

IT-Risikomanagementhandbuch gemäß ISO 31000 und ISO 27005

Inhaltsverzeichnis

Prüfung und Freigabe	2
Änderungshistorie	3
Dokumentensteuerung und Verteilerkreis	4
1 Vorbemerkung zum IT-Risikomanagement	8
2 Vorwort	9
3 Ziel und Zweck des IT-Risikomanagementhandbuchs	10
4 Relevante Normen und Standards	11
5 Abkürzungen	11
6 Begriffe	11
6.1 Anmerkung zum Begriff „IT-Risiko“	11
7 Grundsätze des IT-Risikomanagements	12
7.1 Allgemeines	12
7.2 Zusammenwirken von IT-Risiko und Informationssicherheitsrisiko	13
8 Das IT-Risikomanagementsystem	14
8.1 Allgemeines	14
8.2 Entwicklung eines IT-Risikomanagementsystems	15
8.3 Führung und Verpflichtung	15
8.4 Integration	16
8.5 Gestaltung	18
8.5.1 Verstehen der Organisation und ihres Zusammenhangs	18
8.5.2 Artikulieren der Risikomanagementverpflichtung	18
8.6 Risikoprofilbeschreibung	19
8.6.1 Aussagen zur Risikomanagementstrategie	19
8.6.2 Die IT-Risikomanagementstrategie	20
8.6.3 Risikobeurteilungskriterien	21
8.6.3.1 Allgemeines	21
8.6.3.2 Risikoklassen	21
8.6.3.3 Kumulative finanzielle und wirtschaftliche Auswirkungen (RK 1)	21
8.6.3.4 Verstoß gegen allgemeine Rechtsvorschriften und anzuwendende Standards (RK 2)	22
8.6.3.5 Verstoß gegen spezifische, die Organisation betreffende Rechtsvorschriften (RK 3)	22
8.6.3.6 Verstoß gegen datenschutzrechtliche Vorgaben (RK 4)	23
8.6.3.7 Verstoß gegen Verträge der Organisation als Auftraggeber und Auftragnehmer (RK 5)	23
8.6.3.8 Beeinträchtigung bei der IT-gestützten Aufgabenerfüllung (RK 6)	24
8.6.3.9 Negative Innen- bzw. Außenwirkung (RK 7)	25
8.6.3.10 Seelische und körperliche Unversehrtheit (RK 8)	25
8.6.4 Aufbauorganisation des IT-Risikomanagements	26
8.6.4.1 Allgemeines	26
8.6.4.2 Aufbauorganisation des Informationssicherheitsrisikomanagements	28

8.6.5 Zuweisung von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten	29
8.6.5.1 Risikoeigner (Risk Owner).....	30
8.6.5.2 Risikomanager.....	30
8.6.5.3 Verantwortliche Person für die Informationsbereitstellung (Informationsgeber)	31
8.6.6 Zuordnung von Ressourcen und Fähigkeiten	31
8.6.6.1 Schulung und Unterweisung.....	32
8.6.7 Einrichten der Kommunikation und Konsultation	33
8.7 Implementierung	33
8.8 Bewertung	34
9 Überwachung des IT-Risikomanagementsystems	35
9.1 Allgemeines	35
9.2 Maßnahmen der Überwachung	35
10 Aufrechterhaltung und Verbesserung des IT-Risikomanagementsystems	36
10.1 Allgemeines	36
10.2 Maßnahmen der Aufrechterhaltung und kontinuierlichen Verbesserung	36
11 Dokumentation des IT-Risikomanagementsystems	38
12 Reporting des IT-Risikomanagementsystems.....	38

Abbildungsverzeichnis

Abbildung 1 - IT-Risikomanagement im Kontext der Organisation	14
Abbildung 2 - Die Integration der Querschnittsfunktion IT-Risikomanagement	17

Bitte dieses Dokument an Ihre Organisation anpassen