

BSI FOREIGN DOCUMENTS

ÜBERSETZUNG

BS 7799-2

1999

Management von Informationssicherheit .
Teil 2: Spezifikation für
Informationssicherheits-Managementsysteme

*Original language version
Information security management .
Part 2. Specification for information
security management systems*

*Issued by
British Standards Institution
389 Chiswick High Road
London
W4 4AL*

BSI Foreign Documents has taken all reasonable measures to ensure the accuracy of this translation but regrets that no responsibility can be accepted for any error, omission or inaccuracy.

In cases of doubt or dispute, the original language text only is valid.

© BSI Foreign Documents
389 Chiswick High Road, London W4 4AL
Tel: +44 208 996 7525
Facsimile: +44 208 996 7121

Ausschüsse, die für diese Britische Norm verantwortlich sind:

Die Vorbereitung dieser Britischen Norm wurde dem BSI/DISC Committee BDD/2. Management von Informationssicherheit, übertragen, in dem die folgenden Organisationen vertreten waren

Association of British Insurers
British Computer Society
British Telecommunications plc
The Business Continuity Institute
Department of Trade and Industry (Information Security Policy Unit)
Det Norske Veritas Quality Assurance
HMG Protective Security Authority
HSBC
Indicii Salus
Institute of Chartered Accountants in England and Wales
Institute of Internal Auditors
KPMG plc
L3 Network Security
Lloyds TSB
Logica UK
Marks & Spencer plc
Nationwide Building Society
PCSL
Racal Network Services
RKP Associates
Shell International Petroleum Co Ltd
Unilever plc
Whitbread plc
XiSEC Consultants Ltd/AEXIS Consultants

Diese Britische Norm, die unter der Leitung des DISC Board erarbeitet wurde, erschien mit Genehmigung des Standards Board und gilt ab 15 Mai 1999.

© BSI 05-1999

Veröffentlicht zum ersten Mal
als Teil 2 in Februar 1998

Die folgenden BSI-Verweise beziehen sich auf die Arbeit bezüglich dieser Norm:
Ausschußverweis BDD/2 .Kommentarentwurf 98/682025 DC

Inhaltsverzeichnis

	Seite
Verantwortliche Ausschüsse	Titelrückseite
Vorwort	I
1 Anwendungsbereich	1
2 Begriffe und Definitionen	1
3 Anforderungen an das Managementsystem für Informationssicherheit	1
3.1 Allgemeines.....	1
3.2 Schaffung eines Managementrahmens	1
3.3 Implementierung.....	4
3.4 Dokumentation	4
3.5 Kontrolle der Unterlagen	4
3.6 Aufzeichnungen.....	5
4 Spezifische Maßnahmen	5
4.1 Sicherheitspolitik.....	5
4.2 Organisation der Sicherheit	6
4.3 Einstufung und Kontrolle der Werte	8
4.4 Personelle Sicherheit	8
4.5 Physische und umgebungsbezogene Sicherheit	10
4.6 Management der Kommunikation und des Betriebs	12
4.7 Zugangskontrolle	16
4.8 Systementwicklung und -wartung	21
4.9 Management des kontinuierlichen Geschäftsbetriebs	24
4.10 Einhaltung der Verpflichtungen	25
Annex A (informativ) Änderungen bei der internen Nummerierung	28
Literaturhinweise	29

Vorwort

Dieser Teil der Norm BS 7799 wurde von BDD/2, Management von Informationssicherheit, aufgestellt. Er ersetzt die Norm BS 7799-2:1998, die zurückgezogen wurde.

Die Norm BS 7799 wird in zwei Teilen herausgegeben:

- Teil 1: Leitfaden zum Management von Informationssicherheit
- Teil 2: Spezifikation für Informationssicherheits-Managementsysteme

Diese neue Ausgabe der Norm BS 7799-2 ist notwendig, weil die BS 7799-1 überarbeitet wurde. Das Nummerierungssystem, die Sicherheitsziele und Maßnahmen in Abschnitt 4 wurden direkt von den Abschnitten 3 bis 12 der BS 7799-1 abgeleitet und angepasst. Keine weiteren Änderungen wurden vorgenommen.

Bei der neuen Ausgabe handelt es sich jedoch nicht um eine vollständige Überprüfung oder Überarbeitung der Norm. Diese Aufgabe wird zu gegebener Zeit ausgeführt.

Die Norm BS 7799-2 dient als Basis für die Beurteilung eines Managementsystems für Informationssicherheit (ISMS - Information security management system) für die Gesamtheit oder einen Teil einer Organisation. Sie kann als Basis für ein formales Verfahren zur Zertifizierung verwendet werden.

Diese Spezifikation basiert auf der Norm BS 7799-1, Management von Informationssicherheit, Teil 1: "Leitfaden zum Management von Informationssicherheit", die Richtlinien für das beste Vorgehen bei der Erfüllung der Anforderungen dieser Spezifikation gibt. Die Liste der Sicherheitsziele und Maßnahmen in Abschnitt 4 dieses Teils der Norm BS 7799 ist jedoch nicht erschöpfend. Eine Organisation kann durchaus der Ansicht sein, dass zusätzliche Sicherheitsziele und Maßnahmen notwendig sind.

Nicht alle der beschriebenen Maßnahmen sind für jede Situation relevant. Sie können weder lokale umgebungsbedingte oder technologische Zwänge berücksichtigen, noch können sie in einer Form existieren, die für die Anforderungen jedes potentiellen Anwenders in einer Organisation passend ist. Organisationen müssen eine Risikoanalyse durchführen, um die am besten geeigneten Sicherheitsziele und Maßnahmen zu bestimmen, die zu implementieren und auf die eigenen Anforderungen anwendbar sind. Nach deren Identifikation müssen sie in einer Erklärung zur Anwendbarkeit dokumentiert werden. Diese Erklärung zur Anwendbarkeit muss für Manager, Mitarbeiter und unabhängige Parteien (z.B. Auditoren, Zertifizierer usw.) mit Zugangsberechtigung verfügbar sein. Die in der Erklärung zur Anwendbarkeit dokumentierten Sicherheitsziele und Maßnahmen, die Dokumentationen der Sicherheitspolitik und Verfahren sowie alle anderen relevanten Aufzeichnungen werden als das Managementsystem für Informationssicherheit einer Organisation bezeichnet.

Die in Abschnitt 4 dieses Teils der BS7799 angegebenen Anforderungen sind bewusst allgemein formuliert. Es wird davon ausgegangen, dass Organisationen, die eine Zertifizierung anstreben, die Elemente der in Teil 1 angegebenen besten Praktiken einführen, die nachweislich laut Risikoanalyse für ihre Anforderungen am geeignetsten sind. Alle mit dem Verfahren für die Zertifizierung verbundenen Bedingungen werden separat mit Genehmigung der für das Verfahren zuständigen Person herausgegeben und fallen nicht in den Anwendungsbereich dieser Norm. Zur Zertifizierungsfähigkeit nach dieser Britischen Norm muss das Informationssicherheits-

Managementsystem zur Zufriedenheit einer unabhängigen Zertifizierungsstelle implementiert und aufrechterhalten werden.

