

Prüfkatalog nach DIN ISO/IEC 27001

Zum Inhalt

Konzeption, Implementierung und Aufrechterhaltung eines Informationssicherheits Managementsystems sollten sich an einem Prüfkatalog orientieren, der sowohl für die kontinuierliche Überprüfung während der Aufbau- und der Betriebsphase als auch zur Vorbereitung auf eine ggf. geplante Zertifizierung des Systems geeignet ist.

Ein solcher Prüfkatalog auf Basis der Norm DIN ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Management-

systeme – Anforderungen“ wird im Beitrag dargestellt und erläutert. Der Katalog kann auch für Planungszwecke verwendet werden.

Arbeitshilfen:
Prüfkatalog zur Dokumentation und Bewertung
Muster für Feststellungsberichte

Autoren: Dieter Burgartz
Angelika Plate
E-Mail: dieter.burgartz@picconsult.de
aaxisap@aol.com

1 Einleitung und Überblick

Beispiele für IT- und Information Security Standards

Zur Unterstützung beim Aufbau und Betrieb von Informationssicherheits-Managementsystemen (ISMS) und/oder IT-Sicherheitsmanagement wurden in den letzten Jahren mehrere (konkurrierende) Ansätze entwickelt

Als Beispiele seien hier genannt:

- DIN ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Management-systeme – Anforderungen“
- CobiT: Control Objectives for Information and Related Technologies
- IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik

Für welchen Ansatz man sich auch entscheidet, stets wird die Notwendigkeit bestehen oder es wird wünschenswert sein, dass man

- für Zwecke der Planung,
- zur Sachstandsverfolgung beim Aufbau und in der Betriebsphase,
- zur Vorbereitung eines internen Audits
- oder zur Vorbereitung einer anstehenden Zertifizierung

über einen Prüfkatalog verfügt, der geeignet ist, die Vollständigkeit, Angemessenheit und Wirksamkeit der zu erzielenden Lösung nach dem jeweiligen Standard zu überprüfen und zu dokumentieren.

DIN ISO/IEC 27001

Ein Prüfkatalog auf Basis der DIN ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“ wird im Folgenden vorgestellt und erläutert.

2 Aufbau des Prüfkataloges



03660_a.doc

Der Prüfkatalog orientiert sich an der Norm DIN ISO/IEC 27001.

Das Kapitel 2 des Prüfkataloges umfasst die Forderungen dieser Norm aus deren Kapiteln 4 bis 8 (siehe Tabelle 1).

Die Kapitel 3 bis 13 des Prüfkataloges entsprechen den „Maßnahmenzielen (control objectives) und Maßnahmen (controls)“ im Anhang A der Norm (dort die Abschnitte A.5 bis A.15 – siehe Tabelle 2), die auf Basis einer Risikoeinschätzung auszuwählen sind.

Tabelle 1: Forderungen der Norm ISO/IEC 27001

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
2.1	4	Informationssicherheits-Managementsystem (Information security management system)
2.1.1	4.1	Allgemeine Anforderungen (General requirements)
2.1.2	4.2	Festlegung und Verwaltung des ISMS (Establishing and managing the ISMS)
2.1.2.1	4.2.1	Festlegen des ISMS (Establish the ISMS)
2.1.2.2	4.2.2	Umsetzen und Durchführen des ISMS (Implement and operate the ISMS)
2.1.2.3	4.2.3	Überwachen und Überprüfen des ISMS (Monitor and review the ISMS)
2.1.2.4	4.2.4	Instandhalten und Verbessern des ISMS (Maintain and improve the ISMS)
2.1.3	4.3	Dokumentationsanforderungen (Documentation requirements)
2.1.3.1	4.3.1	Allgemeines (General)
2.1.3.2	4.3.2	Lenkung von Dokumenten (Control of documents)
2.1.3.3	4.3.3	Lenkung von Aufzeichnungen (Control of records)
2.2	5	Verantwortung des Managements (Management responsibility)
2.2.1	5.1	Verpflichtung des Managements (Management commitment)

