination and change of employment* // Änderung der Beschäftigung
  Diese Maßnahme beschreibt den Phaseout eines Mitarbeiters aus einer Position, wobei nicht unterschieden wird, ob er dabei das Unternehmen verlässt oder nur seine Position innerhalb des Unternehmens verändert. Beachtet werden im Standard die Punkte Abgabe der Verantwortlichkeiten, Rückgabe von Unternehmensgütern und Entfernen von Zutritts-, Zugriffs- und Zugangsberechtigungen.

Cryptographic Controls

Aufgrund der sehr technischen Beschreibung im bisherigen Standard und der damit verbundenen Umsetzungsprobleme wurde in dieser Maßnahme weitgehend die technische Beschreibung gestrichen. Die Differenzierung zwischen Message Authentication Codes (MAC), digitalen Signaturen und Anforderungen an spezielle Sicherheitsmaßnahmen erwies sich in der Umsetzung nicht immer als verträglich, da das Wissen darum in den meisten Organisationen nicht verfügbar war.

Der neue Standard fordert hier eine *Policy* // Leitlinie darüber, wo und mit welchem Sicherheitsziel kryptographische Maßnahmen eingesetzt werden sollen und wie die Verantwortlichkeiten dazu aussehen. Wird jedoch Kryptographie in einer Organisation eingesetzt, so wird auch eine Schlüsselverwaltung gefordert. Diese muss dann den Lebenszyklus der verwendeten Schlüssel verwalten. Eine weitere technische Detaillierung findet nicht mehr statt, da die Organisationen selten in der Lage sind, diese umzusetzen. Zudem existieren eine ausreichende Zahl von Standards, die ausschließlich Kryptographie, kryptographische Verfahren und Algorithmen zum Thema haben. Diese werden allerdings nicht referenziert.

Mobile Code

Eine weitere Neuerung stellt eine Schutzmaßnahme zu mobilem Code dar. Damit ist explizit nicht Java oder ActiveX oder anderer „downloadable" Code gemeint, der nur in Zusammenhang mit einer Benutzerinteraktion aktiv werden kann – wozu auch das Anwählen einer Website zählt. Hier geht es um Code wie er in Systemen vorkommt, auf denen sich der Code selbstständig bewegen kann. Solche Systeme sind z. B. Plattformen für mobile Agenten wie Grasshopper, aber auch Grids und .NET-basierte Plattformen können darunter fallen.

Vulnerability Management

Heute werden täglich Schwachstellen in Systemen gefunden – dabei wird die Zeit zwischen der Endeckung einer Schwachstelle und deren Ausnutzung kontinuierlich kürzer. Die überarbeitete Fassung des Standards trägt diesem Sachverhalt Rechnung

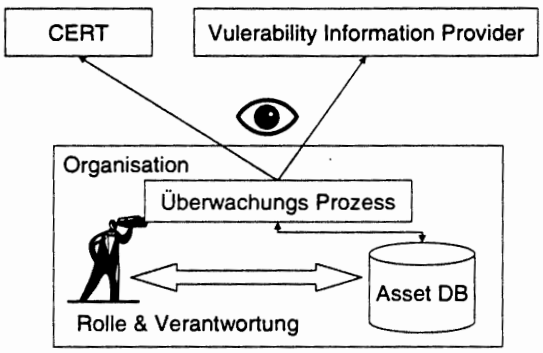

Abbildung 4: Schwachstellen-Überwachung

und definiert Anforderungen an den Umgang mit Schwachstellen. Damit soll sichergestellt werden, dass Schwachstellen den Betroffenen rechtzeitig bekannt werden und sehr zeitnah behandelt werden können.

Abbildung 4 beschreibt schematisch die Maßnahme. Dabei muss zunächst eine Verantwortung für den Prozess definiert werden. Dieser Prozess ermittelt dann für die in der Asset-Datenbank hinterlegten Assets die Schwachstellen, indem Informationsdienste abonniert bzw. beobachtet werden, die Informationen zu Schwachstellen bereitstellen (wie z.B. CERT Services).

Der Standard verlangt in diesem Kontext noch wesentlich mehr als in Abbildung 4 dargestellt, wobei unter anderem auch das Patchen mitbetrachtet wird.

