INTO

CERTIFICATION

Service Description

Public

Contents

1. Into Certification Oy

Into Certification Oy is a FINAS (Finnish Accreditation Service) accredited certification body providing information security certification audits. Into Certification acts as an accredited certification body and as an Information Security Inspection body (*Finnish: Tietoturvallisuuden arviointilaitos*) approved by Traficom.

Accreditation information can be found online:

- FINAS accreditation service (S064)
- Traficom's list of approved information security inspection bodies

Into Certification is an independent company owned by Into Security Oy. Into Certification is headquartered in Finland and provides information security certification services globally.

1.1. Certification audit services

Into Certification provides certification audit services as an accredited certification body and information security inspection body against the following criteria:

- ISO/IEC 27001:2022
- Katakri 2020 TL IV & TL III
- Health care system audits:
  - *Sosiaali- ja terveydenhuollon tietojärjestelmät ja hyvinvointisovellukset* (Asiakastietolaki 703/2023)
- Findata Toisiolaki – Act on Secondary Use of Health and Social Data

In addition to the accredited management system and information security inspection body audit services, Into Certification can provide audits on

- Payment Card Industry Data Security Standard as an approved PCI QSA (Qualified Security Assessor) Company
- Finnish Trust Network / eIDAS strong identification service audits
- Microsoft SSPA

2. Policy on impartiality and independence

2.1. Safeguarding impartiality

Into Certification's management and auditors are committed to ensure independence and impartiality, and that commercial, financial or other pressure cannot affect the results of information security assessments and certifications. The commitment includes the following:

- The results of the audits are based only on objective evidence on how the assessed organization meets the certification criteria.
- Into Certification's audits, operations and organizational structure are independent.
- Prior to every audit, possible risks for independence and impartiality are assessed and minimized as appropriate.
- Into Certification does not certify organizations that could cause uncontrollable risk for independence and impartiality.
- Into Certification does not certify other certification bodies.
- Into Certification does not perform internal audits to certified customers.

Into Certification has appointed an impartiality committee to safeguard its independence and impartiality by assessing its operations annually.

2.2. Conflicts of interest

Into Certification may carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) arrange and participate as a lecturer in training courses related to information security management, information security management systems or auditing by confining to the provision of generic information and advice. Into Certification does not provide company specific advice which contravenes the point b) below:

b) make available or publish information describing the certification body's interpretation of the requirements of the certification audit standards or criteria,

c) conduct activities prior to audit (e.g. pre-audits) which are solely aimed at determining readiness for certification but not at providing recommendations or advice used to justify a reduction in the eventual certification audit duration,
d) add value during certification audits and surveillance visits, e.g., by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

2.3. Confidentiality

Into Certification is responsible for the management of all information obtained or created during the certification activities. The responsibility is ensured by the legally enforceable certification agreements. Maintaining confidentiality of information concerns both internal and external personnel as well as committees at all levels of the certification body. If law or authorization by contractual agreements requires releasing confidential information, the client concerned is informed about the information provided, unless prohibited by law.

3. Certification process

ISO/IEC 27001 certification process is required to follow process guidelines set forth in the current version of ISO/IEC 17021-1 and ISO/IEC 27006 standard. This process is divided to two main stages: stage 1 and stage 2. After the initial certification, a three-year certification cycle begins with ongoing surveillance activities that include surveillance audits and recertification before the expiry of initial certification. The same audit process can be used in other standards unless there are standard specific requirements set for the process.

