DIN EN ISO/IEC 27000:2020-06 (D)

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

Einleitung 6
0.1 Überblick 6
0.2 Zweck dieses Dokuments 6
0.3 Inhalt dieses Dokumentes 6

1 Anwendungsbereich 7

2 Normative Verweisungen 7

3 Begriffe 7

4 Managementsysteme für Informationssicherheit (ISMS) 20
4.1 Allgemeines 20
4.2 Was ist ein ISMS? 21
4.2.1 Überblick und Grundsätze 21
4.2.2 Informationen 21
4.2.3 Informationssicherheit 22
4.2.4 Management 22
4.2.5 Managementsystem 22
4.3 Prozessorientierter Ansatz 23
4.4 Warum ein ISMS wichtig ist 23
4.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS 24
4.5.1 Übersicht 24
4.5.2 Identifizierung von Informationssicherheitsanforderungen 24
4.5.3 Beurteilung von Informationssicherheitsrisiken 25
4.5.4 Behandlung von Informationssicherheitsrisiken 25
4.5.5 Auswahl und Umsetzung von Maßnahmen 26
4.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS 27
4.5.7 Fortlaufende Verbesserung 27
4.6 Kritische Erfolgsfaktoren für das ISMS 27
4.7 Nutzen der ISMS-Normenfamilie 28

5 Die ISMS-Normenfamilie 29
5.1 Allgemeine Informationen 29
5.2 Norm, die einen Überblick und die Terminologie beschreibt: ISO/IEC 27000 (dieses Dokument) 30
5.3 Normen, die Anforderungen festlegen 30
5.3.1 ISO/IEC 27001 30
5.3.2 ISO/IEC 27006 30
5.3.3 ISO/IEC 27009 31
5.4 Normen, die allgemeine Leitfäden beschreiben 31
5.4.1 ISO/IEC 27002 31
5.4.2 ISO/IEC 27003 31
5.4.3 ISO/IEC 27004 32
5.4.4 ISO/IEC 27005 32
5.4.5 ISO/IEC 27007 32

5.4.6 ISO/IEC TR 27008 32
5.4.7 ISO/IEC 27013 33
5.4.8 ISO/IEC 27014 33
5.4.9 ISO/IEC TR 27016 34
5.4.10 ISO/IEC 27021 34
5.5 Normen, die branchenspezifische Leitfäden beschreiben 34
5.5.1 ISO/IEC 27010 34
5.5.2 ISO/IEC 27011 35
5.5.3 ISO/IEC 27017 35
5.5.4 ISO/IEC 27018 35
5.5.5 ISO/IEC 27019 36
5.5.6 ISO 27799 37
Literaturhinweise 38