Anhang 3 – Bericht zur Risikoeinschätzung und Risikobehandlung

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 ISO 27001 Risk Assessment Report".

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.

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 Bereitstellung einer detaillierten Übersicht des Prozesses und der Dokumente die für die Einschätzung und Behandlung von Informationsrisiken bei [Name der Organisation] im Zeitraum [Zeitraum angeben] genutzt wurden.

Commented [27A2]: Geben Sie bitte den Namen Ihrer Organisation an.

Die Risikoeinschätzung wurde auf das gesamte Informationssicherheits-Managementsystem (ISMS) angewendet.

Dieses Dokument ist bestimmt für das Top-Management von [Name der Organisation], [Stellenbezeichnung des Verantwortlichen für Informationssicherheit], die Eigentümer von Informationswerten und alle die mit der Planung, Umsetzung, Überwachung und Verbesserung des ISMS befasst sind.

Commented [27A3]: Geben Sie bitte den Namen Ihrer Organisation an.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte 8.2 und 8.3
- Dokument zum ISMS Anwendungsbereich
- Informationssicherheitspolitik
- Methodik zur Risikoeinschätzung und Risikobehandlung

3. Prozess der Einschätzung und Behandlung von Informationsrisiken

Der gesamte Risikoeinschätzungs- und Risikobehandlungs-Prozess wurde entsprechend des [illegible]

3.1. Zweck des Risikomanagements

[illegible]
Kenngrößen um die Kritikalität der individuellen Risiken festlegen zu können.

[illegible]

3.2. Anwendungsbereich für Risikoeinschätzung und Risikobehandlung

In Übereinstimmung mit dem Dokument zum ISMS Anwendungsbereich wurden Risikoeinschätzung [illegible]

Commented [27A4]: Beziehen Sie nur die Organisationseinheiten ein, in denen die Risikoeinschätzung und Risikobehandlung durchgeführt wurden.

3.3. Zeitraum

Risikoeinschätzung wurde im Zeitraum von [Tag/Monat/Jahr] bis [Tag/Monat/Jahr] durchgeführt.

3.4. Prozessbeteiligte und Informationssammlung

den Namen und die Firma angeben].

Während der Risikoeinschätzung wurden Informationen mittels Fragebögen und Interviews mit

Commented [27A5]: ZB.: Sicherheitsmanager, Informationssicherheitsmanager usw.

Commented [27A6]: Sie können dieses löschen, wenn kein spezialisierter Berater hinzugezogen wurde.

Commented [27A7]: Oder ersetzen Sie das durch andere angewandte Methoden, sofern zutreffend.

3.5. Kurzer Überblick zur angewendeten Methodik

Kurzfassung der Prozessumsetzung wie folgt:

- Auswirkungen des Verlustes von Vertraulichkeit, Integrität und Verfügbarkeit wurden mit den Werten 0 bis 2 bewertet
- Wahrscheinlichkeit errechnet
- Mit 3 und 4 bewertete Risiken wurden als inakzeptable Risiken angesehen
- Sicherheitsmaßnahmquellen

Commented [27A8]: Löschen Sie diesen Text, wenn nur die Maßnahmen aus Anhang A der ISO / IEC 27001 angewendet wurden.

3.6. Überblick zu den im Risikoeinschätzungs- und Risikobehandlungs-Prozess genutzten Dokumenten

und Risikobehandlung genutzt oder erstellt:

- Wahrscheinlichkeit an und berechnet das Risiko.
- Das Verzeichnis der Risikobehandlung (Anhang 2) zeigt die Optionen für die

4. Gültigkeit und Dokumenten- Handhabung

Dieses Dokument ist gültig ab [Datum], Eigentümer dieses Dokuments ist [Stellenbezeichnung].

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

5. Anhänge

- Anhang 1 – Verzeichnis der Risikoeinschätzung
- Anhang 2 – Verzeichnis der Risikobehandlung

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A10]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.