Beim Entwurf dieser Britischen Norm wurde angenommen, dass die Ausführung der Bestimmungen entsprechend qualifizierten und erfahrenen Personen anvertraut wird.

Anhang A hat eine vergleichende Funktion und enthält eine Tabelle, die die Abschnitte der Ausgabe von 1998 zu den Abschnitten der Ausgabe von 1999 in Beziehung setzt.

Eine Britische Norm erhebt nicht den Anspruch, alle notwendigen Bestimmungen eines Vertrags zu enthalten. Anwender von Britischen Normen sind selbst für deren richtige Anwendung verantwortlich.

Die Einhaltung einer Britischen Norm allein entbindet den Anwender nicht von seinen gesetzlichen Verpflichtungen.

1 Anwendungsbereich

Dieser Teil der BS 7799 legt die Anforderungen für die Schaffung, Implementierung und Dokumentation von Managementsystemen für Informationssicherheit (ISMSs - Information security management systems) fest. Er schreibt die Anforderungen für die Sicherheitsmaßnahmen vor, die nach den Erfordernissen der jeweiligen Organisationen zu implementieren sind.

Hinweis: Teil 1 gibt Empfehlungen für die besten Praktiken zur Unterstützung der Anforderungen in dieser Spezifikation. Die in Abschnitt 4 dieses Teils der BS 7799 angegebenen Sicherheitsziele und Maßnahmen stammen aus den in der BS 7799-1 aufgeführten und sind an sie angepasst.

2 Begriffe und Definitionen

Die Definitionen in der Norm BS 7799-1 gelten gemeinsam mit dem folgenden für diesen Teil der BS 7799.

2.1.1 Erklärung zur Anwendbarkeit

Kritische Darstellung der Sicherheitsziele und Maßnahmen, die auf die Anforderungen der Organisation anwendbar sind.

3 Anforderungen an das Managementsystem für Informationssicherheit

3.1 Allgemeines

Die Organisation muss ein dokumentiertes Managementsystem für Informationssicherheit schaffen und erhalten. Das System hat die Aufgabe, sich mit dem Schutz von Werten, der Vorgehensweise der Organisation beim Risikomanagement, den Sicherheitszielen und Maßnahmen sowie dem erforderlichen Grad der Gewährleistung von Sicherheit zu befassen.

3.2 Schaffung eines Managementrahmens

Für die Identifikation und Dokumentation der Sicherheitsziele und Maßnahmen sind folgende Schritte durchzuführen (siehe Bild 1):

- a) Die Informationssicherheitspolitik ist zu definieren.
- b) Der Anwendungsbereich des Managementsystems für Informationssicherheit ist zu bestimmen. Die Grenzen hinsichtlich der Merkmale der Organisation, ihres Standorts, ihrer Werte und ihrer Technologie sind festzulegen.

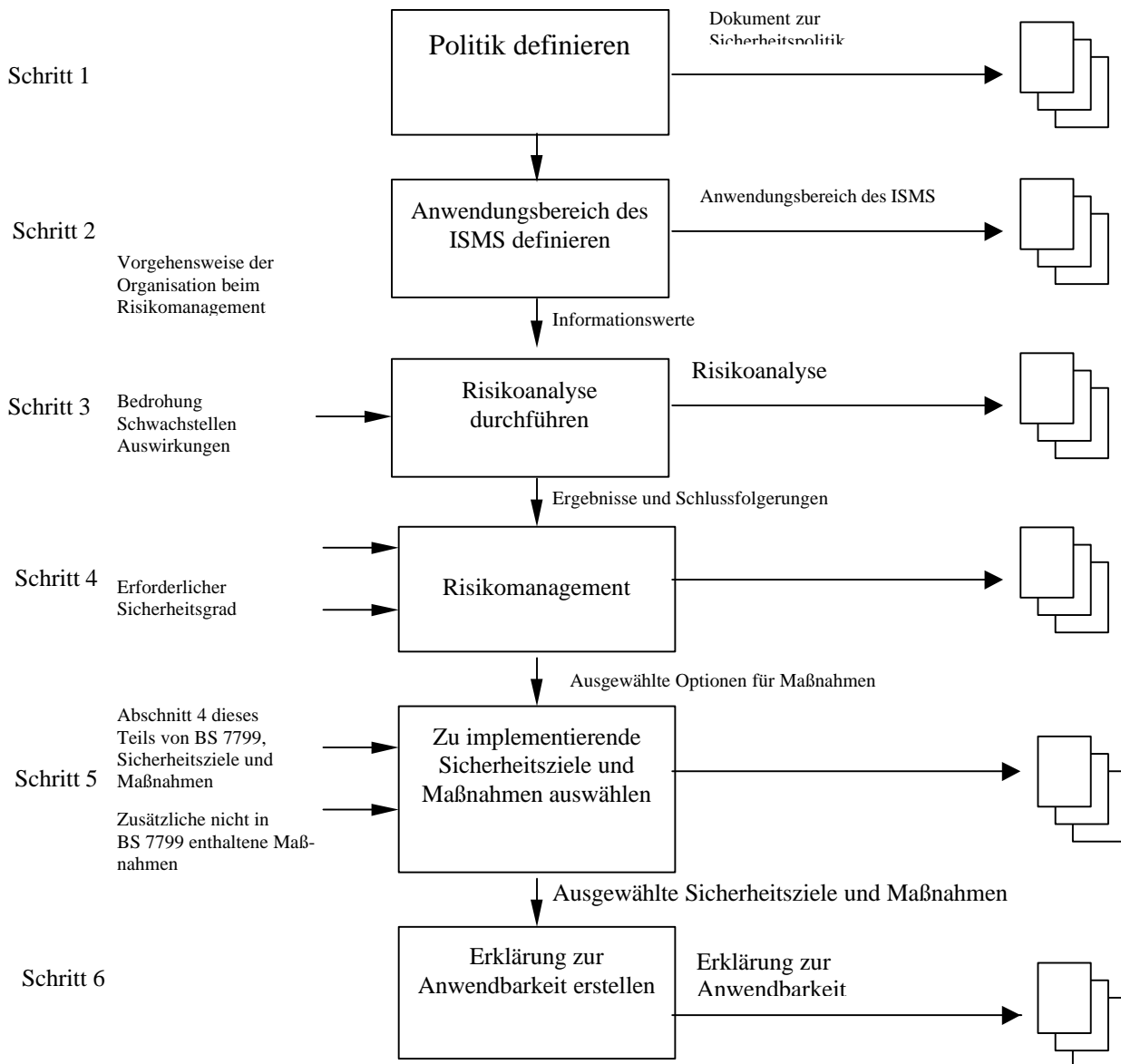
- c) Eine angemessene Risikoanalyse ist durchzuführen. Die Risikoanalyse muss die Bedrohung der Werte, die Schwachstellen und Auswirkungen auf die Organisation identifizieren und die Höhe des Risikos bestimmen.
- d) Die zu verwaltenden Risikobereiche sind auf der Basis der Informationssicherheitspolitik der Organisation und des erforderlichen Grads an Gewährleistung von Sicherheit zu identifizieren.
- e) Geeignete Sicherheitsziele und Maßnahmen sind aus Abschnitt 4 zur Implementierung durch die Organisation auszuwählen, und die Auswahl ist zu begründen.

