[Logo der Organisation]

[Name der Organisation]

METHODIK ZUR RISIKOEINSCHÄTZUNG UND RISIKOBEHANDLUNG

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

Commented [27A1]: Um zu erlernen, wie Sie dieses Dokument ausfüllen und echte Beispiele darüber zu sehen, was Sie schreiben müssen, schauen Sie sich dieses Video-Tutorial an:
"How to Write the ISO 27001 Risk Assessment Methodology".

Um auf das Tutorial zuzugreifen: Suchen Sie in Ihrem Posteingang die E-Mail, die Sie zum Zeitpunkt des Kaufes erhalten haben. Dort finden Sie einen Link und ein Passwort, mit denen Sie auf das Video-Tutorial zugreifen können.

Commented [27A2]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A3]: Um zu erfahren, wie Sie die Methodik beschreiben, lesen Sie diese Artikel:

- ISO 27001 Risikobewertung und Risikobehandlung – 6 grundlegende Schritte
https://advisera.com/27001academy/de/knowledgebase/iso-27001-risikobewertung-und-risikobehandlung-6-grundlegende-schritte/

- How to write ISO 27001 risk assessment methodology
https://advisera.com/27001academy/knowledgebase/write-iso-27001-risk-assessment-methodology/

Commented [27A4]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

Änderungs-Historie

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

Inhaltsverzeichnis

1. 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.

2. 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

3. Methodik zur Risikoeinschätzung und Risikobehandlung

3.1. Risikoeinschätzung

3.1.1. Der Prozess

[redacted] die Einschätzung von Auswirkungen und Wahrscheinlichkeit von den jeweiligen Risiko-Eigentümern durchgeführt wird.

3.1.2. Werte, Schwachstellen und Bedrohungen

[redacted] oder elektronischer Form, Anwendungen und Datenbanken, Personen, ITK Gerätschaften, [redacted] verantwortlich sind.

Commented [27A5]: Geben Sie bitte den Namen Ihres Unternehmens an.

Commented [27A6]: Geben Sie bitte den Namen Ihres Unternehmens an.

Commented [27A7]: Bitte ändern Sie dieses Dokument so, dass es mit dem in Ihrem Unternehmen bereits vorhandenem, übereinstimmt. Wenn Sie kein ähnliches Dokument haben, können Sie ein neues im für Sie am besten geeigneten Format erstellen. Sie können dies auch löschen, wenn Sie diese Richtlinie nicht verwenden.

Commented [27A8]: Diese Methodik muss angepasst werden, sofern dies aufgrund gesetzlicher/behördlicher Anforderungen oder vertraglicher Verpflichtungen erforderlich ist.

Commented [27A9]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Commented [27A10]: Zur Vereinfachung des Prozesses kann festgelegt werden, dass der Eigentümer der Werte jedes Risikos auch gleichzeitig der entsprechende Risiko-Eigentümer ist.

Um das Risikobewusstsein der Bestandsbesitzer zu verbessern, können Sie dieses Sicherheitsbewusstseinstraining verwenden: https://training.advisera.com/awareness-session/security-awareness-training/

Commented [27A11]: Auch andere Werte hinzufügen, die nicht in dieser Liste genannt sind.

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

3.1.3. 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.

Commented [27A12]: Zur Vereinfachung des Prozesses kann festgelegt werden, dass der Eigentümer der Werte jedes Risikos auch gleichzeitig der entsprechende Risiko-Eigentümer ist.

3.1.4. Auswirkungen und Wahrscheinlichkeiten

Sobald die Risiko-Eigentümer identifiziert sind, ist es notwendig festzustellen, welche Auswirkungen von jeder Kombination von Bedrohungen und Schwachstellen für jeden einzelnen Wert ausgehen, wenn sich ein entsprechendes Risiko materialisieren würde.

