DIN EN ISO/IEC 27000:2017-10 (D)

Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie (ISO/IEC 27000:2016); Deutsche Fassung EN ISO/IEC 27000:2017

Inhalt

Seite

Europäisches Vorwort ... 4

Vorwort ... 5

0 Einleitung ... 6
0.1 Überblick ... 6
0.2 ISMS-Normenfamilie ... 6
0.3 Zweck dieser Internationalen Norm ... 7

1 Anwendungsbereich ... 8

2 Begriffe ... 8

3 Managementsysteme für Informationssicherheit (ISMS) ... 21
3.1 Einleitung ... 21
3.2 Was ist ein ISMS? ... 22
3.2.1 Übersicht und Grundsätze ... 22
3.2.2 Informationen ... 23
3.2.3 Informationssicherheit ... 23
3.2.4 Management ... 23
3.2.5 Managementsystem ... 24
3.3 Prozessorientierter Ansatz ... 24
3.4 Warum ist ein ISMS wichtig? ... 24
3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS ... 25
3.5.1 Übersicht ... 25
3.5.2 Identifizierung von Informationssicherheitsanforderungen ... 26
3.5.3 Beurteilung von Informationssicherheitsrisiken ... 26
3.5.4 Behandlung von Informationssicherheitsrisiken ... 26
3.5.5 Auswahl und Umsetzung von Maßnahmen ... 27
3.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS ... 28
3.5.7 Fortlaufende Verbesserung ... 28
3.6 Kritische Erfolgsfaktoren für das ISMS ... 29
3.7 Nutzen der ISMS-Normenfamilie ... 29

4 Die ISMS-Normenfamilie ... 30
4.1 Allgemeine Informationen ... 30
4.2 Normen, die einen Überblick geben und die Terminologie festlegen ... 31
4.2.1 ISO/IEC 27000 (dieses Dokument) ... 31
4.3 Normen, die Anforderungen festlegen ... 31
4.3.1 ISO/IEC 27001 ... 31
4.3.2 ISO/IEC 27006 ... 32
4.4 Normen, die allgemeine Leitfäden beschreiben ... 32
4.4.1 ISO/IEC 27002 ... 32
4.4.2 ISO/IEC 27003 ... 32
4.4.3 ISO/IEC 27004 ... 32
4.4.4 ISO/IEC 27005 ... 33
4.4.5 ISO/IEC 27007 ... 33
4.4.6 ISO/IEC TR 27008 ... 33
4.4.7 ISO/IEC 27013 ... 33

4.4.8 ISO/IEC 27014 ..... **34**
4.4.9 ISO/IEC TR 27016 ..... **34**
4.5 Normen, die branchenspezifische Leitfäden beschreiben **34**
4.5.1 ISO/IEC 27010 ..... **34**
4.5.2 ISO/IEC 27011 ..... **35**
4.5.3 ISO/IEC TR 27015 ..... **35**
4.5.4 ISO/IEC 27017 ..... **35**
4.5.5 ISO/IEC 27018 ..... **36**
4.5.6 ISO/IEC TR 27019 ..... **36**
4.5.7 ISO 27799 ..... **37**

Anhang A (informativ) Verbformen zur Formulierung von Festlegungen **38**

Anhang B (informativ) Begriffe und Zuständigkeit **39**
B.1 Zuständigkeit für Begriffe **39**
B.2 Begriffe, die in diesen Internationalen Standards verwendet werden **39**
B.2.1 ISO/IEC 27001 ..... **39**
B.2.2 ISO/IEC 27002 ..... **40**
B.2.3 ISO/IEC 27003 ..... **40**
B.2.4 ISO/IEC 27004 ..... **40**
B.2.5 ISO/IEC 27005 ..... **40**
B.2.6 ISO/IEC 27006 ..... **41**
B.2.7 ISO/IEC 27007 ..... **41**
B.2.8 ISO/IEC TR 27008 ..... **41**
B.2.9 ISO/IEC 27010 ..... **41**
B.2.10 ISO/IEC 27011 ..... **41**
B.2.11 ISO/IEC 27014 ..... **42**
B.2.12 ISO/IEC TR 27015 ..... **42**
B.2.13 ISO/IEC TR 27016 ..... **42**
B.2.14 ISO/IEC TR 27017 ..... **42**
B.2.15 ISO/IEC TR 27018 ..... **42**
B.2.16 ISO/IEC TR 27019 ..... **43**

Literaturhinweise **44**