Certification Description 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 Sector-Specific-Standards (3S)

The certification of a management system (BCMS, ISMS, SMS) consists of the offer and contract phase, the audit preparation, performance of the Stage 1 audit with evaluation of the management documentation, performance of the Stage 2 audit, issue of certificate and surveillance/ recertification.

If needed the certification procedure for management systems (BCMS, ISMS, SMS) can be added with assessments of „sector-specific-standards“ (3S).

From the ISO 27001 family it is e.g.:

- 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

Or German “Smart Meter Operation law” / Messstellenbetriebsgesetz (MStBG):

- TR03109 Smart Meter Gateway Administration

Certain „Sector-Specific-Standards“ (3S) from TN CERT have an own accreditation or are in an accreditation procedure e.g.

- BNetzA § 11 Abs.1aEnWG / Specific Requirements for Energy Net Operators
- IEC 62443-2-1 – Information Security /Cyber-Security – Requirements for an IACS security management system
- IEC 62443-2-4 – Information Security / Cyber-Security f– Requirements for IACS solution suppliers.
- IEC 62443-3-2 – Information Security / Cyber-Security– Security risk assessment and system design

Some of TÜV NORD CERT individual „Sector-Specific-Standards“ (3S) are made for „critical infrastructures“, e.g..:

- TN CERT Sector-Specific-Standard (3S) Energy
- TN CERT Sector-Specific--Standard (3S) Water
- TN CERT Sector-Specific--Standard (3S) Food
- TN CERT Sector-Specific--Standard (3S) Information Technique und Telecommunication
- TN CERT Sector-Specific--Standard (3S) Health
- TN CERT Sector-Specific--Standard (3S) Finance- and Insurance
- TN CERT Sector-Specific--Standard (3S) Transport und Traffic
- TN CERT Sector-Specific--Standard (3S) State and Administration
- TN CERT Sector-Specific--Standard (3S) Media and Culture

TÜV NORD CERT individual „Sector-Specific-Standards“ (3S) claim legal requirements, requirements of German law for „Bundesamt für Sicherheit in der Informationstechnik (BSIG) - § 8a ff.” Additional statements are given if needed.

The list of „Sector-Specific-Standards“(3S) will be updated permanently. Additional „Sector-Specific-Standards“ (3S) are provided if in demand.

The auditors are selected by the Certification Body of TÜV NORD CERT GmbH in accordance with their approvals for the particular sector and their qualification.

1 Certification procedure

1.1 Audit preparation

Following signing of the contract, the auditor prepares for the audit based on the questionnaire filled in by the organization and the calculation sheet, and discusses and agrees the further procedure with the organization to be audited.

If there should be particular circumstances at the organization which make it necessary to maintain additional security or confidentiality, an additional confidentiality agreement may be signed.
The certification body must be notified in advance if the client has confidential or sensitive documents which cannot be made accessible to the auditors. Before the audit, the certification body shall determine whether the management system can be adequately audited in the absence of these records. If the certification body concludes that it is not possible to adequately audit the management system without reviewing the identified confidential or sensitive records, it shall advise the client organization that the certification audit cannot take place until appropriate access arrangements are granted.

During preparation for the surveillance or recertification audit, the organizations to be audited have the duty to report fundamental changes in their organisational structure or changes in procedure to the certification body.

1.2 Stage 1 audit

The stage 1 audit is conducted in order to

- Obtain and review the management system documentation required by the standard
- Provide a focus for planning the stage 2 audit
- Gaining the organization’s state of preparedness for stage 2 audit (based on understanding the management system in the context of the organization’s policies and objectives).

The client makes all necessary arrangements for the conduct of the certification audit, including provision for examining documentation and the access to all areas, records (including internal audit reports and reports of reviews) and personnel for the purposes of certification audit, recertification audit and resolution of complaints. The client supplies all the documents necessary for the audit, in their current valid version, at least 4 weeks before the audit.

The stage 1 audit includes, but is not be restricted to, the document review. The certification body agrees with the client organization when and where the document review is conducted.

The current management documentation is assessed and consists of:

BCMS – ISO22301	ISMS – ISO 27001	SMS – ISO 20000-1
□ BCM policy and objectives	□ ISMS policies and objectives	□ SSM policies and objectives
□ Scope of the BCMS	□ Area of application/ scope of the ISMS	□ Area of application/ scope of the SMS
□ Procedure(s) of the BCMS	□Procedure(s) and activities of the ISMS,	□ Service management plan
• Business impact analysis • Risk assessment	□ Statement of Applicability	□ Documented service level agreements
□ Business continuity strategy	□ any other relevant documents/ records relating to the standard on which the audit is based	□ Documented processes and procedures required by the Standard
• Incident response structure • Business continuity plans/ Incident management plans • BCM exercising records	□Risk management which includes o Description of risk assessment methodology o Risk assessment report o Risk treatment plan	□ Records required by the Standard

The client shall fill out a standard specific checklist before audit stage 1 in cases of „Sector-Specific-Standards“ (3S) assessments. The client receives the basic form of the checklist before.

The organization receives a written report regarding the results of the stage 1 audit including assessment of the management documentation and therefore also has the opportunity of eliminating any nonconformity before the stage 2 audit. It is also possible to submit statements regarding any items which are not clear.

If nonconformities were identified in the stage 1 audit, these must be corrected by the organization before the stage 2 audit.

If at the end it cannot be established positively that the organization is ready for the stage 2 audit, the audit is broken off after the stage 1 audit.

The lead auditor is responsible for the coordination of the activities of the stage 1 audit and if necessary for coordination and cooperation of the auditors concerned amongst themselves.

