THATER & SCHWIER
CONSULTING

Checkliste

ISO/IEC 27001:2013

Dokumente und Aufzeichnungen

Version: 1.1

Datum: 01.06.2016

Änderungsverfolgung

Version	Datum	Geänderte Seiten / Kapitel	Autor	Bemerkungen
1.0	07.01.2016	Alle	F. Thater	Initiale Erstellung
1.1	01.06.2016	Alle	F. Thater	Ergänzung der Hinweise zum Inhalt der Dokumente

1 Obligatorische Dokumente

1.1 Dokumente

Die folgenden Richtlinien, Verfahren und Dokumente müssen zwingend für ein ISMS erstellt werden und als dokumentierte Information vorliegen.

Bezeichnung / Beschreibung	**Definiert in ISO/IEC 27001:2013, Abschnitt**
Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems (ISMS) *Wofür soll das ISMS gelten? Welcher Kontext ist relevant?* *Welche Parteien sind interessiert und wie lauten deren Anforderungen?* *Welche Schnittstellen gibt es? Was wird selbst, was von anderen durchgeführt?*	4.3
Informationssicherheitspolitik und Zielvorgaben *Welche Sicherheitsziele gibt es? (wenn möglich, messbare Ziele wählen)* *Verpflichtungserklärung, dass diese auch umgesetzt werden* *Verpflichtungserklärung zur kontinuierlichen Verbesserung* *Bekanntmachung im Unternehmen*	5.2 6.2
Informationssicherheitsrisikobeurteilung (Methodik zur Risikoeinschätzung und -behandlung) *Festlegung der Risikoakzeptanz* *Verfahren zur Risikobewertung (Vergleichbarkeit, Reproduzierbarkeit, Konsistenz) in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb des ISMS* *Festlegung von Risikoeigentümern* *Festlegung von Folgen und realistischen Eintrittswahrscheinlichkeiten* *Festlegung eines akzeptablen Risikoniveaus* *Priorisierung der zu behandelnden Risiken*	6.1.2
Erklärung zur Anwendbarkeit *Festlegung der umzusetzenden Maßnahmen aus Anhang A* *Prüfen, dass keine erforderliche Maßnahme ausgelassen wurde* *Begründung für die (Nicht-)Einbeziehung jeder Maßnahme aus Anhang A*	6.1.3, d)
Plan zur Risikobehandlung *Festlegung der zu behandelnden Risiken, Messbare Ergebnisse (s.o.)*	6.1.3, e) 6.2
Ergebnisse der Risikoeinschätzung und Risikobehandlung *Ergebnisse des kontinuierlichen und geplanten Risikobeurteilungsprozesses dokumentieren*	8.2 8.3

1.2 Nachweise, Aufzeichnungen und Protokolle

Bezeichnung / Beschreibung	Definiert in ISO/IEC 27001:2013, Abschnitt
Aufzeichnungen zu Training, Fertigkeiten, Erfahrung, Qualifikationen und Kompetenzen von Mitarbeitern im Bereich Informationssicherheit *Kontinuierliche Schulung und Training der Mitarbeiter im Bereich ISMS, Security Awareness und Verpflichtung zur Einhaltung (Verpflichtungserklärung)*	7.2
Ergebnisse der Überwachung, Messung, Analyse und Bewertung des ISMS *Festlegung was, wann und wie und durch wen überwacht und bewertet wird (Maßnahmen, Prozesse, Methoden zur Messung, Überwachung und Bewertung, Verantwortlichkeiten)*	9.1
Internes Audit-Programm *Festlegung von Abläufen und Methoden (Auditkriterien, Auditoren), zeitlichen Abständen zwischen den Audits, Verantwortlichkeiten und Berichterstattung an zuständige Leitung*	9.2
Ergebnisse des internen Audits *Siehe oben*	9.2
Ergebnisse der Managementprüfung *Bewertung von Maßnahmen, Veränderungen, Rückmeldungen von involvierten Parteien* *Aktueller Stand der Maßnahmenumsetzung zur Risikobehandlung* *Verbesserungsprozess*	9.3
Ergebnisse der Korrekturmaßnahmen *Dokumentieren und Bewerten von Nichtkonformitäten und Ursachen (können ähnliche Nichtkonformitäten an anderer Stelle auftreten?)* *Wirksamkeit der Maßnahme prüfen* *Auswahl neuer Maßnahmen dokumentieren und Effektivität/Ergebnisse der Maßnahme prüfen*	10.1

2 Richtlinien, Verfahren und Strategien

Die folgenden Richtlinien, Verfahren und Dokumente sind abhängig von der Auswahl der entsprechenden Maßnahme zu erstellen und müssen als dokumentierte Information vorliegen.

