

E DIN EN ISO/IEC 27007:2019-12 (D/E)

Erscheinungsdatum: 2019-11-01

Informationstechnik - Sicherheitsverfahren - Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2017); Deutsche und Englische Fassung prEN ISO/IEC 27007:2019

Information technology - Security techniques - Guidelines for information security management systems auditing (ISO/IEC 27007:2017); German and English version prEN ISO/IEC 27007:2019

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
5.1.1 IS 5.1 Allgemeines	7
5.2 Festlegung der Ziele des Auditprogramms	8
5.2.1 IS 5.2 Festlegung der Ziele des Auditprogramms	8
5.3 Aufstellung des Auditprogramms	8
5.3.1 Rollen und Verantwortlichkeiten der Person, die das Auditprogramm managt.....	8
5.3.2 Kompetenz der Person, die das Audit Programm managt.....	8
5.3.3 Festlegung des Umfangs des Auditprogramms.....	8
5.3.4 Identifikation und Beurteilung von Auditprogrammrisiken.....	9
5.3.5 Erstellung von Verfahren für das Auditprogramm	9
5.3.6 Identifikation von Auditprogrammressourcen.....	9
5.4 Umsetzung des Auditprogramms.....	10
5.4.1 Allgemeines	10
5.4.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit	10
5.4.3 Auswahl der Auditverfahren	11
5.4.4 Auswahl der Mitglieder des Auditteams.....	11
5.4.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams.....	11
5.4.6 Management des Ergebnisses des Auditprogramms	11
5.4.7 Management und Pflege der Auditprogrammunterlagen	11
5.5 Überwachung des Auditprogramms	11
5.6 Überprüfung und Verbesserung des Auditprogramms	11
6 Durchführung eines Audits	12
6.1 Allgemeines	12
6.2 Einleitung des Audits	12
6.2.1 Allgemeines.....	12
6.2.2 Herstellung des Erstkontakts mit der auditierten Organisation.....	12
6.2.3 Feststellung der Durchführbarkeit des Audits	12
6.3 Vorbereitung von Auditaktivitäten	12
6.3.1 Durchführung der Dokumentenüberprüfung bei der Vorbereitung auf das Audit.....	12
6.3.2 Erarbeitung des Auditplans	12

6.3.3	Übertragung von Arbeiten an das Auditteam	13
6.3.4	Erarbeitung von Arbeitsdokumenten.....	13
6.4	Durchführung der Auditaktivitäten	13
6.4.1	Allgemeines.....	13
6.4.2	Durchführung der Eröffnungsbesprechung	13
6.4.3	Durchführung der Dokumentenüberprüfung bei der Durchführung des Audits.....	13
6.4.4	Kommunikation während des Audits.....	13
6.4.5	Zuweisung von Rollen und Verantwortlichkeiten von Guides und Beobachtern	13
6.4.6	Erfassung und Überprüfung von Informationen.....	14
6.4.7	Erstellung der Auditfeststellungen	14
6.4.8	Erarbeitung der Auditschlussfolgerungen.....	14
6.4.9	Durchführung der Abschlussbesprechung	14
6.5	Erarbeitung und Verteilung des Auditberichts	14
6.5.1	Erarbeitung des Auditberichts.....	14
6.5.2	Verteilung des Auditberichts.....	15
6.6	Abschluss des Audits.....	15
6.7	Durchführung von Auditfolgemaßnahmen	15
7	Kompetenz und Bewertung von ISMS-Auditoren	15
7.1	Allgemeines.....	15
7.2	Ermittlung der Kompetenz von Auditoren zur Erfüllung der Belange des Auditprogramms	15
7.2.1	Allgemeines.....	15
7.2.2	Persönliches Verhalten	16
7.2.3	Kenntnisse und Fertigkeiten	16
7.2.4	Erreichung der Kompetenz von Auditoren.....	16
7.2.5	Leiter des Auditteams.....	16
7.3	Aufstellung von Kriterien zur Bewertung von Auditoren.....	16
7.4	Auswahl des entsprechenden Verfahrens zur Bewertung von Auditoren	16
7.5	Durchführung der Bewertung von Auditoren.....	17
7.6	Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren.....	17
	Anhang A (informativ) Leitfaden zur praktischen Durchführung von ISMS-Audits	18
A.1	Überblick.....	18
A.2	Allgemeines.....	18
A.2.1	Ziele, Umfang und Kriterien von Audits sowie Auditnachweise.....	18
A.2.2	Strategie zur Auditierung eines ISMS	18
A.2.3	Audit und dokumentierte Informationen	19
A.3	Leitfaden über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001.....	19
A.3.1	Hintergrund	19
A.3.2	Beispiel einer impliziten Anforderung an dokumentierte Information	20
A.3.3	Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen.....	20
A.4	Die Erklärung zur Anwendbarkeit	21
A.5	Sonstige dokumentierte Information	21
A.6	Anmerkungen.....	21
A.7	Leitfaden zur Auditierung eines ISMS	22
	Literaturhinweise	57