



Service Description

Table of Contents

1	Information Security Certification Body	3
2	Policy on Impartiality	3
2.1	Safeguarding Impartiality	3
2.2	Conflicts of interest	4
2.3	Confidentiality	4
3	Certification process	4
3.1	Personnel used in audits	4
3.2	Use of external auditors and technical experts	6
3.3	Pre-certification activities	6
3.3.1	Application for certification	6
3.3.2	Audit programme	6
3.4	Obtaining evidence and control of records	7
3.4.1	Audit methods	7
3.4.2	Control of client records	7
3.5	Stage 1	8
3.6	Stage 2	8
3.7	Certification	8
3.7.1	Certification decision	8
3.7.2	Information for granting or refusing certification	9
3.8	Surveillance activities	10
3.8.1	Surveillance audits	10
3.9	Recertification activities	10
3.9.1	Recertification and corrective actions	10
3.9.2	Audits for expanding scope and short-notice audits	11
3.10	Suspending, withdrawing or reducing the scope of certification	12
4	Handling processes for complaints and appeals	12
4.1	Feedback	13
5	The right to refuse assignment	13
6	Use of certification marks	14
7	Public information	15

1 Information Security

Certification Body

Huld Certification is an independent sister company of Huld Oy providing information security management system certifications based on the standard ISO/IEC 27001. Huld Certification operates in the European Economic Area.

2 Policy on Impartiality

2.1 Safeguarding Impartiality

Huld 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.
- Huld 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.
- Huld Certification does not certify organizations that could cause uncontrollable risk for independence and impartiality.
- Huld Certification does not certify other certification bodies.
- Huld Certification does not perform internal audits to certified customers.

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

2.2 Conflicts of interest

Huld 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. Huld 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

Huld 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 concerned client is informed about the information provided, unless prohibited by law.

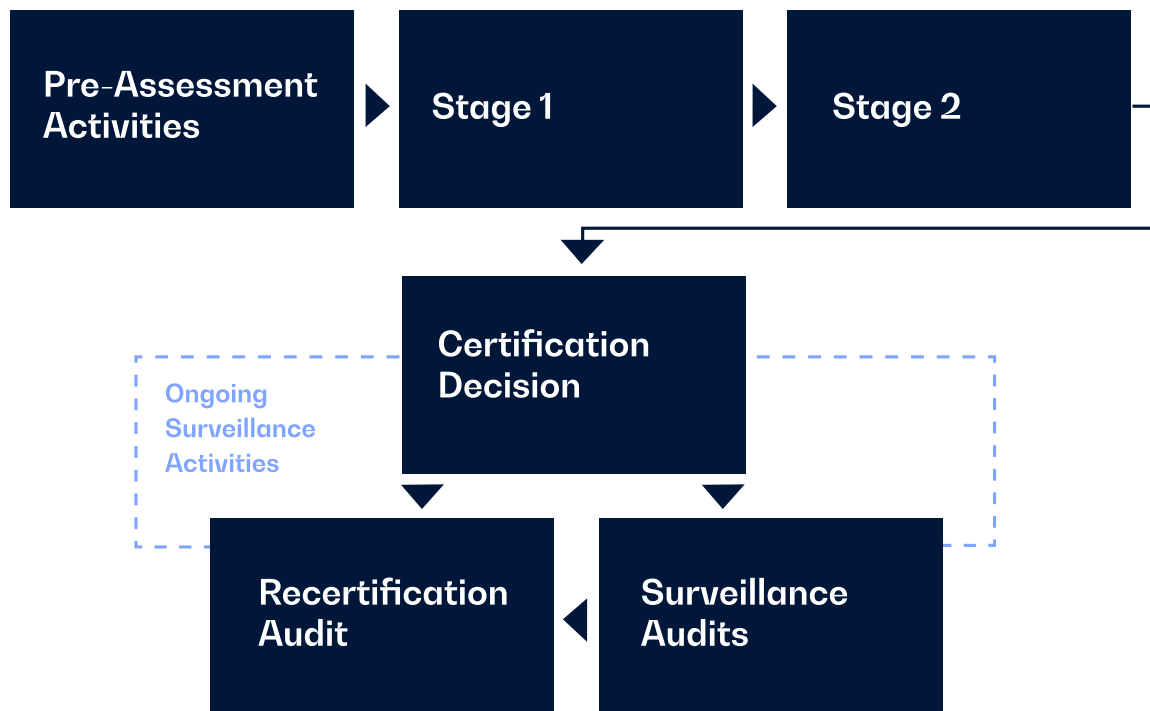
3 Certification process

ISO/IEC 27001 certification process is required to follow process guidelines set forth in 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 includes surveillance audits and recertification before the expiry of initial certification.

