CIS
Certification Procedure

Processes & Actions

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/6/14

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

Table of Contents

Prologue

1 Scope of the Document

This document describes the procedures and processes of a certification procedure for the following standards:

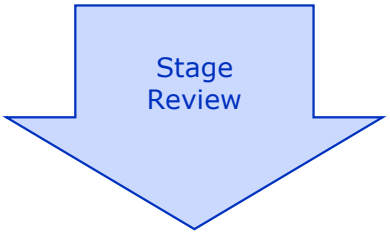
- ISO/IEC 20000
- ISO/IEC 22301
- ISO/IEC 27001
  incl. specific extensions such as: ISO 27018, ISO 27019, ISO 27701
- Assessment according to Energy Industriy Act §11
  (aka Energiewirtschaftsgesetz – EnWG §11)

2 Eligibility

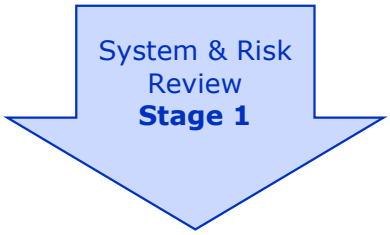
The client must maintain a documented management system for information security (ISO 27001 series incl. Energy Industry Act §11), IT services (ISO 20000) or business continuity (ISO 22301).

3 Course of the Certification Procedure

Based upon the CIS application for certification, the further steps of the certification procedure will be planned as to the schedule and contents, and the scope will be determined. As soon as your organization is in the "Initial Registration & Planning", it formally is in the CIS certification procedure and will therefore also be listed in the CIS registration list.



While organizations are establishing, adapting or improving their management systems, they can have the adequacy and suitability of the actions taken reviewed in the sense of the requirements placed by the standard in the CIS stage review. Therefore, the CIS stage review can also be used as an independent and gradual monitoring of project progress.



The System & Risk Review is aimed at evaluating the company specific interpretation of the requirements placed by the Standard on the basis of risk analyses and assessments made as well as concrete actions. Furthermore, the existing documentation on the Management System will be reviewed and evaluated. The identified opportunities for improvement will be explained. The further need for action before the CIS certification audit will be laid down in a written report.

The CIS certification audit comprises the practical actions taken to completely evidence the fulfilment of the requirements placed by the standard. In this context, ensuring that the systematic way of acting is made traceable by multiple sampling at all the levels of the organization is prioritized upon. The role placed by the technology used is determined by the extent to which it influences the organizational and managerial needs.

By obtaining the Certificate Issuance & Right to Use Licence, the certified organization obtains the right to have a CIS attestation of conformity. After the CIS attestation of conformity has been issued, it will be valid for 3 years and may be used as evidence vis-à-vis third parties, which helps to create their confidence. Furthermore, CIS customer for ISO 20000-1 will also be listed on the homepage of APMG if requested.

Each management system is subject to constant and rapid technological and organizational changes, adjustment and improvement. Therefore, CIS surveillance audits serve to find out how these changes are handled and to identify effectiveness of the overall management system. Upon positive completion of the CIS surveillance audit, the further use of the existing certificate will be applied for. Up to the expiration of the three years' validity of the certificate, two CIS surveillance audits will be performed at an interval of 12 months.

After 3 years, the validity of the certificate needs to be renewed. Therefore, a recertification audit with the full scope of a STAGE 2 Audit is required. Upon successful recertification, the 3-year right to hold the CIS certificate and the CIS conformity mark can be obtained again.

4 Further Explanations on the Certification Procedure

4.1 APPLICATION FOR CERTIFICATION

Upon application, an offer will be made on the basis of the data..

(see also document no. d012e, d013e and d066e respectively)

4.2 PURCHASE ORDER

Will be placed by returning the undersigned copy of the offer or a purchase order.

4.3 SYSTEM & RISK REVIEW – AUDIT STAGE 1

The Audit Stage 1 will take place at your site or remotely.