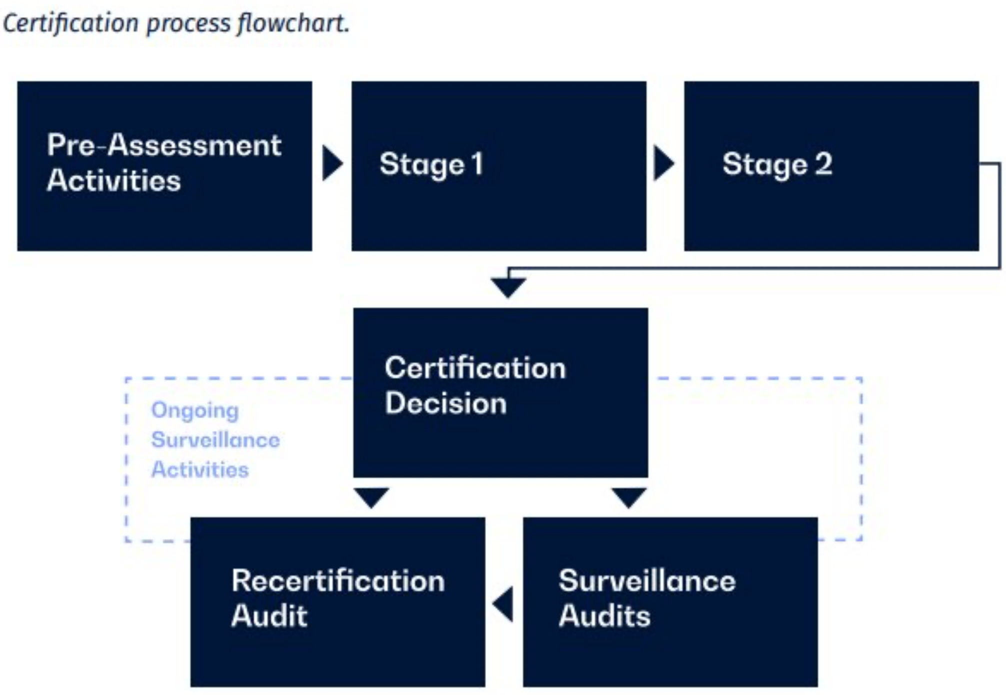
Certification process flowchart.
Pre-Assessment Activities
Stage 1
Stage 2
Certification Decision
Ongoing Surveillance Activities
Recertification Audit
Surveillance Audits

Figure 1 Certification process flowchart

The process flowchart is presented in detail in the following chapters.

3.1. Personnel used in audits

The audit team has an appointed Audit Team Leader, who works as a project manager in the assignment. In addition to the audit team leader, there may be other auditors, technical experts, trainee auditors and observers.

Certification decisions are made by Into Certification's Certification Officer. The Certification Officer is not involved in the audit activities. The Certification Officer may be assisted by independent and competent personnel in the decision making.

The following requirements apply to all auditors of the audit team except b), which can be shared among auditors of the audit team:

a) knowledge of information security,
b) technical knowledge of the activity to be audited,
c) knowledge of management systems,
d) knowledge of the principles of auditing,
e) knowledge of monitoring, measurement, analysis and evaluation of information security management systems.

Into Certification complies with the competence requirements set in ISO/IEC 17021-1 and ISO/IEC 27006 standards. It maintains competence criteria for evaluating personnel competence and identifying training needs. Into Certification monitors auditors' competence actively.

3.1.1. Use of external auditors and technical experts

Into Certification can use individual external auditors and technical experts in its audits according to conditions set forth in ISO/IEC 17021-1 standard. The key requirement is that the external personnel work under the supervision and responsibility of the Audit Team Leader. The use of individual external personnel does not constitute outsourcing. The same confidentiality and impartiality requirements defined above, apply to external personnel.

3.2. Pre-activities and audit programme

Certain mandatory steps are required before any audit assessments are conducted. The audit process begins with a certification application, followed by audit planning activities.

3.2.1. Application for certification

The certification audit process begins with client requesting it from Into Certification. The necessary information for the certification application is collected when Into Certification prepares an offer for certification services.

The client is required to deliver information related to certification including:

- desirable scope of the assessment,
- relevant information about the client organization from the perspective of the certification program which shall include at least the following:

  - Organization’s name, site addresses, relevant processes and operations, human and technical resources, functions, relationships, and any relevant obligations,
- information about outsourced processes,
- standards and other requirements on which the desired certification is based,
- information about any consultancy services undertaken and their providers related to the system to be certificated.

Into Certification conducts a review of the information provided for the application and evaluates the client’s preparedness for certification.

