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 2

2. REFERENZDOKUMENTE 2

3. PROZESS DER EINSCHÄTZUNG UND BEHANDLUNG VON INFORMATIONSRISIKEN 2

3.1. ZWECK DES RISIKOMANAGEMENTS 2
3.2. ANWENDUNGSBEREICH FÜR RISIKOEINSCHÄTZUNG UND RISIKOBEHANDLUNG 2
3.3. ZEITRAUM 2
3.4. PROZESSBETEILIGTE UND INFORMATIONSSAMMLUNG 3
3.5. KURZER ÜBERBLICK ZUR ANGEWENDETEN METHODIK 3
3.6. ÜBERBLICK ZU DEN IM RISIKOEINSCHÄTZUNGS- UND RISIKOBEHANDLUNGS-PROZESS GENUTZTEN DOKUMENTEN 3

4. GÜLTIGKEIT UND DOKUMENTEN- HANDHABUNG 3

5. ANHÄNGE 4

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

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 störenden Risiken 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 Betriebliche Kontinuitätsmanagement System (BKMS) 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 BKMS befasst sind.

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

2. Referenzdokumente

- ISO 22301 Norm, Abschnitt 8.2.3
- Richtlinie zum betrieblichen Kontinuitätsmanagement
- Methodik zur Risikoeinschätzung und Risikobehandlung

Commented [27A4]: Sie finden die Vorlage für dieses Dokument im ISO 22301 Toolkit Ordner "03_Richtlinie_zum_betrieblichen_Kontinuitätsmanagement".

3. Prozess der Einschätzung und Behandlung von Informationsrisiken

Der gesamte Risikoeinschätzungs- und Risikobehandlungs-Prozess wurde entsprechend des Dokuments über die Methodik zur Risikoeinschätzung und Risikobehandlung durchgeführt.

3.1. Zweck des Risikomanagements

Der Zweck der Risikoeinschätzung ist die Identifikation aller Werte, ihrer Schwachstellen und der Bedrohungen, die solche Schwachstellen ausnutzen könnten, sowie die Bewertung dieser Kenngrößen um die Kritikalität der individuellen Risiken festlegen zu können.

[illegible]

3.2. Anwendungsbereich für Risikoeinschätzung und Risikobehandlung

[illegible]

Commented [27A5]: Beziehen Sie nur die Organisationseinheiten ein, in denen die Risikoeinschätzung und Risikobehandlung durchgeführt wurden.

3.3. Zeitraum

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

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

3.4. Prozessbeteiligte und Informationssammlung

Die Risikoeinschätzungs- und Risikobehandlungs-Prozesse wurden von [Name und Stellenbezeichnung] geleitet. Unterstützt wurde er dabei von [falls ein spezialisierter Berater hinzugezogen wurde, hier den Namen und die Firma angeben].

Commented [27A6]: ZB.: Manager der betrieblichen Kontinuität, Sicherheitsmanager, Informationssicherheitsmanager usw.

Commented [27A7]: Sie können dieses löschen, wenn kein spezialisierter Berater hinzugezogen wurde.

Commented [27A8]: Oder ersetzen Sie das durch andere angewandte Methoden, sofern zutreffend.

3.5. Kurzer Überblick zur angewendeten Methodik

Kurzfassung der Prozessumsetzung wie folgt:

- alle Werte und deren jeweiligen Eigentümer wurden identifiziert
- die Eigentümer jedes Risikos wurden identifiziert
- Auswirkungen des Verlustes von Verfügbarkeit wurden mit den Werten 0 bis 2 bewertet

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

Die im Folgenden genannten Dokumente wurden während der Umsetzung der Risikoeinschätzung und Risikobehandlung genutzt oder erstellt:

- Das Verzeichnis der Risikoeinschätzung (Anhang 1) zeigt jede Kombination von Werten, Schwachstellen und Bedrohungen auf, gibt die Werte von Auswirkungen und Wahrscheinlichkeit an und berechnet das Risiko.

4. Gültigkeit und Dokumenten- Handhabung

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

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

Commented [27A9]: ZB.: Manager der betrieblichen Kontinuität, 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.

©2020 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.