Description of the certification procedure
MS – ISO 27001, MS – ISO 22301, MS – ISO 20000-1

Table of contents

If you should require any further information then please do not hesitate to contact us. We will be please to help you.

Please contact us via mail to info.tncert@tuev-nord.de or by telephone 0800 245 74 57 (Free-phone from within Germany) or +49 511 9986-1222 from abroad.

TÜV NORD CERT GmbH

Am TÜV 1

45307 Essen

Germany

www.tuev-nord-cert.com

The certification of a management system based on standard ISO/IEC 27001, ISO 22301 or ISO/IEC 20000-1 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.

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

1 CERTIFICATION PROCEDURE

The certification audit consists of the Stage 1 audit and the Stage 2 audit. Both audits are generally performed at the client's site.

In the context of ISO/IEC 27001 certification procedures it is allowed referring to additional national or international standards (e.g. ISO/IEC 27017 or ISO/IEC 27018) as additional source(s) of control set for controls in the organization's Statement of Applicability (see Section "Sector-specific Standards in addition to ISO/IEC 27001").

1.1 Audit Preparation

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

The certification body has to be informed in advance if the client has confidential or sensitive documented information, which cannot be made accessible to the audit team. Before the audit, the certification body shall determine whether the management system can adequately be audited in the absence of these records. If the certification body concludes that it is not possible adequately auditing the management system without reviewing the identified confidential or sensitive documented information, 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 organizational structure or changes in procedure to the certification body.

1.2 Audit Stage 1

The Stage 1 audit is conducted in order to

- audit the management system documentation of the customer,
- assess the site and site-specific conditions of the customer and hold discussions with the personnel of the organization in order to determine the degree of preparedness for the Stage 2 audit,
- assess the status of the customer and his understanding of the requirements of the standards, particularly with regard to identification of key performance or significant aspects, processes, objectives and operation of the management system,
- to collect necessary information regarding the scope of the management system, processes and location(s) of the client, number of people within the scope, compliance obligations as well as information security aspects

- review the allocation of resources for Stage 2 audit and agree with the client on the details of the Stage 2 audit,
- to create a special focus for the planning of the Stage 2 audit, by gaining sufficient understanding of the client's management system and the activities at the site, together with possible significant aspects,
- evaluate if the internal audits and management review are both planned and performed, and that the level of implementation of the management system demonstrates that the client is ready for the Stage 2 audit.

If weaknesses were identified in the Stage 1 audit, these must be corrected by the customer before the Stage 2 audit.

If at the end it cannot be established positively that the customer 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 Audit Stage 2 – Certification Audit

The customer receives an audit plan at the beginning of the Stage 2 audit. The plan is agreed with the customer in advance.

The audit begins with a kick-off 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. This is based on the standard ISO/IEC 27001, ISO 22301 or ISO/IEC 20000-1.

The task of the auditors is to compare the practical application of the management system with the documented processes and to assess them in relation to fulfilment of the requirements of the standard. This is achieved by means of questioning of the employees, examining the relevant documents, records, orders and guidelines and also by visiting relevant areas of the organization.

A final meeting takes place at the end of the on-site audit. At least those employees take part in the audit who have management functions within the organization and whose areas were included in the audit. The lead auditor reports on the individual elements and explains the positive and negative results. If nonconformities are established, the lead auditor can only recommend issue of the certificate to the organization after acceptance or verification of the corrective actions by the audit team, see Section "Management of nonconformities". Attention must be drawn to this fact in the final meeting.

The audit is documented in the audit report (the documentation must be separate for Stage 1 and Stage 2 audits) and is completed by means of further records (e.g. audit questionnaire and hand-written records), which are generally for internal use only within the certification body.

1.4 Award of Certificate

The certificate is issued when the certification procedure has been reviewed and released by the head of the certification body or his deputy or nominated representative. The person who reviews and releases the procedure may not (i.e. is not permitted to) have participated in the audit.

The certificate can only be issued when the nonconformities have been corrected, i.e. when the corrective actions have been accepted or verified by the audit team.

Normally the certificates are valid for 3 years.

2 SURVEILLANCE AUDIT

Surveillance audits have to be conducted once per year during the period of validity of the certificate with the exception of the years when a recertification audit is performed.

The first surveillance audit, which follows the initial certification has to be carried out by the planning-relevant date, at the latest 12 months after the date of the certification decision. All the subsequent surveillance audits are planned on the basis of the planning-relevant date and must be conducted at least once per calendar year.

Surveillance audits including the verification of measures for the correction of nonconformities, audit reporting and the certification decision must be completed no later than 3 or 4 months (in case of nonconformities) from the last day of the audit.

The client receives a report following the surveillance audit.

