Prüfkatalog nach 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 ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – 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
E-Mail: dieter.burgartz@piqconsult.de

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:

- ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – 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.

ISO/IEC 27001

Ein Prüfkatalog auf Basis der 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 ISO/IEC 27001.

Das Kapitel 2 des Prüfkataloges umfasst die Forderungen dieser Norm aus deren Kapiteln 4 bis 10 (siehe Tabelle 1).

Die Kapitel 3 bis 16 des Prüfkataloges entsprechen den „Maßnahmenzielen (control objectives) und Maßnahmen (controls)" im Anhang A der Norm (dort die Abschnitte A.5 bis A.18 – siehe Tabelle 2), die auf Basis einer Risikoeinschätzung auszuwählen sind.

Tabelle 1: Forderungen der Norm ISO/IEC 27001

Prüfkatalog Abschnitt	Kapitel/ Abschnitt der Norm	Forderungen
2.1	4	Kontext der Organisation
2.1.1	4.1	Verständnis der Organisation und ihres Kontexts
2.1.2	4.2	Verständnis der Bedürfnisse und Erwartungen interessierter Parteien
2.1.3	4.3	Festlegung des Geltungsbereichs des Informations-sicherheits-Managementsystems
2.1.4	4.4	Informationssicherheits-Managementsystem
2.2	5	Führung
2.2.1	5.1	Führung und Engagement
2.2.2	5.2	Leitlinie
2.2.3	5.3	Organisatorische Aufgaben, Zuständigkeiten und Befugnisse
2.3	6	Planung
2.3.1	6.1	Maßnahmen zum Umgang mit Risiken und Chancen
2.3.2	6.2	Informationssicherheitsziele und Pläne für deren Erreichung
2.4	7	Unterstützung
2.4.1	7.1	Ressourcen
2.4.2	7.2	Kompetenz
2.4.3	7.3	Bewusstsein
2.4.4	7.4	Kommunikation
2.4.5	7.5	Dokumentierte Informationen
2.5	8	Einsatz
2.5.1	8.1	Einsatzplanung und -kontrolle
2.5.2	8.2	Informationssicherheitsrisikoeinschätzung
2.5.3	8.3	Informationssicherheitsrisikobehandlung

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

Prüfkatalog Abschnitt	Kapitel/ Abschnitt der Norm	Forderungen
2.6	9	Leistungsauswertung
2.6.1	9.1	Überwachung, Messung, Analyse und Auswertung
2.6.2	9.2	Internes Audit
2.6.3	9.3	Prüfung durch die Leitung
2.7	10	Verbesserung
2.7.1	10.1	Fehler und Korrekturmaßnahmen
2.7.2	10.2	Laufende Verbesserung

Tabelle 2: Maßnahmenziele (control objectives)

Prüfkatalog Abschnitt	Kapitel/ Abschnitt der Norm	Sicherheitsmaßnahmen
3	A5	Sicherheitsleitlinien
3.1	A5.1	Vorgaben der Leitung zur Informationssicherheit
4	A6	Organisation der Informationssicherheit
4.1	A6.1	Interne Organisation
4.2	A6.2	Mobilgeräte und Telearbeit
5	A7	Sicherheit des Personals
5.1	A7.1	Vor der Einstellung
5.2	A7.2	Während der Anstellung
5.3	A7.3	Beendigung und Wechsel der Anstellung
6	A8	Wertemanagement
6.1	A8.1	Verantwortung für Werte
6.2	A8.2	Klassifizierung von Informationen
6.3	A8.3	Umgang mit Medien

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Abschnitt der Norm	Sicherheitsmaßnahmen
7	A9	Zugriffskontrolle
7.1	A9.1	Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle
7.2	A9.2	Benutzerverwaltung
7.3	A9.3	Benutzerverantwortung
7.4	A9.4	Kontrolle des Zugangs auf Systeme und Anwendungen
8	A10	Kryptographie
8.1	A10.1	Kryptographische Maßnahmen
9	A11	Schutz vor physischem Zugang und Umwelteinflüssen
9.1	A11.1	Sicherheitsbereiche
9.2	A11.2	Betriebsmittel
10	A12	Betriebssicherheit
10.1	A12.1	Betriebsverfahren und Zuständigkeiten
10.2	A12.2	Schutz vor Malware
10.3	A12.3	Datensicherungen
10.4	A12.4	Protokollierung und Überwachung
10.5	A12.5	Kontrolle von Software im Betrieb
10.6	A12.6	Mangement technischer Schwachstellen
10.7	A12.7	Auswirkungen von Audits auf Informationssysteme
11	A13	Sicherheit in der Kommunikation
11.1	A13.1	Netzwerksicherheitsmanagement
11.2	A13.2	Informationsübertragung
12	A14	Anschaffung, Entwicklung und Instandhaltung von Systemen
12.1	A14.1	Sicherheitsanforderungen für Informationssysteme

Tabelle 2: Maßnahmenziele (control objectives) – Fortsetzung

Prüfkatalog Abschnitt	Kapitel/ Abschnitt der Norm	Sicherheitsmaßnahmen
12.2	A14.2	Sicherheit in Entwicklungs- und Unterstützungs-prozessen
12.3	A14.3	Prüfdaten
13	A15	Lieferantenbeziehungen
13.1	A15.1	Sicherheit in Lieferantenbeziehungen
13.2	A15.2	Management der Dienstleistungserbringung durch Lieferanten
14	A16	Management von Informationssicherheitsvorfällen
14.1	A16.1	Management von Informationssicherheitsvorfällen und Verbesserungen
15	A17	Informationssicherheitsaspekte des Business Continuity Management
15.1	A17.1	Kontinuität der Informationssicherheit
15.2	A17.2	Redundanzen
16	A18	Richtlinienkonformität
16.1	A18.1	Informationssicherheitsprüfungen
16.2	A18.2	Einhaltung gesetzlicher und vertraglicher Anforderungen

Der Prüfkatalog ist formularmäßig wie in Tabelle 3 dargestellt aufgebaut.

Tabelle 3: Schema des Prüfkataloges

Prüfpunkt/Prüfgegenstand							
		festgelegt		*Praxis*		*Bewertung*	
Forderung/ Thema	*unter-sucht*	*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. „2.5.3 [8.3] Informationssicherheitsbehandlung“.

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

	Risiko-kategorie	***Erläuterung***
-	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).

Projektkontrolle

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 angestrebt, so ist es empfehlenswert, von der ausgewählten Prüfstelle/Zertifizierungsstelle deren Püfkatalog einzusehen.

4 Anpassung des Prüfkataloges

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

Quellen

[1] ISO/IEC 27001:2013
Informationstechnik – IT Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, Originaltitel (englisch):
Information technology – Security techniques – Information security management systems – Requirements

[2] ISO/IEC 27002:2013
Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen, Originaltitel (englisch): Information technology – Security techniques – Code of practice for information security controls

