

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



Inhaltsverzeichnis

1	ZERTIFIZIERUNGSVERFAHREN	2
1.1	Auditvorbereitung	2
1.2	Audit Stufe 1.....	2
1.3	Audit Stufe 2 – Zertifizierungsaudit	3
1.4	Zertifikaterteilung	3
2	ÜBERWACHUNGSAUDIT	4
3	REZERTIFIZIERUNGSAUDIT.....	4
4	ERWEITERUNGSAUDIT.....	4
4.1	Kurzfristig angekündigte Audits	4
4.2	Umstellungsaudits	5
5	ÜBERNAHME VON ZERTIFIZIERUNGEN ANDERER ZERTIFIZIERUNGSSTELLEN.....	5
6	ZERTIFIZIERUNG VON UNTERNEHMEN MIT MEHREREN STANDORTEN	5
7	MANAGEMENT VON NICHTKONFORMITÄTEN	6
8	SEKTORSPEZIFISCHE STANDARDS IN ERGÄNZUNG ZUR ISO/IEC 27001.....	6

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Sie erreichen uns per Mail info.tncert@tuev-nord.de oder persönlich von Montag bis Freitag zwischen 07:30 Uhr und 18:00 Uhr unter 0800 – 2457457.

TÜV NORD CERT GmbH
Am TÜV 1
45307 Essen

www.tuev-nord-cert.de

Dieses Dokument wurde gemäß CERT-401-VA-007 freigegeben. Details zur Freigabe sind von der QM-Stelle verfügbar.

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



Das Zertifizierungsverfahren des Managementsystems auf Basis der Norm ISO/IEC 27001, ISO 22301 oder ISO/IEC 20000-1 besteht aus der Angebots- und Vertragsphase, der Auditvorbereitung, der Durchführung des Audits Stufe 1 mit Bewertung der Management-Dokumentation, der Durchführung des Audits Stufe 2, der Zertifikatserteilung und der Überwachung/Re-Zertifizierung.

Die Auditoren und Fachexperten werden vom Leiter der Zertifizierungsstelle der TÜV NORD CERT GmbH entsprechend der Zulassung für die Branche und Qualifikation ausgewählt.

1 ZERTIFIZIERUNGSVERFAHREN

Das Zertifizierungsaudit besteht aus dem Audit der Stufe 1 und dem Audit der Stufe 2. Beide Audits werden grundsätzlich vor Ort beim Auftraggeber durchgeführt.

Bei Zertifizierungen nach ISO/IEC 27001 können ergänzend nationale oder internationale Standards (z.B. ISO/IEC 27017 oder ISO/IEC 27018) berücksichtigt werden, die als Quelle zusätzlicher Maßnahmen („Controls“) in der Erklärung zur Anwendbarkeit („SoA: Statement of Applicability“) des zu zertifizierenden Kunden aufgeführt sind (siehe hierzu Abschnitt „Sektorspezifische Standards in Ergänzung zur ISO/IEC 27001“).

1.1 Auditvorbereitung

Nach Vertragsabschluss bereitet sich der Auditor an Hand des Interessentenfragebogens und des Kalkulationsblattes auf das Audit vor und stimmt sich mit dem Unternehmen über die weitere Vorgehensweise ab.

Sollten beim Unternehmen vertrauliche oder sensitive Dokumente/Aufzeichnungen vorhanden sein, die den Auditoren nicht zugänglich gemacht werden können, so ist die Zertifizierungsstelle vorher darüber zu unterrichten. Die Zertifizierungsstelle beurteilt vor dem Audit, ob ohne Einsicht in diese Dokumente/Aufzeichnungen ein adäquates Audit durchgeführt werden kann.

Im Rahmen der Vorbereitung auf die Überwachungs- bzw. Re-Zertifizierungsaudits sind die Unternehmen verpflichtet, der Zertifizierungsstelle wesentliche Änderungen in der Aufbau- und Ablauforganisation ihres Unternehmens mitzuteilen.

