

# DIN ISO/IEC 27001:2008-09 (D)

## Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits- Managementsysteme - Anforderungen (ISO/IEC 27001:2005)

---

Inhalt	Seite
Nationales Vorwort .....	3
Nationaler Anhang NA (informativ) Literaturhinweise .....	4
0 Einleitung .....	5
0.1 Allgemeines .....	5
0.2 Prozessorientierter Ansatz .....	5
0.3 Verträglichkeit mit anderen Managementsystemen .....	8
1 Anwendungsbereich .....	8
1.1 Allgemeines .....	8
1.2 Anwendung .....	9
2 Normative Verweisungen .....	9
3 Begriffe .....	9
4 Informationssicherheits-Managementsystem .....	11
4.1 Allgemeine Anforderungen .....	11
4.2 Festlegung und Verwaltung des ISMS .....	11
4.2.1 Festlegen des ISMS .....	11
4.2.2 Umsetzen und Durchführen des ISMS .....	14
4.2.3 Überwachen und Überprüfen des ISMS .....	14
4.2.4 Instandhalten und Verbessern des ISMS .....	15
4.3 Dokumentationsanforderungen .....	15
4.3.1 Allgemeines .....	15
4.3.2 Lenkung von Dokumenten .....	16
4.3.3 Lenkung von Aufzeichnungen .....	17
5 Verantwortung des Managements .....	17
5.1 Verpflichtung des Managements .....	17
5.2 Management von Ressourcen .....	17
5.2.1 Bereitstellung von Ressourcen .....	17
5.2.2 Schulungen, Bewusstsein und Kompetenz .....	18
6 Interne ISMS-Audits .....	18
7 Managementbewertung des ISMS .....	19
7.1 Allgemeines .....	19
7.2 Eingaben für die Bewertung .....	19
7.3 Ergebnisse der Bewertung .....	19
8 Verbesserung des ISMS .....	20
8.1 Ständige Verbesserung .....	20
8.2 Korrekturmaßnahmen .....	20
8.3 Vorbeugungsmaßnahmen .....	20
Anhang A (normativ) Maßnahmenziele und Maßnahmen .....	22
Anhang B (informativ) OECD-Grundsätze und diese Internationale Norm .....	41
Anhang C (informativ) Übereinstimmung zwischen ISO 9001:2000, ISO 14001:2004 und dieser Internationalen Norm .....	43
Literaturhinweise .....	46