3.2.2. Audit programme

An audit programme for the full certification cycle is developed to clearly identify audit activities needed to demonstrate the client compliance of audit criteria. ISO/IEC 27001 certification audit programme includes a two-stage initial audit and surveillance activities. Surveillance activities contain two surveillance audits in the following two years, and recertification audit on a third year before the expiry of certification. Into Certification follows guidelines set in ISO/IEC 17021-1 and ISO/IEC 27006 in its audit and certification processes. The audit programme may vary based on the audited standard.

Any on-going surveillance activities are taken into consideration when developing and planning the audit programme.

Audit time is determined by experienced personnel and Audit Team Leaders regarding following information:

- the requirements of the audit standard or criteria in use,
  - For ISO/IEC 27001 the requirements from ISO/IEC 27006 are used when determining audit time
- complexity of the client and its management system,
- technological and regulatory context,
- any outsourced activities or functions related to assessment subject,
- the results of prior audits,
- size and number of sites, their geographical locations and multi-site locations,
- organizational risks of the client,
- whether audits are combined, joint or integrated.

The estimated audit time and its justification are recorded. Any significant deviations in audit scope related to estimated audit time is discussed with the client.

Where multi-site sampling is used for the audit of a client's management system covering the same activity in various geographical locations, Into Certification may develop a sampling programme to ensure proper audit of the management system.

3.3. Obtaining evidence and control of records

3.3.1. Audit methods

Into Certification uses multiple methods to obtain and verify audit evidence. These methods can include interviews, document review, process observations and technical testing. Depending on the standard used, the methods may be predetermined and standardized.

When applicable, sampling can be used to collect evidence and assess requirements. It should be noted that sampling always involves a certain level of uncertainty.

3.3.2. Control of client records

Into Certification has procedures for controlling client records related to audit and certification processes conforming with requirements. Records are maintained on the audits and other certification activities for all clients including those that have submitted applications and those that have been audited, certified or with certification suspended or withdrawn.

Records on certified clients include:

- application information and audit reports of initial, surveillance and recertification audits,
- certification agreements,
- justification for audit time determination,
- verification of correction and corrective actions,
- records of complaints and appeals and any subsequent correction or corrective actions,
- committee deliberations and decisions if applicable,
- documentation of the certification decisions,
- certification documents such as scope of certification,
- related records necessary to establish the credibility of the certification (evidence of the competence of auditors and technical experts),

- audit programmes.

All the relevant evidence relating to assessment results is retained for six years after the end of assessment operations.

3.4. Stage 1

The objectives of stage 1 are to:

- review the client's management system documented information,
- obtain necessary information regarding the scope including sites, processes, maturity of processes and management system implementation,
- obtain information regarding regulatory and statutory requirements,
- evaluate the planning and execution of internal audits and management reviews,
- determine the readiness for stage 2, and
- identify and resolve possible nonconformities.

A documentation review concerning client's ISMS is conducted and supplemented with interviews. The results of stage 1 are documented in a written report.

3.5. Stage 2

The purpose of stage 2 is to assess the implementation and effectiveness of the client's ISMS and to confirm that the client adheres to its own policies, objectives, and procedures. Stage 2 is conducted mainly on-site. On-site can also mean remote access to electronic systems that contain relevant information about the ISMS.

Stage 2 includes auditing of at least the following items:

- information and evidence about conformity to all requirements of the applicable management system standard or other normative documents,
- performance of the management system,
- operational control of processes,
- internal auditing and management reviews, and
- management responsibilities for policies,

The results of stage 2 are documented in a written report.

3.5.1. Nonconformities found in audit

Nonconformities may be identified during the audit. The grounds for granting a certificate differ in each standard and thus the required follow-up actions may vary. Typically, evidence of corrections and corrective actions are required to address nonconformities. Depending on the standard used the required actions and timeframe for corrective actions to achieve certification may be different.

3.6. Certification

Upon successful completion of the Stage 1 and Stage 2 audits, the audit process proceeds to certification decision.

3.6.1. Certification decision

Certification decisions are made by the Certification Officer assisted by a competent person appointed by the Certification Officer if needed. Into Certification ensures that personnel who make the decision for granting or refusing certification are different from those who carried out the audits. Personnel making the decision have appropriate competence for granting the decision.

