Zertifizierungsbeschreibung BCMS, ISMS, SMS

BCM – Business Continuity Management Systems; ISO 22301
ISMS – Information Security Management System; ISO 27001
SMS –Service Management System; ISO 20000-1

TÜV NORD CERT Sektor-Spezifische-Standards (3S)

Das Zertifizierungsverfahren des Managementsystems (BCMS, ISMS, SMS) 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/Rezertifizierung.

Das Zertifizierungsverfahren des Managementsystems (BCMS, ISMS, SMS) kann bei Bedarf um das Assessment „Sektor-Spezifische-Standards“ (3S) ergänzt werden. Alle unsere „Sektor-Spezifischen-Standards“ (3S) beanspruche ISO 27009 Konformität.

Es sind z.B. aus der ISO 27000 Familie:

- ISO27010 Information security management for inter-sector and inter-organizational communications
- ISO27011Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO27015 Information security management guidelines for financial services
- ISO27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO27799 Information security management in health using ISO/IEC 27000

Oder das Messstellenbetriebsgesetz (MStBG):

- TR03109 Smart Meter Gateway Administration

Bestimmte „Sektor-Spezifische-Standards“ (3S) verfügen bei der TN CERT über eine eigene Akkreditierung oder sind in einem Akkreditierungsverfahren, wie z.B.

- BNetzA § 11 Abs.1aEnWG / Spezifische Anforderungen an die Betreiber von Energienetzen oder
- IEC 62443-2-1 – Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme – Requirements for an IACS security management system
- IEC 62443-2-4 – Informationssicherheit/Cyber-Security für industrielle - Automatisierungssysteme – Requirements for IACS solution suppliers.
- IEC 62443-3-2 – Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme – Security risk assessment and system design

Auch gibt es TÜV NORD CERT individuelle „Sektor-Spezifische-Standards“ (3S), die die spezielle Situation „kritischer Infrastrukturen“ bedienen, wie z.B.:

- TN CERT Sektor-Spezifischer-Standard (3S) Energie
- TN CERT Sektor-Spezifischer-Standard (3S) Wasser
- TN CERT Sektor-Spezifischer-Standard (3S) Ernährung
- TN CERT Sektor-Spezifischer-Standard (3S) Informationstechnik und Telekommunikation
- TN CERT Sektor-Spezifischer-Standard (3S) Gesundheit
- TN CERT Sektor-Spezifischer-Standard (3S) Finanz- und Versicherungswesen
- TN CERT Sektor-Spezifischer-Standard (3S) Transport und Verkehr
- TN CERT Sektor-Spezifischer-Standard (3S) Staat und Verwaltung
- TN CERT Sektor-Spezifischer-Standard (3S) Medien und Kultur

Diese TÜV NORD CERT individuellen „Sektor-Spezifische-Standards“ (3S) haben den Anspruch n gesetzlichen Anforderungen zu genügen, wie z.B. den Anforderungen des deutschen Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) - § 8a ff. - zu genügen. Bei Bedarf werden entsprechende Zusatzerklärungen zur Verfügung gestellt.

Die Liste der „Sektor-Spezifischen-Standards“ (3S) wird permanent aktualisiert. Auf Nachfrage können zusätzliche „Sektor-Spezifischen-Standards“ (3S) zur Verfügung gestellt werden.

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

1 Zertifizierungsverfahren

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 bei dem Unternehmen besondere Umstände vorhanden sein, welche darüber hinausgehende Absicherungen bzgl. der Vertraulichkeit erfordern, so kann eine zusätzliche Vertraulichkeitsvereinbarung geschlossen werden.
Sollten beim Auftraggeber 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. Rezertifizierungsaudits ist das Unternehmen verpflichtet, der Zertifizierungsstelle wesentliche Änderungen in der Aufbau- und Ablauforganisation ihres Unternehmens mitzuteilen

1.2 Stufe 1 Audit

Das Audit der Stufe 1 wird durchgeführt, um

- einen Überblick und ein Review der Managementsystem-Dokumentation gemäß den Anforderungen des Standards zu erhalten,
- die Planung für das Stufe 2 Audit zu ermöglichen,
- den Status der Organisation bezüglich der Erfüllung der Anforderungen für das Stufe 2 Audit basierend auf das Managementsystem und dessen Leitlinien und –Ziele.

