\*\*KOSTENLOSE VORSCHAUVERSION\*\*

[Logo der Organisation]

[Name der Organisation]

**METHODIK ZUR RISIKOEINSCHÄTZUNG UND RISIKOBEHANDLUNG**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Datum der Version: |  |
| Erstellt durch: |  |
| Genehmigt durch: |  |
| Vertraulichkeitsstufe: |  |

**Änderungs-Historie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Erstellt durch** | **Beschreibung der Änderung** |
|  | 0.1 | 27001Academy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc120263600)

[2. Referenzdokumente 3](#_Toc120263601)

[3. Methodik zur Risikoeinschätzung und Risikobehandlung 3](#_Toc120263602)

[3.1. Risikoeinschätzung 3](#_Toc120263603)

[3.1.1. Der Prozess 3](#_Toc120263604)

[3.1.2. Werte, Schwachstellen und Bedrohungen 3](#_Toc120263605)

[3.1.3. Festlegung der Risiko-Eigentümer 4](#_Toc120263606)

[3.1.4. Auswirkungen und Wahrscheinlichkeiten 4](#_Toc120263607)

[3.2. Kriterien für Risikoakzeptanz 5](#_Toc120263608)

[3.3. Risikobehandlung 5](#_Toc120263609)

[3.4. Regelmäßige Überprüfung von Risikoeinschätzung und Risikobehandlung. 5](#_Toc120263610)

[3.5. Erklärung zur Anwendbarkeit und Plan zur Risikobehandlung 6](#_Toc120263611)

[3.6. Berichtswesen 6](#_Toc120263612)

[4. Verwaltung von Aufzeichnungen zu diesem Dokument 6](#_Toc120263613)

[5. Gültigkeit und Dokumenten-Handhabung 7](#_Toc120263614)

[6. Anhänge 8](#_Toc120263615)

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung der Methodik für die Einschätzung und die Behandlung von Informationsrisiken bei [Name der Organisation]. Ebenso dient es der Festlegung von akzeptablen Risikoniveaus entsprechend der ISO/IEC 27001 Norm.

Risikoeinschätzung und Risikobehandlung gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), so z.B. für alle Werte die in der Organisation genutzt werden oder die eine Auswirkung auf die Informationssicherheit im Rahmen des ISMS haben könnten.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation] die mit Risikoeinschätzung und Risikobehandlung befasst sind.

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte 6.1.2, 6.1.8, 8.2 und 8.3
* Informationssicherheitspolitik
* Liste rechtlicher, amtlicher, vertraglicher und anderer Anforderungen
* Sicherheitspolitik für Lieferanten
* Erklärung zur Anwendbarkeit

# Methodik zur Risikoeinschätzung und Risikobehandlung

## Risikoeinschätzung

### Der Prozess

Die Risikoeinschätzung wird auf Basis des Verzeichnisses zur Risikoeinschätzung durchgeführt. Der Prozess der Risikoeinschätzung wird von [Stellenbezeichnung] koordiniert. Die Identifizierung von Bedrohungen und Schwachstellen wird von den jeweiligen Eigentümern der durchgeführt, während die Einschätzung von Auswirkungen und Wahrscheinlichkeit von den jeweiligen Risiko-Eigentümern durchgeführt wird.[Stellenbezeichnung] ist für die Aufnahme der Daten über Bedrohungen, Schwachstellen, Folgen und Wahrscheinlichkeit in die Risikobewertungstabelle verantwortlich.

\*\*ENDE DER KOSTENFREIEN VORSCHAU\*\*

Um die Vollversion dieses Dokumentes herunterzuladen, klicken Sie hier:

<https://advisera.com/27001academy/de/documentation/methodik-zur-risikoeinschaetzung-und-risikobehandlung/>