



ISO
CERTIFICATION
SERVICES
PROCESSES



General Requirements

Client Assessment

During the initial assessment of a new client or a reassessment of an existing client, Schellman will perform a formal review to ensure that engaging the client does not create a conflict of interest. The following requirements are considered during the assessment phase:

- Certification shall not be considered or provided when a relationship poses an unacceptable threat to impartiality. For instance, should a wholly owned subsidiary of Schellman request certification from its parent; certification shall not be provided.
- Certification shall not be considered or provided for another certification body.
- Certification shall not be considered or provided for a company that has received management system consultancy service within the two years following the end of the consultancy.
- Certification shall not be considered or provided to an organization that receives internal audit services from Schellman.
- Certification shall not be considered or provided to an organization that has received management system consultancy or internal audits where there is a threat of partiality.
- Personnel who have provided management system consultancy shall not be used by Schellman to take part in an audit or other certification activities within two years following the end of the consultancy.

Scope & Planning

Prior to establishing the audit plan, a questionnaire will be provided to each certification applicant (“client”) in order to identify the following:

- Audit scope
- Size and complexity of the client
- Locations of the client
- Outsourcing activities and subservice organizations, as applicable
- The standards or other requirements for which the client is seeking certification
- Information concerning the use of consultancy relating to the management system
- Prior year report results, as applicable
- Audit timing
- Project timeline

Scope & Planning (cont.)

Prior to establishing the audit plan, a questionnaire will be provided to each certification applicant (“client”) in order to identify the following:

- Audit scope
- Size and complexity of the client
- Locations of the client
- Outsourcing activities and subservice organizations, as applicable
- The standards or other requirements for which the client is seeking certification
- Information concerning the use of consultancy relating to the management system
- Prior year report results, as applicable
- Audit timing
- Project timeline

After reviewing this information, Schellman will determine whether to enter into a contract with the client to perform ISO 27001, ISO 20000-1, ISO 9001, or ISO 22301 certification services, ensuring that:

- The information about the client and its management system is sufficient for the conduct of the audit.
- The requirements for certification are clearly defined and documented and have been provided to the client.
- Any known difference in understanding between Schellman and the client is resolved.
- The scope of the certification sought, the location(s) of the client’s operations, time required to complete audits, and any other points influencing the certification activity have been taken into account.
- Schellman has the competence and ability to perform the certification activity.
- Records of the justification for the decision to undertake the audit are maintained.

Scope & Planning (cont.)

However, if the application is denied for any of the reasons considered above, a written notification will be sent to the prospect within four weeks noting the decision to decline the application as well as the reasons for the decision.

Should a collaboration between a client and Schellman move forward, the firm will use the information received from the aforementioned prospect questionnaire to determine the timing of the audit and assign the audit team members. Schellman will also communicate to the new client the certification process, any subsequent audits required to maintain certification, the appeals process, the complaints process, and any standard business terms applicable.

The communication of the information noted above can be expressed in a job arrangement letter, which will also address the contractual agreements between the client and Schellman pertaining to the agreed-upon audit scope for ISO 27001, ISO 20000-1, ISO 22301 and/or ISO 9001 audit certification services to be provided by Schellman. Upon execution of the job arrangement letter, Schellman will provide the client with preliminary planning documents, which include but are not limited to, the following:

- An audit plan detailing the testing to be performed by audit team members during the dates of fieldwork
- Relevant dates and deadlines subsequent to the on-site assessment
- Names of assigned audit team members

Certification Phases / Cycles

What follows is a brief overview of the typical order to certification audits:

Initial Certification Audit

Stage 1 – Information gathering and analysis / identification of nonconformities.

Stage 2 – Tests of operating effectiveness. Stage 2 will be scheduled to be performed no less than one month and no more than nine months following the completion of Stage 1.

Surveillance Audits

The mandatory first surveillance audit will be scheduled to commence no later than twelve months from the certification decision date following the Stage 2.

The mandatory second surveillance audit will be scheduled to commence any time during the calendar year for that second year of certification.

Additional surveillance audits that include activities such as on-site visits, questionnaires, interviews, and remote requests of audit documentation will be at the discretion of the engagement team and coordinated with client contacts.

Recertification

In order for clients to maintain their certification, recertification must take place every three years following the date of initial certification. It is recommended to schedule recertification audits to begin within 32 months of the initial certification date to ensure that if nonconformities are identified during the recertification audit, ample time is allotted to address any nonconformities prior to the certificate expiration date.

Prior to recertification, Schellman will determine adjustments to audit time and resources based on modifications to the client scope as well as other factors defined in ISO/IEC 27006:2015. Client personnel are required to disclose any significant changes within their organization to Schellman. Based on these changes within the client environment, Schellman may elect to conduct the recertification audit using the two-stage approach similar to the initial certification audit.

Project Calendar / Assignment of Tasks

Schellman has developed an audit plan template used to communicate audit assignments internally and with client personnel. It contains:

- Detailed tasks that are assigned to each audit team member and communicated to the client organization; and
- Identified dates for audit interviews and testing so as to allow client management adequate time in preparing for the audit and ensuring their availability during the assessment. (Typically, the audit plan will be aligned with the dates agreed upon in the job arrangement letter; however, changes to the audit plan can be requested by either Schellman or client personnel.)

