Deutsche Zertifizierung
in Bildung und Wirtschaft GmbH

Hochschulring 2
15745 Wildau

Certification procedure of information security management system (ISMS) according to ISO/IEC 27001:2013

Document WP04 I - D01e

SUMMARY

- Examination regulations for certification of management systems
- Procedures for certification of Information Security Management Systems (ISMS) according to ISO/ IEC 27001: 2013

Content

Introduction

This document summarizes the procedure of certifying an information security management system (ISMS) in accordance with ISO/ IEC 27001: 2013 combined with ISO/ IEC 27006:2015 of the certification body DeuZert GmbH - cf. Figure No. 1.

The purpose of this document is to inform the company to be certified about the relevant regulations.

This procedure was developed in accordance with the relevant standard EN ISO/ IEC 17021-1:2015 combined with ISO/ IEC 27006:2015.

Initial certification audit

The certification audit of an ISMS consists of the audit stage 1 and the audit stage 2. In addition, an optional pre-audit can be carried out pre-switched.

Pre-audit

The procedure of a pre-audit is optional and unique. The intention of a pre-audit is to determine the readiness for certification by an examination on site. The auditor conducts the audit according to an audit plan that leads to an audit report. The costs for the pre-audit are not included in the costs for the initial certification audit.

Stage 1 audit

During the stage 1 audit the information security management documentation of the company and the conditions on site are audited. If multiple sites are to be certified, the stage 1 audit will take place in the company`s headquarter.

The management documentation provided by the company has to consist of the following items:

- a documented explanation of the ISMS guideline and ISMS objectives,
- the scope of the ISMS,
- Procedures and measures that support the ISMS,
- a description of the risk assessment method,
- the report of the risk assessment,
- the risk treatment plan,
- Documented procedures required by the organization to ensure the effective planning, execution and control of its information security processes, and to describe how to measure the effectiveness of measures.
- Records required by the standard,
- the statement of applicability,
- a current organizational chart / presentation of the organizational structure,
- a list of co- applicable documents and forms,
- a list of documented procedures,

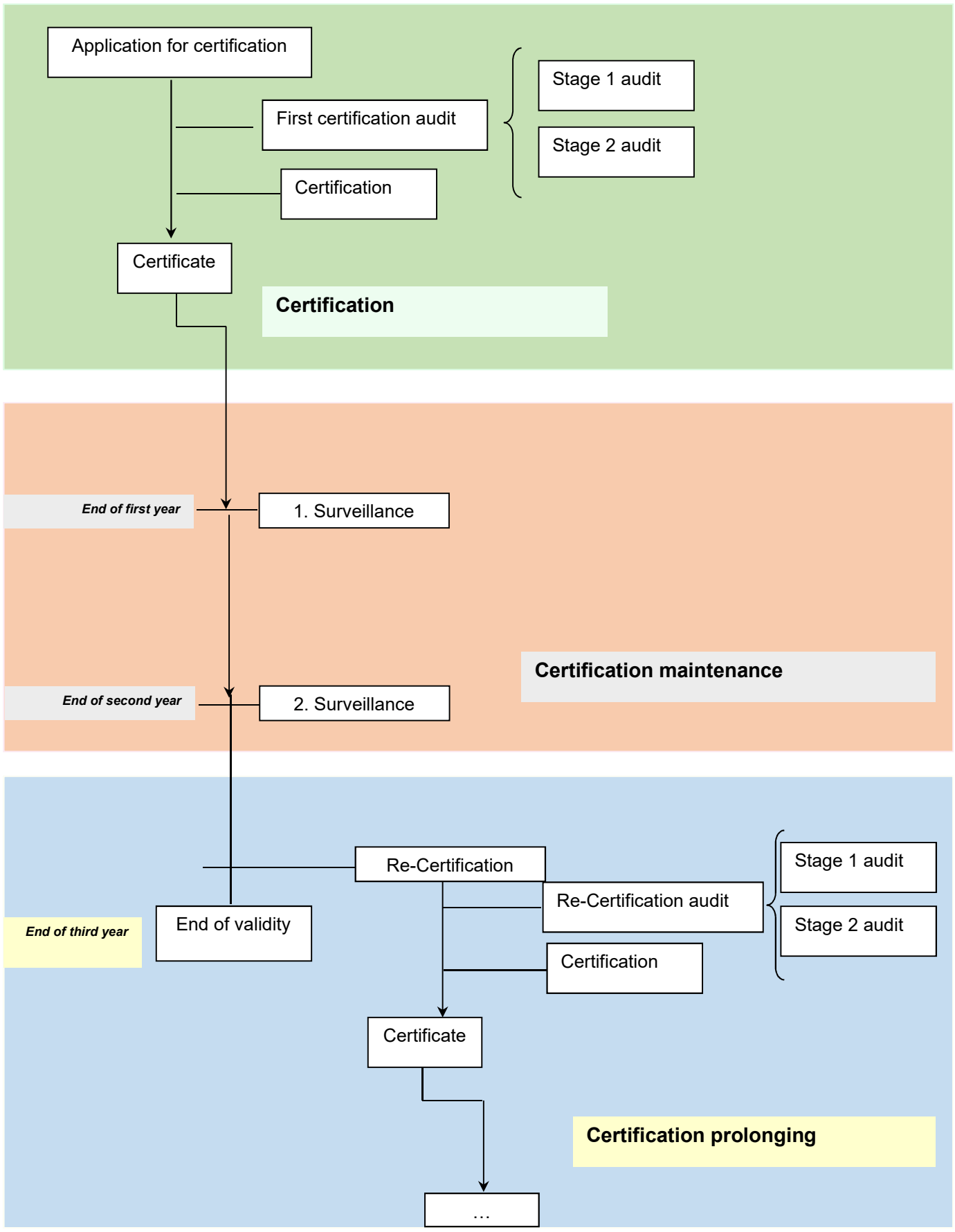
- Process descriptions to:

