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

\*\* KOSTENLOSE VORSCHAU \*\*

|  |  |  |  |
| --- | --- | --- | --- |
| Abschnitt | Anforderung der Norm | Konform? Ja/Nein | Beweis(e) |
| 4.2 | Hat die Organisation die interessierte Parteien identifiziert? |  |  |
| 4.2 | ... |  |  |
| 4.3 | Ist der Anwendungsbereich durch klar definierte Grenzen und Schnittstellen dokumentiert? |  |  |
| 5.1 | ... |  |  |
| 5.1 | Stellt die Leitung sicher, dass ISMS seine Zielvorgaben auch erreicht? |  |  |
| 5.2 | ... |  |  |
| 5.2 | ... |  |  |
| 5.3 | Sind Rollen und Verantwortlichkeiten für Informationssicherheit vergeben und kommuniziert? |  |  |
| 6.1.2 | ... |  |  |
| 6.1.2, 8.2 | Sind die Risiken, deren Eigentümer, Wahrscheinlichkeit, Konsequenzen und die Risikostufe identifiziert? Sind diese Resultate dokumentiert? |  |  |
| 6.1.3 | ... |  |  |
| 6.1.3, 8.3 | Wurden alle nichtakzeptablen Risiken mittels der Optionen und Maßnahmen aus Anhang A behandelt? Sind diese Resultate dokumentiert? |  |  |
| 6.1.3 | ... |  |  |
| 6.1.3, 8.3 | Existiert ein Plan der Risikobehandlung und wurde er von den Risikoeigentümern genehmigt? |  |  |
| 6.2 | ... |  |  |
| 7.1 | Werden für alle Elemente des ISMS angemessene Ressourcen bereitgestellt? |  |  |
| 7.2 | ... |  |  |
| 7.3 | Ist das Personal sich bewusst über die Informationssicherheitspolitik, deren jeweilige Rollen im Rahmen derselben, sowie der Konsequenzen bei Nichteinhaltung der Vorschriften? |  |  |
| 7.4 | ... |  |  |
| 7.5 | .... |  |  |
| 7.5 | Werden Dokumente externer Herkunft kontrolliert/geprüft? |  |  |

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

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/eugdpracademy/de/documentation/iso-27001-interne-audit-checkliste/>