**Projekt–Checkliste für die Umsetzung von ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| **Umsetzungsphasen** | **Aufgaben** | **Zu verwendende Dokumente aus dem Toolkit** | **Erledigt** |
| *Unterstützung des Managements einholen* | Recherchieren Sie, welche Vorteile von ISO 27001 für Ihr Unternehmen anwendbar wären. | - |  |
| Präsentieren Sie dem Management die Vorteile und holen Sie sich dessen Engagement ein. | - |  |
| Holen Sie eine formelle Genehmigung für den Beginn der Projektplanung ein. | - |  |
|  |  |  |
| *Bereiten Sie Ihr Projekt vor* | Schreiben Sie das Verfahren zur Lenkung von Dokumenten. | 01 – Verfahren zur Lenkung von Dokumenten und Aufzeichnungen |  |
| Bilden Sie Ihr Projektteam aus. | - |  |
| Schreiben Sie den Projektplan einschließlich der Definition von Projektleiter, Projektteam, Projektsponsor, erforderlichen Ressourcen und Meilensteinen. | 02 – Projektplan |  |
| Legen Sie fest, welche Beteiligten über jeden Projektschritt informiert werden müssen. | - |  |
| Organisieren Sie ein Kick-off-Meeting. | - |  |
|  |  |  |
| *Identifizieren Sie Anforderungen* | Legen Sie das Verfahren zur Ermittlung der interessierten Parteien fest. | 03 – Verfahren zur Identifikation der Anforderungen |  |
| Identifizieren Sie die Anforderungen der interessierten Parteien. | 03.1 – Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen |  |
|  |  |  |
| *Definieren Sie den Anwendungsbereich, die Managementabsichten und die Verantwortlichkeiten* | Schreiben Sie das Dokument zum ISMS Anwendungsbereich. | 04 – ISMS Anwendungsbereich |  |
| Schreiben Sie die Informationssicherheitspolitik. | 05 – Informationssicherheitspolitik |  |
| Setzen Sie die Informationssicherheitsziele fest. | 05 – Informationssicherheitspolitik |  |
|  |  |  |
| *Führen Sie das Risikomanagement durch* | Entwickeln Sie die Methodik zur Risikoeinschätzung. | 06 – Methodik zur Risikoeinschätzung und Risikobehandlung |  |
| Führen Sie die Risikoeinschätzung durch. | 06.1 – Verzeichnis der Risikoeinschätzung |  |
| Führen Sie die Risikobehandlung durch. | 06.2 – Verzeichnis der Risikobehandlung |  |
| Schreiben Sie den Bericht zur Risikoeinschätzung & Risikobehandlung. | 06.3 – Bericht zur Risikoeinschätzung und Risikobehandlung |  |
|  |  |  |
| *Entwickeln Sie ein Sicherheitsprofil Ihres Unternehmens und einen Aktionsplan zu dessen Erzielung* | Entwickeln Sie die Erklärung zur Anwendbarkeit. | 07 – Erklärung zur Anwendbarkeit |  |
| Akzeptieren Sie die Restrisiken. | 07 – Erklärung zur Anwendbarkeit |  |
| Entwickeln Sie den Plan zur Risikobehandlung. | 08 – Plan zur Risikobehandlung |  |
|  |  |  |
| *Setzen Sie alle Maßnahmen um* | Implementieren Sie alle im Risikobehandlungsplan definierten Maßnahmen. | Die Dokumente befinden sich im Ordner 09\_Anhang\_A\_Sicherheitsmassnahmen |  |
| Führen Sie Aufzeichnungen über die Umsetzung. | Bei ISMS-Dokumenten ist dies durch die Versionsgeschichte eines Dokuments ersichtlich; bei Software könnte dies ein Protokoll über ihre Prüfung und Freigabe sein. |  |
|  |  |  |
| *Führen Sie Schulungs- und Awareness-Programme durch* | Führen Sie Schulungen für alle Mitarbeiter durch, denen die erforderlichen Fähigkeiten fehlen. | 10 – Training und Awareness Plan |  |
| Führen Sie Awareness-Programme für alle Mitarbeiter und Dritte durch, die eine Rolle in Ihrem ISMS haben. | 10 – Training und Awareness Plan |  |
|  |  |  |
| *Setzen Sie Managementverfahren um* | Schreiben Sie das Verfahren für das interne Audit. | 11 – Verfahren für interne Audits |  |
| Entwickeln Sie das Audit-Programm. | 11.1 – Jährliches interne Audit- Programm |  |
| Definieren Sie, welche Messungen in Bezug auf die Ziele für das ISMS und für die Maßnahmen durchgeführt werden sollen. | 12.1 – Messbericht |  |
| Identifizieren Sie Informationsquellen, die bei der Managementbewertung verwendet werden sollen. | 12.2 – Protokoll zur Managementbewertung |  |
| Schreiben Sie das Verfahren für Korrekturmaßnahmen. | 13 – Verfahren zu Korrekturmaßnahmen |  |
|  |  |  |
| *Betreiben Sie das ISMS* | Führen Sie alle Aufzeichnungen, die gemäß Ihren eigenen Richtlinien und Verfahren erforderlich sind. | Verschiedene Aufzeichnungen und Protokolle, die aufgrund von ISMS-Dokumenten erstellt werden - z. B. Backup-Protokoll (von der Backup-Software), ausgefüllte Liste der gesetzlichen, amtlichen und vertraglichen Anforderungen, usw. |  |
| Führen Sie Korrekturmaßnahmen, die sich aus den erforderlichen Verbesserungen im Betrieb des ISMS ergeben, nach Bedarf aus. | 13.1 – Formblatt der Korrekturmaßnahmen |  |
|  |  |  |
| *Überwachen und messen Sie das ISMS* | Stellen Sie sicher, dass Sie alle Ihre Systeme überwachen. | In jedem implementierten Dokument definierte Überwachungsaufzeichnungen, z. B. Anzahl der Vorfälle, Anzahl der Fehler in einem bestimmten System usw. |  |
| Messen Sie, ob Sie die für Ihr ISMS und für Ihre Maßnahmen festgelegten Ziele erreicht haben. | 12.1 – Messbericht |  |
|  |  |  |
| *Führen Sie das interne Audit durch* | Führen Sie (das) interne Audit (s) durch | 11.3 – Interne Audit-Checkliste |  |
| Schreiben Sie einen internen Audit-Bericht | 11.2 – Interner Audit-Bericht |  |
| Ergreifen Sie Korrekturmaßnahmen als Folge der während des internen Audits festgestellten Nichtkonformitäten | 13.1 – Formblatt der Korrekturmaßnahmen |  |
|  |  |  |
| *Führen Sie die Managementbewertung aus* | *Führen Sie die Managementbewertung aus* | - |  |
| Führen Sie Aufzeichnungen über die Managementbewertung | 12.2 – Protokoll zur Managementbewertung |  |
| Ergreifen Sie Korrekturmaßnahmen als Folge der bei der Managementbewertung festgelegten Verbesserungen | 13.1 – Formblatt der Korrekturmaßnahmen |  |
|  |  |  |
| *Zertifizierungsaudit* | Holen Sie Angebote von mehreren Zertifizierungsstellen ein | - |  |
| Wählen Sie die Zertifizierungsstelle aus | - |  |
| Stufe 1 Zertifizierungsaudit | - |  |
| Stufe 2 Zertifizierungsaudit | - |  |
| Überwachungsbegehungen (Surveillance visits) | - |  |
|  |  |  |