Hinweis: Eine Richtschnur für die Auswahl der Sicherheitsziele und Maßnahmen bietet die BS 7799-1. Die in Abschnitt 4 dieses Teils der BS 7799 angegebenen Sicherheitsziele und Maßnahmen sind nicht erschöpfend und können ergänzt werden.

- f) Eine Erklärung zur Anwendbarkeit ist zu erstellen. Die ausgewählten Sicherheitsziele und Maßnahmen sowie die Gründe für ihre Auswahl sind in der Erklärung zur Anwendbarkeit zu dokumentieren. Diese Erklärung muss auch eine Aufzeichnung über den etwaigen Ausschluss bestimmter in Abschnitt 4 angegebenen Maßnahmen enthalten.

Diese Schritte sind in geeigneten festgelegten Abständen nach Bedarf zu überprüfen.

Bild 1 - Schaffung eines Managementrahmens



3.3 Implementierung

Die ausgewählten Sicherheitsziele und Maßnahmen sind effektiv von der Organisation zu implementieren. Die Effektivität der eingeführten Verfahren zur Implementierung der Maßnahmen gemäß 4.10.2 durch Überprüfungen zu verifizieren.

Hinweis: Auf die Empfehlungen in BS 7799-1 wird verwiesen.

3.4 Dokumentation

Die Dokumentation des Managementsystems für Informationssicherheit muss folgende Informationen enthalten:

- a) Nachweis der ausgeführten Aktionen gemäß Festlegung in 3.2;
- b) Zusammenfassung des Managementrahmens einschließlich der Informationssicherheitspolitik sowie der Sicherheitsziele und implementierten Maßnahmen gemäß der Erklärung zur Anwendbarkeit;
- c) eingeführte Verfahren zur Implementierung der Maßnahmen gemäß 3.3; diese Verfahren müssen die Verantwortlichkeiten und die entsprechenden Aktionen beschreiben;
- d) Verfahren, die das Management und den Betrieb des Managementsystems für Informationssicherheit abdecken; diese Verfahren müssen die Verantwortlichkeiten und die entsprechenden Aktionen beschreiben;

Hinweis: Es empfiehlt sich, alle in 3.4 b) und c) aufgeführten Unterlagen in einem Sicherheitspolitik-Handbuch zusammenzufassen.

3.5 Kontrolle der Unterlagen

Die Organisation muss Verfahren zur Kontrolle der gesamten unter 3.4 erforderlichen Unterlagen festlegen und aufrechterhalten, um sicherzustellen, dass die Unterlagen

- a) sofort verfügbar sind;
- b) periodisch überprüft und nach Bedarf in Übereinstimmung mit der Sicherheitspolitik der Organisation überarbeitet werden;
- c) in der richtigen Fassung vorliegen und an allen Orten verfügbar sind, an denen Vorgänge ablaufen, die für das effektive Funktionieren des Managementsystems für Informationssicherheit wesentlich sind;
- d) bei Ungültigkeit unverzüglich aus dem Verkehr gezogen werden;
- e) bei Ungültigkeit identifiziert und aufbewahrt werden und nach Bedarf für rechtliche Zwecke oder für Zwecke der Wissenserhaltung oder für beides verfügbar sind.

- f) Unterlagen müssen leserlich, (mit den Überprüfungsdaten) datiert und leicht identifizierbar sein, ordentlich erhalten und für eine festgelegte Zeit aufbewahrt werden. Verfahren und Verantwortlichkeiten für die Erstellung und Änderung verschiedener Unterlagentypen sind festzulegen und aufrechtzuerhalten.

Hinweis: Unterlagen können in jeder Form, wie z.B. als Hartkopie oder auf elektronischen Datenträgern, vorliegen.

3.6 Aufzeichnungen

Aufzeichnungen, die einen Nachweis für den Betrieb eines Managementsystems für Informationssicherheit erbringen, sind auf geeignete Weise für das System und die Organisation, d.h. in Form von Besucherbüchern, Auditaufzeichnungen und Zugangsberechtigungen, aufrechtzuerhalten, um die Erfüllung der Anforderungen dieses Teils von BS 7799 nachzuweisen.

Organisation muss Verfahren für die Identifikation, Aufrechterhaltung, Aufbewahrung und Entsorgung von Aufzeichnungen, die die Erfüllung der Anforderungen nachweisen, schaffen und aufrechterhalten.

Aufzeichnungen müssen leserlich, identifizierbar und auf die entsprechenden Aktivitäten rückführbar sein. Sie sind so aufzubewahren und zu erhalten, dass sie leicht wiederauffindbar und vor Beschädigung, Qualitätsminderung oder Verlust geschützt sind.

Hinweis: Aufzeichnungen können in jeder Form, wie z.B. als Hartkopie oder auf elektronischen Datenträgern, vorliegen.

4 Spezifische Maßnahmen

4.1 Sicherheitspolitik

4.1.1 Informationssicherheitspolitik

Ziel: Richtungsvorgabe für und Unterstützung durch die Geschäftsführung bei der Informationssicherheit

4.1.1.1 Dokument zur Information Sicherheitspolitik

Von der Geschäftsführung ist ein Dokument zur Informationssicherheitspolitik zu genehmigen, zu veröffentlichen und nach Bedarf an alle Mitarbeiter zu verteilen.

4.1.1.2 Überprüfung und Bewertung

Die Politik ist regelmäßig und im Anschluss an Änderungen, die einen Einfluss auf sie haben könnten, auf ihre weitere Eignung zu überprüfen.

4.2 Organisation der Sicherheit

4.2.1 Infrastruktur der Informationssicherheit

Ziel: Verwaltung von Informationssicherheit innerhalb der Organisation.

4.2.1.1 Managementforum für Informationssicherheit

Es ist ein Managementforum ins Leben zu rufen, das eine klare Ausrichtung und sichtbare Unterstützung des Managements für Sicherheitsinitiativen gewährleistet.

4.2.1.2 Koordination der Informationssicherheit

Abhängig von der Größe der Organisation ist ein Forum mit übergreifender Funktion ins Leben zu rufen, das sich aus Vertretern des Managements der relevanten Bereiche der Organisation zusammensetzt und über das die Implementierung von Maßnahmen zur Informationssicherheit koordiniert wird.

4.2.1.3 Zuweisung der Zuständigkeiten für Informationssicherheit

Zuständigkeiten für den Schutz einzelner Werte und für die Durchführung spezifischer Sicherheitsprozesse sind klar zu definieren.

4.2.1.4 Berechtigungsprozess für Geräte zur Informationsverarbeitung

Für neue Geräte zur Informationsverarbeitung ist ein Prozess zur Gewährleistung der Berechtigung des Managements einzurichten.

4.2.1.5 Fachliche Informationssicherheitsberatung

Hausinterne oder spezialisierte Fachberater sind bei Fragen zur Informationssicherheit zu Rate zu ziehen, und erhaltene Informationen in der gesamten Organisation weiterzuleiten.

4.2.1.6 Kooperation zwischen Organisationen

Entsprechende Kontakte zu Vollzugs- und Aufsichtsbehörden, Informationsdiensteanbietern und Telekommunikationsbetreibern sind aufrechtzuerhalten.