This audit is aimed at a practice oriented discussion of the requirements placed by the standard. It focuses upon identifying the status of a risk analysis already made or upon furnishing approaches for the execution of a corresponding risk analysis in the organization. The „CIS System & Risk Review" will be carried out in co-operation with the employees who assume coordination and steering tasks relating to information security / service management / business continuity within the organization or are responsible for this. The System & Risk Review is aimed at evaluating the company specific interpretation of the requirements placed by the standard on the basis of risk analyses and assessments made as well as concrete actions.

The CIS office team will inform you in writing which CIS employees will carry out Stage 1. The employee(s) will contact you to agree upon a date.

A written report on the results of Stage 1 will be drawn up and delivered to the auditee.

4.4 CERTIFICATION AUDIT - AUDIT STAGE 2

After Stage 1 has been successfully completed, it will be followed by Audit Stage 2.

The CIS office team will communicate the names of the members of the auditor team to you in writing. In justified cases, you can make objections (to individual team members).

As soon as you have agreed to the auditor team, the lead auditor will agree upon an audit date with you.

The CIS certification audit comprises the practical actions taken to completely evidence the fulfilment of the requirements placed by the standard. In this context, ensuring that the systematic way of acting is made traceable by multiple sampling at all the levels of the organization is prioritized upon. The role placed by the technology used is determined by the extent to which it influences the organizational and managerial needs.

A written report on the results of Stage 2 will be drawn up and delivered to the auditee.

If nonconformities are indicated in this report, they will have to be eliminated. The actions taken will have to be reported.

If nonconformities that cannot be settled by handing in additional documentation have been identified, Stage 2 will be repeated.

Upon positive completion of Stage 2, the lead auditor will recommend CIS GmbH to grant a certificate.

4.5 ISSUANCE OF THE CERTIFICATE

Upon positive review of the report and the positive handling of any nonconformities, CIS GmbH will issue the certificate. The validity of the certificate will be starting from the date of the decision of the governing board.

4.6 ANNUAL SURVEILLANCE AUDIT

The date of the surveillance audit always is the data of the audit in Stage 2. The CIS office team will inform you on the auditor entrusted with the surveillance audit 3 months prior to the date of the surveillance audit. This auditor will contact you and agree upon a date with you.

In the course of the surveillance audit, the handling of changes as well as the effectiveness of the overall management system will be identified.

A report on the result of the audit will be written. If nonconformities have been identified, you will have to eliminate them and adequately communicate the actions taken to the CIS auditors. In case of nonconformities that cannot be settled by handing in additional documentation, a post-audit at your site will be carried out.

Upon positive completion of the surveillance audit, the auditor will recommend CIS GmbH to continue the Certificate.

Specifics regarding Energy Industry Act §11:

In connection with the Energy Industry Act §11 assessment according to the conformity assessment program of the Federal Network Agency (Bundesnetzagentur), the case of withdrawal according to point 3 must be reported immediately (E-Mail to it-sicherheitskatalog@bnetza.de).

4.7 RECERTIFICATION

After 3 years, the validity of the certificate needs to be renewed. Therefore, a recertification audit with the full scope of a Stage 2 Audit is required. Upon successful recertification, the 3-year right to hold the CIS certificate and the CIS conformity mark can be obtained again (see Description 4.4, Stage 2).

4.8 CHANGES RELATING TO THE AREA OF VALIDITY OF THE CERTIFIED SYSTEMS

Changes will be treated as new certifications. The clients' feedback on organizational changes will be reviewed by top management of CIS, which will decide upon the further steps.

4.9 CHANGES IN THE REQUIREMENTS FOR CERTIFICATION

Changes in the requirements for certification, such as modification of the standards by which the certification was issued, all certified clients will be informed by e-mail. If further explanatory notes should be required this will be published on the website or by newsletter.

5 Applicable Documents

Generals Terms and Conditions for system certification by CIS – Certification & Information Security Services GmbH (downloadable via www.cis-cert.com).

Note 1:
The CIS certification procedure does not provide any suspension of the certification.

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/6/14

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

Autoren

Robert Jamnik

Klaus Veselko