Das Unternehmen trifft alle erforderlichen Arrangements, um das Audit zu ermöglichen, einschließlich der Bereitstellung der Dokumente zu Dokumentenbewertung, dem Zugang zu allen Bereichen, Aufzeichnungen (einschließlich der Internen Audits und Berichte zum Managementreview), des Personal zur Begleitung der Zertifizierungs-, Überwachungs- und Re-Zertifizierungsaudits und der Beseitigung von Schwachstelen. Das Unternehmen stellt alle aktuellen Dokumente 4 Wochen vor dem Audit zur Verfügung.

Das Stufe 1 Audit beinhaltet u. a. eine Dokumentenbewertung. Die Zertifizierungstelle stellt aufgrund der Unternehmensangaben fest, wo das Stufe 1 Audit stattfinden wird.

Die bestehende Managementdokumentation wird bewertet und besteht u. a. aus:

BCM – ISO22301	ISMS – ISO 27001	SMS – ISO 20000-1
BCM Leitlinie und -Ziele	ISMS-Leitlinie und -Ziele	SMS-Leitlinie und -Ziele
Geltungsbereich des BCM	Geltungsbereich des ISMS	Geltungsbereich des SMS
Verfahren und Dokumente des BCMS	Verfahren und Maßnahmen, des des ISMS	Service Management Plan
• Business Impact Analyse • Risikoberwertung	Erklärung zur Anwendbarkeit	Dokumentierte Service Level Agreements
Business continuity Strategie	Dokumentierte Verfahren	Dokumentierte Prozesse und Verfahren
• Incident response Struktur • Business continuity Pläne/ Incident Management tPläne • Aufzeichnungen über BCMÜbungen	Risiko Management mit o Methode für die Risikoeinschätzung o Bericht der Risikoeinschätzung o Risikobehandlungsplan	Aufzeichnungen, gefordert vom Standard

Im Falle von „Sektor-Spezifischen-Standards“ (3S) soll der Klient vor dem Audit Stufe 1 eine standard-spezifische Checkliste ausfüllen. Die Grundform der Checkliste wird dem Klienten vorher zur Verfügung gestellt.

Die Organisation erhält einen Bericht über die Ergebnisse des Stufe 1 Audits einschließlich der Bewertung der Managementdokumentation und der damit vorhandenen Möglichkeit eventuelle Nichtkonformitäten bis zum Stufe 2 Audit zu beseitigen. Dieser Bericht kann auch Aussagen zu unklaren Punkten beinhalten.

Falls im Audit Stufe 1 Nichtkonformitäten 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 Zertifzierungsaudit (Stufe 2 Audit)

Das Stufe 2 Audit wird gemäß dem abgestimmten Auditplan durchgeführt. Das Unternehmen hat das Recht Auditoren abzulehnen.
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.

Während des Audit ermöglicht das Unternehmen den Zugang zu Aufzeichnungen aus den relevanten Geschäftsbereichen die im Geltungsbereich der Zertifizierung.

Im Audit werden u. a. folgende Punkte betrachtet:
- Dokumente, auf denen die Bewertung des Managementsystems beruht,
- Nachweise über Managementreview und interne Audits, das diese eingeführt, wirksam und gepflegt werden,
- die Wirksamkeit des Managementsystems in dem Geltungsbereich der Zertifizierung,
- Nutzung des Zertifikates und Zertifizierungszeichen (soweit vorhanden)
- Einsprüche gegen das Managementsystem

Wirksamkeit der Korrekturmaßnahmen bzgl. von Nichtkonformitäten aus vorangegangenen Audits.

Das Unternehmen hat die Pflicht alle Einsprüche gegen das Managementsystem sowie deren Behandlung aufzuzeichnen und dies im Audit zugänglich zu machen.

In dem Schlussgespräch werden die Auditergebnisse, einschließlich der dokumentierten Nichtkonformitäten, dem Unternehmen mitgeteilt.

Nichtkonformitäten sind durch das Unternehmen zu untersuchen und geeignete Korrekturmaßnahmen einzuleiten. Ein entsprechender Nachweis ist zu erbringen.

Nichtkonformitäten können zu neuen / geänderten Dokumenten / Verfahren und/ oder einem Nachaudit führen.

Der Auditleiter entscheidet über den Umfang und Bereich des Nachaudits. Nur Aspekte die für die Nichtkonformitäten zutrafen werden auditiert.

