In 6 Schritten erfolgreich zur ISO 27001-Zertifizierung

Ein Ratgeber von handz.on

Unternehmen, die sich erfolgreich nach ISO 27001 zertifizieren wollen, müssen alle für die Informationssicherheit relevanten Prozesse genau festgelegt haben – beginnend beim Anwendungsbereich des ISMS, über die Klassifizierung von Informationen, bis hin zum Umgang mit Vorfällen, die den Geschäftsbetrieb nachhaltig unterbrechen können. Außerdem gilt es, eine erfolgreiche Implementierung und Verwendung eines Informationssicherheits-Risikomanagements sowie die Definition der Behandlung potenzieller Vorfälle sicherzustellen. Ein besonderes Augenmerk des ISO-Standards liegt darüber hinaus auf der Sensibilisierung des gesamten Personals sowie der kontinuierlichen Verbesserung des gesamten ISMS, das jährlich überprüft wird.

Ihr Unternehmen will sich zertifizieren lassen und Sie wissen nicht genau, wie Sie dabei am besten vorgehen? Der folgende Ratgeber gibt Schritt für Schritt wichtige Hilfestellungen und Tipps für eine erfolgreiche Umsetzung der ISO-27001-Zerfizierung.

Die ISO-27001-Zertifizierung

Die ISO 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme (ISMS). Sie bietet Unternehmen einen systematischen und strukturierten Ansatz zur Planung, Umsetzung, Überwachung sowie Verbesserung der betrieblichen Informationssicherheit und trägt dazu bei, vertrauliche Informationen optimal zu schützen. Eine Zertifizierung nach ISO 27001 attestiert dem Unternehmen dabei leider nicht, tatsächlich „sicher“ zu sein, aber sie dokumentiert, dass im Unternehmen Prozesse und Strukturen etabliert wurden, die alle Voraussetzungen dafür schaffen, Informationen risikoangemessen abzusichern.

Von der Leitlinie bis zum Audit – so gehen Sie vor:

1. Vorarbeiten

Bevor das Projekt starten kann, gilt es zunächst, die Projektstruktur klar zu definieren, inklusive der Benennung eines Projektleiters und der Zusammenstellung des Teams. Nicht minder wichtig ist es, im Anschluss daran die Struktur der Projektdokumentation und Archivierung festzulegen (z.B. über Confluence oder Sharepoint) und die Dokumentenvorlagen für das ISMS zu erstellenden Dokumente (Word-Dokumente und Excel-Tabellen mit einem Abschnitt für die Dokumentenlenkung und Versionshistorie) vorzubereiten.

2. Ausarbeitung der Leitlinie

Die Informationssicherheitsleitlinie stellt den Rahmen des ISMS dar. Sie muss formal einige wesentliche Punkte enthalten, um der Norm zu entsprechen. Beispielhaft sei hier nur die Verpflichtung der Geschäftsführung zur kontinuierlichen Verbesserung des ISMS genannt.

Es empfiehlt sich, sehr früh mit der Ausarbeitung der Leitlinie zu beginnen, um einen Startpunkt für die inhaltliche Diskussion mit dem Top-Management und den Leitern der Fachabteilungen zu setzen. Naturgemäß lassen sich zu Beginn nicht alle Themen abschließend behandeln, so dass es ein paar Abstimmungsrunden bedarf, in denen folgende Punkte wichtig sind:

- Das Führungsteam mit ins Boot zu holen. Zum einen können die Leiter der Fachabteilungen wertvollen Input zu interessierten Parteien (z. B: Kunden, Mitarbeiter oder Anteilseigner) und zum Anwendungsbereich des ISMS geben. Zum anderen stellt ein Führungs-Team, das geschlossen hinter dem Vorhaben „ISMS“ steht, auch für spätere Aktivitäten die Voraussetzung für das Gelingen des Projektes dar.

- Die verschiedenen internen und externen Themen sowie die interessierten Parteien und deren Anforderungen in Bezug auf die Informationssicherheit des Unternehmens herauszuarbeiten:

  So haben Kunden beispielsweise ein Interesse daran, dass die Informationen, die sie dem Unternehmen im Laufe der Zusammenarbeit zur Verfügung stellen, nicht in die Hände von Wettbewerbern gelangen. Mitarbeiter hingegen sind an der Vertraulichkeit ihrer personenbezogenen Daten und einem sicheren Arbeitsplatz interessiert. Anteilseigner wiederum sind ihre Gewinne wichtig, die durch die Folgen von Informationssicherheitsvorfällen geschmälert werden könnten und IT-Administratoren wünschen sich klare, möglichst einheitliche Regelungen.