4.2.1.7 Unabhängige Überprüfung von Informationssicherheit

Die Implementierung der Informationssicherheitspolitik ist unabhängig zu überprüfen.

4.2.2 Sicherheit bei dem Zugang durch Fremdunternehmen

Ziel: Erhaltung der Sicherheit organisationseigener Geräte zur Informationsverarbeitung und Informationswerte, zu denen Fremdunternehmen Zugang haben.

4.2.2.1 Identifizierung der Risiken bei dem Zugang von Fremdunternehmen

Die Risiken, die mit dem Zugang zu organisationseigenen Geräten für die Informationsverarbeitung durch Fremdunternehmen verknüpft sind, sind zu beurteilen und entsprechende Sicherheitsmaßnahmen zu implementieren.

4.2.2.2 Sicherheitsanforderungen in Verträgen mit Fremdunternehmen

Arrangements, bei denen Fremdunternehmen Zugang zu organisationseigenen Geräten für die Informationsverarbeitung erhalten, sind in einem formalen Vertrag mit allen erforderlichen Sicherheitsanforderungen festzuhalten.

4.2.3 Outsourcing

Ziel: Aufrechterhaltung der Sicherheit der Informationen, wenn die Verantwortung für die Informationsverarbeitung an eine andere Organisation übertragen wurde.

4.2.3.1 Sicherheitsanforderungen in Outsourcing-Verträgen

Die Sicherheitsanforderungen einer Organisation, die das Management und die Kontrolle für alle oder einige Informationssysteme, Netzwerke und/oder Desktop-Umgebungen auslagert, sind in einem zwischen den Parteien vereinbarten Vertrag zu behandeln.

4.3 Einstufung und Kontrolle der Werte

4.3.1 Zurechenbarkeit für Werte

Ziel: Aufrechterhaltung eines angemessenen Schutzes für organisationseigene Werte.

4.3.1.1 Inventar der Werte

Ein Inventar aller wichtigen Werte ist zu erstellen und laufend zu aktualisieren.

4.3.2 Einstufung von Informationen

Ziel: Sicherstellung eines angemessenen Schutzes für Informationswerte.

4.3.2.1 Richtlinien für die Einstufung

Einstufungen für Informationen und damit verbundene Schutzmaßnahmen sind gemäß der Geschäftsanforderungen für die gemeinsame oder beschränkte Nutzung von Informationen sowie der mit derartigen Anforderungen verbundenen geschäftlichen Folgen festzulegen.

4.3.2.2 Kennzeichnung und Behandlung von Informationen

Es sind Verfahren für die Kennzeichnung und Behandlung von Informationen gemäß der von der Organisation festgelegten Einstufung zu definieren.

4.4 Personelle Sicherheit

4.4.1 Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen

Ziel: Reduzierung der Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch der Einrichtungen.

4.4.1.1 Einbeziehung von Sicherheit in Arbeitsverantwortlichkeiten

Sicherheitsrollen und -verantwortlichkeiten, wie sie in der Informationssicherheitspolitik der Organisation niedergelegt sind, sind sofern zutreffend in Stellenbeschreibungen zu dokumentieren.

4.4.1.2 Überprüfung der Mitarbeiter und Personalpolitik

Überprüfungen bei festangestellten Mitarbeitern sind zum Zeitpunkt der Bewerbung durchzuführen.

4.4.1.3 Vertraulichkeitsvereinbarungen

Von Angestellten ist als Teil ihrer Anstellungsbedingungen eine Vertraulichkeitsvereinbarung zu unterschreiben.

4.4.1.4 Anstellungsbedingungen

In den Anstellungsbedingungen ist auf die Verantwortung des Mitarbeiters für Informationssicherheit hinzuweisen.

4.4.2 Benutzerschulung

Ziel: Gewährleistung, dass Benutzer sich der Bedrohungen und Bedenken bezüglich der Informationssicherheit bewusst sind, und dass sie bei ihrer normalen Arbeitsverrichtung über Mittel zur Unterstützung der organisationseigenen Sicherheitspolitik verfügen.

4.4.2.1 Ausbildung und Schulung in der Informationssicherheit

Für alle Mitarbeiter der Organisation und im Bedarfsfall für Benutzer von Fremdfirmen sind entsprechende Schulungen durchzuführen und regelmäßig aktualisierte Informationen zu Sicherheitspolitiken und Verfahren der Organisation herauszugeben.

4.4.3 Verhalten bei Sicherheitsvorfällen und Störungen

Ziel: Schadensbegrenzung bei Sicherheitsvorfällen und Funktionsstörungen, Überwachung derartiger Vorfälle und Erkenntnisgewinn.

4.4.3.1 Meldung von Sicherheitsvorfällen

Sicherheitsvorfälle sind sobald wie möglich, nachdem der Vorfall entdeckt wurde, über entsprechende Managementkanäle zu melden.

4.4.3.2 Meldung von Sicherheitsschwachstellen

Benutzer von Informationsdiensten haben alle beobachteten oder vermuteten Sicherheitsschwachstellen oder Bedrohungen bezüglich der Systeme oder Dienste aufzuzeichnen und zu melden.

4.4.3.3 Meldung von Softwarestörungen

Für das Melden von Softwarefunktionsstörungen sind entsprechende Verfahren einzurichten und zu befolgen.

4.4.3.4 Lernen aus Vorfällen

Es sind Verfahren einzurichten, mit denen Arten, Umfang und Kosten von Vorfällen und Störungen quantitativ erfasst und überwacht werden können.

4.4.3.5 Disziplinarverfahren

Verstöße von Mitarbeitern gegen organisationseigene Sicherheitspolitiken und Verfahren sind mit formalen Disziplinarverfahren zu ahnden.

4.5 Physische und umgebungsbezogene Sicherheit

4.5.1 Sicherheitszonen

Ziel: Verhinderung von unberechtigtem Zugang, Beschädigung und Störung der Geschäftsräume und Informationen.

4.5.1.1 Physische Sicherheitsgrenze

Von Organisationen sind Sicherheitsgrenzen festzulegen, um Bereiche zu schützen, in denen sich Geräte zur Informationsverarbeitung befinden.

4.5.1.2 Physische Zutrittskontrollen

Sicherheitszonen sind durch entsprechende Zutrittskontrollen zu schützen, um sicherzustellen, dass nur berechtigtem Personal Zutritt gestattet wird.

4.5.1.3 Sicherung von Geschäftsräumen und Geräten

Zum Schutz von Geschäftsräumen und Geräten mit speziellen Sicherheitsanforderungen sind Sicherheitszonen zu schaffen.

4.5.1.4 Arbeiten in Sicherheitszonen

Es sind zusätzliche Maßnahmen und Richtlinien für das Arbeiten in Sicherheitszonen zu implementieren, um die Sicherheit in Sicherheitszonen, die durch die physischen Schutzmaßnahmen gegeben ist, zu erhöhen.

4.5.1.5 Separate Liefer- und Ladebereiche

Liefer- und Ladebereiche sind zu kontrollieren und nach Möglichkeit von Geräten zur Informationsverarbeitung zu trennen, um einen unberechtigten Zugang zu verhindern.

