FAQ – Häufige Fragen zur ISMS-Zertifizierung nach ISO 27001

DEKRA
Alles im grünen Bereich.

Sie möchten die Informationssicherheit in Ihrem Unternehmen optimieren und sich dafür gemäß ISO 27001:2013 zertifizieren lassen, haben jedoch noch einige Fragen zu diesem Thema? Wir haben hier häufige Fragen und Antworten für Sie zusammengestellt, damit Sie sich im Vorfeld besser darüber informieren können.

1. Was ist ISO 27001?

Die ISO 27001 ist eine internationale Norm mit deren Hilfe die Informationssicherheit für Organisationen umgesetzt werden kann. Sie wurde von der International Organisation for Standardization, kurz ISO, veröffentlicht und hat sich als weltweit anerkannter Standard etabliert.

2. Was versteht man unter Informationssicherheit?

Informationssicherheit, auch Information Security, dient als Präventivschutz dazu, die Informationen und Daten von Organisationen vor Schäden und Bedrohungen zu schützen. Dafür werden entsprechende technische und organisatorische Maßnahmen definiert. Mit deren Hilfe können Schwachstellen und Sicherheitslücken erkannt und durch entsprechende Maßnahmen behoben werden.

Die drei Kernziele der Informationssicherheit sind:

- **Vertraulichkeit: Schutz von vertraulichen Informationen vor unberechtigtem Zugriff**
- **Integrität: Minimierung von Risiken und Absicherung der Vollständigkeit und Richtigkeit von Daten und Informationen**
- **Verfügbarkeit: Sicherstellung des verlässlichen Zugangs und der Nutzbarkeit für den berechtigten Zugriff auf Informationen und Informationssysteme**

3. Was sind die Top 5 der Informationssicherheit-Bedrohungen, gegen die ein Unternehmen gewappnet sein muss?

Auf der Liste der Top 5 Bedrohungen steht die Infektion mit Schadsoftware über das Internet weiterhin an oberster Stelle, gefolgt von dem Einschleusen von Schadsoftware über Wechseldatenträger, wie USB-Sticks oder CDs. Aber auch menschliches Fehlverhalten und Social Engineering stellen nicht zu unterschätzende Bedrohungen für Ihre Informationssicherheit dar. Nicht zuletzt gelingt es Angreifern immer wieder auch über Fernwartungszugänge in IT-Systeme einzudringen und so Zugriff auf vertrauliche Informationen oder Daten zu erhalten.

Mit einem effektiven ISMS befähigen Sie Ihr Unternehmen dazu, Schwachstellen zu identifizieren und Maßnahmen zum Schutz vor diesen und weiteren IT-Bedrohungen abzuleiten und umzusetzen.

4. Was ist ein ISMS?

Die Abkürzung ISMS steht für Information Security Management System oder auch Informationssicherheitsmanagementsystem. Das ISMS definiert Regeln, Methoden und Maßnahmen, um die Informationssicherheit zu kontrollieren, zu steuern und sicherzustellen. Ein ISMS wird im Rahmen der Zertifizierung nach ISO 27001 in Ihrem Unternehmen auditiert und auf seine Wirksamkeit überprüft.

5. Warum sollte ich mein Unternehmen nach ISO 27001 zertifizieren?

Eine Zertifizierung nach ISO 27001 bietet Ihnen zahlreiche Vorteile:

- **Sie minimieren Ihre Unternehmens- und Haftungsrisiken**
- **Sie senken Ihre Kosten**
- **Sie erkennen und reduzieren Bedrohungen für Ihr Unternehmen**
- **Sie schützen Ihre vertraulichen Daten und Informationen**
- **Sie sichern sich das Vertrauen von Kunden und Geschäftspartnern**
- **Sie steigern Ihre Wettbewerbsfähigkeit**
- **Sie erfüllen Anforderungen von Wirtschaftsprüfern**