1.2 Audit Stufe 1

Das Audit der Stufe 1 wird durchgeführt, um

- die Managementsystem-Dokumentation des Kunden zu auditieren,
- den Standort und die standortspezifischen Bedingungen des Kunden zu beurteilen sowie Diskussionen mit dem Personal der Organisation des Kunden zu führen, um die Bereitschaft für das Audit Stufe 2 zu ermitteln,
- den Status des Kunden sowie das Verständnis bezüglich der Anforderungen der Norm, insbesondere im Hinblick auf die Identifizierung von Schlüsselleistungen bzw. bedeutsamen Aspekten, Prozessen, Zielen und das Betreiben des Managementsystems zu bewerten,
- notwendige Informationen bezüglich des Anwendungsbereichs des Managementsystems, der Prozesse und des/der Standorts(e) des Kunden, der Anzahl der im Anwendungsbereich tätigen Personen, bindender Verpflichtungen sowie Aspekte zur Informationssicherheit zu sammeln,
- die Zuteilung der Ressourcen für Audits der Stufe 2 zu bewerten sowie die Einzelheiten der Audits der Stufe 2 mit dem Kunden abzustimmen,

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



- einen Schwerpunkt für die Planung des Audits der Stufe 2 zu schaffen, indem ausreichendes Verständnis des Managementsystems des Kunden sowie zu den Standorttätigkeiten zusammen mit möglichen signifikanten Aspekten erlangt wird,
- zu beurteilen, ob die internen Audits und Managementbewertungen geplant und durchgeführt werden und dass der Grad der Umsetzung des Managementsystems belegt und der Kunde für das Audit der Stufe 2 bereit ist.

Falls im Audit Stufe 1 Schwachstellen festgestellt wurden, sind diese vom Kunden bis zum Audit Stufe 2 zu beheben.

Kann abschließend nicht positiv festgestellt werden, dass der Kunde für das Audit der Stufe 2 bereit ist, erfolgt der Abbruch des Zertifizierungsverfahrens nach dem Audit Stufe 1.

Für die Koordinierung der Tätigkeiten des Audits Stufe 1 und ggf. die Abstimmung der beteiligten Auditoren untereinander ist der leitende Auditor verantwortlich.

1.3 Audit Stufe 2 – Zertifizierungsaudit

Mit Beginn des Audits Stufe 2 erhält der Kunde einen mit ihm abgestimmten Auditplan.

Das Audit beginnt mit einem Einführungsgespräch, in dem sich die Teilnehmer vorstellen. Das Vorgehen im Audit wird erläutert. Im Rahmen des Audits im Unternehmen überprüfen und bewerten die Auditoren die Wirksamkeit des eingeführten Managementsystems. Grundlage ist die ISO/IEC 27001, ISO 22301 oder ISO/IEC 20000-1.

Aufgabe der Auditoren ist es, die praktische Anwendung des Managementsystems mit den dokumentierten Verfahren zu überprüfen und auf Erfüllung der Normforderungen hin zu bewerten. Dies erfolgt durch Befragung der Mitarbeiter, Einsichtnahme in mitgeltende Dokumente, Aufzeichnungen, Aufträge, Richtlinien sowie durch Begehung relevanter Bereiche.

Zum Abschluss des Vor-Ort-Audits findet ein Schlussgespräch statt. An diesem Gespräch nehmen mindestens die Mitarbeiter teil, die leitende Funktionen im Unternehmen haben und deren Bereiche in das Audit eingebunden waren. Der leitende Auditor berichtet über die einzelnen Elemente, erläutert positive und negative Ergebnisse. Im Fall von festgestellten Nichtkonformitäten kann der leitende Auditor das Unternehmen erst nach Annahme bzw. Verifizierung der Korrekturmaßnahmen durch das Audit-Team zur Zertifikaterteilung empfehlen, siehe hierzu Abschnitt „Management von Nichtkonformitäten“. Auf diesen Sachverhalt ist im Abschlussgespräch hinzuweisen.

