SICON®

IT-SICHERHEIT · CONSULTING · DATENSCHUTZ

# Information Security Management DIN EN ISO/IEC 27001:2017

HÄUFIG GESTELLTE FRAGEN

# Inhaltsverzeichnis

**SICON GmbH** | Zeppelinstr. 4 | 66740 Saarlouis
**Telefon:** 0 68 31 / 1 22 4 11 | **Fax:** 0 68 31 / 1 22 3 70
**E-Mail:** info@sicon-it.de | datenschutz@sicon-it.de
**Geschäftsführer:** Dipl. Ing. (FH) Dennis W. Nicola



Die ISO 27001 ist ein internationaler Standard, der es durch seinen prozessorientierten Ansatz ermöglicht Risiken im Umgang mit sensiblen Informationen zu erkennen und geeignete Maßnahmen zur Risikominimierung zu ergreifen.

Die Anwendung des Informationssicherheits-Management-Systems trägt zur Verbesserung der Informationssicherheit und des Datenschutzes bei.

Im Folgenden wollen wir Ihnen häufig auftretende Fragen bezüglich der ISO 27001 beantworten und für Sie alle relevanten Informationen zusammenfassen.

## Welche Bedrohungen gefährden die Informationssicherheit?

Es gibt zahlreiche Bedrohungen, die für die Informationssicherheit eine große Gefahr

darstellen. An erster Stelle steht die Gefahr durch Schadsoftware, die beispielsweise über Wechseldatenträger oder Anhänge von E-Mails ins System des Unternehmens gelangen. Genauso wenig zu unterschätzen ist menschliches Fehlverhalten sowie Social-Engineering. Vor allem letzteres ist besonders schwer zu identifizieren. Beliebte Eintrittspforten für Angriffe und den unbefugten Zugriff auf vertrauliche Informationen sind Fernwartungszugänge.

Eine ISO 27001-Zertifizierung minimiert diese Risiken signifikant. Die IT-Sicherheit weist an den Maßnahmen zur Informationssicherheit einen durchschnittlichen Anteil von 50 Prozent auf. Sie definiert sich durch alle Aktivitäten, die zur zuverlässigen Sicherheit der IT beitragen. Dazu zählen Back-up-Verfahren oder der Einsatz abschirmender Sicherheitslösungen oder die Rollenverteilungen innerhalb der Zugriffshierarchien.

## Wo liegt der Unterschied zwischen IT-Sicherheit und Informationssicherheit?

Die Informationssicherheit legt ihren Fokus auf das gesamte Unternehmen und die damit verbundenen Sicherheitsvorkehrungen. Sie definiert Verantwortlichkeiten und Sicherheitsrollen, die verschiedenen Arbeitsabläufe und ist verantwortlich für die



EXTERNER DATENSCHUTZ mit DEKRA-Zertifizierung | www.dsb.saarland
IT-SICHERHEIT Planung·Umsetzung·Begleitung | www.sicon-it.de/secure
ISMS + ISO 27001 CONSULTING PECB zertifizierte Informationssicherheit | www.sicon-it.de/iso
SACHVERSTÄNDIGENBÜRO Bürokommunikation+Informationstechnik | www.sv-nicola.de

Sensibilisierung und Schulung der Mitarbeiter in Sicherheitsfragen. Außerdem sieht sie explizite Regelungen zu Schnittstellen mit Unterauftragnehmern oder Lieferanten vor.

## ISMS, ISO 27001, IT-Grundschutz– was bedeutet das?

ISMS ist die Abkürzung für Informationssicherheits-Managementsystem. Über das ISMS definiert ein Unternehmen alle Richtlinien, Prozesse und Verfahren, die dazu dienen, die Sicherheit, Verfügbarkeit und Integrität der Informationen zu steuern, zu kontrollieren und sicherzustellen. Im Rahmen der ISO 27001-Zertifizierung wird das ISMS auf seine Wirksamkeit hin in der Praxis überprüft.

Eine Zertifizierung nach ISO 27001 bestätigt die erfolgreiche Implementierung eines ISMS nach DIN EN ISO/IEC 27001:2017. Die Norm ist ein international anerkannter und führender Standard für Informationssicherheit. Der Schwerpunkt der ISO 27001 liegt auf den für IT-Infrastrukturen und Verfahrensweisen typischen Risiken und deren Minimierung durch einen prozessorientierten Ansatz. Ziel ist ein angemessener Schutz aller Informationen im Unternehmen zu gewährleisten, diesen kontinuierlichen zu überwachen und aufrechtzuerhalten. Dabei bietet ein ISMS auch ideale Voraussetzungen, um gesetzliche Anforderungen an den Datenschutz zu erfüllen.