Tabelle 1: Forderungen der Norm ISO/IEC 27001 – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
2.2.2	5.2	Management von Ressourcen (Resource management)
2.2.2.1	5.2.1	Bereitstellung von Ressourcen (Provision of resources)
2.2.2.2	5.2.2	Schulungen, Bewusstsein und Kompetenz (Training, awareness and competence)
2.3	6	Interne ISMS-Audits (Internal ISMS audits)
2.4	7	Managementbewertung des ISMS (Management review of the ISMS)
2.4.1	7.1	Allgemeines (General)
2.4.2	7.2	Eingaben für die Bewertung (Review input)
2.4.3	7.3	Ergebnisse der Bewertung (Review output)
2.5	8	Verbesserung des ISMS (ISMS improvement)
2.5.1	8.1	Ständige Verbesserung (Continual improvement)
2.5.2	8.2	Korrekturmaßnahmen (Corrective action)
2.5.3	8.3	Vorbeugungsmaßnahmen (Preventive action)

Tabelle 2: Maßnahmenziele (control objectives)

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
3	A.5	Sicherheitsleitlinie (Security policy)
3.1	A.5.1	Informationssicherheitsleitlinie (Information security policy)
4	A.6	Organisation der Informationssicherheit (Organization of information security)
4.1	A.6.1	Interne Organisation (Internal organization)
4.2	A.6.2	Externe Beziehungen (External parties)
5	A.7	Management von organisationseigenen Werten (Asset Management)
5.1	A.7.1	Verantwortung für organisationseigene Werte (Responsibility for assets)
5.2	A.7.2	Klassifizierung von Informationen (Information classification)
6	A.8	Personelle Sicherheit (Human resources security)
6.1	A.8.1	Vor der Anstellung (Prior to employment)
6.2	A.8.2	Während der Anstellung (During employment)
6.3	A.8.3	Beendigung oder Änderung der Anstellung (Termination or change of employment)
7	A.9	Physische und umgebungsbezogene Sicherheit (Physical and environmental security)

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
7.1	A.9.1	Sicherheitsbereiche (Secure areas)
7.2	A.9.2	Sicherheit von Betriebsmitteln (Equipment security)
8	A.10	Betriebs- und Kommunikationsmanagement (Communications and operations management)
8.1	A.10.1	Verfahren und Verantwortlichkeiten (Operational procedures and responsibilities)
8.2	A.10.2	Management der Dienstleistungs-Erbringung von Dritten (Third party service delivery management)
8.3	A.10.3	Systemplanung und Abnahme (System planning and acceptance)
8.4	A.10.4	Schutz vor Schadsoftware und mobilem Programmcode (Protection against malicious and mobile code)
8.5	A.10.5	Backup (Back-up)
8.6	A.10.6	Management der Netzsicherheit (Network security management)
8.7	A.10.7	Handhabung von Speicher- und Aufzeichnungsmedien (Media handling)
8.8	A.10.8	Austausch von Informationen (Exchange of information)

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
8.9	A.10.9	E-Commerce-Anwendungen (Electronic commerce services)
8.10	A.10.10	Überwachung (Monitoring)
9	A.11	Zugangskontrolle (Access control)
9.1	A.11.1	Geschäftsanforderungen für Zugangskontrolle (Business requirement for access control)
9.2	A.11.2	Benutzerverwaltung User access management
9.3	A.11.3	Benutzerverantwortung User responsibilities
9.4	A.11.4	Zugangskontrolle für Netze Network access control
9.5	A.11.5	Zugangskontrolle auf Betriebssysteme Operating system access control
9.6	A.11.6	Zugangskontrolle zu Anwendungen und Information (Application and information access control)
9.7	A.11.7	Mobile Computing und Telearbeit (Mobile computing and teleworking)
10	A.12	Beschaffung, Entwicklung und Wartung von Informationssystemen (Information systems acquisition, development and maintenance)