  - control of documents,
  - control of records,
  - Internal audits,
  - corrective actions,
  - preventive actions.

- Evidence on the realisation of internal audits and management reviews.

The documentation to be submitted to the certification body should be securely/ encrypted by the company. The auditor collects necessary information regarding the scope of the ISMS, the processes of the company's premises as well as related legal and regulatory aspects and their compliance as well as the associated risks and their evaluation in the audit.
The aim is to evaluate to what extent the requirements of the standard for the implementation of the stage 2 audit are met by the company. In case of nonconformities with the requirements of the standard, the company is given an appropriate period for correction. Only, if the company has carried out the rework within this period, the stage 2 audit can take place. In individual cases, it may be necessary to repeat the stage 1 audit. It should be noted here that the gap between the audit stage 1 and the audit stage 2 may not exceed 3 months. The auditor prepares a report on the result of the audit stage 1. The stage 2 audit can be conducted directly after the stage 1 audit. In this case, any weaknesses encountered during the stage 1 audit can be classified as nonconformities in the stage 2 audit.

Picture Nº 1


Application for certification
First certification audit
Stage 1 audit
Stage 2 audit
Certification
Certificate
Certification
End of first year
1. Surveillance
Certification maintenance
End of second year
2. Surveillance
Re-Certification
Stage 1 audit
Re-Certification audit
Stage 2 audit
End of third year
End of validity
Certification
Certificate
Certification prolonging
…

Stage 2 audit

During the stage 2 audit, the implementation and effectiveness of the company's ISMS is assessed. It is checked if what has been set and/ or documented is actually implemented.

The auditor will conduct the audit according to an audit plan which will be provided to the company in advance. The audit includes the questioning of employees at their workplace as well as inspecting further applicable documents, records or similar documents and the site inspection of the relevant areas.

Attendees on the audit will be recorded on an attendees list by signature. The auditor issues an audit report including all detections of the stage 2 audit as a conclusion - possibly nonconformities can also be documented separately in a report. The company as well as the lead auditor, both sign two copies of the report. One copy stays with the company subject to the approval by DeuZert. The second copy will be brought forward to DeuZert for approval. At last the second copy of the audit report will be filed. The right of property on the audit report stays with DeuZert.

In a closing meeting the auditor will notify the conclusions mentioned in the report about the company. If there are nonconformities the following measures are specified. The follow-up of the nonconformities will cause additional work and expenses.

Certification

The decision of issuing the certificate will be made by the certification board. Members of the certification board are the professional management in terms of contents of certifiction or deputy as well as a qualified auditor who is not involved in the certification process to be decided.

The decision by the certification board is based on the documentation of the certification process, a survey of the recommendation by the auditors and on further relevant information such as public information or a statement of the company on the audit report.

Based on the form for the order of certificates completed by the company, DeuZert creates a certificate draft and sends it to the company. With signature or any other appropriate approval, the company confirms and returns the possibly corrected and signed draft to DeuZert.

The certificate is issued by the date of the certification decision. The certificate is officially registered by granting a registration number. The validity of the certificate is three years from the issuing date.

The scope of services contains the issuing and registration of a maximum of 2 certificates (certificates and sub certificates) without company logo in the format DIN A3 or DIN A4 as well as a .pdf file.

The available languages for certificates are: German, English or Russian. For other or additional requests concerning the certificates please refer to the actual bill of quantities

Certification maintenance and prolonging

Surveillance audit

During the validity of the certificate, annual surveillance audits are carried out on the certified company. The surveillance audits check whether changes have been made to the company's ISMS and whether the company continues to meet all relevant standard requirements.