Der IT-Grundschutz-Katalog ist ein vom Bundesamt für Sicherheit in der Informationstechnik entwickeltes Konzept zur Umsetzung eines ISMS. Das Konzept gibt in Bausteinen konkrete Hilfestellungen zur Gestaltung und Realisierung der Sicherheitsmaßnahmen auf technischer Ebene. Die sehr allgemein gehaltenen Anforderungen der ISO 27001 können praktisch durch die im Grundschutz-Katalogen enthaltenen Konzepte umgesetzt werden. Sowohl ISO 27001 als auch IT-Grundschutz legen bei ihren Umsetzung der Maßnahmen den Fokus auf Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.



EXTERNER DATENSCHUTZ mit DEKRA-Zertifizierung | www.dsb.saarland
IT-SICHERHEIT Planung·Umsetzung·Begleitung | www.sicon-it.de/secure
ISMS + ISO 27001 CONSULTING PECB zertifizierte Informationssicherheit | www.sicon-it.de/iso
SACHVERSTÄNDIGENBÜRO Bürokommunikation+Informationstechnik | www.sv-nicola.de

## Konzentriert sich die ISO 27001 ausschließlich auf die IT?

Bei erfolgreicher Implementierung eines Informationssicherheits-Managementsystems müssen neben den IT-Systemen noch weitere Maßnahmen betrachtet werden. Denn die IT alleine ist nicht in der Lage alle Informationen zu schützen.

Ein erfolgreiches ISMS umfasst sowohl die IT-Struktur als auch ein durchdachtes Personalmanagement, organisatorische Belange oder die Einhaltung von gesetzlichen Anforderungen.

## Clauses, Annex A, Controls – was ist was?

Clauses sind die Anforderungen, die die ISO 27001 an das ISMS stellt und als Grundlage für die Zertifizierung dienen:

4. Kontext der Organisation
5. Führung
6. Planung
7. Unterstützung
8. Betrieb
9. Bewertung der Leistung
10. Verbesserung der Leistung

Der Annex A bildet durch die vorgegebenen Controls die Grundlage, auf der die Konzeption des Sicherheitsmanagements aufbaut.

5. Informationssicherheitsrichtlinien
6. Organisation der Informationssicherheit
7. Personalsicherheit
8. Verwaltung der Werte



EXTERNER DATENSCHUTZ mit DEKRA-Zertifizierung | www.dsb.saarland
IT-SICHERHEIT Planung·Umsetzung·Begleitung | www.sicon-it.de/secure
ISMS + ISO 27001 CONSULTING PECB zertifizierte Informationssicherheit | www.sicon-it.de/iso
SACHVERSTÄNDIGENBÜRO Bürokommunikation+Informationstechnik | www.sv-nicola.de

9. Zugangssteuerung
10. Kryptographie
11. Physische und umgebungsbezogene Sicherheit
12. Betriebssicherheit
13. Kommunikationssicherheit
14. Anschaffung, […] und Instandhalten von Systemen
15. Lieferantenbeziehungen
16. Handhabung von Informationssicherheitsvorfällen
17. Informationssicherheitsaspekte beim BCM
18. Compliance

Es enthält in 18 Abschnitten 114 Kontrollen zu den verschiedensten Sicherheitspunkten. Für die ISO 27001-Zertifizierung wählt ein Unternehmen alle anwendbaren Kontrollpunkte aus, um die entsprechenden Maßnahmen zu entwickeln. Nicht alle 114 Kontrollen müssen verpflichtend angewendet werden.

## Wo liegen die Vorteile einer ISO 27001-Zertifizierung?

Eine ISO 27001-Zertifizierung erhöht die Effizienz von unternehmensinternen Prozessen. Zeitgleich erhalten Unternehmen durch die Transparenz der Sicherheitsmaßnahmen einen umfassenden Überblick hinsichtlich der Informationssicherheit des Unternehmens. Dies wiederum reduziert das Haftungsrisiko und oft wirkt sich die Zertifizierung durch den Wegfall kostenintensiver Vorfälle positiv auf die Betriebskosten aus.

Weitere Vorteile liegen im Vertrauenszuwachs, aus welchem das Unternehmen Wettbewerbsvorteile generiert. Aber es eröffnen sich auch neue Marktchancen. Denn die ISO 27001-Zertifizierung unterstützt Unternehmen dabei die in den meisten Ländern gültigen Gesetze hinsichtlich des Schutzes von Daten und IT-Systemen usw. einzuhalten und dadurch auf einfacherem Wege zu expandieren. Ein weiterer Vorteil liegt darin, dass ein durchdachtes ISMS dazu führt, dass alle Mitarbeiter eines Unternehmens Informationssicherheit nicht als Selbstzweck betrachten, sondern in ihre alltäglichen Arbeitsabläufe integrieren.



