certification rules for the certification of an Information Security Management System (ISMS) ISO/IEC 27001 and IT- security catalog

1 General information

The certification body of Würth IT GmbH has been accredited by the German Accreditation Body, Deutsche Akkreditierungsstelle (DAkkS) according to the current ISO/IEC 17021 under the procedure number D-ZM-18926-01-00. The certification body of Würth IT GmbH offers interested companies its services for the certification of their ISMS according to ISO/IEC 27001:2022 Information security, cyber security and data protection - Information security management systems - Requirements according to DIN EN ISO/IEC 27006:2021 and according to IT security catalog according to § 11 paragraph 1a Energy Industry Act on the basis of the conformity assessment program for the accreditation of certification bodies for the IT security catalog (for network operators) of the Federal Network Agency of 12.01.2023 in the divisions:
- Electricity grid operator
- gas network operator.

See also our accreditation certificate on the website www.ccsec.de in the download area.

2 Scope pf application

These testing and certification regulations govern the certification of ISMS in accordance with ISO/IEC 27001:2022 and the IT security catalog pursuant to Section 11 (1a) EnWG by the certification body of Würth IT GmbH.

3 Certification procedure

3.1 Requirements

By written acceptance of the offer,

- the client, hereinafter referred to as the organization, concludes a certification contract with the certification body of Würth IT GmbH
- at the same time it issues a certification order
- it declares that no other certification body has been appointed to carry out the same procedure

- it accepts these certification conditions.

3.2 Procedure

The certification process based on ISO/IEC 17021 is divided into the following phases:

3.2.1 Phase 1: Customer meeting

The purpose of the customer meeting is to inform the organization's certification officer about the requirements of ISO/IEC 27001:2022, to provide the internal or external auditors with information about the company and to present the interpretation of the standard from the certification body's perspective. Furthermore, the required audit effort is calculated and recorded accordingly.

In the process, the organization gains knowledge of the expectations of the certification body and thus also a basis for deciding whether to continue with the procedure. After the customer meeting, the organization has the option of withdrawing from the procedure without incurring additional costs.

The customer meeting can also be replaced by the Application for certification form.

3.2.2 Phase 2: Development and implementation of the ISMS

The organization carries out a structured risk analysis. This involves recording its tangible and intangible assets and analyzing them for weaknesses. In a further step, the organization draws conclusions from this and implements them in the form of appropriate measures.

These measures are introduced in accordance with ISO/IEC 27001:2022 and documented accordingly.

The documentation must include at least the following items:

- The statements of the management in the information security policy
- The definition of the scope
- The procedures and regulations of the ISMS manual
- The description of the methodology used for risk analysis
- The results of the risk analysis
- The plan for dealing with risks
- The description of the process for implementing and maintaining the ISMS
- Safety-related records (e.g. results from internal audit or management reviews)
- Declaration on the applicability of the regulations required by the standard (Annex A)

3.2.3 Phase 3: Desktop Review

The organization explains the ISMS during an on-site audit and submits the documentation to the Würth IT GmbH certification body. The lead auditor then checks the documentation for conformity

with ISO/IEC 27001:2022. The deviations are recorded in a deviation report, which is then sent back to the organization. If no deviations are found or if the deviations found are only minor, i.e. deviations that would not make certification impossible, the audit can take place. It is not necessary to submit the revised documents before the audit. In the case of major non-conformities, the organization has 8 weeks to rectify them, revise the documentation accordingly and submit the revised version to the certification body. The audit may only be carried out once the certification body no longer identifies any significant non-conformities. If the 8-week period is exceeded, the certification procedure will be temporarily closed by the certification body of Würth IT GmbH and the expenses incurred up to that point will be invoiced to the organization. The organization can apply for the procedure to be resumed within six months of the date of the non-conformity report if it submits the required documents at the same time. In this case, the desktop review will be carried out again in full. After the six-month period from the date of the non-conformity report has elapsed, the procedure is definitively closed. If necessary, a new procedure would then have to be applied for.

