TÜV TRUST IT
TÜV AUSTRIA Group

Zertifizierung

Zertifizierung nach ISO/IEC 27001:2013 durch die TÜV Austria Deutschland GmbH

Informationen sind die Basis für den Ablauf von Geschäfts- und Produktionsprozessen sowie für die Kommunikation mit Kunden und Partnern. Um die Unternehmensinformationen in angemessener Weise zu schützen, bedarf es wirksamer Prozesse, wie sie in einem Informationssicherheitsmanagementsystem (ISMS) abgebildet werden. Der international anerkannte Standard für ISMS ist die Norm ISO/IEC 27001:2013.

Durch die Zertifizierung nach ISO/IEC 27001:2013 unterliegen Prozesse und Maßnahmen eines ISMS der ständigen unabhängigen Überprüfung. Mit Hilfe einer Zertifizierung können Unternehmen zusätzlich auch ihren Kunden und Partnern die Wirksamkeit und Effizienz des ISMS und die regelmäßige Überprüfung durch unabhängige Auditoren, wie die der TÜV TRUST IT, nachweisen. Durch vielfach bewährte Methoden und Tools zur Bewertung des Managements der Informationssicherheit, der Sicherheitskonzepte sowie der organisatorischen und technischen Maßnahmen kann die TÜV TRUST IT gezielt Schwachstellen aufdecken und Verbesserungspotenziale herausstellen.

Vorgehensweise

Bei der Zertifizierung nach ISO/IEC 27001:2013 ist die folgende Vorgehensweise verbindlich, in der die nachfolgend aufgeführten Themen im Fokus stehen (Auszug):

Stage 1: Prüfung der Zertifizierbarkeit des ISMS (Dokumentenprüfung)

- Beurteilung des Standorts und der standortspezifischen Bedingungen des Kunden
- Bewertung des Status des Kunden sowie dessen Verständnis bezüglich der Anforderungen der Norm
- Sammeln der notwendigen Informationen bezüglich des Geltungsbereichs des ISMS
- Bewertung der Zuteilung der Ressourcen für das Stage 2 Audit
- Festlegen der Schwerpunkte für die Planung des Stage 2 Audits
- Beurteilung, ob die internen Audits und Managementbewertungen geplant und durchgeführt werden

Bei erfolgreichem Abschluss dieser Phase kann die nächste Stufe eingeleitet werden.

Stage 2: Prüfung der Wirksamkeit des ISMS

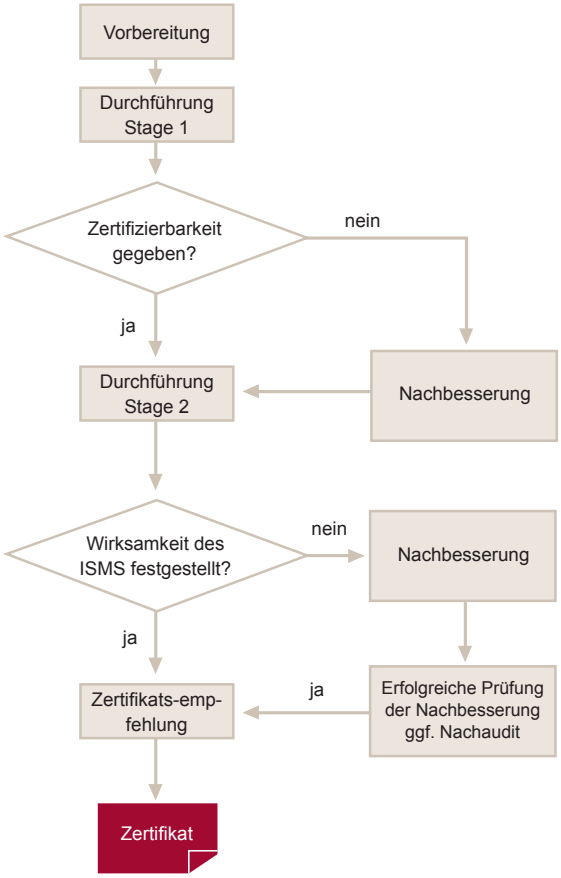
- Bewertung der Informationssicherheitsrisiken
- Die in Kapitel 4-10 geforderte Dokumentation und deren Steuerung
- Auswahl der Kontrollziele und Kontrollen auf Grundlage der Risikobewertung
- Interne ISMS-Audits und Management-Reviews
- Verantwortung des Top-Managements
- Implementierung von Kontrollen

Die Basis für alle Prüftätigkeiten in dieser Phase bilden die eingeführten ISMS-Prozesse. Das Auditteam analysiert alle während Stage 1 und Stage 2 erfassten Informationen und Auditnachweise, um die Auditfeststellungen zu bewerten und sich auf Auditschlussfolgerungen zu einigen. Liegt ein erfolgreicher Auditabschluss vor, werden die Auditoren der Zertifizierungsstelle eine Zertifizierung empfehlen, die bei positiver Kontrolle des Verfahrens das Zertifikat ausstellt.

Ein ISO/IEC 27001:2013 Zertifikat besitzt eine Gültigkeit von drei Jahren. Nach dem Zertifizierungsaudit erfolgen jährliche

Zertifizierung

Überwachungsaudits sowie nach drei Jahren auf Wunsch eine Re-Zertifizierung.



Prozess einer ISO/IEC 27001:2013 Zertifizierung

Ihr Nutzen

- Unabhängiger und international anerkannter Nachweis angemessener Informationssicherheit gegenüber Kunden, Partnern und Behörden
- Dauerhafte Verbesserung der ISMS-Prozesse durch regelmäßige Überprüfung
- Aufdeckung von Schwachstellen und Herausstellung von Verbesserungspotenzialen
- Vermeidung unerwarteter Kosten aus Sicherheitsvorfällen
- Erfahrene und durch die Dakks akkreditierte Auditoren

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com