



Management Service

**Mehr Sicherheit.
Mehr Wert.**

Produktinformation Informationssicherheits-Managementsystem ISO/IEC 27001

In der modernen Wissens- und Informationsgesellschaft sind Unternehmen bei der Verarbeitung von geschäftsrelevanten Daten auf komplexe und schnelle IT-Systeme angewiesen. Die Informationstechnik erleichtert zwar sehr viele Prozesse, birgt aber auch

Risiken in sich. Ein umfassender Schutz von sensiblen Daten und Informationen ist deshalb besonders wichtig. Die Zuverlässigkeit und die Sicherheit der eingesetzten Informationstechnik werden somit zum entscheidenden Erfolgsfaktor eines Unternehmens.

ISO/IEC 27001

Transparenz und Sicherheit mit System

TÜV SÜD Management Service GmbH





Warum ISO/IEC 27001?

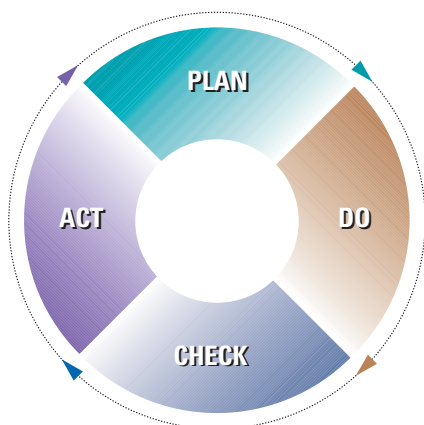
Informationssicherheit wird immer wichtiger. Denn für den Geschäftserfolg eines Unternehmens sind Informationen entscheidende Werte. Diese zu verwalten und zu schützen hat oberste Priorität. Informationen, insbesondere als elektronisch verarbeitete Daten, sind ständigen Bedrohungen und Risiken ausgesetzt, weshalb die Anforderungen an ihre Sicherheit wie Verfügbarkeit, Vertraulichkeit und Integrität steigen. Dabei geht es sowohl um den Schutz der Informations- und Kommunikationssysteme vor den zunehmenden Angriffen durch das Netz, als auch beispielsweise um die Verhinderung von Verlust durch Diebstahl und von Schäden durch äußere Einwirkungen oder die Minimierung der Folgen durch menschliches Fehlverhalten.

Um diesen möglichen Faktoren effizient entgegen zu wirken, reichen technisch-organisatorische Maßnahmen allein nicht aus. Ein sicherheitsbewusstes Verhalten von allen Mitarbeitern auf allen Ebenen ist eine Grundvoraussetzung für einen umfassenden Schutz. Die Implementierung eines Informationssicherheits-Managementsystems (ISMS) auf Basis des internationalen Standards ISO/IEC 27001 unterstützt Unternehmen von der systematischen Identifizierung und Analyse von Risiken, die im Zusammenhang mit der Nutzung von Informationen entstehen, bis hin zur Einführung und Aufrechterhaltung angemessener Kontroll- und Steuerungsmechanismen.

Was bringt das Informationssicherheits-Managementsystem (ISMS)?

Ein Informationssicherheits-Managementsystem ist ein kontinuierlicher Prozess, der auf dem so genannten PDCA-Modell (Plan-Do-Check-Act) basiert. Dieser unterstützt bei der strukturierten Umsetzung aller wesentlichen Sicherheitsaspekte. Mit ihm ermitteln und analysieren Sie Ihre möglichen Risiken, identifizieren Ihren Handlungsbedarf und setzen die notwendigen Maßnahmen um, die Sie laufend überwachen und optimieren. So halten Sie die wesentlichen Sicherheitsziele immer im Blick.