3.2.4 Phase 4: Certification audit

The lead auditor sends out an audit plan approximately 2 weeks before the start of the certification audit. This contains information about the activities to be carried out and the time schedule. The organization then checks the feasibility and can then submit any change requests, which are then taken into account depending on the possibility and feasibility.

During the audit, the organization is required to demonstrate the practical application of its documented procedures and to demonstrate the effectiveness of its implemented measures. At the end of the audit, the organization is informed about the results of the audit in a final meeting.

3.2.5 Phase 5: Reporting and certificate issuance

Following the audit, the non-conformities are recorded in a non-conformance report, which is then sent to the organization within 4 weeks.

All detected non-conformities must be analyzed by the customer for their causes (root cause analysis). The results must be documented and communicated to the certification body.

If no non-conformities were found or if the non-conformities found are only minor, i.e. non-conformities that would not make certification impossible, the organization shall inform the lead auditor in writing within a further two weeks about the measures it will implement or has already implemented to eliminate the non-conformities. Thereupon, the lead auditor recommends issuing the certificate. A post-audit is not necessary in this case.

In the case of significant non-conformities, the organization needs to eliminate them, revise the documentation accordingly and submit the revised version to the certification body within 8 weeks. After expiry of this time, a post-audit is carried out within a further 4 weeks, which is limited to the

areas in which the significant non-conformities were detected. Only when the auditors no longer find any significant non-conformities may the issuance of the certificate be proposed.

If the 2-week (in the case of minor non-conformities) or 8-week (in the case of major non-conformities) deadline is exceeded by the organization, the certification procedure is temporarily closed by the certification body of Würth IT GmbH and the expenses incurred up to that point are settled with the organization. A resumption of the procedure can be requested by the organization within six months from the date of the non-conformance report, if it submits the required documents at the same time. In this case, the certification audit is carried out again in full. After the expiry of the six-month period from the date of the non-conformance report, the procedure is finally closed. If necessary, a new procedure would then have to be applied for.

After a positive review of the documentation of the certification procedure, the certificate is issued by the head of the certification body or their deputy. The decision is based on the assessment of the audit findings and conclusions as well as other relevant information. The certificate is only issued if all significant non-conformities have been resolved.

The ownership of the audit report and the certificate(s) remains with the certification body.

3.2.6 Phase 6: Monitoring

The certificate is valid for three years if an annual surveillance audit is carried out at the organization. In the case of initial certification, the first surveillance audit must take place within 12 months. The surveillance measure must be carried out by means of an on-site audit. After the certificate expires, a recertification audit is carried out. No further surveillance measures are required in the year in which the re-certification audit is carried out. The rules for initial certification apply analogously to the maintenance of the certificate.

Monitoring activities may include:

- Enquiries from the certification body to certified customers on aspects of certification;
- Evaluation of the information provided by the organization with regard to its activities;
- Requests to the organization to provide documents and records; and
- other measures of monitoring the performance of the certified organization.

4 Use of the certificate and mark

The organization's authorization to use the certificate, for example for marketing purposes, is limited to the scope specified in the certificate. Furthermore, traceability to the certification body must be ensured during use. There shall be no ambiguity in the mark or accompanying text regarding the scope and the certification body that granted the certification. The mark of the certification body shall 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 a mark of product conformity.

The organization undertakes to:

- comply with the requirements set out herein when referring to its certification status in communication media;
- not make or permit misleading statements regarding the certification;
- not use or permit the use of certification documents or parts thereof in a misleading manner;
- in the event of suspension or withdrawal of the certification, to stop the use of all promotional materials containing references to the certification status;
- amend the promotional material accordingly, if the certification scope is reduced;
- not allow any reference to the management system certification which might imply that the certification body is certifying a product (including a service) or a process, or does not imply that the certification applies to activities outside the certification scope;
- not use marks of the certification body on laboratory test reports, calibration certificates, inspection reports or certificates;
- not use the certification in a way that brings the certification body and/or the certification system into disrepute and that leads to a loss of public confidence.

A certificate expires when

- the period of validity stated in the certificate has been exceeded,
- the organization renounces the certificate before the expiry of the validity period stated in the certificate,
- the certification contract is terminated by the organization,
- the provisions on which the certificate is based have been changed or other provisions are applicable, e.g. due to a change in use.

