

**IT-Risikomanagementhandbuch
gemäß ISO 31000 und ISO 27005**

LESEPROBE

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 Risikoprofillbeschreibung	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

LESEPROBE

1 Vorbemerkung zum IT-Risikomanagement

Die Ausrichtung dieses Handbuchs soll es ermöglichen, die Identifikation, die Analyse sowie die Bewertung und die Behandlung von Risiken des IT-gestützten Geschäftsbetrieb (IT-Risiken) organisationspezifisch steuern zu können.

Grundsätzlich beschreibt dieses Handbuch die Implementierung, die Integration, den Betrieb sowie die Verbesserung und kontinuierliche Aufrechterhaltung eines Risikomanagementsystems, gemäß der ISO Normenfamilie 310xx, wobei die Ausrichtung dieses Handbuchs die gesonderte Betrachtung von IT-Risiken, und somit respektive die Betrachtung von Informationssicherheitsrisiken gemäß der Norm ISO 27005, adressiert.

Neben den grundlegenden Anforderungen an das Management von Risiken sowie dem Aufbau eines

DGI®

2 Vorwort

Ein systematisches Informationsrisikomanagement muss als integraler Bestandteil eines Informationssicherheitsmanagementsystems umgesetzt und den Anforderungen an die spezifischen Gegebenheiten des Geschäftsbetriebs gerecht werden.

Für eine angemessene Risikobehandlung zur Steuerung der Informationssicherheitsrisiken kommt dem IT-Risikomanagement eine zentrale und tragende Rolle zu.

Die eruierten Informationssicherheitsrisiken der eigenen Organisation dienen der Unternehmensführung für die Priorisierung und zeitgerechte Umsetzung von Maßnahmen zur Sicherstellung der Schutzziele, wie der Umgang mit Daten und Informationen sowie der Betrieb von Infrastruktur, Systemen, Anwendungen und Netzen des Geschäftsbetriebs dies einfordert.

DGI®

Organisationsprozesse kontinuierlich werden, der den einzelnen, stützungsgeleiteten und kontinuierlichen Geschäftsbetrieb, unter Einbeziehung der Unternehmensstrategie, unterstützt und sich an der Vermeidung von unerwünschten Zwischenfällen ausrichtet.

Dies erfordert eine regelmäßige, proaktive sowie nach gravierenden Änderungen und bedeutsamen Sicherheitsvorfällen vorzunehmende, Betrachtung und Beurteilung der Risikosituationen für das eigene Unternehmen sowie die Bewertung der Wirksamkeit bestehender risikominimierender Maßnahmen, um das Risikomanagement kontinuierlich weiterentwickeln zu können.

3 Ziel und Zweck des IT-Risikomanagementhandbuchs

Durch die in diesem Handbuch beschriebenen Grundsätze und Anforderungen soll insbesondere Folgendes sichergestellt werden

- Die Einbettung des Informationssicherheitsrisikomanagement in das zentrale Risikomanagement
- Die Identifikation, Bewertung und Behandlung von Risiken, die sich aus dem IT-gestützten Geschäftsbetrieb ergeben
- Die Identifikation und Umsetzung erforderlicher Maßnahmen der Informationssicherheit
- Die Sicherstellung der Erfüllung von normativen Anforderungen, insbesondere aus der ISO 310xx -Normenfamilie sowie aus der ISO 270xx-Normenfamilie

Um den Anforderungen der Einrichtung eines Überwachungssystems nachzukommen, die den Fortbestand des Unternehmens gefährdende Entwicklungen frühzeitig erkennen müssen, ist die

DGI®

Wirksamkeit von umgesetzten Maßnahmen der Informationssicherheit regelmäßig überprüft werden

Zudem erfüllt das dokumentierte IT-Risikomanagementsystem mögliche Anforderungen, die seitens Dritter, wie von Kunden, Lieferanten, Wirtschaftsprüfern oder Auditoren, an die Organisation gestellt werden.

4 Relevante Normen und Standards

Die Organisation berücksichtigt im Rahmen der Umsetzung des IT-Risikomanagementsystems die ISO 310xx-Normenfamilie sowie die ISO 270xx-Normenfamilie.

Dieses Handbuch erfüllt zudem vollständig die Anforderungen des BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik.

5 Abkürzungen

IT-RMS	IT- Risikomanagementsystem
RMS	Risikomanagementsystem



DGI®

für die Unterstützung des IT-gestützten Geschäftsbetriebs sowie in Anlehnung an einen szenariobasierten Ansatz vorgenommen werden.

Zudem müssen bei der Betrachtung von IT-Risiken neben den strategischen Unternehmensvorgaben für den IT-Betrieb und die Sicherstellung insbesondere der funktionsfähigen Infrastruktur, der funktionsfähigen Systeme, der funktionsfähigen Anwendungen sowie der erforderlichen IT-Supportprozesse zusätzlich zeitliche sowie sonstige kritische Parameter betrachtet werden.

7 Grundsätze des IT-Risikomanagements

7.1 Allgemeines

Das IT-Risikomanagement sollte erforderliche IT Risk Assessments respektive Datenschutzfolgenabschätzungen oder Business Impact Analysen initiieren und die Durchführung begleiten.

Grundsätzliche Aussagen für ein effektives IT-Risikomanagement sind

- Das IT-Risikomanagement ist ein integraler Bestandteil aller Aktivitäten des <UNTERNEHMENSNAME> (nachfolgend als Organisation bezeichnet) und muss einen strukturierten und ganzheitlichen Risikomanagementansatz verfolgen, um konsistente und vergleichbare Ergebnisse zu erzielen.

DGI®

- Zu berücksichtigen gilt es, dass menschliches Verhalten und kulturelle Einwirkungen einen wesentlichen Einfluss auf sämtliche relevanten Aspekte des IT-Risikomanagements haben.
- Die Aufrechterhaltung und kontinuierliche Verbesserung des IT-Risikomanagementsystems, insbesondere unter Einbeziehung der Risikokommunikation und Risikokonsultation sowie der Risikoüberwachung und Risikoüberprüfung, muss als zwingende Verpflichtung angesehen werden und muss durch den Aufbau und die Vermittlung von Wissen sowie durch das Einbringen von Erfahrung unterstützt werden.