4.5.2 Sicherheit der Geräte

Ziel: Verhinderung von Verlust, Beschädigung oder Kompromittierung von Werten und der Unterbrechung von Geschäftsaktivitäten.

4.5.2.1 Positionierung und Schutz der Geräte

Geräte sind so zu positionieren oder zu schützen, dass Risiken durch umgebungsbedingte Bedrohungen und Gefährdungen sowie Gelegenheiten für einen unberechtigten Zugang reduziert werden.

4.5.2.2 Stromversorgung

Geräte sind vor Netzausfällen und anderen elektrischen Störungen zu schützen.

4.5.2.3 Sicherung der Verkabelung

Strom- und Telekommunikationsverkabelung die Daten überträgt oder Informationsdienste unterstützt, ist vor Abhören oder Beschädigung zu schützen.

4.5.2.4 Wartung der Geräte

Geräte sind gemäß der Anweisungen des Herstellers und/oder dokumentierter Verfahren zu warten, um ihre kontinuierliche Verfügbarkeit und Integrität zu gewährleisten.

4.5.2.5 Sicherheit für Geräte außerhalb des Geschäftsgeländes

Zum Schutz von Geräten, die außerhalb des Geländes einer Organisation benutzt werden, sind Sicherheitsverfahren und -maßnahmen zu implementieren.

4.5.2.6 Sichere Entsorgung oder Wiederverwendung von Geräten

Vor der Entsorgung oder Wiederverwendung von Geräten sind alle darauf enthaltenen Informationen zu löschen.

4.5.3 Allgemeine Maßnahmen

Ziel: Verhinderung der Kompromittierung oder des Diebstahls von Informationen und Geräten zur Informationsverarbeitung.

4.5.3.1 Politik zum Aufräumen des Schreibtischs und Löschen des Bildschirms

Von Organisationen ist eine Politik zum Aufräumen des Schreibtischs und Löschen des Bildschirms zu implementieren, um die Risiken eines unberechtigten Zugangs, des Verlusts und der Beschädigung von Informationen zu reduzieren.

4.5.3.2 Entfernung von Eigentum

Geräte, Informationen oder Software, die Eigentum der Organisation sind, sind nicht ohne Genehmigung zu entfernen.

4.6 Management der Kommunikation und des Betriebs

4.6.1 Betriebsverfahren und -verantwortlichkeiten

Ziel: Gewährleistung des korrekten und sicheren Betriebs von Geräten zur Informationsverarbeitung.

4.6.1.1 Dokumentierte Betriebsverfahren

Die in der Sicherheitspolitik identifizierten Betriebsverfahren (siehe 4.1.1.1) sind zu Dokumentieren und auf dem neuesten Stand zu halten.

4.6.1.2 Kontrolle von Veränderungen

Veränderungen bei Geräten und Systemen zur Informationsverarbeitung sind zu überwachen.

4.6.1.3 Verfahren für das Management von Vorfällen

Eis sind Verantwortlichkeiten und Verfahren der Vorfallverwaltung einzurichten, damit schnell, effektiv und ordnungsgemäß auf Sicherheitsvorfälle reagiert werden kann.

4.6.1.4 Pflichtentrennung

Pflichten und Verantwortungsbereiche sind voneinander zu trennen, um Gelegenheiten für unberechtigte Änderungen oder den Missbrauch von Informationen oder Diensten zu reduzieren.

4.6.1.5 Trennung von Entwicklungs- und Betriebsanlagen

Entwicklungs- und Testeinrichtungen sind von laufenden Einrichtungen zu trennen.

4.6.1.6 Externe Verwaltung von Geräten

Bevor Geräte extern verwaltet werden, sind Risiken zu identifizieren und entsprechende Maßnahmen mit dem Auftragnehmer zu vereinbaren und in den Vertrag aufzunehmen.

4.6.2 Systemplanung und -abnahme

Ziel: Einschränkung des Risikos von Systemausfällen.

4.6.2.1 Kapazitätsplanung

Kapazitätsanforderungen sind zu kontrollieren und Vorausberechnungen zukünftiger Kapazitätsanforderungen anzustellen, um zu gewährleisten, dass eine ausreichende Verarbeitungsleistung und Speicherkapazität zur Verfügung stehen.

4.6.2.2 Systemabnahme

Für neue Informationssysteme, Updates und neue Versionen sind Abnahmekriterien festzulegen und vor der Abnahme geeignete Systemtests durchzuführen.

4.6.3 Schutz vor bösartiger Software

Ziel: Schutz der Integrität von Software und Informationen.

4.6.3.1 Maßnahmen zum Schutz vor bösartiger Software

Es sind Erkennungs- und Verhinderungsmaßnahmen zum Schutz vor bösartiger Software sowie entsprechende Verfahren zur Schärfung des Benutzerbewusstseins zu implementieren.

4.6.4 Haushaltsorganisation

Ziel: Aufrechterhaltung der Integrität und Verfügbarkeit von Diensten zur Verarbeitung von Informationen und für die Kommunikation.

4.6.4.1 Back-up von Informationen

Sicherungskopien grundlegender Geschäftsinformationen und Software sind regelmäßig zu erstellen.

4.6.4.2 Bedienerprotokolle

Betriebsmitarbeiter haben ihre Tätigkeiten zu protokollieren.

4.6.4.3 Fehlerprotokoll

Fehler sind zu melden und Korrekturmaßnahmen zu ergreifen.

4.6.5 Netzwerkmanagement

Ziel: Sicherung von Informationen in Netzen und Schutz der unterstützenden Infrastruktur.

4.6.5.1 Netzwerk-Maßnahmen

Zum Erzielen und Bewahren der Sicherheit in Netzen sind eine Reihe von Maßnahmen zu implementieren.

4.6.6 Umgang mit und Sicherheit von Datenträgern

Ziel: Verhinderung von Schäden an Werten und Unterbrechungen des Geschäftsbetriebs.

4.6.6.1 Verwaltung von mobilen Datenträgern

Die Verwaltung mobiler Datenträger, wie Bänder, Platten, Kassetten und gedruckte Aufzeichnungen, ist zu kontrollieren.

4.6.6.2 Beseitigung von Datenträgern

Datenträger sind sicher und zuverlässig zu beseitigen, wenn sie nicht mehr benötigt werden.

4.6.6.3 Verfahren zum Umgang mit Informationen

Es sind Verfahren zur Behandlung und Speicherung von Informationen einzurichten, um diese Informationen vor einer unberechtigten Offenlegung oder einem Missbrauch zu schützen.

4.6.6.4 Sicherheit von Systemdokumentation

Systemdokumentation ist vor unberechtigtem Zugang zu schützen.

4.6.7 Austausch von Informationen und Software

Ziel: Verhinderung von Verlust, Änderung oder Missbrauch von Informationen, die zwischen Organisationen ausgetauscht werden.

4.6.7.1 Vereinbarungen für den Austausch von Informationen und Software

Für den elektronischen oder manuellen Austausch von Informationen und Software zwischen Organisationen sind Vereinbarungen zu treffen, die in einigen Fällen formal sein können.

4.6.7.2 Sicherheit von Datenträgern im Transit

Datenträger, die transportiert werden, sind vor unberechtigtem Zugriff, Mißbrauch oder Verfälschung zu schützen.