Der
PDCA-
Zyklus



Schützen Sie das Wissen und somit die Werte Ihres Unternehmens und sichern Sie sich wertvolle Vorteile durch ein ISMS nach ISO/IEC 27001:

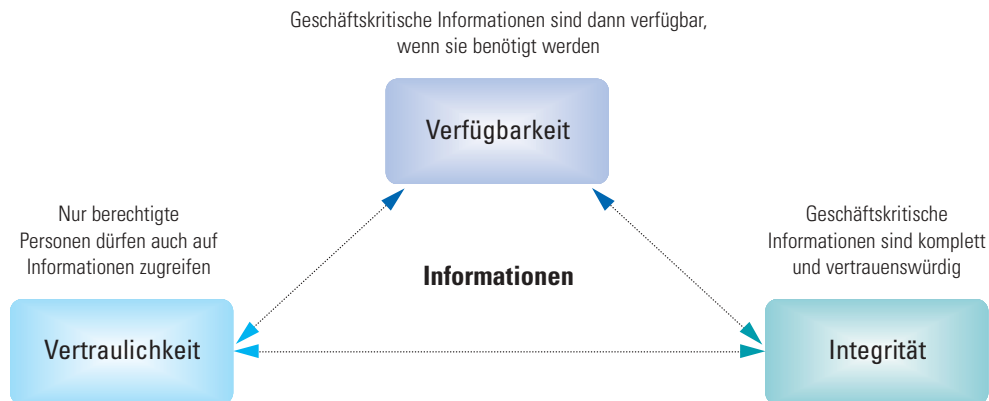
- Verbessertes Verständnis der Geschäftsanforderungen
- Schutz der Informationen vor Bedrohungen
- Erleichterte Identifikation von Schwachstellen
- Ständige Verfügbarkeit der Informationen und somit Gewährleistung eines kontinuierlichen Geschäftsbetriebes
- Hohe Vertrauensbildung bei Geschäftspartnern
- Verringerteres Risiko einer Rufschädigung



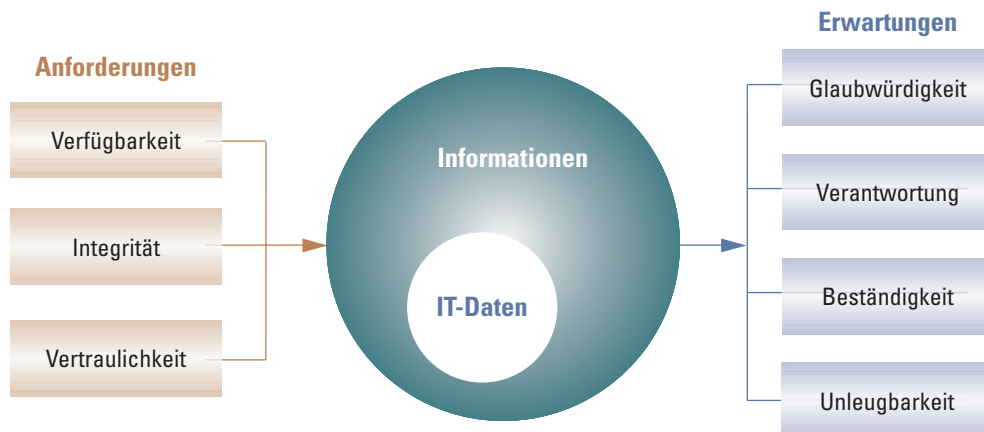


Was sind Grundlagen der Informationssicherheit?

Der Standard ISO/IEC 27001 betrachtet die drei wesentlichen Merkmale einer Information: die Verfügbarkeit, die Vertraulichkeit und die Integrität. Diese Merkmale sind grundlegender Inhalt aller externen Anforderungen, die ein Unternehmen zu leisten hat, wie KontraG, Basel II, SOX oder die der Wirtschaftsprüfer.



Informationen haben nicht nur formale Anforderungen zu erfüllen, sie müssen auch unterschiedlichen Erwartungen gerecht werden. Die wesentlichen Aspekte sind Glaubwürdigkeit, Verantwortung, Beständigkeit und Unleugbarkeit.



