ZERTIFIZIERUNG NACH ISO 27001

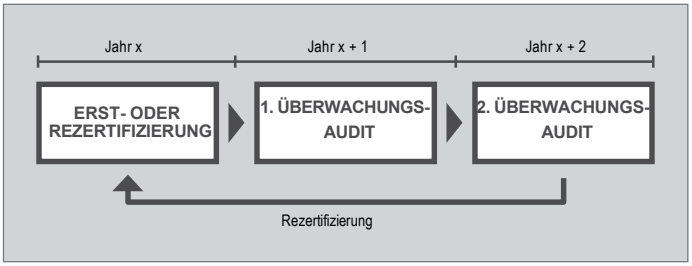
ALLGEMEIN

Eine Zertifizierung nach ISO 27001 erfolgt prinzipiell in 2 Schritten

- Prüfung der Managementdokumentation auf Übereinstimmung mit der Norm
- Umsetzungsprüfung der in der Dokumentation beschriebenen Prozesse
  Die Zertifizierung nach ISO 27001 ist ein fortlaufender Prozess und bedarf nach dem Zertifizierungsaudit einer regelmäßigen Bestätigung durch so genannte Überwachungs- bzw. Rezertifizierungsaudits.

Eine Zertifizierungsperiode umfasst 3 Jahre und beinhaltet jeweils ein Zertifizierungs- oder Rezertifizierungsaudit sowie 2 Überwachungsaudits.

Der folgende Abschnitt beschreibt den Ablauf des Zertifizierungsaudits sowie die weiteren Schritte zur Aufrechterhaltung der Zertifizierung.



ERSTZERTIFIZIERUNG

1 ANMELDUNG UND VORGESPRÄCH

Die Beauftragung der SGS-TÜV Saar GmbH zur Durchführung von Audits erfolgt grundsätzlich auf Basis des Zertifizierungsvertrags.

Bei Bedarf und nach positiver Prüfung durch die Zertifizierungsstelle, kann der Geltungsbereich der Zertifizierung und Auditierung auf einzelne organisatorische Einheiten des Unternehmens beschränkt werden. In diesen Fällen wird die organisatorische Einheit explizit im Zertifikat genannt.

Nach Eingang des Auftrags wird dieser in folgenden Punkten auf seine Durchführbarkeit geprüft

- Vollständigkeit der Angaben und Übereinstimmung mit den Angebotsdaten
- Durchführbarkeit (Standard/Wirtschaftsbranche (Geltungsbereich)/Termine)
  Falls erforderlich kann ein vorbereitender informeller Besuch des Auditleiters beim Kunden stattfinden.

2 AUDITVORBEREITUNG STUFE 1- UND 2 - AUDIT

2.1 Personelle Besetzung

SGS-TÜV Saar GmbH bestimmt zunächst den Auditleiter und – sofern erforderlich – die weiteren Mitglieder des Auditteams. Dabei wird sichergestellt, dass die allgemeinen Qualifikationskriterien für Auditoren erfüllt sind. Die Mitglieder des Auditteams werden dem Kunden rechtzeitig vor Auditbeginn bekannt gegeben.

2.2 Auditplan

Der Auditleiter erarbeitet in Abstimmung mit dem Kunden einen schriftlichen Auditplan für die Durchführung des Audits und stellt diesen dem Unternehmen ca. 2 Wochen vor dem geplanten Audittermin zur Verfügung.

Der Auditplan enthält u. a. folgende Informationen

- Datum und Uhrzeit des Audits
- Name des Auditleiters/Auditors
- Zu auditierender Standard
- Auditsprache
- Auditort
- Zu auditierende(r) Abteilung/ Funktion/ Prozess

2.3 Grundlegende Dokumente

Zur Vorbereitung und fristgerechten Durchführung des Zertifizierungsaudits sind von dem Kunden spätestens 6 Wochen vor dem geplanten Audittermin an den durch die Zertifizierungsstelle mitgeteilten Auditleiter einige grundlegende Dokumente (siehe Zertifizierungsvertrag) elektronisch zu übermitteln.