Bezeichnung / Beschreibung	**Definiert in ISO/IEC 27001:2013, Abschnitt**
Verfahren zur Lenkung von Dokumenten Maßnahmen zur Verwaltung von Aufzeichnungen *Verteilung und Schutz von Dokumenten, Versionierung und Änderungsmanagement*	7.5
Definition der Sicherheitsrollen und –verantwortlichkeiten *Festlegung der Rollen (IT-Sicherheitsbeauftragter, etc.) und Personen*	A.6.1.1
Inventar der Werte *Erstellung und Pflege eines Inventars von Informationen und IT-Systemen im Kontext des ISMS*	A.8.1.1
Zulässige Nutzung der Werte *Festlegung von Richtlinien für die Nutzung von Informationen und IT-Systemen im Kontext des ISMS*	A.8.1.3
Zugangssteuerungsrichtlinie *Festlegung von Zugangsberechtigungen zu Informationen und IT-Systemen im Kontext des ISMS*	A.9.1.1
Betriebliche Verfahren zur IT-Bedienung *Festlegung von Verfahren für Installation und Konfiguration von IT-Systemen (z.B. Virenscanner, verbotene Software,…), Backup, Monitoring, System-Neustart und Recovery, Prüfung und Management von Protokolldateien, Fehlerbehandlung*	A.12.1.1
Festlegung von Grundsätzen für die Analyse, Entwicklung und Pflege sicherer Systeme *Festlegung eines Prozesses zur sicheren Entwicklung/Auswahl von IT-Systemen im Kontext des ISMS* *Anwendbarkeit auf externe Dienstleister prüfen*	A.14.2.5
Informationssicherheitsrichtlinie für Lieferantenbeziehungen *Richtlinie für die Behandlung von Lieferanten im Rahmen des ISMS (Zugriff auf Informationen, Überwachung, Training, Festlegung von Verantwortlichkeiten)*	A.15.1.1
Reaktion auf Informationssicherheitsvorfälle *Festlegung Verantwortlichkeiten, Sammeln von Beweisen*	A.16.1.5

(Protokolldateien, forensische Analyse), Vorfall-Management	
Verfahren zum Umsetzen der Aufrechterhaltung der Informationssicherheit *Festlegung von Verantwortlichkeiten, Qualifikation der verantwortlichen Mitarbeiter, Notfallpläne, Prozesse und Tools*	A.17.1.2
Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen *Identifikation und Festlegung der relevanten gesetzlichen Bestimmungen (Inland, Ausland) und vertraglicher Anforderungen Festlegung von Verantwortlichkeiten*	A.18.1.1
Richtlinie „Bring your own device (BYOD)“	A.6.2.1
Mobilgerät- und Telearbeitsrichtlinie	A.6.2.1
Richtlinie zur Informationsklassifizierung	A.8.2.1 A.8.2.2 A.8.2.3
Kennwort-Richtlinie	A.9.2.1 A.9.2.2 A.9.2.4 A.9.3.1 A.9.4.3
Richtlinie zur Entsorgung und Vernichtung	A.8.3.2 A.11.2.7
Verfahren zum Arbeiten in Sicherheitsbereichen	A.11.1.5
Richtlinie zum aufgeräumten Arbeitsplatz	A.11.2.9
Richtlinie zur Änderungsverwaltung	A.12.1.2 A.14.2.4
Backup-Richtlinie	A.12.3.1
Richtlinie zur Informationsübertragung	A.13.2.1 A.13.2.2 A.13.2.3 A.13.2.4
Geschäftsauswirkungsanalyse	A.17.1.1
Übungs- und Test-Plan	A.17.1.3
Wartungs- und Überprüfungsplan	A.17.1.3
Betriebliche Kontinuitätsstrategie	A.17.2.1
Richtlinie zur Aufbewahrung von Aufzeichnungen	A.18.1.3
Richtlinie zur Privatsphäre und zum Schutz personenbezogener Daten	A.18.1.4

3 Literatur

[ISO 27001]	DIN ISO/IEC 27001, Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014), März 2015
[ISO 27002]	ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security controls, 2013-10-01