4.6.7.3 E-Commerce-Sicherheit

E-Commerce ist vor betrügerischen Tätigkeiten, vertraglichen Streitigkeiten und der Offenlegung oder Änderung von Informationen zu schützen.

4.6.7.4 E-Mail-Sicherheit

Eine Politik für den Gebrauch von E-Mail ist zu entwickeln und Maßnahmen sind zu treffen, um die durch E-Mail entstandenen Sicherheitsrisiken zu reduzieren.

4.6.7.5 Sicherheit elektronischer Bürosysteme

Politiken und Richtlinien für die Kontrolle der Geschäfts- und Sicherheitsrisiken im Zusammenhang mit elektronischen Bürosystemen sind vorzubereiten und zu implementieren.

4.6.7.6 Öffentlich zugängliche Systeme

Es ist ein formaler Genehmigungsprozess einzurichten, bevor Informationen öffentlich bereitgestellt werden können, und die Integrität derartiger Informationen ist zu schützen, um unberechtigte Änderungen zu verhindern.

4.6.7.7 Andere Formen des Informationsaustausches

Es sind Verfahren und Maßnahmen zu implementieren, um den Austausch von Informationen über Sprach-, Fax- und Videokommunikationsgeräte zu schützen.

4.7 Zugangskontrolle

4.7.1 Geschäftsanforderungen an die Zugangskontrolle

Ziel: Kontrolle des Zugangs zu Informationen.

4.7.1.1 Zugangskontrollpolitik

Geschäftsanforderungen an eine Zugangskontrolle sind zu definieren und zu dokumentieren, und der Zugang ist auf das zu beschränken, was in der Zugangskontrollpolitik definiert ist.

4.7.2 Verwaltung der Zugriffsrechte der Benutzer

Ziel: Verhinderung des unberechtigten Zugriffs auf Informationssysteme.

4.7.2.1 Anmeldung von Benutzern

Es ist ein formales Anmeldungs- und Abmeldeverfahren für Benutzer einzurichten, um den Zugriff auf alle Multi-User-Informationssysteme und -dienste zu regeln.

4.7.2.2 Verwaltung von Privilegien

Die Zuteilung und Benutzung von Privilegien ist zu beschränken und zu überwachen.

4.7.2.3 Verwaltung von Benutzerpasswörtern

Die Zuteilung von Passwörtern ist durch einen formalen Verwaltungsprozess zu überwachen.

4.7.2.4 Überprüfung der Zugriffsrechte von Benutzern

Zur Überprüfung der Zugriffsrechte für Benutzer ist in regelmäßigen Abständen ein formaler Prozess durchzuführen.

4.7.3 Verantwortung der Benutzer

Ziel: Verhinderung eines unberechtigten Benutzerzugriffs.

4.7.3.1 Passwortgebrauch

Benutzer haben bei der Wahl und beim Gebrauch von Passwörtern adäquate Sicherheitspraktiken zu befolgen.

4.7.3.2 Unbeaufsichtigte Benutzergeräte

Benutzer haben sicherzustellen, dass unbeaufsichtigte Geräte entsprechend geschützt sind.

4.7.4 Netzzugriffskontrolle

Ziel: Schutz von vernetzten Diensten.

4.7.4.1 Politik zur Benutzung von Netzdiensten

Benutzern ist nur der direkte Zugriff auf Dienste, deren Benutzung ihnen ausdrücklich gestattet wurde, erlaubt.

4.7.4.2 Eingeschränkter Pfad

Der Pfad vom Benutzerterminal zum Rechnerdienst ist zu überwachen.

4.7.4.3 Benutzerauthentisierung für externe Verbindungen

Der Zugriff durch Benutzer an anderen Standorten ist von einer Authentisierung abhängig zu machen.

4.7.4.4 Knoten-Authentisierung

Verbindungen zu entfernten Rechnersystemen sind zu authentisieren.

4.7.4.5 Schutz des Ferndiagnoseports

Der Zugang zu Diagnoseports ist sicher zu überwachen.

4.7.4.6 Trennung in Netzwerken

Es sind Maßnahmen in Netzwerken zur Trennung von Informationsdiensten, Benutzergruppen und Informationssystemen zu treffen.

4.7.4.7 Kontrolle der Netzverbindung

Die Zugriffsberechtigungen von Benutzern in gemeinsamen Netzen ist über die unter 4.7.1.1 spezifizierte Zugangskontrollpolitik zu beschränken.

4.7.4.8 Netzrouting-Kontrolle

Für gemeinsame Netze sind Routing-Kontrollen vorzusehen, um sicherzustellen, dass Rechnerverbindungen und Informationsflüsse nicht gegen die Zugangskontrollpolitik für Geschäftsanwendungen (siehe 4.7.1.1) verstoßen.

4.7.4.9 Sicherheit von Netzdiensten

Es ist eine klare Beschreibung der Sicherheitsattribute aller von der Organisation benutzten Netzdienste vorzulegen.

4.7.5 Kontrolle des Betriebssystemzugriffs

Ziel: Verhinderung von unberechtigten Rechnerzugriffen.

4.7.5.1 Automatische Terminalidentifikation

Es ist eine automatische Terminalidentifikation zu verwenden, um Verbindungen mit spezifischen Standorten und tragbaren Geräten zu authentisieren.

4.7.5.2 Anmeldeverfahren an Terminals

Der Zugriff auf Informationsdienste hat über ein sicheres Anmeldeverfahren zu erfolgen.

4.7.5.3 Benutzeridentifikation und -authentisierung

Allen Benutzern ist eine einmalige Kennung (User-ID) für ihren persönlichen und alleinigen Gebrauch zuzuweisen, damit Aktivitäten auf die verantwortliche Einzelperson zurückgeführt werden können.

4.7.5.4 Passwortverwaltungssystem

Ein Passwortverwaltungssystem ist als effektive, interaktive Einrichtung einzurichten, durch die gute Passwörter sichergestellt werden.

4.7.5.5 Gebrauch von Systemdienstprogrammen

Die Benutzung von Systemdienstprogrammen ist zu beschränken und streng zu überwachen.

4.7.5.6 Zwangsalarm für die Sicherheit der Benutzer

Zwangsalarme sind für Benutzer einzurichten, die Ziel einer Nötigung sein könnten.

4.7.5.7 Terminal-Timeout

Unbenutzte Terminals an Standorten mit erhöhtem Risiko oder die risikogefährdeten Systemen dienen, sind zur Verhinderung des Zugangs durch unberechtigte Personen nach einer definierten Wartezeit abzuschalten.

4.7.5.8 Begrenzung der Verbindungsdauer

Verbindungsdauern sind zu beschränken, um eine zusätzliche Sicherheit für risikogefährdete Anwendungen zu schaffen.

4.7.6 Zugriffskontrolle für Anwendungen

Ziel: Verhinderung des unberechtigten Zugriffs auf Informationen, die sich in Informationssystemen befinden.

4.7.6.1 Beschränkung des Informationszugriffs

Der Zugriff auf Informationen und Anwendungssystemfunktionen ist gemäß der unter 4.7.1.1 spezifizierten Zugangskontrollpolitik zu beschränken.

