CIS certification process for systems (d011e) (EN-US)

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

Content

1 Procedures & processes

1.1 PROLOGUE

1.2 SCOPE OF APPLICATION

This document describes the procedures of a certification process for the following standards:

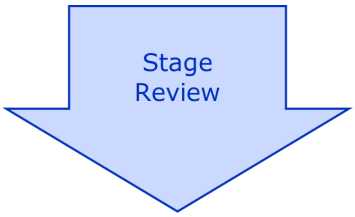
- ISO/IEC 20000
- ISO/IEC 22301
- ISO/IEC 27001 incl. all extensions: ISO 27017/ISO 27018/ISO 27019/ISO 27701
- Audit according to EnWG §11 1a and EnWG 1b (Energy Industry Act)

1.3 ACCESS REQUIREMENTS

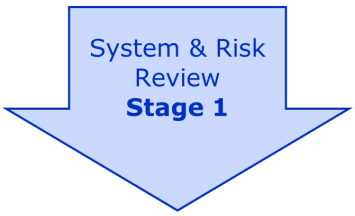
The client must maintain a documented management system for information security (ISO 27001 series incl. EnWG), IT services (ISO 20000) or business continuity (ISO 22301).

2 Certification procedure

Based on the application for certification, the further steps of the certification process are planned in regard to time and content and the scope of the certification is determined. With the "Initial Registration & Planning", your organization is formally in the CIS certification process and is therefore also listed in the CIS registration list.



Organizations can have the adequacy and appropriateness of the precautions and measures taken assessed by the CIS Stage Review in accordance with the standard requirements during the establishment, adaptation or improvement of the management system. The stage review can therefore also be used as an independent and step-by-step monitoring of project progress.



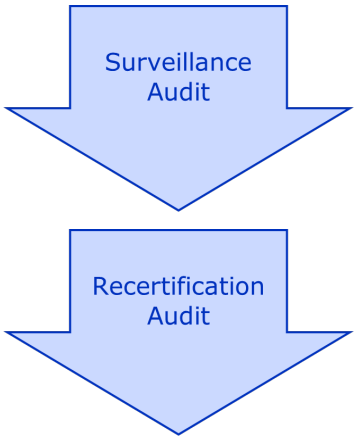
The purpose of the system review is to assess the company's interpretation of the standard requirements on the basis of specific measures and precautions taken. Furthermore, the existing management system documentation will be reviewed and evaluated. The identified weaknesses will be explained and the need for further action before the certification audit will be recorded in a written report.

The scope of the certification audit for management systems is the practical measures for the complete verification of the standard requirements. Particular focus is placed on ensuring that the systematic approach is traceable through multiple spot checks at all levels of the organization. The technology used is important to the extent that it significantly influences the organizational and management requirements.

With the initial issue of the certificate (Certificate Issuance & Right to Use Licence), the certified organization acquires the right to maintain a proof of conformity. This is issued with a 3-year validity and may be used as confidence-building evidence as a reference to third parties.

Furthermore, if desired, CIS customers are listed for ISO 20000-1 on the APMG homepage.

Every management system or data center is exposed to constant and rapidly progressing organizational and technological changes, which make adjustments and improvements necessary.



Surveillance audits therefore determine how these changes are handled and the effectiveness of the entire management system or data center. If the surveillance audit is successfully completed, the continued use of the existing certificate will be applied for. Two surveillance audits are carried out at 12-month intervals until the certificate expires after three years.

The validity of the certificate must be renewed after 3 years. A full recertification audit to the extent of a Stage 2 audit is therefore required. The 3-year right to use the CIS certificate and the CIS conformity mark can be acquired again through successful recertification.

3 Explanations of the certification process

3.1 APPLICATION FOR CERTIFICATION

An offer will be prepared on the basis of the application.

(see document no. d012e for ISO 27001 and sub-standards, d013e for ISO 20000-1, d066e for ISO 22301)

If an integrated offer for Quality Austria and CIS services is desired, the document "Request for quotation for certifications CIS-QA d139e" can be used.

3.2 ORDER

An order is concluded by returning the signed copy of the quotation or order.

3.3 SYSTEM & RISK REVIEW - AUDIT STAGE 1

The Stage 1 audit takes place at your site or as a remote audit.