Information Security Incident Management

Die Behandlung von Sicherheitsvorfällen hat ebenfalls in den Standard Einzug gehalten. Ziel ist es, eine korrekte und zeitnahe Reaktion auf und Meldung von Sicherheitsvorfällen, Schwächen und Ereignissen, als auch der sinnvolle Umgang mit diesen Ereignissen. Neben den Anforderungen an die Verantwortlichkeiten werden vor allem Anforderungen an die Sicherstellung von Evidenz gestellt. Somit soll eine Organisation dann auch in die Lage versetzt werden ggf. juristische Schritte durchzuführen. Dabei wird auf die Anwendbarkeit der Evidenz vor Gericht als auch auf das mögliche Gewicht der Evidenz in einem Streitfall Wert gelegt.

3 Fazit

In einem Umfeld, in dem Risikomanagement immer stärker thematisiert und durch gesetzliche Anforderungen wie z.B. Basel II, SOX oder Solvency II immer wichtiger wird, bietet ein international anerkannter „Code of Practice" eine gute Möglichkeit, um darzustellen, dass eine Organisation tatsächlich um ihre Sicherheit und damit auch um die Verminderung ihrer Risiken bemüht ist.

Der Standard hat sich erheblich weiterentwickelt und ist sicher im 21. Jahrhundert angekommen. Dabei hat er nicht an Flexibilität eingebüßt und ist auch für zukünftige Entwicklungen gewappnet. Das wird offensichtlich auch innerhalb der ISO so gesehen, denn es werden weitere Standards wie z. B. das längst überfällige ISO ISMS und ein Standard zur Messbarkeit/Metrik eines ISMS entwickelt. Was die globale Entwicklung angeht, hat IS 17799 längst das Erbe der ISO 9000 angetreten und ist in fast allen Ländern verfügbar. Gleiches gilt in Deutschland, wo der Standard bereits von einigen Industrien umgesetzt und auch gefordert wird.

Schon jetzt ist die Anwendung des IS 17799:2005 Code of Practice im Rahmen eines ISMS ein durchaus zu empfehlender Schritt, zumal die Verständlichkeit und die Aktualität des Standards einen erheblichen Vorteil gegenüber der Fassung von 1999 schafft.

Ist die Troika der ISO Standards bestehend aus ISO ISMS, ISO 17799:2005 und ISO Metrics zu 17799 erst einmal fertiggestellt, so steht für das Sicherheitsmanagement das gleiche, international verständliche und akzeptierte Instrumentarium zur Verfügung wie für das Qualitätsmanagement. Doch es gibt bereits heute Grund zur Zuversicht, da derzeit mehr als 1000 Unternehmen weltweit bereits nach BS 7799-2:2002, der Grundlage für den ISO ISMS Standard, zertifiziert wurden; die Zahl der Umsetzungen ohne Zertifizierung liegt noch deutlich höher.

Anhang A) Tabelle der Änderungen der Überschriften.

Neu	Change	Alt	Titel	Abweichende alte Bezeichnung
4.	new		Risk Assessment and Treatment	
5.1.2	renamed	5.1.2	Review of the information security policy	Review and evaluation
6	renamed	6	Organizing information security	Organizational security
6.1	renamed	6.1	Internal organization	Information security infrastructure
6.1.1	renamed	6.1.1	Management commitment to information security	Management information security forum
6.1.4	renamed	6.1.4	Approval process for information processing facilities	Authorisation process for information processing facilities
	deleted	6.1.5	Specialist information security advice	
6.1.5	new no.	8.1.3	Confidentiality agreements	
6.1.6	new		Contact with authorities	
6.1.7	new		Contact with special interest groups	
6.1.8	new no.	6.1.7	Independent review of information security	
6.2	renamed	6.2	External partners	Security of third party access
6.2.2	new		Addressing security when dealing with customers	
6.2.3	new no.	6.2.2	Adressing security in third party agreements	Security requirements in third-party contracts