1.3 Certification audit (Stage 2 audit)

The audit is performed in accordance with the audit plan which was agreed with the company before the start of the audit. The organization has the right to reject the auditors who have been named. The company proves the use and effectiveness of the procedures which have been described and laid down in the audit.
The audit begins with a start-up meeting, in which the participants are introduced to each other. The procedure to be followed in the audit is explained. Within the framework of the audit at the

organization's premises, the auditors review and assess the effectiveness of the management system which has been installed.

During the audit, the organization permits the audit team to view the records which refer to the areas which fall within the scope of the audit and allows the team access to the relevant business units.

During the audit, the following items are inspected, among others:

- The documents upon which the assessment is based
- Evidence that the arrangements for management reviews and internal audits have been implemented, are effective, and will be maintained
- The effectiveness of the management system in the areas within the scope of the audit
- Proper use of the certificate/ certification mark (if applicable)
- Objections to the management system
- The effectiveness of corrective actions with regard to nonconformities from the previous audit (if applicable).

The organization has the duty to record all the objections which refer to the management system and their rectification, and to present them during the audit.
In the final meeting, the result of the audit as well as any nonconformities which have been recorded is communicated to the organization.
Nonconformities are requirements which have not been fulfilled, where the organization has to instigate appropriate corrective actions and verify these actions. Corresponding proof must be provided.

The nonconformities can lead to the submission of new/ revised documents/ procedures and/ or to a re-audit.
The lead auditor decides about the scope of the re-audit. Only the aspects which are relevant to the nonconformity are audited (processes, procedures, areas of the company).
After all corrective actions have been implemented and all non-conformities have been corrected and signed off, the audit report is drawn up.

1.4 Issue of certificate

The certificate is issued when the certification procedure has been reviewed and released by the certification body. The person who reviews and releases the procedure may not have participated in the audit.

The certificate can only be issued when the nonconformities have been accepted or verified by the audit team.

The certificates are valid for 3 years.

2 Surveillance audit

The following items are inspected during the surveillance audit:

- The effectiveness of the management system within the entire company by means of a smaller random sample
- Correct use of the certificate/ certification mark
- Objections to the management system
- Effectiveness of corrective actions regarding nonconformities from the previous audit (if applicable)

In the final meeting, the audit result is communicated to the company, including any nonconformities which have been documented.

The client receives a report following the surveillance audit.

Surveillance audits must be conducted once per year during the period of validity of the certificate (3 years).
When the set date / audit-relevant date is set for the surveillance audits, a difference must be made between new clients (initial certification as from 01-Jan-2008) and existing clients (initial certification before 01-Jan-2008).

New clients:

- The planned audit-relevant date for the annual surveillance audit, which follows the certification audit, may not be later than 12 months after the last day of the stage 2 audit.

Existing clients:

- The audit-relevant date for the annual surveillance audit is the date of validity of the certificate which was valid on 01-Jan-2008 (day and month) minus 1 month.

New and existing clients:

- The audit-relevant date controls all the following audits (surveillance and recertification audits).
- Each surveillance audit including review and acceptance and verification, if appropriate, of the measures for correction of nonconformities, drafting of the audit report and release by the certification body, must be completed at the latest 2 months after the audit-relevant date.
- Within the framework of annual surveillance, a surveillance audit can be conducted at the earliest 3 months before the audit-relevant date.

Permissible tolerance for conducting annual surveillance audits: Audit-relevant plan date -3/ +0 months.

3 Recertification audit

Recertification audits must be complete before the end of the period of validity of the certificate, including review of the measures for correction of nonconformities.
In the recertification audit, a review of the documentation of the management system of the organization takes place and an on-site audit is conducted, whereby the results of the previous surveillance programme(s) over the period of the certification are to be taken into consideration. All requirements of the standard are audited.
Activities related to the recertification audit may include a stage 1 audit if there are significant changes in the management system or in connection with the activities of the organization (e.g. changes to the law).

The audit methods used in the recertification audit correspond to those used in a stage 2 audit.

4 Extension audit

If it is intended to extend the scope of an existing certificate, this can be implemented by means of an extension audit. An extension audit can be conducted within the framework of a surveillance audit, a recertification audit or at a time which is set independently.

The period of validity of a certificate does not change as a result. Exceptions must be justified in writing.

5 Takeover of certificates of other certification bodies

In general, only certificates from accredited certification bodies can be taken over. Organizations with certificates which originate from non-accredited certification bodies are treated like new clients.

A "Pre-Transfer-Review“ must be conducted by a competent person from the certification body which is taking over the certificate. This review generally consists of an examination of important documents and a visit to the client.

Certificates which have been suspended, or where there is risk of suspension, may not be taken over. Any nonconformities which have not been corrected should as far as practicable be clarified with the previous Certifier before the takeover. Otherwise they must be dealt with in the audit.

The further surveillance program is based on the program which has been in place up to the time of the takeover of the certificate.

6 Certification of multi-site organizations

If an organization which has several sites certified, these sites must also be audited. Certification of organizations with several production sites/ branch offices/ locations etc. with similar types of activity and which operate under a single management system is by means of random sampling procedure.

7 Management of nonconformities

An analysis of the causes must be performed for each nonconformity and corresponding corrective actions must be implemented. The organization has the duty, depending on the seriousness of the nonconformity, to inform the audit team within 90 days either with regard to the corrective actions which have been laid down and the dates for their implementation or that the corrective actions have been implemented. If this period is not observed, the audit is considered not to be successful, i.e. not to be passed. No certificate can be issued, or an existing certificate is withdrawn.