Die Dokumentation erfolgt im Auditbericht (separat für das Audit Stufe 1 und Audit Stufe 2) und wird durch weitere Aufzeichnungen (z. B.: Auditfrageliste und handschriftliche Aufzeichnungen) ergänzt, die in der Regel nur für interne Zwecke der Zertifizierungsstelle verfügbar sind.

1.4 Zertifikaterteilung

Die Erteilung des Zertifikates erfolgt mit der positiven Prüfung des Zertifizierungsverfahrens durch den Leiter der Zertifizierungsstelle bzw. durch seinen Stellvertreter oder benannte Personen. Der Prüfende darf nicht an der Auditierung beteiligt gewesen sein.

Das Zertifikat kann nur dann erteilt werden, wenn alle Nichtkonformitäten behoben sind, d. h. wenn die Korrekturmaßnahmen vom Audit-Team angenommen bzw. verifiziert sind.

Die Zertifikate haben grundsätzlich eine Gültigkeit von 3 Jahren.

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



2 ÜBERWACHUNGSAUDIT

Innerhalb der Gültigkeit des Zertifikates sind Überwachungsaudits jährlich durchzuführen mit Ausnahme der Jahre, in denen ein Re-Zertifizierungsaudit erfolgt.

Das erste Überwachungsaudit, das der Erstzertifizierung folgt, ist bis zum einplanungsrelevanten Datum, spätestens 12 Monate nach dem Datum der Zertifizierungsentscheidung, durchzuführen. Sämtliche folgenden Überwachungsaudits werden auf der Basis des einplanungsrelevanten Datums eingeplant und müssen mindestens einmal je Kalenderjahr durchgeführt werden.

Jedes Überwachungsaudit einschließlich der Prüfung, Annahme und ggf. Verifizierung von Maßnahmen zur Korrektur von Nichtkonformitäten, der Erstellung des Auditberichts und der Freigabe durch die Zertifizierungsstelle ist spätestens 3 bzw. 4 Monate (bei Feststellung von Nichtkonformitäten) nach dem letzten Tag vor Ort abzuschließen.

Nach dem Überwachungsaudit erhält der Auftraggeber einen Bericht.

3 REZERTIFIZIERUNGSAUDIT

Das Audit zur Re-Zertifizierung muss vor dem Ablauftermin des Zertifikates durchgeführt werden. Für die Bewertung der Korrekturmaßnahmen und eventueller Nachaudits sowie für die Entscheidung zur Re-Zertifizierung im Rahmen des Freigabeverfahrens steht dann noch eine Toleranzzeit von max. 6 Monaten zur Verfügung. Im Re-Zertifizierungsaudit findet eine Überprüfung der Dokumentation des Managementsystems des Unternehmens sowie ein Audit vor Ort statt, wobei die Ergebnisse des/der vorangegangenen Überwachungsprogramms(e) über die Laufzeit der Zertifizierung zu berücksichtigen sind. Es werden alle Normanforderungen auditiert.

Tätigkeiten zu Re-Zertifizierungsaudits können ein Audit der Stufe 1 erfordern, wenn es signifikante Änderungen im Managementsystem oder im Zusammenhang mit den Tätigkeiten des Unternehmens gibt (z. B.: Gesetzesänderungen).

Die Audit-Methodik im Re-Zertifizierungsaudit entspricht der eines Audits Stufe 2.

4 ERWEITERUNGSAUDIT

Soll der Geltungsbereich des bestehenden Zertifikates erweitert werden, so kann das durch ein Erweiterungsaudit geschehen. Die Durchführung des Erweiterungsaudits kann im Rahmen eines Überwachungsaudits, Re-Zertifizierungsaudits oder zu einem eigens angesetzten Termin erfolgen.

Die Gültigkeitsdauer eines Zertifikates ändert sich dadurch nicht. Ausnahmen sind schriftlich zu begründen.

4.1 Kurzfristig angekündigte Audits

Es kann erforderlich sein, kurzfristig angekündigte Audits durchzuführen, um Beschwerden zu untersuchen, als Konsequenz von Änderungen oder als Konsequenz auf ausgesetzte Zertifizierungen. In solchen Fällen:

- legt die Zertifizierungsstelle die Bedingungen, unter denen diese kurzfristigen Begehungen durchgeführt werden, fest;
- besteht nicht die Möglichkeit, gegen Mitglieder des Auditteams Einwand zu erheben.