Neu	Change	Alt	Titel	Abweichende alte Bezeichnung
	deleted	6.3	Outsourcing	
7	renamed	7	Asset management	Asset classification and control
7.1	renamed	7.1	Responsibility for assets	Accountability for assets
7.1.2	new		Ownership of assets	
7.1.3	new		Acceptable use of assets	
8	renamed	8	Human resources security	Personnel security
8.1	renamed	8.1	Prior to employment	Security in job definition and resourcing
8.1.1	renamed	8.1.1	Roles and responsibilities	Including security in job responsibilities
8.1.2	renamed	8.1.2	Screening	Personnel screening and policy
8.1.3	new no.	8.1.4	Terms and conditions of employment	
8.2	renamed	8.2	During employment	User training
8.2.1	new		Management responsibilities	
8.2.2	new no.	8.2.1	Information security awareness, education and training	Information security education and training
8.2.3	new no.	8.3.5	Disciplinary process	
	deleted	8.3	Responding to security incidents and malfunctions	
8.3	new		Termination or change of employment	
8.3.1	new		Termination responsibilities	
8.3.2	new		Return of assets	
	deleted	8.3.3	Reporting software malfunctions	
8.3.3	new		Removal of access rights	
9.1.4	new		Protecting against external and environmental threats	
9.1.5	new no.	9.1.4	Working in secure areas	
9.1.6	new no.	9.1.5	Public access, delivery and loading areas	Isolated delivery and service areas
9.2.2	renamed	9.2.2	Supporting utilities	Power supplies
9.2.7	new no.	9.3.2	Removal of property	
	deleted	9.3	General controls	
10.1	new no.	10.1	Operational procedures and responsibilities	
	deleted	10.1.3	Incident management procedures	
10.1.3	new no.	10.1.4	Segregation of duties	
10.1.4	new no.	10.1.5	Seperation of development, test and operational facilities	Seperation of development and operational facilities
	deleted	10.1.6	External facility management	
10.2	new		Third party service delivery management	
10.2.1	new		Service delivery	
10.2.2	new		Monitoring and review of third party services	
10.2.3	new		Managing changes to third party services	
10.3	new no.	10.2	System planning and acceptance	
10.3.1	new no.	10.2.1	Capacity management	Capacity planning
10.3.2	new no.	10.2.2	System acceptance	
10.4	new no.	10.3	Protection against malicious and mobile code	Protection against malicious software
10.4.1	new no.	10.3.1	Controls against malicious software	Controls against malicious code
10.4.2	new		Controls against mobile code	
10.5	new no.	10.4	Back-up	Housekeeping
10.5.1	new no.	10.4.1	Information backup	
10.6	new no.	10.5	Network security management	Network management
10.6.1	new no.	10.5.1	Network controls	
10.6.2	new no.	11.4.9	Security of network services	
10.7	new no.	10.6	Media handling	Media handling and security
10.7.1	new no.	10.6.1	Management of removable computer media	
10.7.2	new no.	10.6.2	Disposal of media	
10.7.3	new no.	10.6.3	Information handling procedures	
10.7.4	new no.	10.6.4	Security of system documentation	
	deleted	10.7.5	Security of electronic office systems	
	deleted	10.7.7	Other forms of information exchange	
10.8	new no.	10.7	Exchange of information	Exchange of information and software
10.8.1	new		Information and software exchange policies and procedures	
10.8.2	new no.	10.7.1	Exchange agreements	Information and software exchange agreements

