Würth IT 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: 01.11.2015

Version 1.7

Table of Contents

1. General

The Certification Center Security (ccSec) of Würth IT GmbH was accredited under the ISO/IEC 17021:2011 under the case number ZM-18926-01 by the Deutsche Akkreditierungstelle GmbH (national accreditation body for the Federal Republic of Germany) also referred to as “DakkS”. ccSec offers interested enterprises services for certification of their ISMS following the ISO/IEC 27001:2013.

2. Scope

The audit and certification rules establishes the certification of ISMSs following the ISO/IEC 27001:2013 by ccSec.

3. Certification Process

3.1 Prerequisites

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

- The organization, hereafter referred to as “organization” 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 ISO/IEC 17021:2011 is divided into the following phases:

Phase 1: Customer Dialog

The customer dialog serves as an instrument to acquaint the organizations’ certification representative with the requirements of the ISO/IEC 27001:2013, to afford the auditors the opportunity to learn about the enterprise and to explain the certification body’s interpretation of the standard from the certification body’s point-of-view presented as a training measure. Furthermore, the required audit effort will be recorded and calculated.
Hereby, the organization is made aware of the expectations of the certification body and thus a basis for deciding to continue the certification process. After the customer dialog, the organization has the opportunity to opt-out of the process without incurring any additional costs.

Phase 2: ISMS Development and Implementation

The organization 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 27001:2013 is made, implemented and documented.

The documentation must include at least the following:

- Management's statement of information security policy.
- Definition of the scope.
- The process and procedures of the ISMS handbook.
- A description of the methodology utilized for the risk analysis.
- The results of the risk analysis.
- The plan to manage the risks.
- The description of the process for the implementation and maintenance of the ISMS.
- Relevant security records. (i.e. results from the internal audit or from the management assessment)
- Statement of applicability for the requirements of the standard. (Annex A)

Phase 3: Desktop Review

The organization provides the documented ISMS to ccSec. The lead auditor then examines the documentation as to its conformity to the ISO/IEC 27001:2013. The discrepancies to the standard are then documented in the form of a non-conformity report which is returned to the organization. Should the ISMS contain no discrepancies or non-conformities or the discovered non-conformities are of a minor nature and would not preclude the organization 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 organization has 8 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 8 week time-limit be exceeded, ccSec will temporarily discontinue the certification process and invoice the to-date incurred costs to the organization. A resumption of this process can be requested by the organization 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 organization approximately 2 weeks before the commencement of the certification audit. This includes information as to the activities to be accomplished as well as the agenda. The organization 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 organization's responsibility to demonstrate the applicability of their documented process and prove the effectiveness of the measures during the course of the audit. The organization 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 organization the noted deficiencies in a non-conformity report within 4 weeks upon conclusion of the audit.

All non-conformities must be analyzed by the customer in order to determine the cause thereof (root cause analysis). The results are documented and communicated to the certification body.

If no deficiencies were noted or those that were noted are only of a minor nature and would not prevent the certification, then the organization notifies the lead auditor (in writing) within 2 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 organization has 8 weeks' time to 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 conduct within the next 4 weeks that focuses on those areas where the major non-conformities were noted. Only after the auditors determine there are no longer any major non-conformities, can the recommendation be made to issue the certificate.

Should the 2 (by minors) or the 8 (by major) week time-limits be exceeded by the organization, then ccSec will temporarily terminate the certification process and invoice the to-date incurred costs to the organization. A resumption of this process can be requested by the organization 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 monitoring control measures are conducted at the organizations' location each year. The monitoring control measures are performed with a follow-on audit on location. 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.

4. Use of Certificates and Symbols

The organizations' right to use the certificate, for example – marketing purposes, is limited to the scope as indicated on the certificate. Furthermore; with the usage, the association and traceability to the certification body must be proven. There should be no ambiguity regarding the scope and the certification body which granted the certification included in symbols or in the accompanying text. The symbol of the certification body must not be used on products or product packaging that can be seen by consumers or used in any other way that could be interpreted as labeling or marking for product compliance.

The organization is committed to:

- Fulfilling the requirements listed here with a reference to its certification status in communication media.
- Not making or permitting any misleading statements regarding the certification.
- Not allowing the misleading use of certification documents or permitting any parts thereof to be used in a misleading manner.

- Discontinuing the use of all promotional materials, which contain references to the certification status after termination, suspension or withdrawal of certificate.
- Modifying the promotional and marketing materials accordingly in conjunction with a reduction or change in the scope of the certification.
- Allowing any reference to the management system certification, which without comment, could tacitly imply that the certification body certifies a product (including services), or a process which does not imply that the certification applies to activities that are outside the scope of certification.
- Not utilizing the certification in a manner that brings the certification body and / or the certification system into disrepute and loss of public trust.

A certificate expires when:

- The period of validity indicated on the certificate is exceeded.
- The organization waives or renounces the certificate before the end of the expiration period indicated thereon.
- The certification contract is terminated by the organization.
- 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 organization denies or hinders the certification body or it's 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 expiration or the withdrawal 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 organization incurs resulting from failure to issue, the termination or the cancellation of a certificate.

A certificate may be suspended when:

- The certification requirements, including the requirements for the effectiveness of the ISMS, permanently or seriously are not fulfilled.
- The customer does not allow or permit the performance of monitoring or re-certification audits.
- The certified organization has voluntarily requested a suspension.

In the event of suspension of the certificate, the ISMS is temporarily suspended. Accordingly, the organization may not continue to advertise, promote or publish its certification.

The causes which have led to the suspension of the certificate, not resolved or corrected within defined period assigned by the certification body, this leads to a withdrawing or reducing the scope of certification. The restriction of the scope excludes those parts which do not meet the requirements and are in compliance with the requirements of the standard used for certification.

The certification body is authorized to publish the suspension of certification and more, as is deemed appropriate to take action.

5. ccSec Responsibilities

ccSec obliges itself to treat all information provided about the organization'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 organization can release the certification body from its responsibility of confidentiality.

Changes to the certification requirements will be announced to the organization in due time.

Supplemental to our general business conditions and as necessary contract requirements, the liability for cases of deliberate acts or gross negligence of ccSec to the organization or third parties is limited to the legal minimum requirement in the event of intent or gross negligence. Additional claims are excluded. This applies particularly for the execution of network analysis measures.

6. Organization Responsibilities

The following organization 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 interview partners during the interviews.
- Providing the required documentation.
- Comply with new certification requirements (in the event of changes)
- Notification of change pertaining to:
    - The laws or form of economic organization or ownership.
    - Organization and management.
    - Contact addresses and locations.
    - The documented field of activity or trade.
    - Significant changes to the management system as well as their processes.

7. Appeal Process

The organization can object to the auditors scheduled to conduct the audit before the onset thereof. These will be announced by ccSec approximately 2 weeks before the onset of the audit. In the event the organization 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 organization. The contractual legal consequences are derived from the provisions of law.

The organization 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 organization, 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 organization, 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 organization accepts the fact that inspectors from the National Accreditation Body for the Federal Republic of Germany (DAkkS – Deutsche Akkreditierungsstelle) may accompany ccSec auditors in conjunction with witness audits.

9. Taking Effect

These certification rules take effect on 1 January 2015. They apply to all certificates issued within the individual timeframe of validity by ccSec. Future changes to issued certificates or currently executed proceedings can only be made after written permission from the organization.

Ulrike Schröder

Head of Certification Body