3 STUFE 1 - AUDIT

Vor dem Erst – und Re-Zertifizierungsaudit ist obligatorisch ein Stufe 1- Audit durchzuführen. Dieses findet in der Regel 4 bis 6 Wochen vor dem Zertifizierungsaudit beim Kunden vor Ort statt. Das (Re-)Zertifizierungsaudit muss spätestens 6 Monate nach dem Stufe 1- Audit durchgeführt werden. Dabei wird auf Basis ISO 27001 stichprobenartig die Umsetzung des jeweiligen Standards im Managementsystem geprüft. Ein Schwerpunkt liegt dabei auf der Prüfung der Managementsystemdokumentation des Unternehmens hinsichtlich Vollständigkeit und Übereinstimmung mit dem entsprechenden Standard sowie der Fähigkeit die bindenden Verpflichtungen umzusetzen. Des Weiteren wird die Durchführung und Dokumentation der internen Audits sowie die Managementbewertung geprüft. Darüber hinaus dient das Stufe 1-Audit als Vorbereitung auf das (Re-) Zertifizierungsaudit hinsichtlich der Überprüfung des Aufwands und der Planung des Auditablaufs.

Im Anschluss an das Stufe 1-Audit erstellt der Auditor einen Bericht. Werden Feststellung getroffen, welche im Stufe 2 Audit zu Abweichungen führen können, werden diese in den Bericht aufgenommen und bei der Bereitschaftsbewertung berücksichtigt . Alle potentielle Abweichungen müssen bis zum Beginn des Stufe 2 Zertifizierungsaudits behoben sein. Es kann nur ein Stufe 1-Audit absolviert werden.

4 DURCHFÜHRUNG DES ZERTIFIZIERUNGSAUDITS (STUFE 2 - AUDIT)

4.1 Eröffnungsgespräch

Zu Beginn des Audits findet mit der Unternehmensleitung sowie sonstigen, durch den Kunden bestimmte Mitarbeiter, ein Eröffnungsgespräch statt. In dem Gespräch wird noch einmal der genaue Ablauf des Audits besprochen. Ggf. werden in Abstimmung mit dem Kunden noch Änderungen im Auditplan vorgenommen.

4.2 Auditdurchführung

Im Audit wird die Wirksamkeit des eingeführten und nachgewiesenen Managementsystems geprüft. Diese Prüfung schließt die Einsicht in die Managementdokumentation sowie entsprechende Nachweisunterlagen und die Befragung von Mitarbeitern ein.

Werden Abweichungen von der Normforderung festgestellt, so sind folgende Einstufungen möglich

- Hinweis: die Forderungen der Norm werden zwar erfüllt, dennoch gibt es Möglichkeiten der Verbesserung
- Minor Abweichung: die wesentlichen Anforderungen des Standards sind erfüllt, aber durch Einzelfehler ist die Wirksamkeit von Teilen des Managementsystems beeinträchtigt.
- Major Abweichung: Anforderungen an das Managementsystem sind unzureichend geregelt und / oder die vorhandenen Regelungen werden nicht oder unzureichend praktiziert. Dies kann zum Versagen des Managementsystems oder von von Prozessen führen.

4.3 Abschlussgespräch

Nach Beendigung des Audits fasst der Auditleiter die Ergebnisse kurz zusammen und teilt diese dem Kunden mit. Liegen Abweichungen vor, werden diese dem Kunden vom Auditleiter explizit dargestellt.

5 AUDITNACHBEREITUNG / BERICHT

5.1 Auditbericht

Im Anschluss an das Audit wird vom Auditleiter ein schriftlicher Auditbericht erstellt und eine Empfehlung für die Zertifizierungsentscheidung ausgesprochen. Festgestellte Abweichungen werden dokumentiert und sind Bestandteil des Auditberichts.

5.2 Minor Abweichungen

Bei Minor Abweichungen wird zwischen dem Auditleiter und dem Kunden ein Maßnahmenplan vereinbart. Dieser muss vor Ausstellung des Zertifikats vom Auditor akzeptiert worden sein.

5.3 Major Abweichungen

Major Abweichungen machen in der Regel ein Follow-Up Audit nach dem Zertifizierungsaudit notwendig. Alle Korrekturmaßnahmen müssen vor dem Follow-Up Audit erfolgreich vom Kunden umgesetzt worden sein. Auch ohne Follow-Up Audit vor Ort müssen die Major Abweichungen vor einer positiven Zertifizierungsentscheidung anhand vorgelegter Dokumente nachweislich geschlossen sein.