Das Informationssicherheits-Managementsystem (ISMS) berücksichtigt alle Perspektiven einer Information und konzentriert sich nicht nur auf deren elektronische Verwertung:

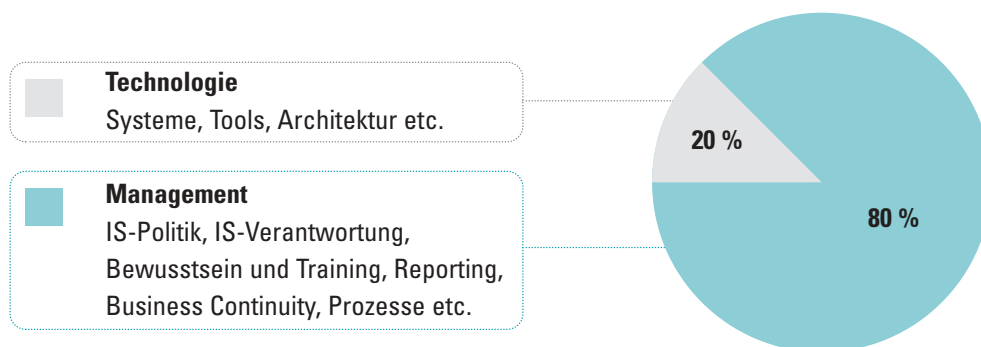
- Information ist mehr als nur elektronisch gespeichert oder verarbeitet
- Informationssicherheit umfasst nicht nur IT-Sicherheit
- Sicherheit bedeutet Vertraulichkeit, Integrität und Verfügbarkeit
- Management ist nicht nur technische Systeme und Werkzeuge





Was erfordert Informationssicherheit?

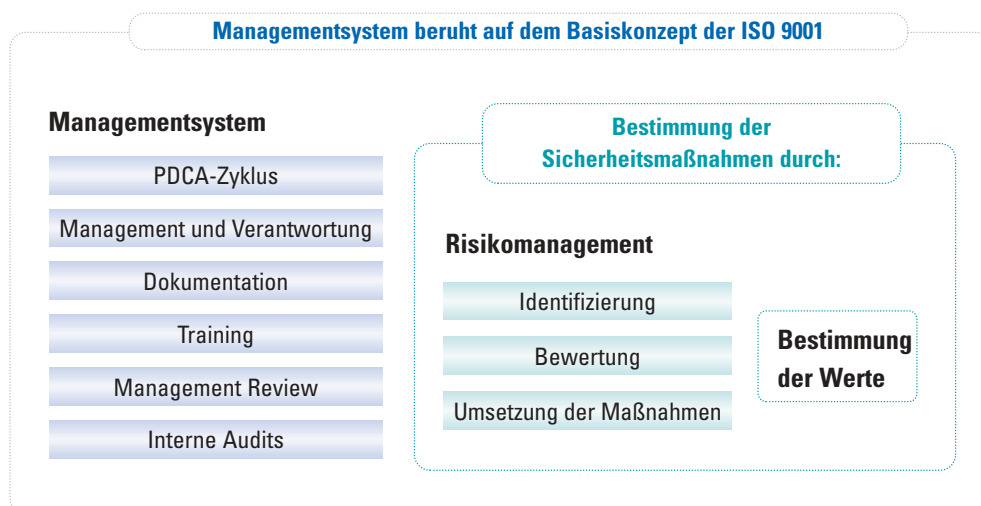
Das Gebiet Informationssicherheit beinhaltet die Technologie, die für die Sicherheit der IT-Systeme und der darin gespeicherten Daten sorgt, sowie das Management aller damit verbundenen Prozesse. Wesentlich dabei ist eine gesamtheitliche Betrachtung. Denn allein mit dem Kauf von Firewalls und Virenscannern ist es nicht getan. Vielmehr bedarf es einer strukturierten Planung und Steuerung sämtlicher Sicherheitsmaßnahmen, um einen zuverlässigen Schutz zu gewährleisten.