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
10.1	A.12.1	Sicherheitsanforderungen von Informationssystemen (Security requirements of information systems)
10.2	A.12.2	Korrekte Verarbeitung in Anwendungen (Correct processing in application)
10.3	A.12.3	Kryptographische Maßnahmen (Cryptographic controls)
10.4	A.12.4	Sicherheit von Systemdateien (Security of system files)
10.5	A.12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen (Security in development and support processes)
10.6	A.12.6	Schwachstellenmanagement (Technical Vulnerability Management)
11	A.13	Umgang mit Informationssicherheitsvorfällen (Information security incident management)
11.1	A.13.1	Melden von Informationssicherheitsereignissen und Schwachstellen (Reporting information security events and weaknesses)
11.2	A.13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen (Management of information security incidents and improvements)
12	A.14	Sicherstellung des Geschäftsbetriebs – Business Continuity Management (Business continuity management)

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Normabschnitt	Forderung(en)
12.1	A.14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs – Business Continuity Management (Information security aspects of business continuity management)
13	A.15	Einhaltung von Vorgaben (Compliance)
13.2	A.15.1	Einhaltung gesetzlicher Vorgaben (Compliance with legal requirements)
13.3	A.15.2	Einhaltung von Sicherheitsregelungen und-standards, und technischer Vorgaben (Compliance with security policies and standards, and technical compliance)
13.4	A.15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen (Information systems audit considerations)

Der Prüfkatalog ist formularmäßig wie in Tabelle 3 dargestellt aufgebaut.

Tabelle 3: Schema des Prüfkataloges

Prüfpunkt/Prüfgegenstand							
Forderung/ Thema	unter- sucht	festgelegt		Praxis		Bewertung	
		Quelle/ Kommentar	B	Kommentar	B	Risiko	FB

Prüfpunkt/-gegenstand Der Katalog besteht aus den in den Tabellen 1 und 2 dargestellten Prüfpunkten bzw. Prüfgegenständen wie z. B. „2.2.2.2 [5.2.2] Schulungen, Bewusstsein und Kompetenz“.

Forderungen Zu jedem Prüfpunkt/-gegenstand sind ein oder mehrere Forderungen aufgeführt. Jede Forderung ist wie folgt zu kommentieren bzw. zu bewerten:

Untersucht? Spalte untersucht
Wurde die Erfüllung der Forderung untersucht?
Mögliche Antworten: Ja
Nein
NR (entfällt, da nicht relevant)
Bei Antwort „NR“ sollte ggf. dokumentiert werden, warum eine Forderung nicht relevant ist.

Festgelegt? Spalte festgelegt
Hier ist anzugeben, ob zu einer Forderung Dokumente bzw. dokumentierte Prozesse im Sinne von Verfahrensanweisungen, Arbeitsanweisungen, Richtlinien, Konzepten, Handbüchern usw. vorhanden sind und ob diese die Forderung angemessen und wirksam erfüllen.
Unter „Quelle/Kommentar“ kann das entsprechende Dokument angegeben und kommentiert werden.

Beispiel: Organisatorische Arbeitsplatzrichtlinie Nr. IS-04-06
Die Festlegungen im Kapitel E-Mail-Nutzung sind zu global.

In der Spalte B erfolgt die Bewertung der Dokumentation nach dem Schema:

- 0 nicht erfüllt
- 1 teilweise erfüllt
- 2 weitgehend erfüllt
- 3 voll erfüllt

Praxis?Spalte **Praxis**

Hier ist anzugeben, ob und wie die festgelegten Verfahren, Richtlinien usw. in der betrieblichen Praxis umgesetzt und angewendet werden.

Unter „Kommentar“ kann die betriebliche Praxis verbal kommentiert und bewertet werden.

Beispiel: Die Richtlinie IS-04-06 ist bei den Mitarbeitern nur zum Teil bekannt: teilweise auch nur in einer veralteten Version.

In der Spalte B erfolgt die Bewertung der betrieblichen Praxis:

0 nicht erfüllt

1 teilweise erfüllt

2 weitgehend erfüllt

3 voll erfüllt

Bewertung?Spalte **Bewertung**

Hier ist zusammenfassend zu bewerten, ob eine Forderung angemessen und wirksam erfüllt ist. In diese Gesamtbeurteilung gehen die Teilaspekte „festgelegt“ und „Praxis“ mit ihren jeweiligen Einzelbewertungen ein. Diese Bewertung erfolgt durch Einstufung in eine „Risikokategorie“ (siehe Tabelle 4).

