ISO 27001

Überblick & Orientierung

www.optiqum.de

www.datenschutzsysteme.com

Sicherung von schützenswerten Daten in Ihrem Unternehmen

Ausgangssituation

In den letzten Jahren ist oft von Cybersicherheit, Cyberangriffen, Ransomware und ähnlichen kriminellen Aktivitäten die Rede, die genau einen Angriffspunkt im Visier haben: den unzureichenden Schutz von Unternehmensdaten. Alle Organisationen ohne Ausnahme können von diesen kriminellen Attacken betroffen sein.

Angesichts dieses Datenschutzbedarfs unterstützt ein Standard die Unternehmen bei der Entwicklung einer wirksamen Sicherheitsstrategie: die ISO 27001.

Vorteile einer Zertifizierung nach ISO 27001

Um sich nach ISO 27001 zertifizieren zu lassen, müssen Unternehmen und Organisationen Ressourcen bereitstellen und Investitionen tätigen. Trotz dieses Aufwands bietet eine Zertifizierung zahlreiche Vorteile.
Nutzen aus der Zertifizierung können beispielsweise sein:

- Optimierung von Prozess- und IT-Kosten
- Nachhaltige Steigerung der Wettbewerbsfähigkeit
- Erhöhen der Vertrauensbasis bei Kunden, Partnern, Lieferanten und in der Öffentlichkeit
- Bedrohungen im Unternehmen vorausschauend erkennen und reduzieren
- Schutz vertraulicher Informationen und Daten vor Missbrauch, Verlust und ungewollter Veröffentlichung
- Senkung von Haftungsrisiken
- Senkung von Geschäftsrisiken
- Senkung von Versicherungsprämien

Mit der Zertifizierung nach ISO 27001 erbringen Sie mit ihrem Unternehmen den Nachweis, dass die Anforderungen der Informationssicherheit eingehalten und die Maßnahmen zum Schutz von Daten umgesetzt sind. Kunden und Geschäftspartner erhalten dank der Zertifizierung einen vertrauenswürdigen Beleg dafür, dass eine ausreichende IT-Sicherheit gewährleistet werden kann. Ihr Unternehmen führt eine kontinuierliche, nachhaltige Eigenkontrolle durch und optimiert ständig die IT-Prozesse im Hinblick auf die Informationssicherheit. Da ISO 27001 einen ganzheitlichen Ansatz verfolgt, ist die Berücksichtigung der Norm in der Organisation über alle Hierarchieebenen hinweg sichergestellt. Sie hilft damit auch, zentralen Anforderungen und diverse Regelungen zu erfüllen und kann von allen Beteiligten im Unternehmen nachhaltig akzeptiert, umgesetzt und gelebt werden.

Was ist die ISO 27001?

Die seit Oktober 2005 bestehende und international anerkannte Norm mit dem vollständigen Namen

„ISO/IEC 27001 IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“

spezifiziert die Anforderungen für die Einrichtung, die Umsetzung, die Aufrechterhaltung sowie die kontinuierliche Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems, kurz ISMS.

Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Herausforderungen und Bedürfnisse von Unternehmen und Organisationen.

Wie auch andere aktuelle Managementnormen basiert die DIN ISO IEC 27001 auf der High Level Structure (kurz HLS).

Das Vorgehen

In der Vergangenheit haben wir von OPTIQUM erfolgreich Unternehmen der verschiedensten Branchen auf ihrem Weg zum erfolgreichen ISO 27001 – Audit begleitet und aus diesen Erfahrungen eine Best Practice erarbeitet.

One Size fits all? Warum Pauschalen bei ISO 27001 nicht funktionieren!

Zunächst wird der der Reifegrad Ihres Managementsystems und der Aufbau Ihrer IT-Infrastruktur inkl. der IT-Dokumentation benötigt. Wir wissen, dass viele Anbieter pauschal ein Angebot über die Erstellung eines Informationssicherheitsmanagementsystem (ISMS) abgeben. Das ist aus unserer Sicht unseriös und hat meistens zur Folge das im Laufe des Projektes Nachforderungen gestellt werden. Warum genau?

Unternehmen sind in jeglicher Hinsicht äußerst unterschiedlich: Zum Beispiel existieren manchen Organisationen als Dienstleister praktisch nur in der Cloud, andere wiederum haben mehrere hundert Mitarbeiter an verschiedenen Standorten mit unterschiedlicher Vernetzung. Manche Unternehmen haben perfekt aufgestellte und gelebte Informationssicherheitsmanagementsysteme mit optimaler Dokumentation, bei anderen wiederum steckt dies noch in den Kinderschuhen und ist nur rudimentär entwickelt. Wie Sie sehen, sind die Anforderungen, mittels derer die Zertifizierung nach ISO 27001 erreicht wird derart unterschiedlich, dass eine einfache pauschale Einschätzung den individuellen Gegebenheiten innerhalb Ihres Unternehmens gar nicht gerecht werden kann.

