



Comgroup GmbH, Certification Body for Information Security
following the ISO/IEC 27001

Certification Rules

General conditions and rules for the certification of Information Security
Management Systems (ISMS) following the ISO/IEC 27001

As of date: 30.01.2012

Version 1.3



Table of Contents

1. General.....	3
2. Scope	3
3. Certification Process	3
3.1 Prerequisites.....	3
3.2 Process.....	3
3.3 Modular Certification.....	6
4. Use of Certificate	7
5. CCSEC Responsibilities.....	8
6. Client Responsibilities.....	8
7. Appeal Process.....	9
8. Witness Audits by the Accreditation Body	9
9. Taking Effect.....	9



1. General

The Certification Center Security (CCSEC) of Comgroup GmbH (CCSEC) was accredited under the DIN EN 45012 and EA 07/03 by the German Council of Accreditation (TGA) under the DAR-Registration Number TGA-ZM-10-99-20. CCSEC offers interested enterprises services for certification of their ISMS following the ISO/IEC 27001.

2. Scope

The audit and certification organization establishes the certification of ISMSs following the ISO/IEC 27001 by CCSEC.

3. Certification Process

3.1 Prerequisites

With the written acceptance of offer attached to this document as an attachment:

- The client, hereafter referred to as “client” enters into a contract for certification with CCSEC.
- Simultaneously submits the certification order.
- Confirms that no other certification body has been authorized to perform this certification.
- Accepts the terms and conditions for the certification.

3.2 Process

The certification process based on the DIN EN 45012 is divided into 6 phases:



Phase 1: Workshop

The workshop serves as an instrument to acquaint the clients' certification representative with the requirements of the ISO/IEC 27001, to afford the auditors the opportunity to learn about the enterprise and to explain the certification body's interpretation of the standard. During this workshop, the client learns the expected actions of the certification body as well as the basic requirements necessary to continue the process. After the workshop, the client has the opportunity to halt the process without further costs being incurred. In this case, the client will only be invoiced for the costs of the workshop.

Phase 2: ISMS Development and Implementation

The client conducts a structured risk analysis. Herewith, the materialistic and idealistic assets are determined and their vulnerabilities analyzed. In a subsequent step in this process, the determination of appropriate measures necessary to reduce or mitigate these vulnerabilities under consideration of the ISO/IEC 27001 is made, implemented and documented.

The documentation must include at least the following:

- General documentation pertaining to the ISMS framework.
 - Management's statement of information security policy.
 - Definition of the scope.
- Documentation pertaining to the Risk analysis.
 - A description of the methodology utilized for the risk analysis.
 - The results of the risk analysis.
 - The plan to manage the risks.
- Documentation pertaining to the IS process.
 - The description of the process for the implementation and maintenance of the ISMS.
 - Relevant security records.
 - The process and procedures of the ISMS handbook.
 - Statement of applicability for the requirements of the standard. (Annex A)



Phase 3: Desktop Review

The client provides the documented ISMS to CCSEC. The lead auditor then examines the documentation as to its conformity to the ISO/IEC 27001. The discrepancies to the standard are then documented in the form of a non-conformity report which is returned to the client. Should the ISMS contain no discrepancies or non-conformities or the discovered non-conformities are of a minor nature and would not preclude the client from becoming certified, then an audit can be conducted. The presentation of revised documentation to CCSEC before the audit is not required in this case. With major non-conformities, the client has eight weeks time to correct these, revise their documentation accordingly and present them to the certification body. Only then, when there are no longer major non-conformities detected, can the audit be conducted. Should the eight week time limit be exceeded, CCSEC will temporarily discontinue the certification process and invoice the to-date incurred costs to the client. A resumption of this process can be requested by the client within a half-year of the date of the non-conformity report when the required documents are simultaneously provided. In this case, the desktop review will be conducted in its' entirety. After the expiration of the half-year period from the date of the non-conformity report, the certification process will be permanently terminated. If required, a new certification process is to be requested.

Phase 4: Certification Audit

The lead auditor sends an audit plan to the client approximately two weeks before the commencement of the certification audit. This includes information as to the activities to be accomplished as well as the agenda. The client then reviews this as to the feasibility and can indicate proposed changes that can be considered for by the certification body if possible or feasible.

It is the client's responsibility to demonstrate the applicability of their documented process and prove the effectiveness of the measures during the course of the audit. The client will be informed as to the results of the audit during the course of a closing meeting.

Phase 5: Report Preparation and Certificate Issuance

The certification body will forward the client the noted deficiencies in a non-conformity report within two weeks upon conclusion of the audit. If no deficiencies were noted or those that were noted are only of a minor nature and would not prevent the certification, then the client notifies the lead auditor (in writing) within two weeks as to which measures have been implemented or will be implemented to eliminate them. Thereupon, the lead auditor recommends the issuance of the certificate and a follow-on audit is not necessary in this case.



With major non-conformities, the client has eight weeks time eliminate them, correct the documentation appropriately and submit the changed version to the certification body. After the expiration of this time limit, a follow-on audit will have to be conducted within the next four weeks that focuses on those areas where the major non-conformities were noted. Only after the auditors determine there are longer any major non-conformities, can the recommendation be made to issue the certificate.

Should the two (by minors) or the eight (by major) week time-limits be exceeded by the client, then CCSEC will temporarily terminate the certification process and invoice the to-date incurred costs to the client. A resumption of this process can be requested by the client within one half-year from the date of the non-conformity report as long as the required documents are simultaneously provided. In this case, a complete new certification audit must be conducted. If necessary, a new certification process request may be required.