Es wird empfohlen, die relativ abstrakten Definitionen der o. a. Risikokategorien unternehmensspezifisch zu konkretisieren, damit die Einstufungen handhabbar und nachvollziehbar werden. Hierzu bietet sich z. B. an, die Risikokategorien über die Kriterien Eintrittswahrscheinlichkeit und Schadenshöhe (materiell/immateriell) oder andere Kennzahlen abzugrenzen.

**Feststellungs-
berichte**

03660_b.doc

Spalte FB

Bei Empfehlungen und Risikoeinstufungen kann die Spalte FB verwendet werden, um z. B. auf einen „Feststellungsbericht“ (laufende Nr. oder Ähnliches) zu verweisen, in dem nähere Angaben zur Bewertung und zu den vereinbarten Korrektur- oder Verbesserungsmaßnahmen festgelegt sind. Ein Muster für einen solchen Feststellungsbericht liegt auf der CD-ROM vor.

Tabelle 4: Risikokategorien

<i>Risiko- kategorie</i>		<i>Erläuterung</i>
-	kein Risiko	Es liegt kein erkennbares Risiko vor. Die Forderung/der Prozess ist angemessen und wirksam festgelegt und umgesetzt.
E	Empfehlung	Es liegt kein erkennbares Risiko vor; es wird dennoch eine Empfehlung ausgesprochen. Empfehlungen dienen der Verbesserung von Prozessen und Maßnahmen. Die Umsetzung einer Empfehlung liegt im Ermessen des Unternehmens.
N	niedrig	Es liegt ein leichtes Defizit vor. Korrekturmaßnahmen sollten vereinbart und in einem angemessenen Zeitraum durchgeführt werden.
M	mittel	Es liegt ein mittleres Defizit vor. Korrekturmaßnahmen müssen vereinbart und terminiert werden. Die Umsetzung der Korrekturmaßnahmen wird überwacht.
H	hoch	Es liegt ein erhebliches Defizit vor. Korrekturmaßnahmen müssen vereinbart und terminiert werden. Die Umsetzung der Korrekturmaßnahmen erfolgt mit hoher Priorität und wird kontinuierlich überwacht.

3 Anwendung des Prüfkataloges

Wie bereits oben dargelegt kann der Prüfkatalog in unterschiedlichen Phasen eines ISMS angewendet werden.

Beim Aufbau eines ISMS kann in der Planungsphase in der Spalte „Quelle/Kommentar“ vermerkt werden, welche Festlegungen (Dokumente) bereits bestehen und welche noch zu erstellen sind.

In der Spalte „Praxis“ kann vermerkt werden, welche Maßnahmen zur Umsetzung und Einführung erforderlich sind (z. B. spezielle Schulungsmaßnahmen).

Projekt- kontrolle

In den Spalten „Quelle/Kommentar“ und „Praxis“ kann der jeweils aktuelle Stand des Projektes „Aufbau des ISMS“ dokumentiert werden.

Die Planung, Durchführung und Dokumentation eines internen ISMS-Audits oder Check-ups ist der Schwerpunkt des hier vorgestellten Prüfkataloges.

Bei der Vorbereitung auf ein externes Audit dient die Anwendung des Prüfkatalogs zur eigenen Standortbestimmung. Ist eine Zertifizierung nach DIN ISO/IEC 27001: 2005 angestrebt, so ist es empfehlenswert, von der ausgewählten Prüfstelle/Zertifizierungsstelle deren Prüfkatalog einzusehen.

4 Anpassung des Prüfkataloges

Der vorgestellte Prüfkatalog sollte – insbesondere bei regelmäßigem Gebrauch für interne Zwecke – unternehmensspezifisch angepasst und ergänzt werden.

**Literatur-
verzeichnis**

- [1] DIN ISO/IEC 27001
Informationstechnik – IT Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Managementsysteme – Anforderungen, Originaltitel (englisch):
Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001)

- [2] DIN ISO/IEC 27002
Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management, Originaltitel (englisch): Information technology – Security techniques – Code of practice for information security management (ISO/IEC 27002)