Foto: TÜV Rheinland ©

FAQ – Informationssicherheit ISO 27001

Unsere Experten haben für Sie häufig gestellte Fragen zur Zertifizierung 27001 Informationssicherheit beantwortet. Sie möchten mehr erfahren über die ISO 27001? **Kontaktieren Sie uns!**

1. WELCHE ZIELE HAT DIE ISO 27001?

Ziel der ISO 27001 ist ein einheitliches und zentral gesteuertes Managementsystem zum Informationsschutz. Außerdem wird durch effektives Monitoring und Steuerung der IT-Sicherheitsrisiken die Gefährdung aller Geschäftsprozesse reduziert.

2. WELCHEN NUTZEN HAT DIE ZERTIFIZIERUNG ISO 27001 FÜR MEIN UNTERNEHMEN?

Mit der Einhaltung des IT-Sicherheitsgesetzes schützen Sie Ihr Unternehmen vor Cyber-Angriffen, dem Verlust von Daten und den dadurch entstehenden wirtschaftlichen Einbußen oder Imageschäden. Rechtliche Absicherungen sollen überprüft und Angriffe von Hackern und deren Zugriff auf sensible Daten reduziert werden. Weitere Vorteile der ISO 27001 Zertifizierung sind:

- Gesicherte Verfügbarkeit Ihrer IT-Systeme und -Prozesse
- Vertraulichkeit Ihrer Informationen
- Wettbewerbsvorteil durch Kundenvertrauen
- Minimierung der IT-Risiken und möglicher Schäden
- Aufdeckung und Beseitigung von Schwachstellen
- Kontrolle von IT-Risiken
- Sicherstellung der Compliance-Anforderungen
- Kostensenkung

3. WAS BEDEUTET ISMS?

Ein Informationssicherheitsmanagement-System (ISMS) ist eine systematische Herangehensweise, die technische und menschliche Faktoren berücksichtigt. Es hilft Ihnen dabei einen kontinuierlichen Optimierungs- und Überwachungsprozess in Ihrem Unternehmen zu etablieren. Auf Basis des von Ihnen selbst vorgegebenen Schutzbedarfs. Die ISO 27001 beschreibt die Anforderungen an die Umsetzung sowie die Dokumentation eines ISMS bis ins Detail.

www.tuv.com/iso27001

TÜVRheinland®
Genau. Richtig.

4. WELCHE BEREICHE WERDEN BEI ZERTIFIZIERUNG GEMÄSS ISO 27001 BEWERTET?

- Informationssicherheitsrichtlinien
- Personalsicherheit
- Werteverwaltung
- Physische und umgebungsbezogene Sicherheit
- Zugangssteuerung
- Kryptographie
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhalten von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte beim Business Continuity Management
- Compliance

5. WIE IST DER ABLAUF DER ZERTIFIZIERUNG NACH ISO 27001 FÜR INFORMATIONSSICHERHEIT?

Unsere Experten prüfen und zertifizieren Ihr Unternehmen in folgenden Schritten:

1. Bestandsaufnahme / Voraudit (optional)
Unsere Auditoren erfassen zunächst den Ist-Zustand Ihres Unternehmens vor Ort anhand eines Vor-Audits (Bestandsaufnahme).

2. Zertifizierungsaudit (Stufe 1)
Wir bewerten und dokumentieren Ihre Managementsystem-Unterlagen anhand eines Auditprotokolls. Unter anderem werden in diesem Schritt Ihr Standort beurteilt und gesetzliche sowie behördliche Regelungen überprüft.

3. Zertifizierungsaudit (Stufe 2)
Sie demonstrieren die praktische Anwendung Ihres Informationssicherheits-Management-Systems. Unsere Auditoren prüfen zudem die Angemessenheit und Wirksamkeit. Am Ende des Audits erhalten Sie in einem Abschlussgespräch die Auditergebnisse.

4. Zertifikatserteilung
Sind alle Kriterien erfüllt, erhält Ihr Unternehmen das ISO 27001 Zertifikat. Es bescheinigt die Normkonformität und Funktionsfähigkeit Ihres Managementsystems. Darüber hinaus wird Ihr Unternehmen in unsere Online-Zertifikatsdatenbank Certipedia aufgenommen. Erfahren Sie mehr über das Thema „Werben mit TÜV Rheinland“.