Was enthält die ISO/IEC 27001?

Die ISO/IEC 27001 besteht aus zwei Teilen: dem Managementsystem und den notwendigen Maßnahmen (Controls), die auf jeden Fall zu betrachten sind. Die folgende Grafik zeigt schematisch den Inhalt der beiden Teile.

Überblick
Inhalte
ISO/IEC
27001



Die Sicherheitsmaßnahmen (Controls) betreffen folgende Aspekte:

- Physikalische Sicherheit
- Personelle Sicherheit
- Sicherheit des IT-Betriebs
- Zutritts- und Zugangsschutz
- Sicherheit bei der Entwicklung
- Sicherheitsvorfälle
- Vorgehen im Notfall
- Compliance

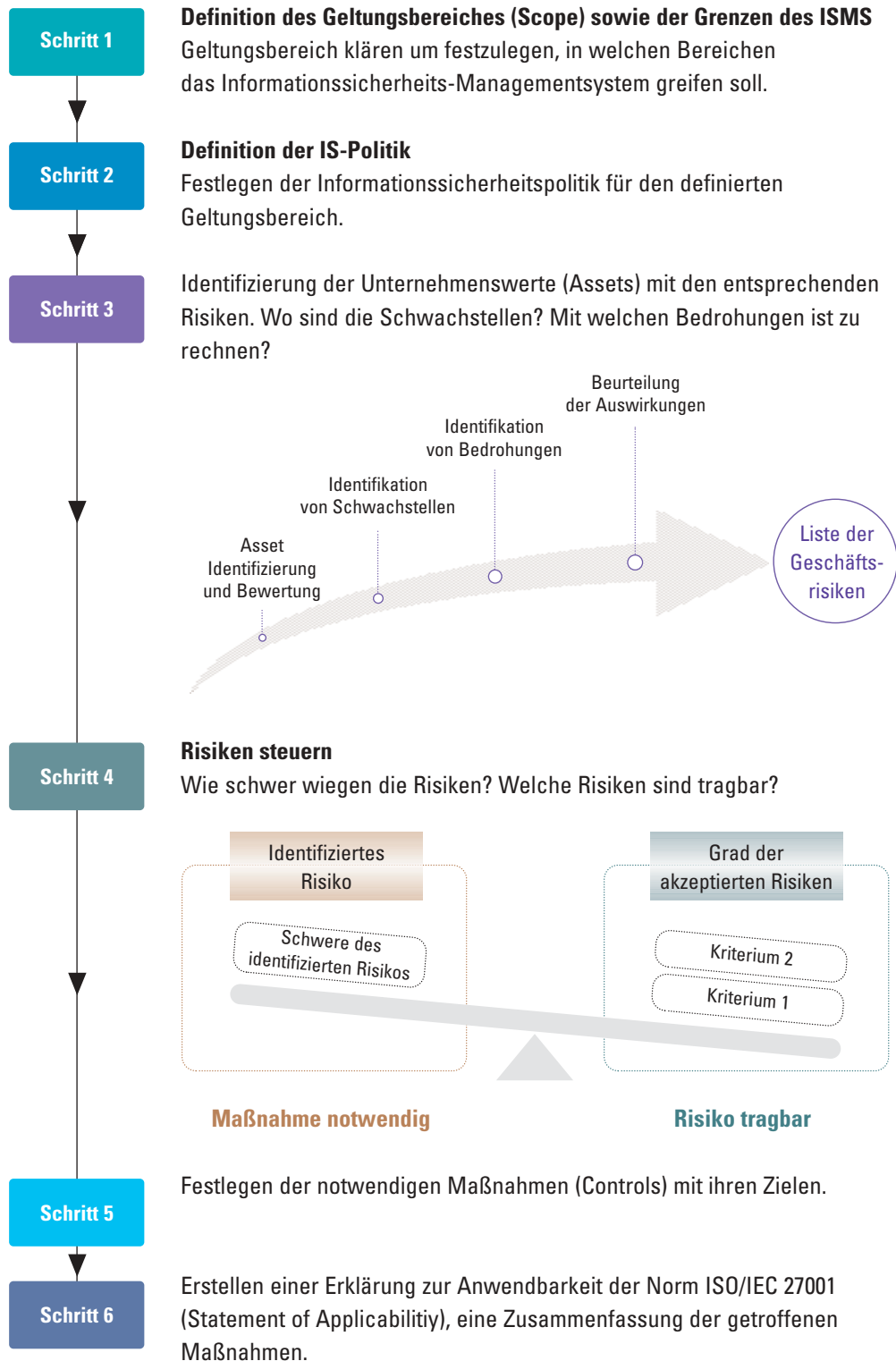




Wie wird die ISO/IEC 27001 implementiert?

Die sechs notwendigen Schritte für die Implementierung Ihres Informationssicherheits-Managementsystems nach ISO/IEC 27001.

6 Schritte
zur Imple-
mentierung





Was sind die kritischen Erfolgsfaktoren?

Um eine erfolgreiche Implementierung Ihres Informationssicherheits-Managementsystems nach ISO/IEC 27001 zu erreichen, sollten folgende Faktoren berücksichtigt werden:

Informationssicherheits Politik, -Ziele und Maßnahmen	müssen sich auf die Geschäftsziele beziehen
Vorgehen und Vorgehensmodell (PDCA-Framework)	in Übereinstimmung mit der Unternehmenskultur
Unterstützung und Zustimmung vom Management	aus allen Hierarchieebenen
gutes Verständnis von Risiko-Bewertung und -Management	Training aller Betroffenen
Kenntnis der Informationssicherheits Politik	Schulung von Managern, Mitarbeitern und Andere
Budgets für Informationssicherheits-Management Aktivitäten bereitstellen	realistische Kosten einplanen
vernünftiges Problem-Bewußtsein herbeiführen	„Erziehung“ im Schulungsplan aufnehmen
wirksamen Prozess für Informationssicherheits-Vorfälle einrichten	klare Anforderungen vorgeben
Effizienz und Verbesserung des Informationssicherheits-Management gewährleisten	Aufbau eines Kennzahlen-Systems

Was leistet der TÜV SÜD für Sie?

Gerne helfen wir Ihnen mit unterschiedlichen Maßnahmen bei der Einführung Ihres Informationssicherheits-Managementsystems.