Geringe Auswirkung	0	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt weder den Zahlungsfluss, noch die rechtlichen oder vertraglichen Verpflichtungen oder das Ansehen der Organisation.
Mittlere Auswirkung	1	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität verursacht zusätzliche Kosten und hat geringe oder mäßige Auswirkung auf rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.
Hohe Auswirkung	2	Ein Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität hat beträchtliche und/oder unmittelbare Auswirkung auf den Zahlungsfluss, den Betrieb, rechtliche oder vertragliche Verpflichtungen oder das Ansehen der Organisation.

Nach Einschätzung der Auswirkungen ist es notwendig, die Eintrittswahrscheinlichkeit eines solchen Risikos festzustellen, z.B. die Wahrscheinlichkeit, dass eine Bedrohung die Schwachstelle des betroffenden Werte ausnutzen könnte.

Geringe Wahrschein-lichkeit	0	Bestehende Sicherheitsmaßnahmen sind solide und lieferten bisher ein angemessenes Schutzniveau. Neue Vorfälle werden zukünftig nicht erwartet.
Mittlere Wahrschein-lichkeit	1	Bestehende Sicherheitsmaßnahmen sind modernd und lieferten meist ein angemessenes Schutzniveau. Neue Vorfälle sind zukünftig möglich, jedoch nicht sehr wahrscheinlich.
Hohe Wahrschein-lichkeit	2	Bestehende Schutzmaßnahmen sind auf einem niedrigen Niveau oder unwirksam. Für zukünftige Vorfälle besteht eine hohe Eintrittswahrscheinlichkeit.

Nach dem Eintragen der Werte für Auswirkung und Eintrittswahrscheinlichkeit im Vorgängers zur Risikoeinschätzung wird das Risikoniveau automatisch durch Addieren der zwei Werte berechnet.

[redacted]

3.2. Kriterien für Risikoakzeptanz

Die Werte 0, 1 und 2 sind akzeptable Risiken, während die Werte 3 und 4 inakzeptable Risiken sind. Inakzeptable Risiken müssen behandelt werden.

3.3. Risikobehandlung

[redacted] werden. Risikobehandlung wird von [Stellenbezeichnung] durchgeführt.

Commented [27A13]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Eine oder mehrere Optionen zur Risikobehandlung müssen für die mit 3 oder 4 bewerteten Risiken ausgewählt werden:

1. [redacted]
2. [redacted] Unterzeichnung eines Vertrages mit Lieferanten oder Partnern
3. Risikovermeidung durch Beendigung einer Geschäftsaktivität, welches dieses Risiko [redacted]
4. [redacted] Auswirkung im Fall dass sich das Risiko materialisiert.

Commented [27A14]: Bei der Auswahl der [redacted]

Commented [27A15]: Zum Beispiel: Norm ISO 27001 Anhang A Maßnahmen, NIST Spezialpublikationen, etc.

Für die Auswahl der Optionen wird das Verzeichnis zur Risikobehandlung genutzt. Üblicherweise wird [redacted] Spezifikation des Risikos zusätzliche Zeilen ein.

Die sich auf ausgelagerte Prozesse beziehende Risikobehandlung muss in den mit den [redacted]

Commented [27A16]: Löschen falls Sie diese Politik nicht anwenden.

[redacted] nach der Umsetzung der Maßnahmen einen neuen Risikowert ergibt.

Commented [27A17]: Dieser neue Wert wird „Restrisiko“ genannt.

Im Fall der Option 1 (Auswahl von Sicherheitsmaßnahmen) ist es notwendig, den neuen Wert für [redacted]

3.4. Regelmäßige Überprüfung von Risikoeinschätzung und Risikobehandlung.

[redacted] häufiger, falls es bedeutende organisatorische Änderungen, technische Änderungen, Änderungen der Geschäftsziele, Veränderungen im Geschäftsumfeld, etc. geben sollte.

3.5. Erklärung zur Anwendbarkeit und Plan zur Risikobehandlung

[Stellenbezeichnung] muss das folgende in der Erklärung zur Anwendbarkeit dokumentieren: Welche [illegible]

Im Namen des Risiko-Eigentümers anerkennt [Top-Management] sämtliche Restrisiken mittels der Erklärung zur Anwendbarkeit.

