



ask tami, ...



TÜV AUSTRIA > Solution > Industrie > Informationssicherheits-Zertifizierung | ISO 27001



Solution: Informationssicherheits- Zertifizierung | ISO 27001.


Audit & Certification




Ing. Klaus Mlekus, MBA


 TÜV AUSTRIA Informationssicherheits-Zertifizierung nach ISO 27001 


 In welcher Region benötigen Sie diese Lösung? 



 Austria



 Cyprus



Alle Regionen



 Romania

 Germany

 Ablauf ISO 27001-Zertifizierung 

 Fachliche Aus- und Weiterbildung 

 Akkreditierung 

 +43 5 0454 6067 E-Mail
senden TÜV
AUSTRIA-
Platz 1
2345 Brunn
am Gebirge
Österreich[Lösung anfragen](#) [Zu My Bundle
hinzufügen](#)

Weitere Tags:

Audit

Auditierung

Compliance

Cybersecurity

Digitale Bedrohung

Hackerangriff

Haftungsrisiko

Informationssicherheit

Informationstechnologie

ISO-Norm

ISO-Zertifikat

IT Prozess

IT Security

Managementsystem

Managementsystemnorm

Managementsystemzertifizierung

Norm

Prozessoptimierung

Rechtssicherheit

Risikomanagement

Schutzziele

Zertifikat

Zertifizierung

Zertifizierungsaudit

Informationen.

Die rasch voranschreitende digitale Transformation birgt gerade im Informationstechnologie-Bereich Chancen wie auch Risiken. Zu den Risiken zählen **akute Bedrohungen wie Hackerangriffe, weltweite Virusattacken, unvorhersehbarer Datenverlust** oder der generelle Missbrauch von vertraulichen Informationen, die eine wichtige Geschäftsgrundlage bilden. Diese Szenarien können zu einer **ernsten Bedrohung für betriebliche IT-Prozesse** werden und schlimmstenfalls sogar den gesamten Geschäftsbetrieb lahmlegen. **ISO 27001 (Factsheet)**, der **international einzige Standard für Informationssicherheit**, trägt durch einen systematischen und strukturierten Ansatz dazu bei, diese Risiken gezielt zu erkennen und zu minimieren.

Der Standard erlaubt es **Unternehmen und Organisation jeglicher Größe und Branche** Informationssicherheit zu implementieren und laufend zu evaluieren.

Die Voraussetzung dafür ist ein **dokumentiertes und in der Organisation integriertes bzw. gelebtes Informationssicherheitsmanagementsystem**. Die ISO 27001 berücksichtigt verstärkt den Bereich des Risikomanagements. Auf Basis der Risikobewertung (auch Risikoanalyse genannt) kommt die "Anwendung der Sicherheitskontrollen" aus Anhang A (14 Abschnitte) der Norm zu Tragen, um jedes nicht annehmbare Risiko zu entschärfen.

Das Zertifikat (siehe **Musterzertifikat**) besitzt eine **Gültigkeitsdauer von drei Jahren** und darf entsprechend der **Zertifizierungsordnung** zu Werbezwecken verwendet werden. Das Zertifizierungslogo kann beispielsweise auf Briefpapier, der Website (jeweils in Zusammenhang mit der Organisation) verwendet werden. Die jeweils geplante Verwendung muss aus rechtlichen Gründen durch die Zertifizierungsstelle freigegeben bzw. bestätigt werden.

Ablauf ISO 27001-Zertifizierung.

Ein Zertifizierungsprozess dauert in der Regel zwischen drei und fünf Wochen. Den genauen Aufwand, sowie Dauer und Kosten legen wir mit Ihnen gemeinsam vor dem Zertifizierungsprozess fest.

1. Informationsgespräch

Bei einem unverbindlichen und kostenlosen Gespräch informieren wir Sie über die Vorgehensweise zur Erlangung Ihres Zertifikats. Weiters werden u.a. folgende Punkte geklärt:

- Grundsätzliche Voraussetzungen für eine Zertifizierung
- Ziele und Nutzen der Zertifizierung
- Abgleich der Unternehmensdaten und Festlegung des Geltungsbereichs

Vorteile.

- Durch eine Zertifizierung nach ISO 27001 **erhöhen** Sie die **Datensicherheit in Ihrem Unternehmen**. Der Standard trägt aktiv dazu bei, Ihre vertraulichen **Daten vor missbräuchlichen Zugriffen, Datenverlust oder Hackerangriffen zu schützen**. Ebenso ist die schnelle Wiederherstellung nach dieser Art von Angriffen gewährleistet.
- Das strukturierte und weltweit anerkannte Informationssicherheits-Managementsystem hilft dabei, **bevorstehende Bedrohungen rechtzeitig zu erkennen** und systematisch zu reduzieren.
- Mit ISO 27001 werden Sie **externen Anforderungen** (z.B. operationelle Risiken unter Basel II) gerecht. Das Informationssicherheits-Managementsystem berücksichtigt dabei die drei **IT-Schutzziele** von Informationen: **Vertraulichkeit, Verfügbarkeit und Integrität**.
- Durch eine Zertifizierung wird laufend die **betriebliche IST-Situation analysiert** und kann bei Bedarf jederzeit optimiert und an die **SOLL-Situation angepasst** werden. Dies führt zu einer kontinuierlichen Verbesserung der internen Abläufe.
- Der ganzheitliche Ansatz des Managementsystems sorgt dafür, dass die **Norm in der Praxis gelebt** und leicht in den Arbeitsalltag integriert werden kann. Die Verantwortung des Managements wird ebenso eingefordert wie regelmäßige Trainings und interne Audits.