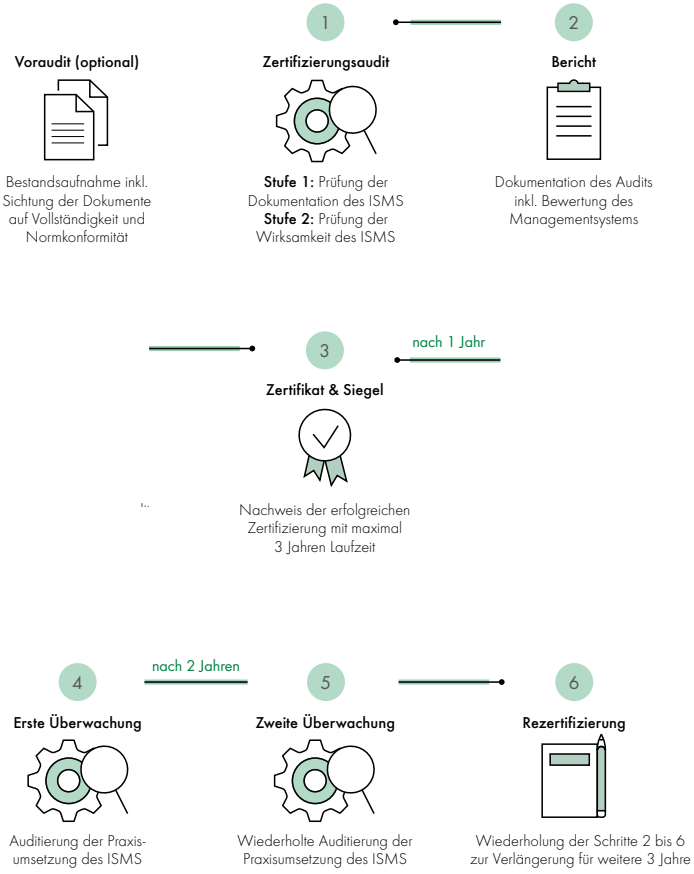
6. Welche Branchen sollten sich nach ISO 27001 zertifizieren lassen?

Die ISO 27001 eignet sich für jede Branche, da in der heutigen Zeit nahezu alle Unternehmen informationstechnische Systeme nutzen und auf deren Sicherheit angewiesen sind. Die Anforderungen der ISO 27001:2013 sind so gehalten, dass sie sich auf jedes Unternehmen, unabhängig von Branche und Große, übertragen lassen.

Finden Sie jetzt mit unserer Checkliste heraus, wie gut Ihr Unternehmen auf die ISO 27001 Zertifizierung vorbereitet ist.

7. Wie ist der Ablauf der ISO 27001 Zertifizierung?

Wir zertifizieren Ihr Unternehmen gemäß ISO 27001 in folgenden Schritten:



8. Was beinhaltet der Zertifizierungsprozess nach ISO 27001?

Unter anderem umfasst der Zertifizierungsprozess:

- Vorbereitung von Seiten des Kunden:
  - Festlegung des Anwendungsbereiches des ISMS
  - Definition einer Informationssicherheits-Richtlinie und der Ziele
  - Entwicklung einer Risikobewertungs- und Risikobehandlungsmethodik
  - Erstellung einer Anwendbarkeitserklärung
  - Erstellung eines Risikobehandlungsplans und eines Risikobewertungsberichts
  - Definition der Sicherheits-Rollen und Verantwortlichkeiten
  - Erstellung eines Verzeichnisses der Assets
  - Sicherstellung der akzeptablen Nutzung des Assets
  - Definition von Richtlinien wie z.B. für die Zugriffskontrolle laut Annex A der ISO 27001

- Durchführung des Zertifizierungsaudits:
  - Stufe 1: Prüfung der ISMS- Dokumentation und Feststellung, ob das Unternehmen zur Zertifizierung bereit ist (Bereitschaftsanalyse) mit Begehung des Unternehmens und Interview mit dem ISMS-Verantwortlichen.
  - Stufe 2: Audit zur Überprüfung der Wirksamkeit des ISMS mit Interviews der verantwortlichen Leitung sowie Mitarbeitern in den verschiedenen Bereichen Ihres Unternehmens.
  - Die Auditoren erstellen einen Auditbericht mit Dokumentation des Audits und Bewertung des ISMS Ihres Unternehmens.
  - Anschließend erfolgt die Ausstellung des Zertifikates und des Siegels mit maximal drei Jahren Laufzeit.
  - Innerhalb eines Jahres erfolgt das erste Überwachungsaudit und im Folgejahr das zweite Überwachungsaudit.
  - Vor Ablauf der Gültigkeitsdauer des Zertifikats von drei Jahren muss ein Rezertifizierungsaudit erfolgen und abgeschlossen sein.
  - Daran anschließend erfolgen wiederum ein erstes und zweites Überwachungsaudit wie zuvor beschrieben.

