E DIN ISO 31000:2011-01 (D)

Erscheinungsdatum: 2011-01-10

Risikomanagement - Grundsätze und Leitlinien (ISO 31000:2009)

Inhalt

Seite

1 Anwendungsbereich ... 8

2 Begriffe ... 8

3 Grundsätze ... 15

4 Risikomanagementrahmen ... 16
4.1 Allgemeines ... 16
4.2 Mandat und Verpflichtung ... 17
4.3 Gestaltung des Rahmens für die Behandlung von Risiken ... 18
4.3.1 Verstehen der Organisation und ihres Zusammenhangs ... 18
4.3.2 Festlegung der Risikomanagementpolitik ... 19
4.3.3 Verantwortlichkeit ... 19
4.3.4 Integration in Organisationsprozesse ... 19
4.3.5 Ressourcen ... 20
4.3.6 Aufbau von Mechanismen für die interne Kommunikation und Berichterstattung ... 20
4.3.7 Aufbau von Mechanismen für die externe Kommunikation und Berichterstattung ... 20
4.4 Umsetzung des Risikomanagements ... 21
4.4.1 Umsetzung des Rahmens für die Behandlung von Risiken ... 21
4.4.2 Umsetzung des Risikomanagementprozesses ... 21
4.5 Überwachung und Überprüfung des Rahmens ... 21
4.6 Kontinuierliche Verbesserung des Rahmens ... 21

5 Prozess ... 22
5.1 Allgemeines ... 22
5.2 Kommunikation und Konsultation ... 22
5.3 Erstellen des Zusammenhangs ... 23
5.3.1 Allgemeines ... 23
5.3.2 Erstellen des externen Zusammenhangs ... 24
5.3.3 Erstellen des internen Zusammenhangs ... 24
5.3.4 Erstellen des Zusammenhangs für den Risikomanagementprozess ... 25
5.3.5 Festlegung von Risikokriterien ... 26
5.4 Risikobeurteilung ... 26
5.4.1 Allgemeines ... 26
5.4.2 Risikoidentifikation ... 26
5.4.3 Risikoanalyse ... 27
5.4.4 Risikobewertung ... 27
5.5 Risikobewältigung ... 28
5.5.1 Allgemeines ... 28
5.5.2 Auswahl von Maßnahmen zur Risikobewältigung ... 28
5.5.3 Erstellung und Umsetzung von Risikobewältigungsplänen ... 29
5.6 Überwachung und Überprüfung ... 29
5.7 Aufzeichnungen über den Risikomanagementprozess ... 30

Anhang A (informativ) Merkmale eines erweiterten Risikomanagements ... 31
A.1 Allgemeines ... 31
A.2 Wesentliche Ergebnisse ... 31
A.3 Merkmale ... 31
A.3.1 Kontinuierliche Verbesserung ... 31
A.3.2 Vollständige Verantwortung für Risiken ... 31
A.3.3 Anwendung des Risikomanagements in allen Entscheidungen ... 32
A.3.4 Kontinuierliche Kommunikation ... 32
A.3.5 Vollständige Integration in die Unternehmensführung der Organisation ... 32