5. Zertifizierungsaudit Stufe 2

Im Rahmen der Stufe 2 wird in Ihrem Unternehmen die Wirksamkeit des eingeführten Managementsystems überprüft. Dabei werden in Abteilungen bzw. Organisationseinheiten und entlang der Prozessketten Stichproben zu allen Anforderungen gezogen.

Grundlagen der Auditierung sind:

- Auditplanung
- die jeweilige Zertifizierungsnorm bzw. darin festgelegte einzelne Normforderungen
- organisationsspezifische Dokumente
- allgemeine und branchenspezifische Grundlagen (Gesetze, weiterführende, branchenspezifische, erforderliche Normierungen,...)

Nach Auswertung und Bewertung der Ergebnisse werden Ihnen im Rahmen des Abschlussgesprächs bereits das Auditergebnis sowie eventuelle Mängel bzw. Abweichungen mitgeteilt. Bei Abweichungen werden Korrekturmaßnahmen festgelegt.

ches der Zertifizierung

- Besprechung Ihrer spezifischen Anforderungen und Wünsche
- Festlegung der nächsten erforderlichen Schritte in Richtung Zertifizierung

Auf Basis dieses Informationsgesprächs erhalten Sie ein individuelles und auf Ihre Organisation maßgeschneidertes Angebot.

2. Beauftragung

Sind Sie mit dem gestellten Angebot zufrieden, wird die Zertifizierungsstelle beauftragt. Nachdem Sie eine Auftragsbestätigung erhalten haben, beginnt der Zertifizierungsprozess mit einer gemeinsamen terminlichen Abstimmung mit dem/der verantwortlichen Auditor_in.

3. Voraudit (optional)

Auf Wunsch kann ein Voraudit durchgeführt werden. Anhand eines gemeinsam definierten Rahmens werden entweder spezielle Bereiche bzw. Prozesse oder die Gesamtsituation Ihrer Organisation auditiert. Dabei werden etwaige Schwachstellen in der Dokumentation und der Implementierung des Systems aufgezeigt. Ein Voraudit kann Ihnen auf Wunsch einen Statusbericht in Bezug auf die grundsätzliche Zertifizierungsfähigkeit, eine Detailexpertise zu einzelnen Prozessen oder der Konformität zu einzelnen Forderungspunkten der jeweiligen Norm geben. Die Auditmethodik entspricht dabei jener des Zertifizierungsaudits.

4. Zertifizierungsaudit Stufe 1

Das Stufe-1-Audit dient zur Feststellung Ihrer Zertifizierungsfähigkeit. Standortspezifische Bedingungen werden beurteilt und notwendige Informationen bezüglich des Geltungsbereichs gesammelt. Folgende Hauptpunkte werden vorwiegend in der Auditstufe 1 behandelt:

- Prüfung der Dokumentation auf Konformität und Vollständigkeit im Abgleich mit den jeweiligen Normanforderungen.
- Status der Implementierung des Managementsystems im Unternehmen: Lässt das vorhandene Management sowie der Implementierungsgrad des Managementsystems in der Organisation grundsätzlich eine Zertifizierung zu oder fehlen noch entscheidende Details?

Vor Durchführung der Auditstufe 2 wird mit dem erlangten Wissen zu Ihrer Organisation und dem Managementsystem eine Auditplanung für das eigentliche Zertifizierungsaudit erstellt und mit Ihnen abgestimmt.

6. TÜV AUSTRIA-Zertifikat

Die tatsächliche Zertifizierung wird nach erfolgter erfolgreicher Auditierung und Berichtslegung auf Basis des Auditberichtes durch die Zertifizierungsstelle des TÜV AUSTRIA ausgesprochen. Das Zertifikat wird ausgestellt, sofern die folgenden Zertifizierungsvoraussetzungen erfüllt sind:

- Dokumentation und Implementierung des Managementsystems
- Zertifizierungsübereinkommen (Bestätigung des Zertifizierungsangebots, der Zertifizierungsordnung und der AGB)
- positiv absolviertes Audit und damit eine entsprechende Empfehlung Ihres Auditteams an die Zertifizierungsstelle

Ein Zertifikat wird für eine Laufzeit von drei Jahren ausgestellt. Um die Gültigkeit des Zertifikates über die gesamte Laufzeit aufrecht zu erhalten, ist die jährliche Durchführung bzw. der jeweils positive Abschluss eines Überwachungsaudits (12 Monate und 24 Monate nach Ausstellung des Zertifikates) erforderlich.