  Wer sich in die Position der interessierten Parteien versetzen kann und überlegt, warum diese Interessengruppen mit dem Unternehmen zusammenarbeiten, erhält einen guten ersten Entwurf, den es mit Vertretern dieser Interessengruppen zu besprechen gilt. Die verschiedenen Fachabteilungen können hier einen guten Beitrag leisten.

- Den Scope herauszuarbeiten und festzulegen. Ausgehend von den internen und externen Themen sowie den relevanten Parteien mit ihren Interessen, wird der Anwendungsbereich des ISMS grob abgesteckt. (Beispiel: „Entwicklung, Vertrieb und Bereitstellung von Software an Unternehmenskunden im SaaS-Modell“)

- Die Management-Ziele beschreiben (Warum möchte das Management ein ISMS einführen?) und daraus dann die Informationssicherheitsziele abzuleiten und festzuschreiben.

- Grundlegende Regeln im Umgang mit Risiken festzulegen (z. B. nach einem qualitativen Schema mit Eintrittswahrscheinlichkeitsklassen bzw. Schadenausmaßklassen)

- Die in der Leitlinie klar dokumentierte Selbstverpflichtung der Geschäftsführung zur kontinuierlichen Verbesserung einzuholen. Dies muss auch die erklärte Bereitschaft des Top-Managements einschließen, dem ISMS-Team ausreichend Zeit für die Erfüllung der Aufgaben zur Verfügung zu stellen und andere Aufgaben möglicherweise zu depriorisieren.

3. Sammlung und Strukturierung der Anforderungen

Bei der Analyse der Anforderungen muss das Projektteam strukturiert vorgehen und sämtliche Normkapitel der ISO 27001 und des Anhangs A durcharbeiten. Ggf. ergeben sich in diesem Schritt auch weitere, neue Anforderungen, die es dann ebenso zu berücksichtigen gilt. Im Hinblick auf den Anhang A bedeutet das, 114 nach Themenbereichen (so genannte Maßnahmenziele) sortierte einzelne Maßnahmen (Control Statements) durchzuarbeiten und begründet zu entscheiden sowie zu dokumentieren, welche davon für das Unternehmen relevant sind und welche nicht. Selbstredend hat eine Spedition mit Laderampen, über die Fremde ins Lager eindringen können, andere Anforderungen, als ein IT-Dienstleister.

Das Ergebnis ist eine erste Arbeitsversion der so genannten „Erklärung zur Anwendbarkeit“ (engl. Statement of applicability oder kurz „SOA“). Ganz abgesehen davon, dass dies ein Pflichtdokument ist, stellt es darüber hinaus eine hervorragende Grundlage zur Steuerung und Fortschrittsdokumentation der Aktivitäten dar. Das Gruppieren der Anforderungen bildet im nächsten Schritt dann das Gerüst für die zu erstellenden Richtlinien-Dokumenten.

4. Erstellung der Richtlinien

Wichtig ist es, die Richtlinien „bottom up“, also in sehr enger Abstimmung mit IT-Administratoren, der Personalabteilung, der Software-Entwicklung sowie den Leitern und Mitarbeitern der Fachabteilungen zu erstellen und Lücken im Dialog mit der Geschäftsführung und den Fachabteilungen zu schließen. So ist gewährleistet, dass alle Mitarbeiter bereits vor der Umsetzung informiert und mit im Boot sind. Auf diese Weise erhält das ISMS-Team einen guten Überblick darüber, welche Prozesse im Unternehmen alle bereits in Übereinstimmung mit der Norm funktionieren und welche noch nicht.

