DGI® Deutsche Gesellschaft für Informationssicherheit AG

IT-Risikomanagementhandbuch gemäß ISO 31000 und ISO 27005

Inhaltsverzeichnis

Abbildungsverzeichnis

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) organisationsspezifisch 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

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 den Geschäftsbetrieb dies erfordert.

Organisationsprozess verstanden werden, der den sicheren, ordnungsgemäßen und konformen 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, untersucht u. a. 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.

- 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.