A review process prior to making any decisions related to certification (including changes in the scope of the certification, renewing, suspending or restoring certification) contains the following steps:

a) ensuring that the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification,
b) ensuring that the correction and corrective actions for any major nonconformities are reviewed, accepted and verified,
c) ensuring that the client's plan for correction and corrective actions for any minor nonconformities is revied and accepted.

It should be noted that some standard schemes expect that all nonconformities are corrected and reassessed successfully before a certificate can be granted.

3.6.2. Information for granting or refusing certification

Each certification decision is recorded including any additional information or clarification sought from the audit team or other sources. The audit team provides the following information to decision makers:

- the audit report,
- comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client,
- confirmation of the information provided to the certification body used in the application review,
- confirmation that the audit objectives have been achieved,
- a recommendation whether or not to grant certification, together with any conditions or observations.

If Into Certification is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, stage 2 will be repeated prior to recommending certification.

If Into Certification would be accepting certification due to transfer of certification from another certification body, it implements a process for obtaining sufficient information for certification decision.

3.6.3. Maintaining Certification

The default surveillance activities include reacting to client notifications about changes that may affect the certified system's compliance against the audit requirements. The activities include also on-site auditing of the certified client. Other surveillance activities may be:

- enquiries to the client about the status of certification, reviewing client's statements with respect to its operations (e.g. promotional material, webpages),
- requests to client to provide documented information,

3.6.3.1. Surveillance audits

Surveillance audits are on-site audits but are not necessarily full system audits and they are conducted at least once in a calendar year. The following activities are always included in the surveillance audit programmes:

- the system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action,
- communications from external parties as required by ISO/IEC 27001 and other documents required for certification,
- changes to the documented system,
- areas subject to change,

- selected requirements of ISO/IEC 27001,
- other selected areas as appropriate.

3.7. Recertification

A recertification audit is planned and conducted to evaluate the continued fulfilment of all the requirements of the used standard. It is planned and conducted in due time to enable timely renewal before the certificate expiry date.

Recertification activities include the review of previous surveillance audit reports and consider the performance of the ISMS over the most recent certification cycle. By default, the activities include only stage 2 of the audit process. Stage 1 may need to be included in cases where significant changes to the ISMS, the organization, or the context of information security (e.g. changes in legislation).

3.7.1. Recertification and corrective actions

The time allowed to implement corrective actions is determined based on the severity of the nonconformity and the associated information security risk. All corrective actions shall be implemented and verified before the expiration of certification. When recertification activities are successfully completed prior to the expiry date of the existing certification, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate is on or after the recertification decision.

If Into Certification has not completed the recertification audit or it is unable to verify the implementation of corrections and corrective actions for any major nonconformity prior to the expiry date of the certification, then recertification is not recommended, and the validity of the certification is not extended. The client is informed, and the consequences are explained.

Following expiration of certification, Into Certification can restore certification within six months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 audit will be conducted. The effective date on the certificate is on or after the recertification decision and the expiry date is based on the prior certification cycle.

3.8. Audits for expanding scope and short-notice audits

Into Certification responds to an application for expanding the scope of the granted certification by reviewing the application and determining audit activities necessary to decide about the extension. Audit for expanding the scope of certification can be conducted in conjunction with surveillance audits.

Short-notice audits may be conducted in case of investigating complaints, response to changes or as follow up on suspended clients. In these cases, Into Certification makes known to the certified clients in advance the conditions under which such audits will be conducted.

3.9. Suspending, withdrawing or reducing the scope of certification

Into Certification has determined the following as default cases for suspending certification (certification is temporarily invalid under suspension), however the list is not conclusive:

- the client's certified ISMS has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the ISMS,
- the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies,
- the certified client is in breach of contract,
- the certified client has voluntarily requested a suspension.