EXTERNER DATENSCHUTZ mit DEKRA-Zertifizierung | www.dsb.saarland
IT-SICHERHEIT Planung·Umsetzung·Begleitung | www.sicon-it.de/secure
ISMS + ISO 27001 CONSULTING PECB zertifizierte Informationssicherheit | www.sicon-it.de/iso
SACHVERSTÄNDIGENBÜRO Bürokommunikation+Informationstechnik | www.sv-nicola.de

## Ist die ISO 27001-Zertifizierung für jede Organisation sinnvoll?

Im Prinzip ist die ISO 27001-Zertifizierung für jede Organisation, unabhängig von Art und Größe, sinnvoll. Denn die Anforderungen dieser Norm sind so gestaltet, dass sie problemlos auf jedes Unternehmen übertragbar sind. Allerdings erfordert die Entwicklung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementssystems entsprechende personelle Ressourcen. Diese sind vor allem in kleinen Unternehmen oder anderen Organisationen oft nicht vorhanden.

- Automobilindustrie
- Banken & Finanzdienstleister
- Einzelhandel
- IT-Branche & Betreiber von Rechenzentren
- Telekommunikationsunternehmen
- Versicherungen
- Alle datenverarbeitenden Unternehmen

## ISO 9001 wurde bereits umgesetzt - profitiert das Unternehmen davon bei der ISO 27001-Zertifizierung?

Unternehmen, die bereits nach ISO 9001 zertifiziert sind, profitieren davon bei der ISO 27001-Zertifizierung. Denn der Annex SL der ISO sieht vor, dass bei der Implementierung von Managementsystemen eine gemeinsame übergeordnete Struktur angewendet wird. So erfordern viele Elemente, wie beispielsweise interne Audits, das Dokumentationsmanagement, Korrekturmaßnahmen oder die Managementbewertung für die ISO 27001-Zertifizierung nur geringfügige Änderungen. Dies vereinfacht die Implementierung eines ISMS nach ISO 27001.

## Wie gestaltet sich die ISO 27001-Implementierung und Zertifizierung?

Die ISO 27001-Implementierung besteht aus insgesamt fünf Schritten, die ein Unternehmen erfolgreich absolvieren muss.



EXTERNER DATENSCHUTZ mit DEKRA-Zertifizierung | www.dsb.saarland
IT-SICHERHEIT Planung·Umsetzung·Begleitung | www.sicon-it.de/secure
ISMS + ISO 27001 CONSULTING PECB zertifizierte Informationssicherheit | www.sicon-it.de/iso
SACHVERSTÄNDIGENBÜRO Bürokommunikation+Informationstechnik | www.sv-nicola.de

- Eine Bestandsaufnahme dient der Dokumentensichtung auf Vollständigkeit und Normkonformität.
- Erforderliche Maßnahmen werden umgesetzt und in einem ersten internen Audit werden die Dokumentation des ISMS und die Bereitschaft einer Organisation zur Zertifizierung überprüft.
- Das Stufe 2-Audit prüft die Wirksamkeit des ISMS und dessen Umsetzung vor Ort.
- Der Auditor erstellt den Auditbericht und legt ihn der Zertifizierungsstelle vor.
- Abschluss des Audits mit Zertifizierung.

## Wie lange ist die Zertifizierung gültig?

Die erstmalige erfolgreiche ISO 27001-Zertifizierung ist maximal drei Jahre gültig und muss nach diesem Zeitraum durch eine Re-Zertifizierung bestätigt werden. Diese gilt wiederum drei Jahre.

Zwischen Erst- und Re-Zertifizierung erfolgen typischerweise jährlich durchgeführte Überwachungen. Diese dienen der Auditierung der praktischen Wirkung des ISMS und wiederholen sich, solange ein Unternehmen die wiederholte Re-Zertifizierung anstrebt.

## Wie viel Zeit nimmt die Umsetzung von ISO 27001 in Anspruch?

Auf Basis von Erfahrungswerten erfordert die Umsetzung von ISO 27001 bei kleineren Unternehmen zwischen drei und sechs Monaten. Größere Unternehmen ab 500 Mitarbeitern benötigen durchschnittlich acht Monate bis zu einem Jahr oder sogar etwas länger.

Wie lange die Umsetzung bis zur ISO 27001-Zertifizierung tatsächlich dauert, hängt vor allem davon ab, welchen Status das aktuelle Informationssicherheits-Management eines Unternehmens besitzt und welche Strukturen und Verfahren hierzu vorhanden sind

**Gerne stehen wir Ihnen für eine persönliche Beratung zur Verfügung**

**Sie erreichen unsere Teams von Montag bis Freitag zwischen 8 - 17 Uhr**

**SICON GmbH**

**- Datenschutz - Datensicherheit -ISMS - ISO 27001 -**

**06831 - 122 411**

**info@sicon-it.de**