**Anhang 3 – Interne Audit-Checkliste für ISO 27001 und ISO 22301**

\*\* KOSTENLOSE VORSCHAU \*\*

# Interne Audit-Checkliste für ISO 27001

|  |  |  |  |
| --- | --- | --- | --- |
| Abschnitt | Anforderung der Norm | Konform? Ja/Nein | … |
| 4.2.1 | Hat die Organisation die interessierte Parteien identifiziert? |  |  |
| … | … |  |  |
| 4.2.2 | Hat die Organisation einen Prozess festgelegt, um die geltenden und behördlichen Anforderungen zu erfüllen? |  |  |
| … | … |  |  |
| 5.2 | Ist das BKMS kompatibel mit dem Zweck des Unternehmens? |  |  |
| … | … |  |  |
| 5.2 | Existiert eine Richtlinie für betriebliche Kontinuität und definiert sie den Rahmen für die Festlegung von Zielen? |  |  |
| … | … |  |  |
| 5.3 | Wurde die für das BKMS verantwortliche Person ernannt und hat diese Person ausreichende Befugnisse? |  |  |
| … | … |  |  |
| 6.1.2 | Ist das Risikoeinschätzungsverfahren dokumentiert, einschließlich der Kriterien zur Risikoakzeptanz und Kriterien zur Risikoeinschätzung? |  |  |
| … | … |  |  |
| 6.1.3 | Ist das Risikobehandlungsverfahren dokumentiert, einschließlich der Optionen für die Risikobehandlung? |  |  |
| … | … |  |  |
| 6.1.3 | Wurde die Erklärung zur Anwendbarkeit einschließlich der Rechtfertigungen und dem Status für jede Maßnahme erstellt? |  |  |
| … | … |  |  |
| 6.2 | Definiert der Plan der Risikobehandlung, wer für die Umsetzung welcher Maßnahmen verantwortlich ist, welche Ressourcen dafür herangezogen werden und welche Auswertungsmethode angewendet wird? |  |  |
| … | … |  |  |
| 7.1 | Werden für alle Elemente des ISMS angemessene Ressourcen bereitgestellt? |  |  |
| … | … |  |  |
| 7.3 | Ist das Personal sich bewusst über die Informationssicherheitspolitik, deren jeweilige Rollen im Rahmen derselben, sowie der Konsequenzen bei Nichteinhaltung der Vorschriften? |  |  |
| … | … |  |  |
| … | … |  |  |
| 7.5 | Werden Dokumente externer Herkunft kontrolliert/geprüft? |  |  |
| … | … |  |  |
| 8.3.2 | Werden Strategien und Lösungen der betrieblichen Kontinuität identifiziert? |  |  |
| 8.3.3 | Werden Strategien und Lösungen ausgewählt, die auf den für jede Aktivität festgelegten Wiedererholungszielen basieren? |  |  |
| … | … |  |  |
| 8.6 | Werden regelmäßige Überprüfungen der Dokumentation durchgeführt und alle Anforderungen bewertet? |  |  |
| … | … |  |  |
| 8.6 | Wird die Leistungsfähigkeit der betrieblichen Kontinuität bei Lieferanten und Partnern bewertet? |  |  |
| … | … |  |  |
| 9.1 | Sind die Messresultate dokumentiert und werden an die verantwortliche Person gemeldet? |  |  |
| … | … |  |  |
| … | … |  |  |

# Interne Audit-Checkliste für ISO 22301

|  |  |  |  |
| --- | --- | --- | --- |
| Abschnitt | Anforderung der Norm | Konform? Ja/Nein | … |
| 4.2 | Hat die Organisation interessierte Parteien festgelegt? |  |  |
| … | … |  |  |
| 4.3 | Ist der Anwendungsbereich dokumentiert, definiert er, welche Produkte und Dienstleistungen eingeschlossen sind, und werden die Ausnahmen erklärt? |  |  |
| … | … |  |  |
| 5.2 | Ist das BKMS kompatibel mit der Firmenstrategie? |  |  |
| … | … |  |  |
| 5.2 | Wurde eine für das BKMS verantwortliche Person ernannt und verfügt diese Person über ausreichend Authorität? |  |  |
| … | … |  |  |
| 5.3 | Wird die Richtlinie zum betrieblichen Kontinuitätsmanagement innerhalb der Firma kommuniziert? |  |  |
| … | … |  |  |
| 6.1 | Hat die Organisation alle Risiken und Gelegenheiten identifiziert? |  |  |
| … | … |  |  |
| 6.2 | Wurden die Zielvorgaben der betrieblichen Kontinuität festgelegt und wurden sie an alle relevanten Mitarbeiter kommuniziert? |  |  |
| … | … |  |  |

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

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/27001academy/de/documentation/pruefliste-fuer-das-interne-audit/>