DIN EN ISO/IEC 27006:2021-05 (D)

Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020); Deutsche Fassung EN ISO/IEC 27006:2020

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Grundsätze 7
5 Allgemeine Anforderungen 7
5.1 Rechts- und Vertragsfragen 7
5.2 Handhabung der Unparteilichkeit 8
5.2.1 IS 5.2 Interessenskonflikte 8
5.3 Haftung und Finanzierung 8
6 Strukturelle Anforderungen 8
7 Anforderungen an Ressourcen 8
7.1 Kompetenz des Personals 8
7.1.1 IS 7.1.1 Allgemeine Betrachtungen 9
7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien 9
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist 13
7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren 13
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten 14
7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams 14
7.4 Aufzeichnungen über Personal 14
7.5 Ausgliederung 15
8 Anforderungen an Informationen 15
8.1 Öffentliche Informationen 15
8.2 Zertifizierungsdokumente 15
8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente 15
8.3 Verweis auf Zertifizierung und Zeichennutzung 15
8.4 Vertraulichkeit 15
8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation 15
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden 15
9 Anforderungen an Prozesse 16
9.1 Tätigkeiten vor der Zertifizierung 16
9.1.1 Antrag 16
9.1.2 Antragsprüfung 16
9.1.3 Auditprogramm 16
9.1.4 Ermittlung des Auditzeitaufwandes 17
9.1.5 Stichprobenprüfung an mehreren Standorten 17
9.1.6 Mehrfach-Managementsysteme 19

9.2 Planung von Audits 19
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien 19
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung 19
9.2.3 Auditplan 20
9.3 Erstzertifizierung 20
9.3.1 IS 9.3.1 Erstzertifizierungsaudit 20
9.4 Durchführen von Audits 22
9.4.1 IS 9.4 Allgemeines 22
9.4.2 IS 9.4 Spezifische Elemente des ISMS-Audits 22
9.4.3 IS 9.4 Auditbericht 22
9.5 Zertifizierungsentscheidung 23
9.5.1 IS 9.5 Zertifizierungsentscheidung 23
9.6 Aufrechterhaltung der Zertifizierung 23
9.6.1 Allgemeines 23
9.6.2 Überwachungstätigkeiten 23
9.6.3 Re-Zertifizierung 24
9.6.4 Audits aus besonderem Anlass 25
9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung 25
9.7 Einsprüche 25
9.8 Beschwerden 25
9.8.1 IS 9.8 Beschwerden 25
9.9 Aufzeichnungen zu Kunden 25

10 Managementsystemanforderungen für Zertifizierungsstellen 25
10.1 Optionen 25
10.1.1 IS 10.1 ISMS-Umsetzung 25
10.2 Option A: Allgemeine Managementsystemanforderungen 25
10.3 Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001 25

Anhang A (informativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung 26

Anhang B (normativ) Auditzeitaufwand 28

Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands 34

Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2013, Anhang A 40

Literaturhinweise 51