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



4.2 Umstellungsaudits

Als Folge der Änderungen eines Standards für Managementsysteme kann es zur Aufrechterhaltung der Zertifizierung erforderlich werden, entsprechende Umstellungsaudits durchzuführen. Nach einer erfolgreichen Umstellung werden dann Zertifikate für die neuen Standards ausgestellt, ohne dass sich das Ablaufdatum der bestehenden Zertifizierungen ändert.

Sollten solche Umstellungen nötig werden, dann informiert die Zertifizierungsstelle rechtzeitig über die notwendigen vorgeschriebenen Maßnahmen.

5 ÜBERNAHME VON ZERTIFIZIERUNGEN ANDERER ZERTIFIZIERUNGSSTELLEN

Generell können nur Zertifikate von akkreditierten Zertifizierungsstellen, wobei der Akkreditierer Unterzeichner der Multilateralen Agreements (MLA) von EA (European co-operation for Accreditation) ist, übernommen werden. Unternehmen mit Zertifikaten, die von nicht akkreditierten Zertifizierungsstellen ausgestellt wurden, sind als Neukunde zu behandeln.

Die ausstellende Zertifizierungsstelle wird über den geplanten Transfer informiert. Sobald von der ausstellenden Zertifizierungsstelle und dem Kunden keine Gründe bekannt sind, die einen Transfer des gültigen Zertifikats nach IAF MD 2:2017 ausschließen, kann der Transfer durchgeführt werden.

Es ist ein „Pre-Transfer-Review“ durch eine kompetente Person der übernehmenden Zertifizierungsstelle durchzuführen, das aus der Durchsicht wichtiger Dokumente oder gegebenenfalls einem Besuch beim Kunden besteht.

Nach dem positiven Abschluss des Pre-Transfer Reviews kann TÜV NORD CERT als anerkennende Zertifizierungsstelle die Übertragung der Zertifizierung vornehmen.

Der normale Zertifizierungsentscheidungsprozess ist einzuhalten. Dabei dürfen die Zertifizierungsentscheidungen nicht von denselben Personen getroffen werden, die das Pre-Transfer Review durchführen.

TÜV NORD CERT als anerkennende Zertifizierungsstelle führt eine Zertifizierungsentscheidung durch, bevor Überwachungs- oder Re-Zertifizierungsaudits geplant werden.

Der Zertifizierungszyklus des übertragenen Zertifikates basiert auf dem vorherigen. TÜV NORD CERT erstellt das Auditprogramm für den Rest des Zertifizierungszyklus.

Werden beim Pre-Transfer Review Probleme festgestellt, die den Abschluss der Übertragung verhindern, behandelt die anerkennende Zertifizierungsstelle den zu übertragenden Kunden wie einen neuen Kunden.

Ausgesetzte Zertifikate oder solche, bei denen die Gefahr einer Aussetzung besteht, dürfen nicht übernommen werden.

Die ausstellende Zertifizierungsstelle wird informiert, sobald das Zertifikat erfolgreich transferiert ist.

6 ZERTIFIZIERUNG VON UNTERNEHMEN MIT MEHREREN STANDORTEN

Bei Organisationen mit mehreren Standorten kann das Stichprobenverfahren („Multisite-Zertifizierung“) angewandt werden. In diesem Fall versichert der Auftraggeber, dass die nachfolgend genannten Voraussetzungen für alle Standorte im Geltungsbereich des Zertifikates erfüllt sind. Änderungen bzw. die Nichterfüllung einer oder mehrerer Voraussetzungen sind der Zertifizierungsstelle umgehend mitzuteilen.