[illegible] der Risiko-Eigentümer.

3.6. Berichtswesen

[Stellenbezeichnung] dokumentiert die Ergebnisse der Risikoeinschätzung und der Risikobehandlung, [illegible]

[illegible]

4. Verwaltung von Aufzeichnungen zu diesem Dokument

Name der Aufzeichnung	*Aufbewahrungs-Ort*	*Verantwortlicher für Aufbewahrung*	*Maßnahme zum Schutz der Aufzeichnung*	*Aufbewahrungs -Dauer*
Verzeichnis der Risikoeinschätzung (elektronische Form - Excel Dokument)	Rechner von [Stellenbezeichnung]	[Stellenbezeichnung des Eigentümers des Verzeichnisses zur Risikoeinschätzung]	Nur [Stellenbezeichnung] ist berechtigt, Einträge oder Änderungen am Verzeichnis zur Risikoeinschätzung vorzunehmen.	Die Daten werden dauerhaft aufbewahrt.
Verzeichnis der Risikobehandlung (elektronische Form - Excel Dokument)	Rechner von [Stellenbezeichnung]	[Stellenbezeichnung des Eigentümers des Verzeichnisses zur Risikobehandlung]	Nur [Stellenbezeichnung] ist berechtigt, Einträge oder Änderungen am Verzeichnis zur Risikobehandlung vorzunehmen.	Die Daten werden dauerhaft aufbewahrt.
Bericht zur	Rechner von	[Stellenbezeichnung	Der Bericht wird in	Der Bericht

Commented [27A18]: Sollte diese Risikoübernahme aus [illegible]

Commented [27A19]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Commented [27A20]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Commented [27A21]: Dies ist lediglich eine Empfehlung. Häufigkeit nach Bedarf anpassen.

Commented [27A22]: Zum Beispiel: CEO, Verantwortlicher für den Geschäftsbereich, etc.

Commented [27A23]: Die Daten in dieser Spalte entsprechend der wirklichen Bedürfnisse anpassen.

Commented [27A24]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Commented [27A25]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Risikoeinschätzung und Risikobehandlung (elektronische Form – PDF Format)	[Stellenbezeichnung]	des Eigentümers des Berichts]	schreib-geschütztem PDF-Format erstellt	wird für den Zeitraum von 3 Jahren aufbewahrt
Erklärung zur Anwendbarkeit (elektronische Form – PDF Format)	Rechner von [Stellenbezeichnung]	[Stellenbezeichnung des Eigentümers des Berichts]	Nur [Stellenbezeichnung] ist berechtigt, Einträge oder Änderungen an der Erklärung zur Anwendbarkeit vorzunehmen.	Ältere Versionen der EzA werden für den Zeitraum von 3 Jahren aufbewahrt
Plan zur Risikobehandlung (elektronische Form – Word Dokument)	Rechner von [Stellenbezeichnung]	[Stellenbezeichnung der für den Plan zur Risikobehandlung verantwortlichen Person]	Lediglich [Stellenbezeichnung] ist befugt, Eingaben in den Plan zur Risikobehandlung zu machen und Änderungen vorzunehmen	Ältere Versionen des Plans zur Risikobehandlung werden für den Zeitraum von 3 Jahren aufbewahrt

Nur [Stellenbezeichnung] kann anderen Mitarbeitern Zugang zu jeglichen der oben genannten Dokumente gewähren.

Commented [27A26]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum].

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich prüfen und aktualisieren muss, bevor die reguläre Überprüfung der Risikoeinschätzung stattfindet.

Commented [27A27]: ZB.: Informationssicherheitsmanager, Sicherheitsmanager usw.

Commented [27A28]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- [illegible]
- [illegible]
- [illegible]

6. Anhänge

- Anhang 1 – Verzeichnis der Risikoeinschätzung
- Anhang 2 – Verzeichnis der Risikobehandlung
- Anhang 3 – Bericht zur Risikoeinschätzung und Risikobehandlung

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A29]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.