E DIN EN ISO/IEC 27005:2024-05 (D/E)

Erscheinungsdatum: 2024-04-05

Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022); Deutsche und Englische Fassung prEN ISO/IEC 27005:2024

Information security, cybersecurity and privacy protection - Guidance on managing information security risks (ISO/IEC 27005:2022); German and English version prEN ISO/IEC 27005:2024

Inhalt

Seite

Europäisches Vorwort 8

Vorwort 9

Einleitung 10

1 Anwendungsbereich 11

2 Normative Verweisungen 11

3 Begriffe 11
3.1 Begriffe im Zusammenhang mit Informationssicherheitsrisiken 11
3.2 Begriffe im Zusammenhang mit der Handhabung von Informationssicherheitsrisiken 15

4 Aufbau dieses Dokuments 18

5 Handhabung von Informationssicherheitsrisiken 18
5.1 Prozess zur Handhabung von Informationssicherheitsrisiken 18
5.2 Zyklen des Informationssicherheitsrisikomanagements 20

6 Kontextfestlegung 21
6.1 Organisatorische Aspekte 21
6.2 Identifizierung grundlegender Anforderungen von interessierten Parteien 21
6.3 Anwendung der Risikobeurteilung 22
6.4 Festlegung und Aufrechterhaltung der Informationssicherheitsrisikokriterien 22
6.4.1 Allgemeines 22
6.4.2 Risikoakzeptanzkriterien 23
6.4.3 Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen 24
6.5 Wahl eines angemessenen Verfahrens 28

7 Prozess zur Beurteilung von Informationssicherheitsrisiken 28
7.1 Allgemeines 28
7.2 Identifizierung von Informationssicherheitsrisiken 29
7.2.1 Identifizierung und Beschreibung von Informationssicherheitsrisiken 29
7.2.2 Identifizierung von Risikoeigentümern 32
7.3 Analyse von Informationssicherheitsrisiken 32
7.3.1 Allgemeines 32
7.3.2 Beurteilung potentieller Folgen 33
7.3.3 Beurteilung der Wahrscheinlichkeit 34
7.3.4 Bestimmung der Risikoniveaus 36
7.4 Bewertung der Informationssicherheitsrisiken 36
7.4.1 Vergleich der Ergebnisse der Risikoanalyse mit den Risikokriterien 36
7.4.2 Priorisierung der analysierten Risiken für die Risikobehandlung 37

8 Prozess zur Informationssicherheitsrisikobehandlung 38
8.1 Allgemeines 38
8.2 Auswahl geeigneter Optionen zur Behandlung von Informationssicherheitsrisiken 38

8.3 Festlegung aller Maßnahmen, die zur Umsetzung der gewählten Optionen für die Informationssicherheitsrisikobehandlung erforderlich sind ... 39
8.4 Vergleich der festgelegten Maßnahmen mit denen in ISO/IEC 27001:2022, Anhang A ... 42
8.5 Erstellung einer Erklärung zur Anwendbarkeit ... 43
8.6 Behandlungsplan für Informationssicherheitsrisiken ... 44
8.6.1 Ausarbeitung des Risikobehandlungsplans ... 44
8.6.2 Zustimmung durch die Risikoeigentümer ... 45
8.6.3 Akzeptanz der Restrisiken für die Informationssicherheit ... 46

9 Betrieb ... 47
9.1 Durchführung des Prozesses zur Risikobeurteilung der Informationssicherheit ... 47
9.2 Durchführung des Prozesses zur Risikobehandlung der Informationssicherheit ... 47

10 Nutzung verbundener ISMS-Prozesse ... 48
10.1 Kontext der Organisation ... 48
10.2 Führung und Verpflichtung ... 49
10.3 Kommunikation und Konsultation ... 49
10.4 Dokumentierte Informationen ... 51
10.4.1 Allgemeines ... 51
10.4.2 Dokumentierte Informationen über Prozesse ... 52
10.4.3 Dokumentierte Informationen über Ergebnisse ... 53
10.5 Überwachen und Überprüfen ... 53
10.5.1 Allgemeines ... 53
10.5.2 Überwachung und Überprüfung der die Risiken beeinflussenden Faktoren ... 54
10.6 Managementbewertung ... 55
10.7 Korrekturmaßnahme ... 56
10.8 Fortlaufende Verbesserung ... 56

Anhang A (informativ) Beispiele für Techniken zur Unterstützung des Risikobeurteilungsprozesses ... 59
A.1 Risikokriterien für die Informationssicherheit ... 59
A.1.1 Kriterien im Zusammenhang mit der Risikobeurteilung ... 59
A.1.2 Risikoakzeptanzkriterien ... 64
A.2 Praktische Verfahren ... 65
A.2.1 Risikokomponenten für die Informationssicherheit ... 65
A.2.2 Vermögenswerte ... 66
A.2.3 Risikoquellen und gewünschter Endzustand ... 67
A.2.4 Ereignisbasierter Ansatz ... 71
A.2.5 Auf Vermögenswerten basierender Ansatz ... 73
A.2.6 Beispiele für Szenarien, die in beiden Ansätzen anwendbar sind ... 80
A.2.7 Überwachung risikobehafteter Ereignisse ... 81

Literaturhinweise ... 84

Bilder

Bild 1 — Prozess zur Handhabung von Informationssicherheitsrisiken ... 19

Bild A.1 — Komponenten für die Risikobeurteilung der Informationssicherheit ... 66

Bild A.2 — Beispiel eines Diagramms der Abhängigkeiten von Vermögenswerten ... 67

Bild A.3 — Identifizierung der interessierten Parteien des Ökosystems ... 72

Bild A.4 — Risikobeurteilung anhand von Risikoszenarien ... 80

Bild A.5 — Beispiel für die Anwendung des SFDT-Modells ... 83

Tabellen

Tabelle A.1 — Beispiel einer Folgenskala 59

Tabelle A.2 — Beispiel einer Wahrscheinlichkeitsskala 61

Tabelle A.3 — Beispiel für einen qualitativen Ansatz bei den Risikokriterien 61

Tabelle A.4 — Beispiel einer logarithmischen Wahrscheinlichkeitsskala 63

Tabelle A.5 — Beispiel einer logarithmischen Folgenskala 64

Tabelle A.6 — Beispiel für eine Bewertungsskala in Kombination mit einer Drei-Farben-Risikomatrix 65

Tabelle A.7 — Beispiele und übliche Angriffsmethoden 68

Tabelle A.8 — Beispielhafte Klassifizierung von Motivationen, die den DES zum Ausdruck bringen 69

Tabelle A.9 — Beispiele für Zielvorgaben 70

Tabelle A.10 — Beispiele für typische Bedrohungen 73

Tabelle A.11 — Beispiele für typische Schwachstellen 75

Tabelle A.12 — Beispiele für Risikoszenarien in beiden Ansätzen 80

Tabelle A.13 — Beispiel für ein Risikoszenario und eine Überwachung risikobehafteter Ereignisse 82