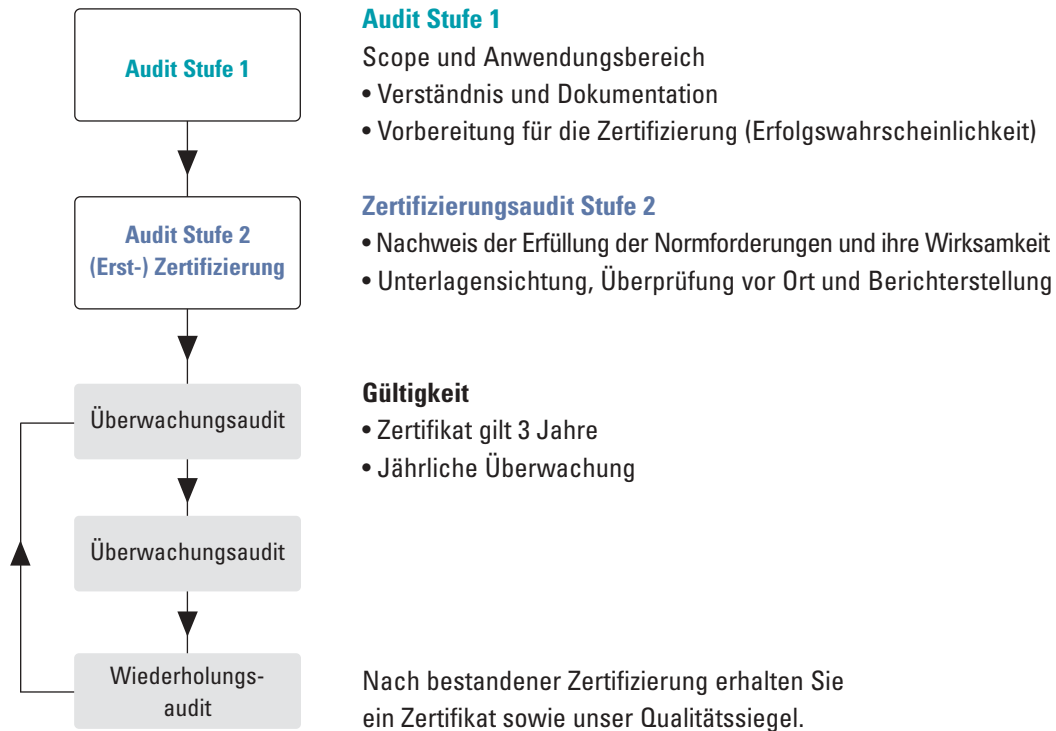
- **GAP-Analyse:** Sie bietet Ihnen einen Überblick über das, was Sie bereits implementiert haben und welche Aufgaben noch durchzuführen sind.
- **Voraudit:** Ein Voraudit bereitet Ihr Unternehmen optimal auf eine Zertifizierung vor und ist besonders empfehlenswert, um offene Fragen Ihrer Mitarbeiter hinsichtlich des eigentlichen Audits zu beantworten.
- **Schulungen in Zusammenarbeit mit der TÜV SÜD Akademie:** Wir bieten Ihnen Übersichtskurse zu ISO/IEC 27001 sowie Kurse für Ihre internen Auditoren.





Wie läuft die Zertifizierung ab?

Ein Zertifizierungsverfahren nach ISO 27001 durch die TÜV SÜD Management Service GmbH wird in zwei Stufen durchgeführt. Während das Audit Stufe 1 vor allem dazu dient, Ihr Unternehmen und dessen Sicherheitsrelevanz kennen zu lernen, wird in Stufe 2 die Erfüllung der einzelnen Normforderungen überprüft.



Ein Zertifikat bedeutet Weitblick

Zertifikat



Kommunizieren Sie Ihren Erfolg an Ihre Mitarbeiter, Lieferanten, Partner und Kunden.

Werben Sie mit unserer starken Marke und binden Sie diese aktiv in Ihre interne und externe Unternehmenskommunikation ein, beispielsweise im Rahmen einer Marketingkampagne.

Nutzen Sie das Prüfzeichen in Ihrem Internet-Auftritt, auf Ihren Geschäftspapieren, Flyern, Broschüren etc.





Zusammenfassung

In Unternehmen erhält der gezielte Umgang mit Informationen einen immer größeren Stellenwert. Nur wer berechtigt ist, sollte Zugriff auf die immer und jederzeit verfügbaren Informationen erhalten. Gleichzeitig müssen auch Anforderungen an diese Informationen von Externen, wie Behörden oder Kunden, berücksichtigt werden.

Nur durch ein strukturiertes Vorgehen mittels eines Managementsystems für Informationssicherheit sind alle Forderungen, die auf eine Organisation einwirken, zu erfüllen. Wird dieses Informationssicherheits-Managementsystem auch noch von einem externen Spezialisten geprüft und zertifiziert, eröffnen sich mit dem Prüfzeichen zusätzliche Möglichkeiten für die eigene Marketingkommunikation.

Notizen

.....

.....

.....

.....

.....

.....

.....

TÜV SÜD Management Service GmbH

Ridlerstraße 65
80339 München
Deutschland
Tel: +49 (89) - 57 91 - 13 64
Fax: +49 (89) - 51 55 - 10 97
it-zertifizierung@tuev-sued.de