In advance of the annual surveillance audits, DeuZert updates the existing information about the company, in particular the number of employees and locations. Detected changes can lead to an adjustment to the original audit duration. In case of such a change, DeuZert will determine the change within audit duration and/ or the contents of the audit.

Surveillance audits are covering the following issues:

- Examination if there were internal audits as well as management reviews performed and documented.
- Evaluation of the measures taken based on conclusions of the previous audit.
- Examination of the complaint management and the handling security problems.
- Examination of the effectiveness of the management system according to the achievement of ambitions.
- Examination of the progress in the area of continual improvement.
- Examination if there is a prolonged management.
- Evaluation of corporate data such as number of employees, number of sites and so on.
- Utilisation of signs.

The target date of a surveillance audit shall not be performed 12 / 24 month after the last day of the stage 2 audit also surveillance audits shall not be performed 3 months before the target date. Surveillance audits may take place at the earliest 3 months before the scheduled date. About four months before the scheduled date, DeuZert informs the company about the target date of the upcoming audit and agrees with him a period of 2 weeks during which the surveillance audit is to be carried out. The auditor will arrange the precise target date with the company. The auditor will perform the surveillance audit in similar manner to a stage 2 audit. The surveillance audit leads to an audit report similar to the audit report of the certification audit - possibly nonconformities can also be documented separately in a report. The certification board decision on the maintenance of the certification will be based on the procedural documents to be assessed, the auditor's audit review, and other relevant information (for example public information or a statement of the company on the audit report).

Re-Certification (certification prolong)

A certification can be prolonged for further 3 years if the re-certification audit including the examination of corrective actions of nonconformities and the recommendation of the auditor for issuing the certificate are finished before the end of the validity of the former certificate.

The target date for re-certification is the end of the validity period of the certificate minus 3 months. The company applies for re-certification not later than 4 months before the end of the validity period of the actual certificate. If there are significant changes in the organisation of the company or the function of the ISMS, there could be a necessity for a stage 1 audit similar to the stage 1 audit on page 2. The re-certification audit consists of a stage 2 audit similar to the stage 2 audit on page 5. The decision on the prolonging of the certificate will be similar to the decision of certification also described on page 5.

Further regulations

Further regulations are listed below:

- The head of sales network/ customer service or an authorised representative employee examines the application on correctness and completeness. A further examination on if the application meets the scope of functions and the sphere of authority as well as if there are qualified auditors available. If those preconditions are met, an offer is made based on the specifications in the application. If the application is denied, reason for the denial is provided to the company in writing.

- The company may object to any nomination of any auditor or expert. On request the company will be provided with names and further information to every member of the audit team. The consideration on data protection in this case is mandatory.

- If during an audit is discovered that the objectives of the audit will not meet respectively an immediate considerable risk may exists (e.g. security), the auditor has to inform the company immediately and, if possible, the certification body. Further the auditor has to initiate reasonable actions. This includes also any need for changes concerning the audit scope. Those issues are documented in the audit report. In the case of different opinions about those issues the auditor and the company will try to resolve those differences in a common constructive manner. If this is not possible, the difference of opinion is documented in the audit report.

- There is always the possibility of objections against the certification decision as well as complaints about it. Complainants are not penalised for objecting or complaining against the certification decision. Within 4 weeks after the certification decision comes to the attention of the company, there is the possibility of submitting a complaint in writing. Any time complaints may provide to DeuZert in writing.

- DeuZert provides the company with notification of changes of the requirements concerning the certification in due time. The company pledges oneself to implement adjustments that result out of the notification of changes.

- The utilisation of the DeuZert - Logo is part of a stipulation. Those stipulations are part of the document WP04 – D001: Certification of management systems § 29 "Right of utilisation of token and certificates".

- DeuZert keeps records of all valid certifications. The record consists of the name of the certified company, the certification standard, the area of application of the certification, the certified sites and the validity of the certificate. DeuZert has the right to reveal this register by request.

- DeuZert has the right to provide an interested party about the status of the certification by request. Further information about the company is handled confidential with highest priority and are only revealed to third parties if the company has given his approval in writing. If DeuZert is legally obligated to reveal confident information about the company to third parties, the company will be notified in advance about the information to be revealed.

- The company grants DeuZert the right to perform witness audits on the part of the accreditation body. This does not lead to additional costs.

- The company has to inform DeuZert about any issues that could compromise the capability of the ISMS without the least delay. Such issues can be for example the change of the legal form of the company or the form of organisation, the financial conditions or land tenure, the organisation and their management (such as changes in senior management personal in executive positions, executives or experts), contact address and sites inside the scope of the ISMS, significant changes to the ISMS and the processes as well as any other events which may result in certification requirements being temporarily or permanently lost among other things.