DGI® Deutsche Gesellschaft für Informationssicherheit AG

Vorgehen und Prüfpunkte für die Auditierung eines ISMS gemäß ISO 27001

- Richtlinie -

Inhaltsverzeichnis

Prüfung und Freigabe ... 2
Änderungshistorie ... 3
Dokumentensteuerung und Verteilerkreis ... 4
1 Angaben zum Audit ... 7
2 Festlegungen zum Audit ... 8
2.1 Auditkriterien ... 8
2.2 Auditprüfpunkte ... 8
2.3 Festlegung der Prüfkriterien ... 9
2.4 Festlegung der Bewertungskriterien ... 9
3 Hinweise für den Umgang mit der Auditcheckliste ... 10
3.1 Allgemeines ... 10
3.2 Umgang mit den Auditfeststellungen ... 10
4 Prüfpunkte ... 12
4.1 Allgemeines ... 12
4.2 Prüfpunkte gemäß ISO 27001 ... 12
Begriffe ... 12
Verstehen der Organisation und ihres Kontextes ... 13
Verstehen der Erfordernisse und Erwartungen interessierter Parteien ... 14
Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems ... 15
Informationssicherheitsmanagementsystem ... 16
Führung und Verpflichtung ... 17
Politik ... 18
Rollen, Verantwortlichkeiten und Befugnisse in der Organisation ... 19
Maßnahmen zum Umgang mit Risiken und Chancen ... 20
Informationssicherheitsziele und Planung zu deren Erreichung ... 21
Ressourcen ... 22
Kompetenz ... 23
Bewusstsein (Awareness) ... 24
Kommunikation ... 25
Dokumentierte Information (Dokumentation) ... 26
Betriebliche Planung und Steuerung ... 27
Informationssicherheitsrisikobeurteilung ... 28
Informationssicherheitsrisikobehandlung ... 29
Überwachung, Messung, Analyse und Bewertung ... 30
Internes Audit ... 31
Managementbewertung ... 32
Nichtkonformität und Korrekturmaßnahmen ... 33
Fortlaufende Verbesserung ... 34

4.3 Prüfpunkte zum Anhang A gemäß ISO 27001 35
A.5 Informationssicherheitsrichtlinien 35
A.6 Organisation der Informationssicherheit 36
A.7 Personalsicherheit 37
A.8 Verwaltung der Werte 38
A.9 Zugangssteuerung 39
A.10 Kryptographie 41
A.11 Physische und umgebungsbezogene Sicherheit 42
A.12 Betriebssicherheit 44
A.13 Kommunikationssicherheit 46
A.14 Anschaffung, Entwicklung und Instandhalten von Systemen 47
A.15 Lieferantenbeziehungen 49
A.16 Handhabung von Informationssicherheitsvorfällen 50
A.17 Informationssicherheitsaspekte beim Business Continuity Management 51
A.18 Compliance 52