9. Welche Änderungen gibt es mit der ISO 27001:2017?

Die international gültige Norm ISO/IEC 27001:2013 ist die Basis für die ISO 27001-Zertifizierung. Bei der DIN ISO/IEC 27001:2017 handelt es sich um die deutsche Übersetzung der ISO/IEC 27001:2013.

Mit der EN ISO/IEC 27001:2017-06 erschien eine vom CEN (European Committee for Standardization) abgestimmte Version. Sie vereint nun 2 Berichtigungen Cor 1:2014 und Cor 2:2015 (Corrigenda):

- Cor 1:2014
  änderte im Anhang A das Control A.8.1.1 und in ISO/IEC 27002 Kapitel 8.3.3 die „Implementation Guidance".
- Cor 2:2015
  stellte den Artikel 6.1.3 d der ISO/IEC 27001 übersichtlicher dar.
  Alt: Eine Erklärung zur Anwendbarkeit zu erstellen, welche die erforderlichen Maßnahmen (siehe 6.1.3 b) und c)) und Gründe für deren Einbeziehung, unabhängig davon, ob sie nun umgesetzt sind oder nicht, sowie Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A enthält;
  Neu: Eine Erklärung zur Anwendbarkeit zu erstellen, welche
  - die erforderlichen Maßnahmen (siehe 6.1.3 b) und c));
  - Gründe für deren Einbeziehung;
  - ob sie umgesetzt sind oder nicht; sowie
  - Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A enthält;

Beide Korrekturen sind in der EN ISO/IEC 27001:2017-06 enthalten. Die mit der Korrektur verbundenen Änderungen beinhalten lediglich eine verbesserte Beschreibung der damit verbundenen Forderungen und keine zusätzlichen Forderungen. Daher wird bei der Dekra Certification GmbH keine Umstellung auf diese Fassung erfolgen. Neue Zertifikate werden auf der Basis der bisherigen Fassung ausgestellt.

Weitere Leistungen, von denen Sie profitieren

Sie haben ebenfalls die Möglichkeit, weitere Qualitäts-, Umwelt- und Sicherheits-Managementsysteme, z.B. nach ISO 14001, ISO 45001 und IATF sowie deren Kombinationen, von uns zertifizieren zu lassen. Über 40 Akkreditierungen beinhaltet unser Portfolio! Darüber hinaus bietet Ihnen die DEKRA Gruppe rund um das Thema Qualität:

- Bewertungen zur Einhaltung eigener Regeln, z.B. Lieferantenanforderungen
- Trainings und Schulungen, z.B. Qualitätsmanagement-Beauftragter
- Personen-Zertifizierungen, z.B. Ihres Qualitäts-verantwortlichen
- Produktprüfungen und Zertifizierungen, z.B. EMV, CE, GS für elektrische und elektronische Geräte

Ausgezeichnet – das DEKRA Siegel

Setzen Sie ein Ausrufezeichen für höchste Qualität und Zuverlässigkeit – branchenübergreifend und international. Das DEKRA Siegel leistet beste Dienste als Imageträger, Marketinginstrument und um sich vom Wettbewerb abzuheben. So zeigen Sie Ihren Kunden und Geschäftspartnern, dass Leistung bei Ihnen ihr Geld wert ist. Wir unterstützen Sie gerne dabei.

Sie haben weitere Fragen zur Zertifizierung Ihrer Informationssicherheit nach ISO 27001? Dann kontaktieren Sie uns jetzt!

DEKRA Certification GmbH
AUSTRIA
campus 21
Businesspark Wien Süd, F05
2345 Brunn am Gebirge
Fon: +43.2235.40 900 20
Mobil: +43.664.88 2999 11
roland.schimpl@dekra.com
www.dekra.at