Nachdem alle Korrekturmaßnahmen implementiert sind wird der Auditbericht erstellt.

1.4 Zertifikaterteilung

Die Erteilung des Zertifikates erfolgt mit der positiven Prüfung des Zertifizierungsverfahrens durch die Zertifizierungsstelle. 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 eine Gültigkeit von 3 Jahren.

2 Überwachungsaudit

Innerhalb der Gültigkeit des Zertifikates (3 Jahre) sind Überwachungsaudits einmal jährlich durchzuführen.
Folgende Punkte werden in dem Überwachungsaudit betrachtet:

- Wirksamkeit des Managementsystems im Geltungsbereich an ausgesuchten Beispielen
- korrekte Nutzung des Zertifikates und des Zertifizierungszeichens
- Einsprüche gegen das Managementsystem
- Wirksamkeit der Korrekturmaßnahmen bzgl. Von Nichtkonformitäten aus vorangegangenen Audits.

In dem Schlussgespräch werden die Auditergebnisse, einschließlich der dokumentierten Nichtkonformitäten, dem Unternehmen mitgeteilt.

Das Unternehmen erhält einen Auditbericht.

Bei der Festlegung des Solltermins / auditrelevanten Datums für die Überwachungsaudits ist zwischen Neukunden (Erstzertifizierung ab dem 01.01.2008) und Bestandskunden (Erstzertifizierung vor dem 01.01.2008) zu unterscheiden.

<u>Neukunden:</u>

- Das auditrelevante Plan-Datum für das jährliche Überwachungsaudit, das dem Zertifizierungsaudit folgt, darf nicht später als 12 Monate nach dem letzten Tag des Audits der Stufe 2 liegen.

<u>Bestandskunden:</u>

- Das auditrelevante Plan-Datum für das jährliche Überwachungsaudit ist das Gültigkeitsdatum des am
  01.01.20xy gültigen Zertifikats (Tag und Monat) minus 1 Monat.

<u>Neukunden und Bestandskunden:</u>

- Das auditrelevante Datum steuert sämtliche Folgeaudits (Überwachungs- und Rezertifizierungsaudits).
- 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 Monate nach dem auditrelevanten Datum abzuschließen.
- Im Rahmen der Jahresüberwachung kann ein Überwachungsaudit frühestens 3 Monate vor dem auditrelevanten Datum durchgeführt werden.

Erlaubte Toleranz bei der Durchführung der jährlichen Überwachungsaudits: geplantes auditrelevantes Plan-Datum -3/+ 0 Monate.

3 Rezertifizierungsaudit

Rezertifizierungsaudits müssen – einschließlich der Prüfung von Maßnahmen zur Korrektur von Nichtkonformitäten – vor dem Ablauf der Geltungsdauer des Zertifikats abgeschlossen sein.
Im Rezertifizierungsaudit 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 Rezertifizierungsaudits 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 Rezertifizierungsaudit 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, Rezertifizierungsaudits oder zu einem eigens angesetzten Termin erfolgen.

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

5 Übernahme von Zertifizierungen anderer Zertifizierungsstellen

Generell können nur Zertifikate von akkreditierten Zertifizierungsstellen übernommen werden. Organisationen mit Zertifikaten, die von nicht akkreditierten Zertifizierungsstellen ausgestellt wurden, sind als Neukunde zu behandeln.

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

Ausgesetzte Zertifikate oder solche, bei denen die Gefahr einer Aussetzung besteht, dürfen nicht übernommen werden. Offene Abweichungen sollten, soweit praktikabel, noch vor der Übernahme mit dem bisherigen Zertifizierer geklärt werden. Anderenfalls müssen sie im Audit behandelt werden.

Das weitere Überwachungsprogramm richtet sich nach dem bisherigen.

6 Zertifizierung von Unternehmen mit mehreren Standorten

Wird ein Unternehmen, das mehrere Standorte unterhält zertifiziert, so sind diese Standorte ebenfalls zu auditieren. Die Zertifizierung von Unternehmen mit mehreren Produktionsstätten/Niederlassungen/Standorten etc. mit ähnlichem Tätigkeitsprofil und unter einem einheitlichen Managementsystem erfolgt durch die Anwendung eines Stichprobenverfahrens.

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 90 Tagen 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.