7. Überwachungsaudits

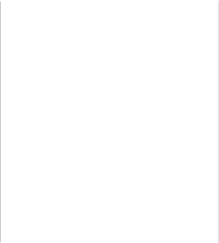
Beim jährlich durchzuführenden Überwachungsaudit werden die Wirksamkeit und die Weiterentwicklung des Managementsystems stichprobenartig überprüft. Überwachungsaudits sind in Bezug auf den Auditumfang kürzer und umfassen einerseits von Akkreditierern vorgegebene Themen, im Auditplan genannte Schwerpunkte und gehen auf die Mängel des letzten Audits ein.

8. Re-Zertifizierungsaudit

Dieses muss vor Ablauf der Gültigkeit des Zertifikats (i. d. Regel nach drei Jahren) durchgeführt werden. In einem Re-Zertifizierungsaudit (oft auch Wiederholungsaudits genannt) werden wie bei einem Zertifizierungsaudits alle Forderungspunkte stichprobenartig überprüft. Der Aufwand dieses wiederholenden Zertifizierungsverfahrens ist gegenüber einem Erstzertifizierungsverfahren verkürzt (ca. 2/3 der Auditzeit eines Erstzertifizierungsverfahrens).

Nach positiver Zertifizierungsentscheidung wird erneut ein Zertifikat mit einer Gültigkeit von drei Jahren ausgestellt.

Verwandte Beiträge aus derselben Branche: Zertifizierung



Personenzertifizierung:
zertifizierte/r
Qualitätstechniker/in

Zertifizierung

Automotive

Bildungsnachweis

Erstzertifizierung

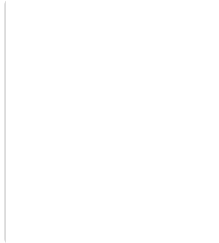
ISO 17024

Personenqualifikation

Personenzertifikat

mehr anzeigen

Zu My Bundle hinzufügen



Personenzertifizierung:
Energiebeauftragte/r EnMS

Zertifizierung

Bildungsnachweis

Energiemanagement

Erstzertifizierung

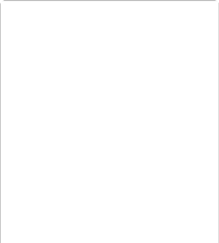
ISO 17024

Personenqualifikation

Personenzertifikat

mehr anzeigen

Zu My Bundle hinzufügen



Personenzertifizierung:
zertifizierte/r Safety
Specialist ISO 26262

Zertifizierung

Anlagensicherheit

Bildungsnachweis

Erstzertifizierung

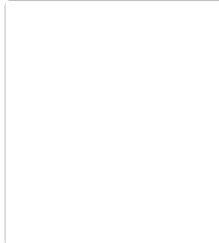
ISO 17024

Personenqualifikation

Personenzertifikat

mehr anzeigen

Zu My Bundle hinzufügen



Personenzertifizierung:
zertifizierte
Datenschutzbeauftragte

Zertifizierung

Bildungsnachweis

Compliance

Datenschutz

Erstzertifizierung

ISO 17024

IT

mehr anzeigen

Zu My Bundle hinzufügen

[Alle Lösungen](#)

Entdecken Sie weitere Branchen:

Automotive

Bau & Real Estate

Elektronik

Energie

Freizeit &
Unterhaltung

Gemeinden

Gesundheit &
Medizin**Alle Branchen anzeigen**

Beliebte Lösungen

ISO 9001 Zertifizierung
(Qualitätsmanagement)

Räder- und Reifen

Digitale Assistenzsysteme

Anlagenüberwachung

Dampfkessel

ISO 14001 (Umweltmanagement)

Interessante Neuigkeiten

TÜV AUSTRIA News

White Paper & Leading Innovation

#tüvaustria150

Häufig genutzte Branchen

Automotive

Freizeit & Unterhaltung

Gemeinden

Handel & Gewerbe

Maschinen

IT & Security

Transport & Verkehr

Zertifizierung



Service & Leistungen

Audit & Certification

Consulting

Testing & Inspection

Training

Über TÜV AUSTRIA

#TÜVAUSTRIA150

Über uns

Unsere Lösungen A-Z

Standorte

PV Anlage Wien

News

Karriere

Rechtliches

AGB

Datenschutzerklärung

Impressum

Presse

Kundencenter

Anfrage

Beschwerde/Einspruch

Login für Mitarbeiter*innen &
Kunden*innen

Dienstausweis-Überprüfung

Green Action

tami

Photovoltaik Park Technology &
Innovation Center

tami Mobile Installation &
Datenschutzerklärung

Follow us!



© 2022 | TÜV Austria | powered by