\*\* KOSTENLOSE VORSCHAU \*\*

[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** |
| TT.MM.JJJJ | 0.1 | EUGDPRAcademy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc505023302)

[2. Referenzdokumente 3](#_Toc505023303)

[3. Methodik zur Risikoeinschätzung und Risikobehandlung 3](#_Toc505023304)

[3.1. Risikoeinschätzung 3](#_Toc505023305)

[3.1.1. Der Prozess 3](#_Toc505023306)

[3.1.2. Werte, Schwachstellen und Bedrohungen 3](#_Toc505023307)

[3.1.3. Festlegung der Risiko-Eigentümer 4](#_Toc505023308)

[3.1.4. Auswirkungen und Wahrscheinlichkeiten 4](#_Toc505023309)

[3.2. Kriterien für Risikoakzeptanz 5](#_Toc505023310)

[3.3. Risikobehandlung 5](#_Toc505023311)

[3.4. Regelmäßige Überprüfung von Risikoeinschätzung und Risikobehandlung. 5](#_Toc505023312)

[3.5. Erklärung zur Anwendbarkeit und Plan zur Risikobehandlung 5](#_Toc505023313)

[3.6. Berichtswesen 6](#_Toc505023314)

[4. Verwaltung von Aufzeichnungen zu diesem Dokument 6](#_Toc505023315)

[5. Gültigkeit und Dokumenten-Handhabung 7](#_Toc505023316)

[6. Anhänge 8](#_Toc505023317)

# 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, einschließlich personenbezogener Daten, 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.

### Werte, Schwachstellen und Bedrohungen

Der erste Schritt bei der Risikoeinschätzung ist die Identifikation aller Werte im Rahmen des ISMS Anwendungsbereichs; also z.B. aller Werte, die Auswirkung auf die Vertraulichkeit, Integrität und Verfügbarkeit von Information in der Organisation haben. Werte können Dokumente in Papierform oder elektronischer Form, Anwendungen und Datenbanken, Personen, ITK Gerätschaften, Infrastruktur und externe Services/ausgegliederte Prozesse sein. Bei der Identifikation von Werten ist es ebenso notwendig, deren „Eigentümer“ zu identifizieren, also die Personen oder Organisationseinheiten, die für den jeweiligen Wert verantwortlich sind.

Im nächsten Schritt werden alle Bedrohungen und Schwachstellen identifiziert, die dem jeweiligen Wert zuordenbar sind. Bedrohungen und Schwachstellen werden auf Basis der im Verzeichnis zur Risikoeinschätzung enthaltenen Kataloge identifiziert. Jeder Wert kann mit verschiedenen Bedrohungen verbunden sein und jede Bedrohung kann mit verschiedenen Schwachstellen zusammenhängen.

### Festlegung der Risiko-Eigentümer

Für jedes Risiko muss ein Risiko-Eigentümer identifiziert werden, also eine Person oder Organisationseinheit, die für das jeweilige Risiko verantwortlich ist. Diese Person kann die gleiche sein wie der Eigentümer des Wertes; oder auch nicht.

\*\* ENDE DER KOSTENLOSEN VORSCHAU \*\*

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/27001academy/de/documentation/methodik-zur-risikoeinschaetzung-und-risikobehandlung/>