Neu	Change	Alt	Titel	Abweichende alte Bezeichnung
10.8.3	new no.	10.7.2	Physical media in transit	Security of media in transit
10.8.4	new no.	10.7.4	Electronic messaging	Security of electronic mail
10.9	new		Electronic commerce services	
10.9.1	new no.	10.7.3	Electronic commerce	Electronic commerce security
10.9.2	new		On-Line Transactions	
10.9.3	new no.	10.7.6	Publicly available information	Publicly available documents
10.10	new no.	11.7	Monitoring	Monitoring system and access use
10.10.1	new		Audit logging	
10.10.2	new no.	11.7.2	Monitoring system use	
10.10.3	new		Protection of log information	
10.10.4	new no.	10.4.2	Administrator and operator logs	Operator logs
10.10.5	new no.	10.4.3	Fault logging	
10.10.6	new no.	11.7.3	Clock synchronisation	
11.3.3	new no.	9.3.1	Clear desk and clear screen policy	
	deleted	11.4.2	Enforced path	
11.4.2	new no.	11.4.3	User authentication for external connections	
11.4.3	new no.	11.4.4	Equipment identification in the network	Node authentication
11.4.4	new no.	11.4.5	Remote diagnostic and configuration port protection	Remote diagnostic port protection
11.4.5	new no.	11.4.6	Segregation in networks	
11.4.6	new no.	11.4.7	Network connection control	
11.4.7	new no.	11.4.8	Network routing control	
	deleted	11.5.1	Automatic terminal identification	
11.5.1	new no.	11.5.2	Secure log-on procedures	Terminal log-on procedures
11.5.2	new no.	11.5.3	User identification and authentication	
11.5.3	new no.	11.5.4	Password management system	
11.5.4	new no.	11.5.5	Use of system utilities	
11.5.5	new no.	11.5.7	Session time-out	Terminal time-out
	deleted	11.5.6	Duress alarm to safeguard users	
11.5.6	new no.	11.5.8	Limitation of connection time	
11.7	new		Mobile computing and teleworking	
	deleted	11.7.1	Event logging	
11.7.1	new no.	11.8.1	Mobile computing and communications	Mobile computing
11.7.2	new no.	11.8.2	Teleworking	
12	renamed	12	Information systems acquisation, development and maintenance	System development and maintenance
12.1	renamed	12.1	Security requirements of information systems	Security requirements of systems
12.2.3	renamed	12.2.3	Message integrity	Message authentication
12.3.1	new no.	12.3.1	Policy on the use of cryptographic controls	
	deleted	12.3.2	Encryption	
12.3.2	new no.	12.3.5	Key management	
	deleted	12.3.3	Digital signatures	
	deleted	12.3.4	Non-repudation services	
12.4.3	renamed	12.4.3	Access control to program source code	Access control to program source library
12.5.2	renamed		Technical review of applications after operating system changes	Technical review of operating system changes
12.5.4	renamed		Information leakage	Covert channels and trojan code
12.6	new		Vulnerability management	
12.6.1	new		Control of vulnerabilities	
13	new		Information security incident management	
13.1	new		Reporting information security events and weaknesses	
13.1.1	new no.	8.3.1	Reporting information security events	
	deleted	13.1.1	Aspects of business continuity management	
13.1.2	new no.	8.3.2	Reporting security weaknesses	
13.2	new		Management of information security incidents and improvements	
13.2.1	new		Responsibilities and procedures	
13.2.2	new no.	8.3.4	Learning from information security incidents	
13.2.3	new no.	14.1.7	Collection of evidence	
14	new no.	13	Business continuity management	

Neu	Change	Alt	Titel	Abweichende alte Bezeichnung
14.1	new no.	13.1	Information security aspects of business continuity management	Aspects of business continuity management
14.1.1	new no.	13.1.2	Including information security in the business continuity management process	Business continuity management process
14.1.2	new no.	13.1.3	Business continuity and risk assessment	Business continuity and impact analysis
14.1.3	new no.	13.1.4	Developing and implementing continuity plans including information security	Writing and implementing continuity plans
14.1.4	new no.	13.1.5	Business continuity planning framework	
14.1.5	new no.	13.1.6	Test, maintaining and re-assessing business continuity plans	
15	new no.	14	Compliance	
15.1	new no.	14.1	Compliance with legal requirements	
15.1.1	new no.	14.1.1	Identification of applicable legislation	
15.1.2	new no.	14.1.2	Intellectual property rights (IPR)	
15.1.3	new no.	14.1.3	Safeguarding of organisational records	
15.1.4	new no.	14.1.4	Data protection and privacy of personal information	
15.1.5	new no.	14.1.5	Prevention of misuse of information processing facilities	
15.1.6	new no.	14.1.6	Regulation of cryptographic controls	
15.2	new no.	14.2	Compliance with security policies and standards	Reviews of security policy and technical compliance
15.2.1	new no.	14.2.1	Compliance with security policy and standards	Compliance with security policy
15.2.2	new no.	14.2.2	Technical compliance checking	
15.3	new no.	14.3	Information systems audit considerations	System audit considerations
15.3.1	new no.	14.3.1	Information system audit controls	System audit controls
15.3.2	new no.	14.3.2	Protection of information system audit tools	Protection of system audit tools