

**Management des
Informationssicherheitsrisiko-
managementprozesses
gemäß ISO 27005**

- Durchführung der Risikobeurteilung und der
Risikobehandlung von Informationssicherheitsrisiken -

- Konzept -

Inhaltsverzeichnis

| | |
|---|----|
| Prüfung und Freigabe | 2 |
| Änderungshistorie | 3 |
| Dokumentensteuerung und Verteilerkreis | 4 |
| 1 Ziel und Zweck | 8 |
| 2 Geltungsbereich | 8 |
| 3 Verantwortlichkeiten für das Management dieser Regelung | 8 |
| 4 Begriffe | 9 |
| 4.1 Anmerkung zum Begriff „Informationssicherheitsrisiko“ | 9 |
| 5 Management des Informationssicherheitsrisikomanagementprozesses | 11 |
| 5.1 Allgemeines | 11 |
| 5.2 Zusammenwirken von IT-Risiko und Informationssicherheitsrisiko | 11 |
| 6 Der Informationssicherheitsrisikomanagementprozess | 12 |
| 6.1 Allgemeines | 12 |
| 6.2 Umsetzung des Informationssicherheitsrisikomanagementprozesses | 13 |
| 6.3 Festlegung des Kontexts für das Informationssicherheitsrisikomanagement | 15 |
| 6.3.1 Allgemeines | 15 |
| 6.3.2 Zuweisung von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten | 15 |
| 6.3.3 Anforderungen der interessierten Parteien (Stakeholder) | 16 |
| 6.3.4 Festlegung und Aufrechterhaltung von Kriterien für die Informationssicherheitsrisiken | 17 |
| 6.3.4.1 Allgemeines | 17 |
| 6.3.4.2 Kriterien für die Ermittlung der Risikoakzeptanz | 18 |
| 6.3.4.3 Kriterien für die Ermittlung der Risikobewertung | 19 |
| 6.3.5 Entwicklung der Kriterien für die Durchführung der Informationssicherheitsrisiko-Assessments | 21 |
| 6.3.5.1 Allgemeines | 21 |
| 6.3.5.2 Kriterien für die Bewertung der Folgen eines Informationssicherheitsvorfalls | 23 |
| 6.3.5.3 Kriterien für die Bewertung der Eintrittswahrscheinlichkeit eines Informationssicherheitsvorfalls | 25 |
| 6.3.5.4 Kriterien für die Bewertung des Risikoniveaus | 27 |
| 7 Umsetzung des Informationssicherheitsrisiko-Assessment (Risikobeurteilung) | 28 |
| 7.1 Allgemeines | 28 |
| 7.2 Verantwortung der obersten Leitung | 30 |
| 7.3 Identifizierung von Informationssicherheitsrisiken | 31 |
| 7.3.1 Allgemeines | 31 |
| 7.3.2 Identifizierung und Beschreibung von Informationssicherheitsrisiken | 33 |
| 7.3.3 Identifizierung von Risikoeignern | 33 |
| 7.4 Analyse von Informationssicherheitsrisiken | 34 |
| 7.4.1 Allgemeines | 34 |
| 7.4.2 Abschätzung und Bewertung möglicher Folgen | 35 |

| | |
|--|----|
| 7.4.3 Bewertung der Eintrittswahrscheinlichkeit | 36 |
| 7.4.4 Bestimmung des Risikoniveaus..... | 38 |
| 7.5 Bewertung der Akzeptanz der Informationssicherheitsrisiken..... | 39 |
| 7.6 Priorisierung der analysierten Risiken für die Risikobehandlung | 40 |
| 8 Umsetzung der Risikobehandlung | 41 |
| 8.1 Allgemeines | 41 |
| 8.2 Auswahl der geeigneten Optionen für die Risikobehandlung..... | 42 |
| 8.2.1 Optionen der Risikobehandlung..... | 43 |
| 8.3 Festlegung der Maßnahmen für die Risikobehandlung..... | 44 |
| 8.4 Erstellung der Pläne für die Risikobehandlung..... | 46 |
| 8.4.1 Allgemeines..... | 46 |
| 8.4.2 Umsetzung der Maßnahmen eines Risikobehandlungsplans..... | 47 |
| 8.4.3 Genehmigung durch die Risikoeigner | 48 |
| 8.4.4 Bewertung der Akzeptanz der Restrisiken der Informationssicherheit | 48 |
| 9 Berücksichtigung des Zusammenwirkens mit ISMS-Prozessen | 50 |
| 9.1 Allgemeines | 50 |
| 9.2 Interne und externe Kommunikation..... | 50 |
| 9.2.1 Allgemeines..... | 50 |
| 9.2.2 Durchführung der internen und externen Kommunikation | 51 |
| 9.3 Dokumentation der Prozesse und Ergebnisse | 53 |
| 9.3.1 Allgemeines..... | 53 |
| 9.3.2 Dokumentation des Risikobewertungs- und Risikobehandlungsprozesses | 53 |
| 9.3.3 Dokumentation der Ergebnisse der Risikobewertung und Risikobehandlung..... | 54 |
| 9.4 Überwachung und Überprüfung..... | 55 |
| 9.4.1 Allgemein..... | 55 |
| 9.4.2 Überwachung und Überprüfung der Risikofaktoren..... | 55 |
| 9.4.3 Überwachung und Überprüfung des Informationssicherheitsrisikomanagementprozesses | 56 |
| 9.5 Managementbewertung | 58 |
| 9.5.1 Allgemeines..... | 58 |
| 9.5.2 Durchführung der Managementbewertung | 58 |
| 9.6 Einleitung von Korrekturmaßnahmen | 59 |
| 9.7 Aufrechterhaltung und Verbesserung des Informationssicherheitsrisikomanagementprozesses..... | 59 |
| 9.7.1 Allgemeines..... | 59 |
| 9.7.2 Maßnahmen der Aufrechterhaltung und kontinuierlichen Verbesserung..... | 60 |
| 10 Sanktionen..... | 61 |
| 11 Referenzierte Dokumente..... | 61 |

Abbildungsverzeichnis

| | |
|---|----|
| Abbildung 1 - Informationssicherheitsrisikomanagementprozess gemäß ISO 27005 | 13 |
| Abbildung 2 - Darstellung der organisationsspezifisch festgelegten Risikobewertungskriterien für finanzielle und wirtschaftliche Schadensauswirkungen | 22 |
| Abbildung 3 - Darstellung der organisationsspezifisch festgelegten Risikobewertungskriterien für die Beeinträchtigung bei der IT-gestützten Aufgabenerfüllung | 22 |
| Abbildung 4 - Darstellung der organisationsspezifisch festgelegten Risikoklassen für die Bewertung der Schadensauswirkungen | 24 |
| Abbildung 5 - Darstellung der organisationsspezifisch festgelegten Bewertungskriterien für die Bestimmung der Eintrittswahrscheinlichkeit eines Informationssicherheitsvorfall | 26 |
| Abbildung 6 - Darstellung der organisationsspezifisch festgelegte Methode für die Bestimmung des Risikoniveaus | 27 |
| Abbildung 7 - Darstellung einer semiquantitativen Bewertungsmöglichkeit für die Bestimmung des Risikoniveaus eines zu betrachtenden Risikoszenarios, in Kombination mit einer dreifarbigem Risikomatrix | 39 |
| Abbildung 8 - Optionen der Risikobehandlung gemäß ISO 27005 | 44 |