5. Umsetzung und Optimierung

Da die einzelnen Richtlinien meist nicht gleichzeitig, sondern nach und nach verabschiedet werden, ist es im Laufe des Projektes die Aufgabe des ISMS-Teams, die Kolleginnen und Kollegen regelmäßig über den Projektstatus zu informieren. (Welche neuen Richtlinien gibt es? Was ist ab sofort zu beachten?). Oft gibt es gerade mit der Veröffentlichung der ersten Dokumente Kritik von den Mitarbeitenden. Egal, ob es sich dabei nur um Unzufriedenheit mit einzelnen Prozessen oder das Aufdecken tatsächlicher Widersprüche und Verbesserungspotentiale handelt, beides ist wertvoll und leitet den kontinuierlichen Verbesserungsprozess und ggf. ein Überdenken einzelner Regelungen ein. Daher gilt es, alle Vorschläge zu dokumentieren, zu bewerten (Verhältnis von Aufwand und Nutzen) und zu priorisieren.

Auch das ISMS-Team selbst wird beim Erstellen der einen oder anderen Richtlinie bemerken, dass es einzelne Punkte gibt, die bereits in anderen Richtlinien beschrieben wurden und nun entweder redundant oder widersprüchlich sind. Beides gilt es unbedingt zu vermeiden. Ein gut gepflegtes SOA-Dokument hilft hier, den Überblick zu behalten.

6. Vorbereitung auf den Audit

Darüber, ob vor dem Erstzertifizierungsaudit zwingend ein interner Audit über das gesamte ISMS erfolgt sein soll oder nicht, lässt sich streiten. Es ist jedoch in jedem Fall lohnenswert, vor dem externen Erstzertifizierungsaudit einmal einen neutralen Auditor auf das ISMS schauen zu lassen und so zertifizierungsverhindernde „Hauptabweichungen“ zu vermeiden. Dies meint z.B. das Nichterfüllen einer oder mehrerer Normenforderungen für das Managementsystem oder ein Sachverhalt, der erheblichen Zweifel an der Fähigkeit des Managementsystems aufkommen lässt, wie etwa ein nicht umgesetztes Risiko-Management).

Darüber hinaus ist es wichtig, dass die definierten Prozesse vor dem Zertifizierungsaudit bereits eine Weile gelebt und ihre Outputs und Ergebnisse dokumentiert wurden. Das zeigt dem Auditor, dass das ISMS im Unternehmen verstanden und umgesetzt wird.

Für den ersten Überprüfungsaudit nach einem Jahr gilt es dann sicherzustellen, dass bis dahin die Findings aus dem ersten Audit sowie ggf. neuen Risiken, Vorfälle und Verbesserungspotentiale identifiziert und Maßnahmen eingeleitet wurden. Sprich es muss klar ersichtlich sein, dass das Unternehmen nach der Erstzerfizierung mit seinem Optimierungsvorhaben weitergekommen ist.

Fazit: Positive Auswirkungen auf Ihr Business

Ein zentraler Punkt, warum die Zertifizierung nicht nur Pflichterfüllung ist, um dem internationalen Standard zu entsprechen, sondern sich vielmehr ganz direkt und positiv auf das eigene Business auswirkt, liegt in der Erschließung neuer Zielgruppen. So verschaffen sich zerftifizierte Unternehmen optimalen Zugang zu besonders sicherheitssensiblen Kunden, denen die ISO-Zertifizierung die Gewissheit verschafft, dass die Geschäftsprozesse des Dienstleisters den höchsten Standards an die Informationssicherheit entsprechen, sodass sie annehmen dürfen, dass ihre Informationswerte sicher sind.

Ein weiterer wichtiger Punkt ist, dass speziell kleinere und mittlere Unternehmen durch den Zertifizierungsprozess Erfahrungen gewinnen in puncto Aufbau und Pflege von Managementsytemen. Dieses Know-how können sie als Blaupause nutzen, wenn es im Laufe der Unternehmensentwicklung dann darum geht, das Risikomanagement nicht nur für die Informationssicherheit, sondern als unternehmensweiten Prozess aufzusetzen.

Über den Autor

Sebastian Welke ist Senior Consultant und Teamlead Information Security Management bei der handz.on GmbH, einem auf Enterprise Service Management und Informationssicherheit spezialisieren Münchner IT-Dienstleister. Dort betreut er hauptsächlich Unternehmen aus dem Finanzsektor und Institutionen des Gesundheitswesens.

Noch Fragen? Wir beraten Sie gerne!

Sie haben Fragen oder möchten sich noch tiefergehend bzgl. der Zertifizierung informieren? Wir helfen Ihnen gerne weiter. Rufen Sie uns einfach an unter +49 89 7167 767-0 oder schreiben Sie uns eine E-Mail an sebastian@on.de.