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



Voraussetzungen für die Multisite-Zertifizierung:

- Eine Organisation mit mehreren Standorten braucht keine einzelne juristische Person zu sein, allerdings müssen alle Standorte eine rechtliche oder vertragliche Verbindung mit der Zentrale der Organisation haben und einem gemeinsamen Managementsystem unterliegen, das durch die Zentrale festgelegt und eingerichtet wird und regelmäßiger Überwachung sowie internen Audits durch die Zentrale unterliegt. Dies bedeutet, dass die Zentrale das Recht besitzt, von den Standorten zu fordern, Korrekturmaßnahmen umzusetzen, wenn diese an einem Standort erforderlich sind.
- Die Prozesse müssen an allen Standorten im Wesentlichen gleichartig sein und mit ähnlichen Methoden und Verfahren durchgeführt werden.
- Das Managementsystem der Organisation muss unter einem zentral kontrollierten Plan zentral verwaltet werden und einer zentralen Managementbewertung unterliegen. Alle zugehörigen Standorte (einschließlich der zentralen Verwaltungsfunktion) müssen dem internen Auditprogramm der Organisation unterliegen und in Übereinstimmung mit diesem Programm auditiert werden.
- Es muss nachgewiesen werden, dass die Zentrale der Organisation ein Managementsystem in Übereinstimmung mit der maßgeblichen Managementsystem-Norm, der das Audit unterliegt, eingerichtet hat und dass die gesamte Organisation die Anforderungen der Norm erfüllt.
- Die Organisation muss ihre Fähigkeit, Daten von allen Standorten einschließlich der zentralen Verwaltungsfunktion und deren Führung zu sammeln und zu analysieren, nachweisen und erforderliche organisatorische Veränderungen veranlassen:
 - Managementbewertung,
 - Beschwerden,
 - Bewertung der Korrekturmaßnahmen,
 - Planung interne Audits und Bewertung der Ergebnisse,
 - rechtliche Anforderungen.
- Der Abschluss einer Vereinbarung zwischen Auftraggeber und Zertifizierungsstelle, die an allen Niederlassungen/Produktionsstätten rechtlich durchsetzbar ist.

7 MANAGEMENT VON NICHTKONFORMITÄTEN

Für jede Nichtkonformität ist vom Unternehmen eine Ursachenanalyse durchzuführen und entsprechende Korrekturmaßnahmen sind zu implementieren. Das Unternehmen hat die Pflicht in Abhängigkeit der Schwere der Nichtkonformität, das Audit-Team innerhalb von 6 Wochen nach dem letzten Tag des Audits entweder über die festgelegten Korrekturmaßnahmen und Zieltermine oder über die Umsetzung der Korrekturmaßnahmen zu unterrichten. Wird diese Frist nicht eingehalten, gilt das Audit als nicht bestanden. Es kann kein Zertifikat erteilt werden bzw. das Zertifikat wird zurückgezogen.

8 SEKTORSPEZIFISCHE STANDARDS IN ERGÄNZUNG ZUR ISO/IEC 27001

TÜV NORD CERT kann zurzeit Audits und Zertifizierungen nach ISO/IEC 27001 anbieten, die folgende nationale bzw. internationale Standards als zusätzliche Quelle von Maßnahmen („Controls“) nutzen.

Beschreibung des Zertifizierungsverfahrens

MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1



Region	Standard	Inhalt
International	ISO/IEC 27017	Informationssicherheitsmaßnahmen für Cloud-Dienste
International	ISO/IEC 27018	Personenbezogene Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung
International	ISO/IEC 27019	Informationssicherheitsmaßnahmen für die Energieversorgung
Deutschland	BSI TR 01201	De-Mail
Deutschland	BSI TR 3109-6	Smart Meter Gateway Administration

Die zutreffenden Maßnahmen („Controls“) aus diesen Standards müssen in der Erklärung zur Anwendbarkeit aufgeführt sein und in den Audits angemessen berücksichtigt werden. Der Verweis auf diese Standards im Zertifikat für ISO 27001 zeigt nicht an, dass es sich um eine Zertifizierung nach diesen Standards handelt. Gesonderte Zertifikate, Zertifikatsergänzungen oder sonstige Bescheinigungen dürfen dafür nicht ausgestellt werden.