E DIN EN ISO/IEC 27006-1:2023-05 (D/E)

Erscheinungsdatum: 2023-03-31

Informationstechnik, Cybersicherheit und Datenschutz - Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren - Teil 1: Allgemeines (ISO/IEC DIS 27006-1.2:2023); Deutsche und Englische Fassung prEN ISO/IEC 27006-1:2023

Information technology, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC DIS 27006-1.2:2023); German and English version prEN ISO/IEC 27006-1:2023

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.....	17
6 Strukturelle Anforderungen.....	18
7 Anforderungen an Ressourcen.....	18
7.1 Kompetenz des Personals.....	18
7.1.1 Allgemeines.....	18
7.1.2 Allgemeine Betrachtungen.....	18
7.1.3 Bestimmung der Kompetenzkriterien.....	18
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist.....	22
7.2.1 Allgemeines.....	22
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren.....	22
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 ISMS-Zertifizierungsdokumente und branchenspezifische Normen.....	24
8.2.4 Anforderungen an interessierte Parteien.....	24
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.....	25
9.1	Tätigkeiten vor der Zertifizierung.....	25
9.1.1	Antrag.....	25
9.1.2	Antragsprüfung.....	25
9.1.3	Auditprogramm	25
9.1.4	Ermittlung des Auditzeitaufwands.....	27
9.1.5	Stichprobenprüfung an mehreren Standorten.....	27
9.1.6	Mehrfach-Managementsysteme	28
9.2	Planung von Audits.....	29
9.2.1	Festlegung der Auditziele, des Auditumfangs und der Auditkriterien.....	29
9.2.2	Auswahl des Auditteams und Aufgabenzuordnung	29
9.2.3	Auditplan	29
9.3	Erstzertifizierung	30
9.3.1	Allgemeines.....	30
9.3.2	Erstzertifizierungsaudit.....	30
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	33
9.6.3	Re-Zertifizierung	33
9.6.4	Audits aus besonderem Anlass	34
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung....	34
9.7	Einsprüche.....	34
9.8	Beschwerden	34
9.8.1	Allgemeines.....	34
9.8.2	Beschwerden	34
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.....	35
10.2	Option A: Allgemeine Managementsystemanforderungen.....	35
10.3	Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001	35
Anhang A (normativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung.....		36
A.1	Übersicht.....	36
Anhang B (normativ) Auditzeitaufwand		37
B.1	Einleitung.....	37
B.2	Konzepte	38
B.2.1	Anzahl der von der Organisation gesteuerten Personen	38
B.2.2	Auditortag.....	38
B.2.3	Temporärer Standort.....	38
B.3	Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit	39
B.3.1	Allgemeines.....	39
B.3.2	Methoden zur Durchführung von Fernaudits	39
B.3.3	Berechnung des Auditzeitaufwands.....	39
B.3.4	Bestimmung der ursprünglichen Personenanzahl	39
B.3.5	Faktoren für die Anpassung des Auditzeitaufwands	41
B.3.6	Einschränkung der Abweichung von der Auditzeit.....	42

B.3.7	Vor-Ort-Auditzeitaufwand.....	42
B.4	Auditzeitaufwand für das Überwachungsaudit	42
B.5	Auditzeitaufwand für das Re-Zertifizierungsaudit	42
B.6	Auditzeitaufwand für mehrere Standorte.....	43
B.7	Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs.....	43
B.8	Auditzeitaufwand für eine branchenspezifische Norm	43
Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands		44
C.1	Allgemeines.....	44
C.2	Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	44
C.3	Beispiel für die Auditzeitaufwandberechnung.....	47
Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2022, Anhang A		50
D.1	Zweck	50
D.2	Anwendung von Tabelle D.1	50
D.2.1	Allgemeines.....	50
D.2.2	Spalte „Systemprüfung“	51
D.2.3	Spalte „Sichtprüfung“	51
D.2.4	Möglicher Nachweis der Gestaltung und Umsetzung von Maßnahmen.....	51
Anhang E (informativ) Anforderungen und Einschränkungen bei Zertifizierungen nach branchenspezifischen Normen		73
E.1	Allgemeines.....	73
Anhang F (normativ) Anforderungen an die Zertifizierung einschließlich branchenspezifischer Normen		74
F.1	Allgemeines.....	74
Anhang G (informativ) Weitere Kompetenzbetrachtungen.....		75
G.1	Allgemeine Kompetenzbetrachtungen.....	75
G.2	Spezielle Betrachtungen zu Wissen und Erfahrung	75
G.2.1	Typisches Wissen in Bezug auf ISMS.....	75
Literaturhinweise		77

Tabellen

Tabelle A.1	— Tabelle zum Wissen und zu den Fertigkeiten für ISMS-Audits und -Zertifizierung	36
Tabelle B.1	— Auditzeitaufwandstabelle	40
Tabelle C.1	— Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	44
Tabelle C.2	— Mit dem Geschäft und der Organisation zusammenhängende Faktoren (ohne IT).....	47
Tabelle C.3	— Mit der IT-Umgebung zusammenhängende Faktoren.....	48
Tabelle C.4	— Auswirkung der Faktoren auf die Auditzeit	49
Tabelle D.1	— Bewertung der Maßnahmen	52
Tabelle E.1	— Verweisung auf Anforderungen und Leitlinien für branchenspezifische Erweiterungen	73