3 RECERTIFICATION AUDIT

The audit for recertification has to be conducted before the expiry date of the certificate. A tolerance period of max. 6 months is then available for evaluation of the corrective actions and for any necessary re-audits and also for the decision on recertification within the framework of the release procedure. In the recertification audit, a review of the documentation of the management system of the organization is undertaken, as well as an on-site audit. Here, the results of the previous surveillance programme(s) over the term of the certification have to be taken into consideration. All the 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 OF SCOPE AUDIT

If it is intended extending 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.

4.1 Short Notice Audits

It may be necessary to perform audits at short notice to investigate complaints, in response to changes or as follow up on suspended clients. In such cases,

- the certification body shall describe the conditions under which these short notice audits are to be conducted,
- it is not possible to object to members of the audit team.

4.2 Transition Audits

As a result of changes to a management system standard, it may be necessary to perform corresponding transition audits in order to maintain certification. After a successful transition, certificates are then issued for the new standards without changing the expiration date of the existing certifications.

Should such changes become necessary, then the certification body will timely inform about the necessary prescribed measures.

5 TRANSFER OF CERTIFICATION FROM OTHER CERTIFICATION BODIES

In general, only certificates from accredited certification bodies can be taken over where the accreditation body is a signatory to the Multilateral Agreement (MLA) of the EA (European co-operation for Accreditation). Organizations with certificates, which originate from non-accredited certification bodies, are treated as new clients.

The issuing certification body is informed about the planned transfer. As soon as no reasons are known from the issuing certification body and the customer that exclude a transfer of the valid certificate according to IAF MD 2:2017, the transfer can be carried out.

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.

After positive completion of the pre-transfer review, TÜV NORD CERT, as the accepting certification body, can carry out the transfer of certification.

The normal certification decision making process shall be followed, including the requirement that the personnel making the certification decision are different from those carrying out the pre-transfer review.

TÜV NORD CERT, as the accepting certification body, shall take the decision on certification before any surveillance or recertification audits are initiated.

The certification cycle of the transferred certificate is based on the previous one. TÜV NORD CERT shall establish the audit programme for the remainder of the certification cycle.

Where the accepting certification body is required to treat the client as a new client as a result of the pre-transfer review, the certification cycle shall begin with the certification decision.

Certificates, which have been suspended or where there is risk of suspension, may not be taken over.

The issuing certification body is informed as soon as the certificate has been successfully transferred.

6 CERTIFICATION OF COMPANIES WITH MULTIPLE LOCATIONS (MULTI-SITE)

A sampling procedure can be used for organizations with several sites (“multisite certification”). In this case, the client assures the certification body that the following requirements are met for all the sites, which fall within the scope of the certificate. Any changes or non-fulfilment of one or several prerequisites shall (i.e. must) be communicated to the certification body immediately.

Prerequisites for multisite certification:

- A multi-site organization does not have to be one single legal entity. However, all the sites shall (i.e. must) have a legal or contractual relationship with the headquarters (“central office”) of the organization and be

subject to a common management system, which is specified and installed by the central office and is subject to regular monitoring and internal audits by the central office. This means that the central office has the right to require the sites to implement corrective actions, if these are necessary at a particular site.

- The processes must be basically the same at all sites and must be implemented using similar methods and procedures.
- The management system of the organization has to be administered under a centrally controlled plan and must be subject to a central management review. All the individual sites within the multi-site system (including the central administration (central office) function must be subject to the internal audit programme of the organization and must be audited in compliance with this programme.
- It has to be demonstrated that the central office of the organisation has installed a management system in compliance with the relevant management system standard(s), which form the basis for the audit and that the entire organization fulfils the requirements of the standard.
- The organization must demonstrate its ability to collect and analyze data from all sites, including the central administration function (central office) and its management, and shall instigate any necessary organizational changes, including those related to:
  - Management review,
  - Complaints,
  - Evaluation of the corrective actions,
  - Planning of internal audits and evaluation of the results,
  - Legal requirements.
- A contract has to be concluded between the client and the certification body, which is legally enforceable at all branches/production sites.

7 MANAGEMENT OF NON-CONFORMITIES

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 6 weeks after the last day of the audit 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. A certificate must not be issued, or an existing certificate is withdrawn respectively.

8 SECTOR-SPECIFIC STANDARDS IN ADDITION TO ISO/IEC 27001

TÜV NORD CERT can currently offer audits and certifications according to ISO/IEC 27001 using the following national or international standards as an additional source of controls.

Region	Standard	Content
International	ISO/IEC 27017	Information security controls for cloud services

International	ISO/IEC 27018	Personally identifiable information (PII) in public clouds acting as PII processors
International	ISO/IEC 27019	Information security controls for the energy utility industry
Germany	BSI TR 01201	De-Mail
Germany	BSI TR 3109-6	Smart Meter Gateway Administration

The applicable controls from these standards must be listed in the Statement of Applicability ("SoA") and must be adequately taken into account in the audits. Reference to these standards in the certificate for ISO 27001 does not indicate that certification to these standards is involved. Separate certificates, certificate supplements or other attestations must not be issued for this purpose.