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 audit team leader, there may be other auditors, technical

Certification process flowchart.



experts, trainee auditors and observers. The audit team consists of at least two people, including the Audit Team Leader.

Managing Director is responsible for the certification decision. The Managing Director may be assisted by independent and competent personnel in the decision making.

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.

Huld Certification complies with the minimum competence requirements set in ISO/IEC 17021-1 and ISO/IEC 27006 standards. It maintains competence criteria for evaluating personnel competence and to identify training needs. Security clearances are in place for all auditors.

3.2 Use of external auditors and technical experts

Huld 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. Use of individual external personnel does not constitute outsourcing. The same confidentiality and impartiality requirements defined above, apply to external personnel.

3.3 Pre-certification activities

3.3.1 Application for certification

Assignment for certification begins with client requesting it from Huld Certification by delivering Application for Certification. 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 (name, site addresses, 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 system to be certificated.

Huld Certification conducts a review of the application and evaluates the client's preparedness for the certification.

3.3.2 Audit programme

An audit programme for 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 two-stage initial audit and surveillance activities. Surveillance activities contains two surveillance audits in the following two years, and



recertification audit on a third year before the expiry of certification. Huld Certification follows guidelines set in ISO/IEC 17021-1 and ISO/IEC 27006 in its audit and certification processes.

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

- the requirements of the audit standard or criteria in use,
- 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 is 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, Huld Certification may develop a sampling programme to ensure proper audit of the management system.

3.4 Obtaining evidence and control of records

3.4.1 Audit methods

Huld Certification uses approved methods to obtain and verify audit evidence. These methods include interviews, document review and technical testing.

3.4.2 Control of client records

Huld 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.

3.5 Stage 1

The objectives of stage 1 are to determine the readiness for the stage 2, and to identify and resolve possible nonconformities. A documentation review concerning client's ISMS is conducted and supplemented with interviews. The results of the stage 1 are documented in a written report.

3.6 Stage 2

The purpose of stage 2 is to assess the implementation and effectiveness of the client's ISMS and to confirm that 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 system that contains relevant information about the ISMS.

3.7 Certification

3.7.1 Certification decision

Certification decisions are made by the Managing Director assisted by a competent person appointed by the Managing Director. Huld 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 are reviewed and accepted.

3.7.2 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. 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 Huld 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, the stage 2 will be repeated prior to recommending certification.

If Huld 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.



3.8 Surveillance activities

The default surveillance activities include reacting to client notifications about changes that may affect to 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,
- other possible monitoring activities.

3.8.1 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.

3.9 Recertification activities

A recertification audit is planned and conducted to evaluate the continued fulfilment of all the requirements of ISO/IEC 27001 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 the 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)

3.9.1 Recertification and corrective actions

The time allowed to implement corrective actions is determined on the basis of 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 Huld 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, Huld Certification can restore certification within six months provided that the outstanding recertification activities are completed, otherwise at least stage 2 will be conducted. The effective date on the certificate is on or after the recertification decision and the expiry date is based on prior certification cycle.

3.9.2 Audits for expanding scope and short-notice audits

Huld 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, Huld Certification makes known to the certified clients in advance the conditions under which such audits will be conducted.

3.10 Suspending, withdrawing or reducing the scope of certification

Huld Certification has determined the following as default cases for suspending certification (certification is temporarily invalid under suspension):

- 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 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 Managing Director 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 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.

Huld 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.

Huld 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

Managing Director and Quality Assurance is informed when Huld Certification receives 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 Huld 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:

- To maintain independency, complaints and appeals are handled by the external QA. Managing Director cannot handle appeals that consider certification decisions, because Managing Director is responsible for making them.
- All needed additional information 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.
- Huld Certification gives formal notice about the end of the handling process.

Submission, investigation and decision on complaints and appeals does not result in any discriminatory actions against the client. Non-discrimination in Huld Certification is ensured by Quality Assurance.

4.1 Feedback

Huld Certification also welcomes any free-form feedback on its operations.

5 The right to refuse assignment

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

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

6 Use of certification marks

The certification mark (certificate) is a public reference 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 Huld 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.

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



7 Public information

Huld Certification will provide 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

Huld Certification does not provide full list of clients or answer to requests which contains information of several companies. Access to certain information can be limited on the request of the client (e.g. for security reasons).

Company name
Huld Certification Oy

VAT-number
3203038-6

Address
Keilasatama 5
02150 Espoo
Finland

huld | Certification