4.7.6.2 Isolierung sensibler Systeme

Sensitive Systeme sind in einer dedizierten (isolierten) Rechnerumgebung aufzustellen.

4.7.7 Überwachung des Systemzugriffs und der Systembenutzung

Ziel: Aufdeckung unberechtigter Tätigkeiten.

4.7.7.1 Protokollieren von Vorfällen

Auditprotokolle, in denen Ausnahmefälle und andere sicherheitsrelevante Vorfälle verzeichnet werden, sind zu erstellen und über einen vereinbarten Zeitraum aufzubewahren, um zukünftige Untersuchungen und die Überwachung der Zugangskontrolle zu unterstützen.

4.7.7.2 Kontrolle der Systembenutzung

Es sind Verfahren zur Kontrolle der Benutzung von Geräten zur Informationsverarbeitung zu entwickeln, und das Ergebnis der Kontrolltätigkeiten ist in regelmäßigen Abständen zu überprüfen.

4.7.7.3 Uhrensynchronisation

Rechneruhren sind zu synchronisieren, um exakte Aufzeichnungen zu garantieren.

4.7.8 Mobile Computing und Telearbeit

Ziel: Informationssicherheit beim Einsatz von Mobile Computing und Telearbeit.

4.7.8.1 Mobile Computing

Zum Schutz vor Risiken, die beim Arbeiten mit Mobile Computing-Geräten und insbesondere in ungeschützten Umgebungen entstehen, sind eine formale Politik einzuführen und entsprechende Maßnahmen zu treffen.

4.7.8.2 Telearbeit

Es sind Politiken und Verfahren zur Genehmigung und Überwachung der Telearbeit zu entwickeln.

4.8 Systementwicklung und -wartung

4.8.1 Sicherheitsanforderungen an Systeme

Ziel: Sicherheit in Informationssysteme einzubauen.

4.8.1.1 Analyse und Spezifikation der Sicherheitsanforderungen

In Geschäftsanforderungen für neue Systeme oder für Verbesserungen an bestehenden Systemen sind die Forderungen für Maßnahmen zu spezifizieren.

4.8.2 Sicherheit in Anwendungssystemen

Ziel: Verhinderung von Verlust, Änderung oder Missbrauch von Benutzerdaten in Anwendungssystemen.

4.8.2.1 Validierung der Eingabedaten

Die Dateneingabe in Anwendungssysteme ist zu validieren, um sicherzustellen, dass sie korrekt und passend ist.

4.8.2.2 Kontrolle der internen Verarbeitung

In Systeme sind Validierungsprüfungen zu integrieren, um Verfälschungen der verarbeiteten Daten zu erkennen.

4.8.2.3 Nachrichtenauthentisierung

Nachrichtenauthentisierung ist in Anwendungen einzusetzen, bei denen eine Sicherheitsanforderung besteht, die Integrität des Nachrichteninhalts zu schützen.

4.8.2.4 Validierung der Ausgabedaten

Datenausgaben aus einem Anwendungssystem sind zu validieren, um sicherzustellen, dass die gespeicherten Informationen richtig verarbeitet wurden und den Umständen angemessen sind.

4.8.3 Kryptographische Maßnahmen

Ziel: Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen.

4.8.3.1 Politik für den Einsatz kryptographischer Maßnahmen

Eine Politik für den Einsatz kryptographischer Maßnahmen zum Schutz von Informationen ist zu entwickeln und zu befolgen.

4.8.3.2 Verschlüsselung

Zum Schutz der Vertraulichkeit sensitiver oder kritischer Informationen sind Verschlüsselungsmethoden einzusetzen.

4.8.3.3 Digitale Signaturen

Zum Schutz der Authentizität und Integrität elektronischer Informationen sind digitale Signaturen zu verwenden.

4.8.3.4 Nicht-Abstreitbarkeitservice

Der Nicht-Abstreitbarkeitservice ist zur Lösung von Streitfällen über den Vorfall bzw. Nicht-Vorfall eines Ereignisses oder einer Tat zu verwenden.

4.8.3.5 Schlüsselmanagement

Zur Unterstützung der kryptographischen Verfahren ist ein Schlüsselmanagementsystem zu verwenden, das auf vereinbarten Normen, Verfahren und Methoden beruht.

4.8.4 Sicherheit von Systemdateien

Ziel: Gewährleistung, dass IT-Projekte und Supportaktivitäten auf sichere Art und Weise durchgeführt werden.

4.8.4.1 Kontrolle von Software in laufenden Systemen

Die Implementierung von Software in laufenden Systemen ist zu kontrollieren.

4.8.4.2 Schutz von Systemtestdaten

Testdaten sind zu schützen und zu kontrollieren.

4.8.4.3 Zugriffskontrolle zur Programmquellenbibliothek

Der Zugriff auf Programmquellenbibliotheken ist streng zu kontrollieren.

4.8.5 Sicherheit bei Entwicklungs- und Supportprozessen

Ziel: Sicherheit von Software und Informationen im Anwendungssystem erhalten.

4.8.5.1 Änderungskontrollverfahren

Zur Minimierung von Verfälschungen in Informationssystemen sind Implementierungen von Änderungen über formale Änderungskontrollverfahren streng zu kontrollieren.

4.8.5.2 Technische Beurteilung der Änderungen am Betriebssystem

Anwendungssysteme sind nach Änderungen zu überprüfen und zu testen.

4.8.5.3 Beschränkungen für Änderungen an Softwarepaketen

Von Änderungen an Softwarepaketen ist abzuraten, und grundlegende Änderungen sind streng zu kontrollieren.

4.8.5.4 Verdeckte Kanäle und trojanischer Code

Der Kauf, die Benutzung und Änderung von Software sind zum Schutz vor eventuellen verdeckten Kanälen und trojanischem Code zu kontrollieren und zu prüfen.

4.8.5.5 Softwareentwicklung außerhalb der Organisation (Outsourcing)

Zur Sicherung von Softwareentwicklungen außerhalb der Organisation sind Maßnahmen zu treffen.

4.9 Management des kontinuierlichen Geschäftsbetriebs

4.9.1 Aspekte zur Aufrechterhaltung des Geschäftsbetriebs

Ziel: Einleitung von Maßnahmen gegen Unterbrechungen von Geschäftsaktivitäten und Schutz der kritischen Geschäftsprozesse vor den Auswirkungen großer Ausfälle oder Katastrophen.

4.9.1.1 Prozess für das Management des kontinuierlichen Geschäftsbetriebs

Organisationsweit ist ein verwalteter Prozess für die Entwicklung und Aufrechterhaltung des Geschäftsbetriebs einzuführen.

4.9.1.2 Aufrechterhaltung des Geschäftsbetriebs und Auswirkungsanalyse

Es ist ein strategischer Plan, beruhend auf einer entsprechenden Risikoanalyse, für den Gesamtansatz zur Aufrechterhaltung des Geschäftsbetriebs zu entwickeln.

4.9.1.3 Verfassen und Implementieren von Plänen zur Aufrechterhaltung des Geschäftsbetriebs

Es sind Pläne zur Aufrechterhaltung oder zügigen Wiederherstellung von Geschäftsabläufen nach einer Unterbrechung oder dem Ausfall kritischer Geschäftsprozesse zu entwickeln.

