ISO 27001 Checkliste

Lesen Sie unseren Artikel zur ISO 27001 Checkliste

Element	Beschreibung
1. Anwendungsbereich festlegen	Bestimmen Sie, welche Informationen und Bereiche in den Geltungsbereich des ISMS fallen.
2. Erklärung zur Anwendbarkeit (SoA)	Dokumentieren Sie die Auswahl der Sicherheitsmaßnahmen im Statement of Applicability (SoA), welche spezifischen Sicherheitskontrollen aus dem Annex A innerhalb des definierten Anwendungsbereichs umgesetzt werden und liefern Begründungen für die Auswahl oder den Ausschluss jeder Kontrolle.
3. Rollen und Verantwortlichkeiten	Definieren Sie klar die Rollen und Verantwortlichkeiten für die Informationssicherheit im Unternehmen. Aktualisieren Sie Ihre Organigramme und kommunizieren Sie alles an alle Mitarbeiter.
4. Informationssicherheitsrichtlinie	Entwickeln und dokumentieren Sie eine Informationssicherheitsrichtlinie, die die Ziele und Vorgaben des ISMS beschreibt. Diese Aufgabe übernimmt der Informationssicherheitsbeauftragte. Er trägt auch sorge dafür, dass alle betroffenen Mitarbeitenden (mit und ohne PC) davon Kenntnis haben. Die Informationssicherheitsrichtlinie muss von der Geschäftsleitung der Organisation genehmigt werden.
5. Informationsswerte identifizieren	Ermitteln und klassifizieren Sie alle informationsrelevanten Werte (Assets), die für die Organisation von Bedeutung sind, einschließlich physischer, digitaler und personengebundener Informationen.
6. Risikomanagementprozess	Implementieren Sie einen Prozess zur Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Desweiteren identifizieren Sie Ihre Informationswerte. Dazu gehören IT und Non-IT Assets. Bereiten Sie die Inventarisierungen sowie die Klassifizierungen der Assets vor. Danach folgt die Risikobewertung.
7. Risikobewertung durchführen	Führen Sie eine umfassende Risikobewertung durch, um potenzielle Bedrohungen und Schwachstellen zu identifizieren.
8. Risikobehandlung planen und umsetzen	Erstellen Sie Pläne zur Risikobehandlung, einschließlich der Auswahl geeigneter Sicherheitsmaßnahmen. Legen Sie die Verantwortlichkeiten der geplanten Maßnahmen fest und verfolgen Sie deren Umsetzung.
9. ISMS-Dokumentation erstellen	Erstellen und pflegen Sie die erforderliche Dokumentation, einschließlich unterstützenden Richtlinien, Verfahren und Arbeitsanweisungen.

10. Mitarbeiterschulung und -bewusstsein	Schulen und sensibilisieren Sie Mitarbeiter regelmäßig zu Informationssicherheitsrichtlinien und -verfahren.
11. Sicherheitsvorfälle verwalten	Implementieren Sie Verfahren zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen.
12. Notfallmanagement	Entwickeln und testen Sie Notfallpläne zur Gewährleistung der Geschäftskontinuität im Falle eines Sicherheitsvorfalls.
13. Überwachung und Messung	Überwachen und messen Sie regelmäßig die Leistung des ISMS und die Einhaltung der Sicherheitsrichtlinien mit festgelegten KPIs.
14. Interne Audits	Führen Sie regelmäßige und unabhängige interne Audits durch, um die Wirksamkeit des ISMS zu überprüfen und Schwachstellen zu identifizieren.
15. Korrekturmaßnahmen	Ergreifen Sie Korrekturmaßnahmen zur Behebung von Nichtkonformitäten und zur Verbesserung des ISMS.
16. Managementbewertung	Führen Sie regelmäßige Managementbewertungen durch, um die Eignung, Angemessenheit und Wirksamkeit des ISMS sicherzustellen.
17. Externes Audit und Zertifizierung	Bereiten Sie sich auf das externe Audit vor und arbeiten Sie mit dem Zertifizierungsunternehmen zusammen, um die ISO 27001 Zertifizierung zu erlangen.
18. Kontinuierliche Verbesserung	Implementieren Sie Prozesse zur kontinuierlichen Verbesserung des ISMS, basierend auf den Ergebnissen von Überwachungen, Audits und Bewertungen.