



ISO 27001 bei Indico Solutions

Stand November 2025



Nach der Benennung der wesentlichen Rollen wie **Beauftragter der obersten Leitung (BdOL)**, **Informationssicherheitsbeauftragter (ISB)** und Qualitätsmanagementbeauftragter wurden die Regeldokumente nach Kapitel 0 und 4–10 der Norm sukzessive erstellt. Wichtiger Bestandteil direkt zu Beginn ist dabei die Definition eines Organigramms mit Beschreibung des eigentlichen **Gültigkeitsbereichs der ISO 27001**. So kann die gesamte Firma oder auch nur Teilbereiche in den Geltungsbereich des Zertifikats aufgenommen werden. Bei Indico Solutions erstreckt sich der Geltungsbereich auf den **Remote Service**, d. h. alle Prozesse und Tätigkeiten, die im Bereich Remote Service angesiedelt sind, müssen die Kriterien nach ISO 27001 erfüllen. Diese vorgenannten Dokumente sind momentan nahezu fertiggestellt, ebenso wie der Großteil notwendiger Richtlinien und Notfallpläne.

Zentraler Punkt der ISO 27001 ist der sogenannte **Anhang A**, welcher eine Vielzahl bestimmter klassifizierter Sicherheitskontrollen beinhaltet, die dazu benötigt werden, um die Einhaltung der durch die Norm vorgegebenen Behandlungsstandards von Informationssicherheitsrisiken sowie

das zugehörige **Statement of Applicability (SoA)** nachzuweisen. Die SoA ist dabei die Festlegung, welche Kontrollen gemäß Anhang A durch die jeweilige Firma umgesetzt werden, um die Anforderungen der Norm zu erfüllen, sowie die Begründungen dafür, dass bestimmte Kontrollen nicht umgesetzt werden. Der Anhang A und die SoA sind aktuell zu ca. **90 % fertiggestellt**.

Das letztendliche Ziel von ISO 27001 ist der Betrieb eines dokumentierten **Informationssicherheitsmanagementsystems**, speziell zugeschnitten und abgestimmt auf die Bedingungen eines bestimmten Unternehmens – hier: Indico Solutions. Die ISO-Richtlinien liefern dafür die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung. Daher steht im Fokus der aktuellen Tätigkeiten die **Auswahl eines für Indico Solutions passenden Informationssicherheitsmanagement-Tools** zur Abbildung aller notwendigen Tätigkeiten und Nachweise. Dazu gehört zuerst die Erstellung eines Pflichtenhefts, welches alle unsere Anforderungen auflistet, um damit ein entsprechendes Tool testen und auswählen zu können. Für ISO 27001 ist es notwendig,

dass ein Tool (oder mehrere Tools) genutzt wird/werden, mit dem/denen zum einen die Vorgaben (Richtlinien, Notfallpläne, Prozessdokumentationen ...) strukturiert und automatisch versioniert abgelegt werden können und zum anderen alle notwendigen Informationen, Vorkommnisse, jährliche Neubewertungen (Unternehmensziele, Risiken, Stärken, Schwächen, Chancen, Personalentwicklungsmaßnahmen, Ziele der Informationssicherheit ...), Protokollierungen von durchgeführten Tätigkeiten, ergriffenen Maßnahmen sowie zeitliche Planungen und das Tracking durchzuführender Aktivitäten dargestellt und nachgewiesen werden können.

Nach der Auswahl eines (oder mehrerer) Tools werden die identifizierten notwendigen Tätigkeiten, Abhängigkeiten, Tabellen ... in das Tool übertragen und konfiguriert. Parallel dazu werden erste Prozesse beschrieben, Stellenbeschreibungen erstellt, und die interne IT setzt die ersten speziellen technischen Anforderungen um. Zudem wird das **interne Audit**, welches als Vorbereitung für die Zertifizierungsaudits dient und noch offene Punkte identifizieren soll, vorbereitet bzw. geplant.

Gemeinsam mit Ihnen erarbeiten wir die für Sie beste Lösung.

Gerne besprechen wir mit Ihnen weitere Details. Rufen Sie an unter +49 421 807 117 0 oder schicken Sie eine E-Mail an moin@indico-solutions.com.