5. Überwachungsaudits
Unsere jährlichen Überwachungsaudits unterstützen Sie bei der kontinuierlichen Optimierung Ihrer IT-Prozesse.

6. Re-Zertifizierung
Mit der Re-Zertifizierung nach drei Jahren setzen Sie Ihren kontinuierlichen Verbesserungsprozess dauerhaft fort. Ihren Kunden zeigen Sie nachhaltig Ihre Initiative für ein sicheres Rechenzentrum.

6. WIE LANGE IST MEIN ISO 27001 ZERTIFIKAT GÜLTIG?

Ihr Zertifikat ist drei Jahre gültig. Durch das jährliche Überwachungsaudit und die Re-Zertifizierung vor Ablauf der drei Jahre wird Ihr kontinuierlicher Verbesserungsprozess festgehalten.

7. WIE KÖNNEN UNTERNEHMEN INFORMATIONSSICHERHEIT ERREICHEN?

Unternehmen sind verpflichtet ihre Netzwerke nach Mindeststandards auszurüsten. Die Errichtung einer Kontaktstelle zum Bundesamt für Sicherheit in der Informationstechnik (BSI) ist maßgeblich um die IT-Sicherheitsstandards den Mindestanforderungen des BSI anzupassen. Außerdem müssen technische und organisatorische Vorkehrungen getroffen werden, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Daten sicherzustellen. Hackerangriffe müssen unverzüglich gemeldet werden. Bei Nichteinhaltung des Gesetzes ist mit einer Geldstrafe zu rechnen.

8. ERFÜLLE ICH MIT DER ZERTIFIZIERUNG NACH ISO 27001 MEINE PFLICHT ZUR INFORMATIONSSICHERHEIT NACH DEM IT-SICHERHEITSGESETZ?

Der IT-Sicherheitskatalog verlangt das Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 als Basis. Somit erfüllen Sie mit der Implementierung eine grundlegende Pflicht des IT-Sicherheitsgesetzes. Weitere Implementierungen sind branchenabhängig und ziehen zusätzliche Voraussetzungen mit sich. Sehen Sie hier alle Vorteile eines ISMS für KRITIS-Betreiber.

9. WELCHE UNTERNEHMEN SIND NACH DEM IT-SICHERHEITSGESETZ ZU EINER IMPLEMENTIERTEN IT-SICHERHEIT VERPFLICHTET?

Nach dem von der Bundesregierung beschlossenen IT-Sicherheitsgesetz sind Betreiber von Webangeboten, Telekommunikationsunternehmen und Betreiber Kritischer Infrastrukturen (KRISTIS) verpflichtet ein Mindestmaß an IT-Sicherheit zu gewährleisten. Die Reglementierungen treffen auch Unternehmen aus wichtigen Wirtschaftsbereichen wie Energieversorger, Krankenhäuser oder Banken.

Bund und Länder haben sich auf eine einheitliche Sektoreneinteilung verständigt. Es gibt nun diese neun Sektoren für Kritische Infrastrukturen mit den entsprechenden Branchen:

- Energie
- Ernährung
- Finanz- und Versicherungswesen
- Gesundheit
- Informationstechnik und Telekommunikation
- Medien und Kultur
- Staat und Verwaltung
- Transport und Verkehr
- Wasser

10. WIE KANN ICH HERAUSFINDEN, WO ICH MIT MEINEM UNTERNEHMEN STEHE BEI DER EINFÜHRUNG EINES ISMS?

In unserem Online Quick Check erhalten Sie einen ausführlichen Überblick über das Informationssicherheits-Management Ihres Unternehmens. Im Anschluss an den Test, der nur 5 - 8 Min. dauert, erhalten Sie direkt eine Online-Auswertung inklusive Kurzbeurteilung. Hier den Online Quick Check starten.

UNSERE EXPERTEN STEHEN IHNEN NATÜRLICH AUCH FÜR EIN KOSTENFREIES INFORMATIONSGESPRÄCH ZUR VERFÜGUNG. SPRECHEN SIE UNS HIERZU GERNE AN!

ONLINE KONTAKT

TÜV Rheinland Cert GmbH
Am Grauen Stein
51105 Köln
Tel. +49 800 888 2378
Fax. +49 800 888 3296
tuvcert@de.tuv.com
www.tuv.com/iso27001

TÜVRheinland®
Genau. Richtig.