DIN EN ISO/IEC 27006-1:2024-08 (D)

Informationssicherheit, Cybersicherheit und Datenschutz - Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren - Teil 1: Allgemeines (ISO/IEC 27006-1:2024); Deutsche Fassung EN ISO/IEC 27006-1:2024

Inhalt

Seite

Europäisches Vorwort ... 9
Vorwort ... 10
Einleitung ... 12
1 Anwendungsbereich ... 13
2 Normative Verweisungen ... 13
3 Begriffe ... 13
4 Grundsätze ... 17
5 Allgemeine Anforderungen ... 17
5.1 Rechts- und Vertragsfragen ... 17
5.2 Handhabung der Unparteilichkeit ... 17
5.2.1 Allgemeines ... 17
5.2.2 Interessenkonflikte ... 17
5.3 Haftung und Finanzierung ... 18
6 Strukturelle Anforderungen ... 18
7 Anforderungen an Ressourcen ... 18
7.1 Kompetenz des Personals ... 18
7.1.1 Allgemeines ... 18
7.1.2 Allgemeine Kompetenzanforderungen ... 18
7.1.3 Bestimmung der Kompetenzkriterien ... 18
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist ... 21
7.2.1 Allgemeines ... 21
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren ... 21
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten ... 23
7.4 Aufzeichnungen über Personal ... 23
7.5 Ausgliederung ... 23
8 Anforderungen an Informationen ... 23
8.1 Öffentliche Informationen ... 23
8.2 Zertifizierungsdokumente ... 23
8.2.1 Allgemeines ... 23
8.2.2 ISMS-Zertifizierungsdokumente ... 23
8.2.3 Verweis auf andere Normen in den ISMS-Zertifizierungsdokumenten ... 23
8.3 Verweisung auf Zertifizierung und Zeichennutzung ... 24
8.4 Vertraulichkeit ... 24
8.4.1 Allgemeines ... 24
8.4.2 Zugang zu den Aufzeichnungen der Organisation ... 24
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden ... 24
9 Anforderungen an Prozesse ... 24
9.1 Tätigkeiten vor der Zertifizierung ... 24
9.1.1 Antrag ... 24
9.1.2 Antragsprüfung ... 25
9.1.3 Auditprogramm ... 25

9.1.4 Ermittlung des Auditzeitaufwands ... 26
9.1.5 Stichprobenprüfung an mehreren Standorten ... 26
9.1.6 Mehrfach-Managementsysteme ... 28
9.2 Planung von Audits ... 28
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien ... 28
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung ... 29
9.2.3 Auditplan ... 29
9.3 Erstzertifizierung ... 29
9.3.1 Allgemeines ... 29
9.3.2 Erstzertifizierungsaudit ... 29
9.4 Durchführen von Audits ... 31
9.4.1 Allgemeines ... 31
9.4.2 Spezifische Elemente des ISMS-Audits ... 31
9.4.3 Auditbericht ... 31
9.5 Zertifizierungsentscheidung ... 32
9.5.1 Allgemeines ... 32
9.5.2 Zertifizierungsentscheidung ... 32
9.6 Aufrechterhaltung der Zertifizierung ... 32
9.6.1 Allgemeines ... 32
9.6.2 Überwachungstätigkeiten ... 32
9.6.3 Rezertifizierung ... 33
9.6.4 Audits aus besonderem Anlass ... 33
9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung ... 33
9.7 Einsprüche ... 33
9.8 Beschwerden ... 33
9.8.1 Allgemeines ... 33
9.8.2 Beschwerden ... 33
9.9 Aufzeichnungen zu Kunden ... 34

10 Managementsystemanforderungen für Zertifizierungsstellen ... 34
10.1 Optionen ... 34
10.1.1 Allgemeines ... 34
10.1.2 ISMS-Umsetzung ... 34
10.2 Option A: Allgemeine Managementsystemanforderungen ... 34
10.3 Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001 ... 34

Anhang A (normativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung ... 35
A.1 Übersicht ... 35

Anhang B (informativ) Weitere Kompetenzbetrachtungen ... 36
B.1 Allgemeine Betrachtungen zu Kompetenzen ... 36
B.2 Betrachtungen zu besonderen Kenntnissen und Erfahrungen ... 36
B.2.1 Typische Kenntnisse mit Bezug zu ISMS ... 36

Anhang C (normativ) Auditzeitaufwand ... 38
C.1 Allgemeines ... 38
C.2 Konzepte ... 39
C.2.1 Anzahl der von der Organisation gesteuerten Personen ... 39
C.2.2 Auditortag ... 39
C.2.3 Temporärer Standort ... 39
C.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit ... 40
C.3.1 Allgemeines ... 40
C.3.2 Methoden zur Durchführung von Fernaudits ... 40
C.3.3 Berechnung des Auditzeitaufwands ... 40
C.3.4 Bestimmung der anfänglichen Personenanzahl ... 40
C.3.5 Faktoren für die Anpassung des Auditzeitaufwands ... 42
C.3.6 Einschränkung der Abweichung von der Auditzeit ... 43
C.3.7 Vor-Ort-Auditzeitaufwand ... 43
C.4 Auditzeitaufwand für das Überwachungsaudits ... 44
C.5 Auditzeitaufwand für das Rezertifizierungsaudit ... 44

C.6 Auditzeitaufwand für mehrere Standorte ... 44
C.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs ... 44

Anhang D (informativ) Methoden für Berechnungen des Auditzeitaufwands ... 46
D.1 Allgemeines ... 46
D.2 Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands ... 46
D.3 Beispiel für die Auditzeitaufwandberechnung ... 49

Anhang E (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2022, Anhang A ... 52
E.1 Zweck ... 52
E.2 Anwendung von Tabelle E.1 ... 52
E.2.1 Allgemeines ... 52
E.2.2 Spalte „Systemprüfung“ ... 53
E.2.3 Spalte „Sichtprüfung“ ... 53
E.2.4 Möglicher Nachweis der Gestaltung und Umsetzung von Maßnahmen ... 53

Literaturhinweise ... 76

Tabellen

Tabelle A.1 — Tabelle zum Wissen und zu den Fertigkeiten für ISMS-Audits und -Zertifizierung ... 35

Tabelle C.1 — Auditzeitaufwandstabelle ... 41

Tabelle D.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands ... 46

Tabelle D.2 — Mit dem Geschäft und der Organisation zusammenhängende Faktoren (ohne IT) ... 49

Tabelle D.3 — Mit der IT-Umgebung zusammenhängende Faktoren ... 50

Tabelle D.4 — Auswirkung der Faktoren auf die Auditzeit ... 51

Tabelle E.1 — Bewertung der Maßnahmen ... 54