A certificate may be revoked by the certification body if

- major non-conformities are found,
- the organization does not allow or obstructs the agreed audits of its ISMS by the certification body or its appointed auditing body,
- misleading or otherwise inadmissible advertising is carried out in connection with the certificate,
- due to facts that would prevent a certification and that were not apparent at the time the certificate was issued.

The certification body may publish the expiry or withdrawal at its own discretion.

The certification body is entitled to inform the supervisory authorities, the accreditation bodies, other certification bodies and the licensing authorities about the expiry or withdrawal of certificates.

The certification body shall not be liable for any disadvantage suffered by the organization as a result of the non-issuance, expiry or withdrawal of a certificate.

A certificate may be suspended if

- the certification requirements, including the requirements for the effectiveness of the ISMS, are persistently or seriously not met,
- the certified organization does not allow the surveillance or re-certification audit to be carried out,
- the certified organization has voluntarily requested a suspension.

In case of suspension of the certificate, the management system certification is temporarily suspended. In this case, the organization is prohibited from continuing to advertise its certification.

If the causes which led to the suspension of the certificate are not resolved within a period of time specified by the certification body, this will result in the withdrawal or restriction of the scope of the certification. The restriction of the scope excludes those parts which do not meet the requirements and is in accordance with the requirements of the standard used for certification.

The certification body is entitled to publish the suspension of certification and to take any further action deemed appropriate.

The certification body publishes the name, scope, geographic location (city and country), status of the certification and a link to the website of the certified customers on its Certification Center Security website, in short ccSec.

5 Duties of the certification body of Würth IT GmbH

The certification body of Würth IT GmbH undertakes to treat all provided information about the customer's company confidentially and to evaluate it only for the agreed purpose. Documents made accessible will not be passed on to third parties. Excluded from this is the detailed reporting to the arbitration board in cases of dispute. The customer may release the certification body from this obligation for specific reasons.

Changes to the certification requirements will be communicated to the organization in a timely manner.

In addition to our General Terms and Conditions and as a necessary contractual condition, the liability of the certification body of Würth IT GmbH towards the organization or third parties is limited to the statutory minimum claim in the event of intent or gross negligence. Further claims are excluded. This applies in particular to the conduction of network analysis measures.

6 Duties of the organization

The following obligations shall be fulfilled by the organization before, during and after the certification procedure:

- Provision of suitable workplaces for the auditors during the audits
- If necessary, provision of suitable network access for the performance of network analyses
- Provision of competent interview partners during the interviews
- Provision of the necessary documentation
- Compliance with new certification requirements (in case of changes)
- Notification of changes regarding
    - the legal or organizational form, the economic conditions or the ownership structure
    - organization and management
    - contact addresses and locations
    - the field of activity covered
    - significant changes to the management system and processes

7 Opposition procedures

Prior to the audit, the organization can object to the auditors to be used during the audit. These will be communicated to the organization by the certification body of Würth IT GmbH approx. 2 weeks before the audit. If the organization objects to one or more auditors, the LC checks if alternatives are available or the audit can still be performed. The LC then discusses the further procedure with the organization. For consequences under contract law, legal provisions apply.

The organization may also appeal against other unsatisfactory decisions of the certification/registration body in the certification/registration process carried out. The certification body shall then provide the organization with detailed reasons for its decision, if it has not already done so, with references to the relevant parts of the project documentation, if applicable.

If the justification given by the certification body is not comprehensible to the organization or if the organization does not accept it, it may lodge an appeal with the steering committee of the certification body. The steering committee then makes the final decision.

8 Witness audits by the accreditation body

If necessary, the organization tolerates the accompaniment of the certification body of Würth IT GmbH auditors by assessors of the DAkkS (Deutsche Akkreditierungsstelle, German Accreditation Body).

9 Entry into force

These certification rules come into force on 27.11.2023 They apply in principle to all certificates issued by the certification body of Würth IT GmbH during the period of validity. Future changes can only be applied to existing certificates after written agreement of the holders.

Ulrike Schröder

Head of certification body Würth IT GmbH, ccSec