

DIN EN ISO/IEC 27007:2022-10 (D)

Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020); Deutsche Fassung EN ISO/IEC 27007:2022

Inhalt	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze der Auditierung	7
5 Management eines Auditprogramms.....	7
5.1 Allgemeines.....	7
5.2 Festlegung der Ziele des Auditprogramms	7
5.3 Ermittlung und Beurteilung von Risiken und Chancen im Zusammenhang mit Auditprogrammen	8
5.4 Aufstellung des Auditprogramms	8
5.4.1 Rollen und Verantwortlichkeiten der Person(en), die das Auditprogramm steuert (steuern)	8
5.4.2 Kompetenz von Person(en), die das Auditprogramm steuert (steuern)	8
5.4.3 Festlegung des Umfangs des Auditprogramms.....	8
5.4.4 Ermittlung von Auditprogrammressourcen.....	9
5.5 Umsetzung des Auditprogramms.....	9
5.5.1 Allgemeines.....	9
5.5.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit	9
5.5.3 Auswahl und Festlegung von Auditmethoden	10
5.5.4 Auswahl von Mitgliedern des Auditteams.....	10
5.5.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams.....	10
5.5.6 Management des Ergebnisses des Auditprogramms	10
5.5.7 Management und Pflege der Auditprogrammunterlagen	11
5.6 Überwachung des Auditprogramms	11
5.7 Überprüfung und Verbesserung des Auditprogramms	11
6 Durchführung eines Audits	11
6.1 Allgemeines.....	11
6.2 Einleitung des Audits	11
6.2.1 Allgemeines.....	11
6.2.2 Herstellung des Kontakts mit der auditierten Organisation.....	11
6.2.3 Feststellung der Durchführbarkeit des Audits	11
6.3 Vorbereitung von Auditaktivitäten	11
6.3.1 Überprüfung dokumentierter Informationen	11
6.3.2 Planung des Audits.....	12
6.3.3 Übertragung von Arbeiten an das Auditteam	12
6.3.4 Vorbereitung dokumentierter Informationen für das Audit.....	12
6.4 Durchführung der Auditaktivitäten	12
6.4.1 Allgemeines.....	12
6.4.2 Zuweisung von Rollen und Verantwortlichkeiten von Guides und Beobachtern.....	12

6.4.3	Durchführung der Eröffnungsbesprechung	12
6.4.4	Kommunikation während des Audits	12
6.4.5	Verfügbarkeit von und Zugang zu Auditinformationen	12
6.4.6	Überprüfung der Dokumentinformationen während der Durchführung des Audits	12
6.4.7	Erfassung und Überprüfung von Informationen	13
6.4.8	Erstellung der Auditfeststellungen	13
6.4.9	Erarbeitung der Auditschlussfolgerungen	13
6.4.10	Durchführung der Abschlussbesprechung	13
6.5	Erarbeitung und Verteilung des Auditberichts	13
6.5.1	Erarbeitung des Auditberichts	13
6.5.2	Verteilung des Auditberichts	13
6.6	Abschluss des Audits	14
6.7	Durchführung von Auditfolgemaßnahmen	14
7	Kompetenz und Bewertung von ISMS-Auditoren	14
7.1	Allgemeines	14
7.2	Ermittlung der Kompetenz von Auditoren	14
7.2.1	Allgemeines	14
7.2.2	Persönliches Verhalten	14
7.2.3	Kenntnisse und Fertigkeiten	14
7.2.4	Erreichung der Kompetenz von Auditoren	15
7.2.5	Erreichung der Kompetenz des Leiters des Auditteams	15
7.3	Aufstellung von Kriterien zur Bewertung von Auditoren	15
7.4	Auswahl der entsprechenden Methode zur Bewertung von Auditoren	15
7.5	Durchführung der Bewertung von Auditoren	15
7.6	Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren	15
Anhang A (informativ) Anleitung zur praktischen Durchführung von ISMS-Audits		16
A.1	Überblick	16
A.2	Allgemeines	16
A.2.1	Ziele, Umfang und Kriterien von Audits sowie Auditnachweise	16
A.2.2	Strategie zum Auditieren eines ISMS	16
A.2.3	Audit und dokumentierte Informationen	17
A.3	Anleitung über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001	17
A.3.1	Hintergrund	17
A.3.2	Beispiel einer impliziten Anforderung an dokumentierte Informationen	18
A.3.3	Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen	18
A.4	Die Erklärung zur Anwendbarkeit	19
A.5	Sonstige dokumentierte Informationen	19
A.6	Anmerkungen	19
A.7	Anleitung zur Auditierung eines ISMS	20
Literaturhinweise		54