Upon a successful examination of the documentation for the certification process, the head of the certification body will issue the certificate. The certificate will only be issued after all major non-conformities have been eliminated.

Phase 6: Monitoring

The validity period of the certificate is three years as long as a monitoring control measures is conducted at the clients' location each year. This can be in the form of a desktop review or through a follow-on audit. The determination hereof is made by the head of the certification body based on the currently attained project documentation. Upon expiration of the certificate, a re-certification audit will be conducted. During the year in which the re-certification audit is conducted, there are no monitoring measures required. To maintain the certificate, the same rules apply as for the initial certification.

3.3 Modular Certification

CCSEC created the modular certification in order for clients to display their current accomplishments should they experience delays with the entire certification process. Accordingly, an interim certificate (Level 1) can be issued after the evaluation of a structured risk analysis by CCSEC. This serves as the proof that the client has conducted a risk analysis which is standard-conform and hence is aware their risks. At this point, the described documents in Phase 2 "General documentation pertaining to the ISMS framework and "Documentation pertaining to the risk analysis" exist.



Another interim certificate (Level 2) can be issued when Phase 3 is completed. This certificate verifies (dependant upon the documentation) that the client has documented and standard-conform ISMS.

The thrid certificate (Level 3) can be issued when all of the requirements of the ISO/IEC 27001 are fulfilled (i.e. after Phase 4 and 5). This certificate equates to an accredited certificate and verifies that the client has established and implemented a standard-conform ISMS.

The interim certficates for Level 1 and 2 are not subject to an accreditation, are not conform with the DIN EN 45012 and accordingly do not include the usual accreditation characteristics. The deadlines for elimination of non-conformities within the individual phases as well as the necessity to conduct follow-on audits for the retention of the certificate apply analogue to the modular approach. As long as the certificates for Level 1 or 2 (through follow-on audits) are maintained, no other additional time requirements must be met for the completion of further steps. The completion of the entire certification process can be continued at any time.

4. Use of Certificate

The clients' right to use the certificate, for example – marketing purposes, is limited to the scope as indicated on the certificate.

A certificate expires when:

- The period of validity indicated on the certificate is exceeded by six months (tolerance period).
- The client waives or renounces the certificate before the end of the expiration period indicated thereon.
- The certification contract is terminated by one of the parties specified therein within the period of notice.
- The basic established rules that govern the certificate are changed or other rules are to be applied, i.e. based on the changed use thereof.

A certificate can be rescinded by the certification body when:

- Major non-conformities are determined.



- The client denies or hinders the certification body or its entity in the examination of the ISMS.
- Misleading or inappropriate advertising is conducted in conjunction with the certificate.
- Based on facts, that at the time of certificate issuance was not known and would rule out certification.

The certification body can publicize the termination or the cancellation as it so chooses.

The certification body is entitled to inform the regulatory authorities, the accreditation bodies, other certification bodies and the statutory approval bodies of the termination or the cancellation of certificates.

The certification body is not responsible for any disadvantages or inconveniences the client incurs resulting from failure to issue, the termination or the cancellation of a certificate.

5. CCSEC Responsibilities

CCSEC obliges itself to treat all information provided about the client's enterprise confidentially and only to analyze it for the contractually agreed purposes. Documents made available will not be given to third parties. Excluded, is the detailed report provided to the arbitration board during disputes. The client can release the certification body from its responsibility of confidentiality.

Supplemental to our general business conditions and as necessary contract requirements, the liability for cases deliberate acts or gross negligence of CCSEC to the client or third parties is limited to the minimal legal requirements. Additional claims are excluded. This applies particularly for the execution of network analysis measures.

6. Client Responsibilities

The following client responsibilities are to be fulfilled before, during and after the certification process:

- Providing an appropriate work space for the auditors during the audit.
- Providing the appropriate network accesses to conduct network analyses.

- Providing competent interviewees during the interviews.
- Providing the required documentation.

7. Appeal Process

The client can object to the auditors scheduled to conduct the audit before the onset thereof. These will be announced by CCSEC approximately two weeks before the onset of the audit. In the event the client objects to one or more auditor, the head of the certification body will determine if alternatives are possible, rather if the audit can still be conducted. Afterwards, he will discuss further courses of action with the client. The contractual legal consequences are derived from the provisions of law.

The client can also object to or file grievance against to the certification body for other unsatisfactory decisions of the certification body in conjunction with the certification process. The certification body then explains the decision to the client, as much as necessary, in detail and if required, with reference to the appropriate portions of the project documentation.

Should the certification body's explanation seem inapplicable or unacceptable to the client, then they can file a complaint to the steering committee of the certification body. The steering committee makes the final decision.

8. Witness Audits by the Accreditation Body

As required, the client accepts the fact that inspectors from the German Council for Accreditation (TGA) may accompany certification body auditors in conjunction with witness audits.

9. Taking Effect

These certification rules take effect on 1 January 2006 and are subject to a change management process. The date and version can be found on the first page of this document. In each case, the current version is relevant from the time of contract negotiation. The rules for certification apply to all proceedings within the individual timeframe of validity which have been started by CCSEC.



Future changes to issued certificates or currently executed proceedings can only be made after written permission from the client.

A handwritten signature in black ink, appearing to read "M. Tomas". The signature is fluid and cursive, with a long horizontal stroke extending from the end of the name.

Michael Tomas, LL.M.

Head of Certification Body