4.9.1.4 Rahmen für die Pläne zur Aufrechterhaltung des Geschäftsbetriebs

Es ist ein Rahmen für Pläne zur Aufrechterhaltung des Geschäftsbetriebs aufrechtzuerhalten, damit die Konsistenz aller Pläne gewährleistet wird und Prioritäten für das Testen und das Aufrechterhalten der Pläne identifiziert werden.

4.9.1.5 Testen, Aufrechterhaltung und erneute Analyse von Plänen zur Gewährleistung des kontinuierlichen Geschäftsbetriebs

Pläne zur Aufrechterhaltung des Geschäftsbetriebs sind in regelmäßigen Abständen zu testen und zu überprüfen, um ihre Aktualität und Effektivität sicherzustellen.

4.10 Einhaltung der Verpflichtungen

4.10.1 Einhaltung gesetzlicher Verpflichtungen

Ziel: Vermeidung von Verletzungen jeglicher Gesetze des Straf- oder Zivilrechts, gesetzlicher, behördlicher oder vertraglicher Verpflichtungen und jeglicher Sicherheitsanforderungen.

4.10.1.1 Identifikation anwendbarer Gesetze

Für jedes Informationssystem sind alle relevanten gesetzlichen, behördlichen und vertraglichen Anforderungen explizit zu definieren und zu dokumentieren.

4.10.1.2 Rechte zum Schutz des geistigen Eigentums

Es sind geeignete Verfahren zu implementieren, um zu gewährleisten, dass rechtliche Beschränkungen über den Gebrauch von Material, für das Rechte zum Schutz des geistigen Eigentums bestehen, und über den Gebrauch proprietärer Softwareprodukte eingehalten werden.

4.10.1.3 Schutzmaßnahmen für organisationseigene Aufzeichnungen

Wichtige Aufzeichnungen einer Organisation sind vor Verlust, Zerstörung und Fälschung zu schützen.

4.10.1.4 Datenschutz und Geheimhaltung persönlicher Informationen

Es sind Maßnahmen zu treffen, um persönliche Informationen gemäß der relevanten Gesetzgebung zu schützen.

4.10.1.5 Vorbeugung gegen den Missbrauch von Geräten zur Informationsverarbeitung

Die Benutzung von Geräten zur Informationsverarbeitung ist vom Management zu genehmigen, und es sind Maßnahmen zu treffen, um den Missbrauch solcher Geräte zu verhindern.

4.10.1.6 Regelung kryptographischer Maßnahmen

Es sind Maßnahmen zu treffen, um sicherzustellen, dass nationale Vereinbarungen, Gesetze, Regelungen oder andere Instrumente zur Kontrolle des Zugriffs auf oder der Verwendung von kryptographischen Maßnahmen eingehalten werden.

4.10.1.7 Sammeln von Beweisen

Sofern es sich bei der Ahndung einer Straftat einer Person oder Organisation um ein gerichtliches Verfahren, ob zivil- oder strafrechtlich, handelt, haben die vorgelegten Beweise im Einklang mit den Regeln für Beweise zu stehen, die im relevanten Gesetz oder in den Regeln des spezifischen Gerichts niedergelegt sind, vor dem der Fall verhandelt wird. Dazu gehört auch die Einhaltung aller veröffentlichten Normen oder Leitfäden für die Erstellung zulässiger Beweise.

4.10.2 Überprüfung der Sicherheitspolitik und technischen Normerfüllung

Ziel: Sicherstellung der Erfüllung organisationseigener Sicherheitspolitiken und Normen durch Systeme.

4.10.2.1 Einhaltung der Sicherheitspolitik

Von Managern ist sicherzustellen, dass alle Sicherheitsverfahren innerhalb ihres jeweiligen Verantwortungsbereichs korrekt ausgeführt werden, und alle Bereiche innerhalb der Organisation sind einer regelmäßigen Überprüfung zu unterziehen, um die Einhaltung der Sicherheitspolitiken und -normen sicherzustellen.

4.10.2.2 Prüfung der Einhaltung technischer Normen

Informationssysteme sind regelmäßig auf die Einhaltung der Normen für die Sicherheitsimplementierung zu prüfen.

4.10.3 Überlegungen zum Systemaudit

Ziel: Maximierung der Effektivität und Minimierung der Störungen beim Systemauditprozess.

4.10.3.1 Maßnahmen für Systemaudits

Audits an laufenden Systemen sind zu planen und zu vereinbaren, um das Risiko von Störungen der Geschäftsprozesse zu minimieren.

4.10.3.2 Schutz der Systemaudittools

Der Zugang zu Systemaudittools ist zu schützen, um einen möglichen Missbrauch oder eine Kompromittierung zu verhindern.

Annex A (informativ)
Änderungen bei der internen Nummerierung

Tabelle A. 1 zeigt die Beziehung zwischen den Abschnittsnummern der ersten Ausgabe dieses Teils der BS 7799 und den Abschnittsnummern dieser Ausgabe.

Tabelle A.1 – Beziehung zwischen internen Nummerierungen in verschiedenen Ausgaben dieses Teils der BS 7799

Abschnittsnummer der Ausgabe 1998	Abschnittsnummer der Ausgabe 1999
Einleitung	Einleitung
I Allgemeines	
1.1 Anwendungsbereich	1 Anwendungsbereich
1.2 Definitionen	2 Begriffe und Definitionen
2 Anforderungen an das	3 Anforderungen an das
Managementsystem für	Managementsystem für
Informationssicherheit	Informationssicherheit
2.1 Allgemeines	3.1 Allgemeines
2.2 Schaffung eines	3.2 Schaffung eines Verwaltungsrahmens
Verwaltungsrahmens	
2.3 Implementierung	3.3 Implementierung
2.4 Dokumentation	3.4 Dokumentation
2.5 Kontrolle der Unterlagen	3.5 Kontrolle der Unterlagen
2.6 Aufzeichnungen	3.6 Aufzeichnungen
3 Spezifische Maßnahmen	4 Spezifische Maßnahmen
3.1 Informationssicherheitspolitik	4.1 Sicherheitspolitik
3.2 Organisation der Sicherheit	4.2 Organisation der Sicherheit
3.3 Klassifizierung und Überwachung	4.3 Einstufung und Kontrolle der Werte
der Anlagen und Bestände	
3.4 Sicherheit des Personals	4.4 Personelle Sicherheit
3.5 Physische und umgebungsbezogene	4.5 Physische und umgebungsbezogene
Sicherheit	Sicherheit
3.6 Rechner- und Netzverwaltung	4.6 Management der Kommunikation und
	des Betriebs
3.7 Systemzugriffskontrolle	4.7 Zugangskontrolle
3.8 Systementwicklung und -wartung	4.8 Systementwicklung und -wartung
3.9 Geschäftskontinuitätsplanung	4.9 Management des kontinuierlichen
	Geschäftsbetriebs
3.10 Einhaltung der Verpflichtungen	4.10 Einhaltung der Verpflichtungen

Literaturhinweise

**Veröffentlichungen von Normen
BRITISH STANDARDS INSTITUTION, London**

**BS7799- 1:1999, Management von Informationssicherheit Teil 1 Leitfaden zum
Management von Informationssicherheit**