Wenn Sie sich noch unsicher sind, bieten wir von OPTIQUM einen Einführungs-Workshop zur Erarbeitung der individuellen Anforderungen Ihres Unternehmens zur ISO 27001 an. Der Workshop gliedert sich in:

- ½ Tag Vorstellung der ISO-Norm
- ½ Tag FAQ: Beantwortung Ihrer Fragen zum Thema ISO 27001

Sprechen Sie uns dazu einfach an.

Ist und Soll vergleichen

Unser Vorgehen besteht üblicherweise aus einer GAP Analyse, in der eine Dokumentensichtung und ein internes Vor-Ort/Remote Audit an Ihrem Unternehmensstandort erfolgt. Das Ergebnis ist eine Übersicht der offenen Normpunkt in ausführlicher Darstellung. Das Ergebnis können Sie nachfolgend auch mit anderen Unternehmen umsetzen.

Auf dieser Basis kann nun der Gesamtaufwand für Ihr Projekt abgeschätzt werden und Sie können wählen:

- Was möchten Sie intern erarbeiten?
- Wobei bedürfen Sie externer Unterstützung?

Unterstützungsphase

Die Unterstützungsphase besteht üblicherweise aus mehreren Workshops zu den im Bericht aufgeführten Themen. Auf die Workshops folgt jeweils eine Umsetzungsphase der im Workshop erarbeiteten Aufgaben.

Im folgenden Workshop werden die Ergebnisse überprüft und das nächste Thema angegangen. Der Reifegradbericht wird dann entsprechend angepasst. In jeder Workshoprunde kann der Aufgabenbereich neu gemäß ihren verfügbaren Ressourcen verteilt werden (Was erledigen Sie/geben Sie an Extern ab).

Nach Abarbeitung der Berichtsthemen, führen wir nun ein internes Audit durch inklusive der entsprechenden Dokumentation.

Außerdem können wir Sie bei der Auswahl und Beauftragung der Prüforganisation, sowie als Begleitung bei dem offiziellen ISO 27001 Audit unterstützen.

ISO 27001

Ablauf einer Zertifizierung

Vorabprüfung
Beurteilung zur Feststellung der Situation vor Ort.

Stufe 1
Bewertung der ISMS-Dokumentation.

Stufe 2
Prüfung der praktischen Anwendung des ISMS und seiner Wirksamkeit.

Zertifizierung
der Organisation. Gültig für drei Jahre (unter Bedingungen).

Kontrollprüfung
Jährliches internes Audit zur Bewertung der Optimierung von Prozessen und der Bestätigung des Standards.

Erneuerung der Zertifizierung
vor Ablauf von drei Jahren.

Wie beginnen?

Sie ist gefallen, die Entscheidung, dass Sie Ihr Unternehmen nach ISO 27001 zertifizieren lassen. Um gut starten zu können, hier die wichtigsten Basics:

- Stellen Sie sicher, dass vor Projektbeginn die entsprechenden involvierten Abteilungen, auf jeden Fall immer die IT, informiert sind und alle Dokumente, die relevant werden könnten, gesichtet und griffbereit sind. Informieren Sie jede Person mit Kundenkontakt wie beispielsweise Projektmanager und Vertriebsmitarbeiter, dass die ISO 27001 als Anforderung in Ausschreibungen, Einkaufsbedingungen, etc. integriert sein könnte und stellen Sie sicher, dass vor Projektbeginn entsprechende Dokumente vorab unter dem Aspekt der Informationssicherheit gesichtet werden. Dadurch gewährleisten Sie, dass Sie von einer möglichen Anforderung zum Nachweis der Zertifizierung nach ISO 27001 nicht überrascht werden – und sich im Zweifelsfall noch gegen eine Abgabe eines Angebotes entscheiden können.

- Stellen Sie sicher, dass jede Person im Unternehmen Prüfanforderungen jedweder Art entlang von Meldeketten im Unternehmen frühzeitig adressiert. Nur wenn die gesamte Organisation einschließlich der Geschäftsleitung informiert ist, dass eine Prüfung bevorsteht, können notwendige Ressourcen bereitgestellt und eine gute Vorbereitung zur Prüfung sichergestellt werden.

Wir von OPTIQUM sind für Sie da, um Sie zu Ihren Anliegen in Bezug auf Informationssicherheit und Datenschutz zu beraten.

Telefon: +49 221 82 95 91 0
datenschutzsysteme@optiqum.de

OPTIQUM GmbH
Siegburger Straße 223
D-50679 Köln

+49 221 82 95 91 0
info@optiqum.de