6 ZERTIFIKAT

Für die Zertifikatserteilung ist eine positive Zertifizierungsentscheidung durch die Zertifizierungsstelle der SGS-TÜV Saar GmbH notwendig. Voraussetzung hierfür ist die komplett vorliegende Auditdokumentation, einschl. der Dokumentation zu den ggf. vorhandenen Abweichungen. Vorbehaltlich der Bestätigung durch die jährlichen Überwachungsaudits hat das Zertifikat – gerechnet vom Datum der Zertifizierungsentscheidung – eine Laufzeit von 3 Jahren. Bei einer erfolgreichen Rezertifizierung wird das Zertifikat auf 3 Jahre verlängert. Im Zertifikat ist die juristische Person mit Anschrift, der Standard und der Geltungsbereich ausgewiesen. Sofern weitere Standorte im Geltungsbereich der Zertifizierung erfasst sind, können Unterzertifikate für einzelne Standorte ausgestellt werden.

Es erfolgt eine Registrierung des Zertifikats im Verzeichnis der durch SGS-TÜV Saar GmbH zertifizierten Unternehmen.

ÜBERWACHUNGSAUDITS

Zur Aufrechterhaltung der Gültigkeit des Zertifikats müssen mindestens jährlich Überwachungsaudits durchgeführt werden.

Im Rahmen des Überwachungsaudits werden primär die Korrekturmaßnahmen der im letzten Audit festgestellten Abweichungen sowie Änderungen im Managementsystem und deren Anwendung überprüft.

Die Überwachungsaudits müssen 12 bzw. 24 Monate nach dem letzten Tag des Zertifizierungs-/ Rezertifizierungsaudits vor Ort abgeschlossen sein. Der Audittermin wird zwischen dem Kunden und der SGS-TÜV Saar GmbH vereinbart.

Werden die Termine nicht eingehalten, so muss die Gültigkeit des Zertifikats ausgesetzt werden.

Der Ablauf erfolgt analog zum Zertifizierungsaudit. Bei Minor Abweichungen muss der Maßnahmenplan spätestens nach 90 Tagen an die SGS-TÜV Saar GmbH kommuniziert werden. Major Abweichungen müssen ebenfalls nach 90 Tagen geschlossen sein. In diesen Fällen wird sonst die Gültigkeit des Zertifikats ausgesetzt.

REZERTIFIZIERUNG

Das Rezertifizierungsaudit soll spätestens 60 Tage vor Ablauf der Zertifikatsgültigkeit durchgeführt werden.

Rezertifizierungsaudits sind so zu planen, dass ausreichend Zeit für die Überprüfung und den Abschluss von Nichtkonformitäten zur Verfügung steht. Wenn dieser Zeitrahmen nicht eingehalten werden kann, z.B. aufgrund von Einschränkungen seitens des Kunden, wird der Kunde über die potentiellen Risiken informiert, z.B. über den Ablauf des Zertifikats vor dem Abschluss der Abweichung.

Der Umfang des Rezertifizierungsaudits wird aufgrund der Ergebnisse der durchgeführten Überwachungsaudits festgelegt. Im Rahmen des Rezertifizierungsaudits werden hauptsächlich die seit dem letzten Audit durchführten Korrekturmaßnahmen geprüft. Außerdem werden neue, bzw. veränderte Verfahren und ihre Umsetzung stichprobenweise untersucht.

Der Ablauf erfolgt analog zum Zertifizierungsaudit.

ÜBERNAHMEAUDITS

Gültige akkreditierte Zertifikate können im Rahmen von Überwachungs- oder Rezertifizierungsaudits übernommen werden. Alle anderen Zertifikate werden wie Neukunden behandelt.

Grundsätzlich muss vor der Umschreibung des Zertifikates auf die SGS-TÜV Saar GmbH ein Audit vor Ort stattgefunden haben.

Im Rahmen dieses Audits wird mindestens geprüft, ob das bisherige Zertifikat noch Gültigkeit hat. Hierzu werden durch den Auditor alle Berichte der bisherigen Zertifizierungsstelle und Behörden; der Schriftverkehr bzgl. Beschwerden und zur Abarbeitung von Abweichungen eingesehen und bewertet.