The purpose of this audit is a practical examination of the standard requirements. The focus here is to determine the status of a risk analysis that has already been carried out or to provide indications and approaches for carrying out a corresponding risk analysis in the company. The "System & Risk Review" is carried out together with those employees who take on or are responsible for coordination and control tasks in relation to the company's information security / service management / business continuity / data protection. The intention of the System & Risk Review is to assess the company-related interpretation of the standard requirements on the basis of risk analyses and assessments which have been carried out, as well as concrete measures and precautions.

The CIS Office will inform you about the CIS employees who will carry out Stage 1. The employees will contact you to arrange an appointment.

A written report on the results of Stage 1 will be prepared and submitted to you.

3.4 CERTIFICATION AUDIT - STAGE 2 AUDIT

After positive results at Stage 1, Audit Stage 2 follows.

Audit Stage 2 takes place at your company.

The CIS Office will inform you about the names of the auditor team, and in justified cases you can raise objections (against individual team members).

If you agree to the team of auditors, the lead auditor will arrange an audit appointment with you.

The CIS certification audit for management systems covers the practical measures for the complete verification of the standard requirements. Special focus is placed on ensuring that the systematic approach is traceable through multiple spot checks at all levels of the organization. The technology used is relevant to the extent that it significantly influences the organizational and management requirements.

A written report will be prepared on the result of Stage 2 and brought to the client's knowledge.

If deviations are identified, these must be rectified and the measures implemented must be reported.

If deviations are identified that cannot be resolved by the subsequent submission of documents, Stage 2 will be repeated.

After positive completion of Stage 2, the audit team leader makes a recommendation to CIS GmbH to provide the certificate.

3.5 ISSUE OF CERTIFICATE

After a positive evaluation of the report and any possible settlement of deviations, the certificate will be issued by CIS GmbH. The validity of the certificate is calculated from the date of the decision by the CIS management.

3.6 ANNUAL SURVEILLANCE (CONDITIONS FOR MAINTENANCE)

The monitoring date is always the date of the Stage 2 audit. The CIS Office will inform you about the appointed auditor 3 months before the date of the monitoring audit. The auditor will contact you and arrange an appointment.

As part of the surveillance, the handling of changes and the effectiveness of the entire management system will be determined.

In the case of data center certifications, the maintenance of the determined technical availability class, energy efficiency capability and the determined level of physical and environmental security are reviewed.

A report will be drawn up on the results. If deviations are found, you must remedy them and demonstrate the measures taken to the CIS auditors in an appropriate manner. In the event of deviations that cannot be resolved by the subsequent submission of documents, a follow-up audit will be carried out on site. In the case of management system certificates, the auditor will

recommend the continuation of the certificate to CIS GmbH following the positive conclusion of the surveillance audit. If deviations are not rectified on time, the certificate will be withdrawn.

3.7 SPECIAL FEATURES REGARDING ENWG §11

The conformity check according to §11 1a is carried out on the basis of the IT security catalog according to EnWG §11 1a of the Federal Network Agency, considering the conformity assessment program according to EnWG §11 1a.

The conformity check according to §11 1b is performed on the basis of the IT security catalog according to EnWG §11 1b of the Federal Network Agency, taking into consideration the conformity assessment program according to EnWG §11 1b.

In conjunction with an audit in accordance with the Energy Industry Act §11, the case of withdrawal is reported immediately by CIS to the Federal Network Agency (e-mail to it-sicherheitskatalog@bnetza.de).

The certification body sends the Federal Network Agency a list of the companies that have received a certificate. The list is transferred on June 30 and December 31 of each year.

3.8 RE-CERTIFICATION

After 3 years, a re-certification audit will be performed to the same extent as a Stage 2 audit (see description in section Audit Stage 2)

3.9 CHANGES TO THE SCOPE OF THE CERTIFIED SYSTEMS:

Changes are handled in the same way as new certifications. Feedback from clients regarding organizational changes will be assessed by the management. It decides on the further steps that should be taken.

3.10 CHANGES TO THE CERTIFICATION REQUIREMENTS:

All certified customers will be notified by e-mail of any changes to the certification requirements, e.g. changes to the standards according to which certification was granted. If further information and explanations are required, these will be published on the homepage or by newsletter.

4 Other applicable documents

General Terms and Conditions for System Certification and Assessment of
CIS - Certification & Information Security Services GmbH (Document No. d007e - Download).

> ***Note 1:***
> ***The CIS certification process does not provide for suspension of certification.***

CIS certification process for systems (d011e) (EN-US)

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