Checkliste ISO 27001 – IT-Sicherheitsmanagement

DEKRA
Alles im grünen Bereich.

Erhalten Sie in unserer Checkliste schnell und einfach Auskunft darüber, ob Ihr Unternehmen bereits ausreichend für die Zertifizierung nach ISO 27001:2017 für ein integriertes Informations-Sicherheitsmanagementsystem vorbereitet ist.

ISO 27001 Zertifizierung – Beurteilen Sie Ihr Informationssicherheitsmanagement richtig!

Der Aufbau der folgenden Fragen erfolgt in der Reihenfolge der Grundstruktur für Managementsystemnormen. Eine zustimmende Antwort markieren Sie durch ein Häkchen. So erkennen Sie auf einen Blick, in welchen Bereichen Ihr Unternehmen die Anforderungen der ISO 27001 bereits erfüllt und mit welchen Themen Sie sich noch intensiver beschäftigen müssen.

Kontext der Organisation

- [ ] Sie haben die genaue Organisation Ihres Unternehmens aufgeschlüsselt (z.B. als Organigramm).
- [ ] Sie haben den Geltungsbereich Ihres ISMS (insbesondere für die Stakeholder) festgelegt.
- [ ] Sie haben eine Erklärung zur Anwendbarkeit (engl.: Statement of Applicability, SoA) angelegt, worin die begründeten Entscheidungen zur Umsetzung der Maßnahmen dokumentiert sind.
- [ ] Sie haben eine Umfeldanalyse für die Einordnung des ISMS im Unternehmen durchgeführt.
- [ ] Sie haben eine Anforderungsanalyse hinsichtlich der jeweiligen Interessengruppen (Stakeholder) durchgeführt.
- [ ] Sie haben eine Übersicht aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen, die einen Einfluss auf die Informationssicherheitsstrategie und das ISMS haben, zusammengestellt.

Führung

- [ ] Sie haben die Geschäftsziele und Anforderungen im Zusammenhang mit der Informationssicherheitspolitik im Unternehmen klar definiert und dokumentiert.
- [ ] Sie haben eine konkrete Informationssicherheitsstrategie festgelegt.
- [ ] Sie haben das „Top-Management" definiert, welches für die Steuerung des ISMS der zu schützenden Organisation verantwortlich ist und über den Ressourceneinsatz entscheidet.
- [ ] Sie haben eine Informationssicherheitsleitlinie (engl. Information Security Policy) implementiert.

Planung

- [ ] Sie besitzen ein dokumentiertes Risikobewertungsverfahren.
- [ ] Sie verfügen über eine umfassende Dokumentation zum Risikobeurteilungsprozess und Risikobehandlungsprozess/-plan.
- [ ] Sie besitzen alle Aufzeichnungen und Ergebnisse von Risk Assessments bzw. Risikoanalysen.
- [ ] Sie haben alle Aufzeichnungen und Ergebnisse von Risikiobehandlungen dokumentiert.
- [ ] Sie haben alle Sicherheitsziele für Ihr Unternehmen und Stakeholder definiert.

Unterstützung

- [ ] Sie verfügen über einen Kommunikationsplan bzw. -matrix für die Dokumentation aller Kommunikation im Unternehmen mit Bezug auf die Informationssicherheit.
- [ ] Sie können die erforderlichen Personen und die Infrastruktur für die Umsetzung und Steuerung des ISMS zur Verfügung stellen.
- [ ] Sie verfügen über eine Strategie für den Umgang mit dokumentierten Informationen.
- [ ] Sie verfügen über eine Übersicht über alle relevanten Ressourcen (z.B. Budget, Personal).
- [ ] Sie haben eine detaillierte Rollenbeschreibung von Mitarbeitern im Geltungsbereich des ISMS (z.B. ISB bzw. CISO oder DSB) angelegt und sämtliche Nachweise über deren Kompetenzen dokumentiert
- [ ] Sie haben eine Dokumentation zum Awareness- bzw. Schulungskonzept mit Bezug auf das ISMS angelegt.

Sie verfügen über Schulungsunterlagen zum ISMS und Nachweise über die Teilnahme Ihrer Mitarbeiter an jeweiligen Schulungsmaßnahmen. ☐

Sie haben ein Verfahren zur internen und externen Kommunikation festgelegt. ☐

Betrieb

Sie besitzen Nachweise zur korrekten Ausführung der ISMS-Prozesse und für die Kontrolle und Leistungsmessung des ISMS. ☐

Sie verfügen über Dokumentationen über interne Auditprogramme und Auditergebnisse. ☐

Sie haben einen Incident Response Plan (IRP), inklusive aktueller Kontaktlisten und Eskalationspläne definiert. ☐

Sie verfügen über eine umfangreiche Dokumentation der Messstruktur für alle KPIs (Key Performance Indicators) sowie über die Messergebnisse und die daraus abgeleiteten Managementberichte zur Eskalation. ☐

Ihre Dokumentation umfasst Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten, Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen sowie Berichte von Informationssicherheits-Vorfällen. ☐

Sie verfügen über Nachweise über die Art von Nichtkonformitäten sowie über sämtliche umgesetzte reaktive Maßnahmen und über die Resultate zu sämtlichen korrigierenden Maßnahmen. ☐

Sie besitzen eine Übersicht über die Ergebnisse der Risikobewertung (z.B. Risikobewertungsberichte, Risikokennzahlen) und Risikobehandlung (z.B. Kontrolltestberichte, Penetrationstestberichte). ☐

Wir unterstützen Sie bei der erfolgreichen Zertifizierung Ihres Qualitätsmanagementsystems gemäß der ISO 27001. Kontaktieren Sie noch heute unsere Experten!

DEKRA Certification GmbH
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-2566
Telefax +49.711.7861-2615
Mail certification.de@dekra.com
Web www.dekra-certification.de