E DIN EN ISO/IEC 27007:2026-08 (D/E)

Erscheinungsdatum: 2026-07-03

Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC DIS 27007:2026); Deutsche und Englische Fassung prEN ISO/IEC 27007:2026

Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing (ISO/IEC DIS 27007:2026); German and English version prEN ISO/IEC 27007:2026

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 7
1 Anwendungsbereich 8
2 Normative Verweisungen 8
3 Begriffe 8
4 Grundsätze der Auditierung 17
5 Steuerung eines Auditprogramms 17
5.1 Allgemeines 17
5.2 Festlegen der Auditprogrammziele 17
5.3 Ermittlung und Beurteilung von Risiken und Chancen im Zusammenhang mit Auditprogrammen 18
5.4 Festlegen des Auditprogramms 18
5.4.1 Rollen und Verantwortlichkeiten der Person(en), die das Auditprogramm steuert (steuern) 18
5.4.2 Kompetenz von Person(en), die das Auditprogramm steuert (steuern) 18
5.4.3 Festlegung des Umfangs des Auditprogramms 18
5.4.4 Ermittlung von Auditprogrammressourcen 19
5.5 Umsetzung des Auditprogramms 19
5.5.1 Allgemeines 19
5.5.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit 19
5.5.3 Auswahl und Festlegung von Auditmethoden 20
5.5.4 Auswahl von Mitgliedern des Auditteams 20
5.5.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams 20
5.5.6 Management des Ergebnisses des Auditprogramms 20
5.5.7 Management und Pflege der Auditprogrammunterlagen 20
5.6 Überwachung des Auditprogramms 21
5.7 Überprüfung und Verbesserung des Auditprogramms 21
6 Durchführung eines Audits 21
6.1 Allgemeines 21
6.2 Einleitung des Audits 21
6.2.1 Allgemeines 21
6.2.2 Herstellung des Kontakts mit der auditierten Organisation 21
6.2.3 Feststellung der Durchführbarkeit des Audits 21
6.3 Vorbereitung der Auditaktivitäten 21
6.3.1 Überprüfung dokumentierter Informationen 21
6.3.2 Planung des Audits 21
6.3.3 Übertragung von Arbeiten an das Auditteam 22
6.3.4 Vorbereitung dokumentierter Informationen für das Audit 22
6.4 Durchführung der Auditaktivitäten 22
6.4.1 Allgemeines 22
6.4.2 Zuweisung von Rollen und Verantwortlichkeiten von Betreuern und Beobachtern 22
6.4.3 Durchführung der Eröffnungsbesprechung 22
6.4.4 Kommunikation während des Audits 22

6.4.5 Verfügbarkeit von und Zugang zu Auditinformationen . . . 22
6.4.6 Überprüfung der Dokumentinformationen während der Durchführung des Audits . . . 22
6.4.7 Erfassung und Überprüfung von Informationen . . . 22
6.4.8 Erstellung der Auditfeststellungen . . . 23
6.4.9 Erarbeitung der Auditschlussfolgerungen . . . 23
6.4.10 Durchführung der Abschlussbesprechung . . . 23
6.5 Erarbeitung und Verteilung des Auditberichts . . . 23
6.5.1 Erarbeitung des Auditberichts . . . 23
6.5.2 Verteilung des Auditberichts . . . 23
6.6 Abschluss des Audits . . . 23
6.7 Durchführung von Auditfolgemaßnahmen . . . 23
7 Kompetenz und Bewertung von ISMS-Auditoren . . . 23
7.1 Allgemeines . . . 23
7.2 Ermittlung der Kompetenz von Auditoren . . . 24
7.2.1 Allgemeines . . . 24
7.2.2 Persönliches Verhalten . . . 24
7.2.3 Kenntnisse und Fertigkeiten . . . 24
7.2.4 Erreichung der Kompetenz von Auditoren . . . 24
7.2.5 Erreichung der Kompetenz des Leiters des Auditteams . . . 25
7.3 Aufstellung von Kriterien zur Bewertung von Auditoren . . . 25
7.4 Auswahl der entsprechenden Methode zur Bewertung von Auditoren . . . 25
7.5 Durchführung der Bewertung von Auditoren . . . 25
7.6 Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren . . . 25
Anhang A (informativ) **Anleitung zur praktischen Durchführung von ISMS-Audits . . . 26**
A.1 Überblick . . . 26
A.2 Allgemeines . . . 26
A.2.1 Ziele, Umfang und Kriterien von Audits sowie Auditnachweise . . . 26
A.2.2 Strategie zum Auditieren eines ISMS . . . 26
A.2.3 Audit und dokumentierte Informationen . . . 27
A.3 Anleitung über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001 27
A.3.1 Hintergrund . . . 27
A.3.2 Beispiel einer impliziten Anforderung an dokumentierte Informationen . . . 28
A.3.3 Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen . . . 28
A.4 Die Erklärung zur Anwendbarkeit . . . 28
A.5 Sonstige dokumentierte Informationen . . . 29
A.6 Anmerkungen . . . 29
A.7 Anleitung zur Auditierung eines ISMS . . . 30
Literaturhinweise . . . 73

Tabellen

Tabelle A.1 — Anforderungen an dokumentierte Informationen in ISO/IEC 27001:2022 . . . 27
Tabelle A.2 — Leitfaden für das Auditieren nach ISO/IEC 27001 . . . 30