If the client disputes the nonconformities affecting the suspension, withdrawal or reduction of the certification scope, these nonconformities are reported to the CEO by the Audit Team Leader who performed the audit. In this case, a short-notice re-audit may be arranged with different Audit Team Leader and audit team to ensure the basis for suspending, withdrawing or reducing the scope of the certification. The initial audit report and other working papers are then reviewed under the direction of the Audit Team Leader other than the one who performed the initial audit. The decision for suspension is made if there are no mistakes found in the initial audit.

Into Certification restores the suspended certification if the issue that has resulted in the suspension has been resolved. Failure to resolve the issues that have resulted in the suspension in a time established by the certification body results in withdrawal or reduction of the scope of certification.

Into Certification reduces the scope of certification to exclude the parts not meeting the requirements when the certified client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction is in line with the requirements of the ISO/IEC 27001. A reduced certificate is then issued for the client.

4. Handling processes for complaints and appeals

Into Certification management is informed when Into Certification receives a complaint or appeal related to certifications, work quality or company's independence. The certification body informs also the complainant about the receipt of the appeal. If the complaint relates to certification activities that Into Certification is responsible for, the complaint is investigated. If the complaint relates to certified client, the examination of the complaint considers the effectiveness of the certified management system. Responsive actions are determined case by case taking into account previous similar complaints. All complaints, appeals and related decisions are tracked and recorded.

Default actions for every complaint and appeal are described below:

- The person acting in the role of Certification Officer cannot handle appeals that consider certification decisions made by themself, because they are responsible for making them. A qualified person or persons (with competence to act as a Certification Officer) are appointed to assess the appeal.
- All additional information needed is gathered for the handling process.
- Needed decisions as well as correction and corrective actions are taken.
- Any decisions or actions (progress reports and results of the handling processes) are communicated to the client and related parties.
- Into Certification gives formal notice about the end of the handling process.

Submission, investigation and decision on complaints and appeals do not result in any discriminatory actions against the client.

4.1. Feedback

Into Certification also welcomes any free form feedback on its operations.

5. The right to refuse an assignment

Into Certification has the right to refuse an assignment. Refusal is exceptional and will be justified heavily. Refusal may be considered if:

- the assignment threatens the independence or impartiality of the Into Certification,
- the assignment causes exceptional occupational safety or security risks for Into Certification or its personnel,
- the assignment poses other threats to the operations, reputation or clients of Into Certification,
- views of auditee and Into Certification do not meet with respect to the scope and limitations of the assessment,
- Into Certification sees other apparent reason for refusal.

6. Use of certification marks

The certification mark and the certificate are public references to the certification which the certified client may use in its communication media, for example on webpages or in other documents. The terms and conditions below shall be followed when referring to certificate:

- the reference shall indicate the scope of the certificate and Into Certification, which is the issuing certification body,
- the reference shall not imply that the certificate covers areas other than what was defined in the scope of the certificate or be a guarantee of absolute information security,
- if the scope of the certification changes, all references to certification must be changed to correspond to the new certification scope,
- certification shall not be referred to in any context after the expiration of the certification,
- If the standard or criteria on which the certification is issued has become a new version and the client is certified against the previous version, the client shall not claim to be certified against the new standard/criteria version.

References to certification issued for information security management system (ISMS) shall not imply that:

- products, processes or service is certified by this means,
- the certificate applies to laboratory test, calibration or inspection reports.

The certification mark is delivered in electronic format. When utilizing the certification mark, the certified customer can alter the size of the certification mark, but the dimensions of the certification mark shall remain unaltered. The size of the certification mark must remain large enough so that all texts are fully legible. Another kind of altering of the certification mark is forbidden.

Into Certification has the ownership of certificates and certification marks and exercises proper control if client misuses the certificate marks or any references to certification. These actions may include requests for correction and corrective actions, suspension, withdrawal of certification, publication of the transgression and legal actions if necessary.

7. Public information

Into Certification will provide the following information on request:

- the name of the certified client,
- the name, the scope of the certification and geographical location(s) of the client,
- standard/criteria on which the certification is issued,
- the status of certification.

Into Certification does not provide a full list of clients or answer requests which contain information of several companies. Access to certain information can be limited on the request of the client (e.g. for security reasons). For example, in the case of Katakri-certificates, the status or existence of a certificate may be kept undisclosed by default.