When performing an audit, auditors are required to:

- Examine and verify the structure, policies, processes, procedures, records, and related documents of the client organization relevant to the management system;
- Determine that the abovementioned items meet all the requirements relevant to the intended scope of certification;
- Determine that the processes and procedures are established, implemented, and maintained effectively to provide a basis for confidence in the client's management system; and
- Communicate the results the audit to the client, as well as any inconsistencies between the client's policy, objectives, and targets (consistent with the expectations in the relevant management system standard or other normative document) so that action may take place.

Sampling Guidelines

Schellman has established a standard sampling methodology based on IAF MD-1. For any clients with multi-site locations, the audit team must determine the sample sizes required by location function, and if necessary, apply IAF MD-1, depending on the management system standard or normative document.

Identification of Nonconformities

The audit team is responsible for communicating inconsistencies and nonconformities (“nonconformities” or “discrepancies”) to appropriate client personnel in a timely manner. Information related to the identified discrepancies must be included within internal memorandums and supporting audit documentation.

Upon notification of nonconformities, the client must analyze, document, and take corrective actions to remedy the identified issues—corrective actions include root cause analysis, the creation of a remediation timeline, and subsequent evidence of remediation. Details regarding the corrective actions must be submitted to Schellman for review, after which point the audit team will determine if subsequent or additional testing is required. If an additional full or limited audit is required, Schellman will inform the client of the audit timeframe and additional work to be performed. Schellman will also document the results of the re-testing performed in internal memorandums.

Audit Deliverables

Audit Reports

Schellman will issue a written audit report upon completion of each stage of each audit cycle (certification, surveillance, and recertification). In the audit report, the team lead will recommend whether the client should receive the relevant certification or identify the reasons for not issuing the certificate.

The audit report is submitted to the certificate decision maker who will then concur or reject the team lead's recommendation upon confirming the following:

- Review, acceptance, and verification of the effectiveness of correction and corrective actions, as necessary, for all noted nonconformities that represent:
 - Failure to fulfill one or more requirements of the management system standard; or

- A situation that raises significant doubt about the ability of the client's management system to achieve its intended outputs.
- Review and acceptance of the client's planned correction and corrective action for any other nonconformities, including evidence that the nonconformities were corrected.
- That the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification.

Certificates

Upon the decision maker's concurrence of a team lead's recommendation to issue a certificate, Schellman will undergo its internal process for quality review prior to the release of the certificate to the client. Certificates are issued in conformance with the relevant normative standards.

Initial Audit & Certification

Stage 1:

The first stage of the initial certification audit consists of the review of the Management System framework – ISMS (27001), SMS (20000-1), Quality Management System (QMS) (9001), or Business Continuity Management Systems (BCMS) (22301) – and relevant / required documents and ensuring that the framework is consistent with the respective management system requirements. The review is performed to:

- Audit the client's management system documentation.
- Evaluate both the client's location and site-specific conditions and undertake discussions with the client's personnel to determine the preparedness for the Stage 2 audit.
- Assess the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives, and operation of the management system.
- Collect necessary information regarding the scope of the management system, processes, and location(s) of the client, as well as related statutory and regulatory aspects of compliance (e.g. quality, environmental, legal aspects of the client's operation, associated risks, etc.).
- Assess the allocation of resources for Stage 2 audit and agree with the client on the details of the Stage 2 audit.
- Provide a focus for planning the Stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects.
- Evaluate if the internal audits and management review are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the Stage 2 audit.

Initial Audit & Certification (cont.)

For most reviews, it is recommended that at least part of the Stage 1 audit be carried out at the client's premises in order to achieve the objectives stated above. An opening meeting will be conducted, as applicable, to ensure the objectives of the audit are re-communicated to client personnel.

Stage 1 audit findings are documented and communicated to the client at the conclusion of the Stage 1 review, including identification of any areas of concern that could be classified as a nonconformity during the Stage 2 audit. Depending on the readiness of the client to undergo the Stage 2 audit, Schellman, together with the client, will also determine the interval necessary between Stage 1 and Stage 2 audits. A closing meeting will be conducted at the conclusion of the Stage 1 review.

Stage 2:

The second stage of the initial certification audit consists of either on-site or remote fieldwork that includes in-depth testing of the framework and testing procedures to determine the design and operating effectiveness of the control objectives and control activities related to the scope of the management system. Each management system standard is assessed against its specific requirements to ensure full conformance to the standard as well as its status as an effectively operating management system.

At the conclusion of the Stage 2 audit, the audit team is required to meet with the client and conduct a closing meeting prior to leaving the client's premises. At this time, the audit team will provide the client with an indication regarding the conformity of the client's management system with the specific standard requirements. The client will then have the opportunity to ask questions about the findings and the audit results.

Initial Audit & Certification (cont.)

Also at the conclusion of the Stage 2 audit, the audit team will analyze the resulting information and evidence gathered during the Stage 1 and Stage 2 audits, review the findings, and agree on the audit conclusions, which effectively will become the recommendation to the certification decision maker making the decision to either issue or deny the certification.

The information provided by the audit team for the certification decision shall include, at a minimum:

- 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 Schellman used in the application review; and
- A recommendation whether or not to grant certification, together with any conditions or observations.

Schellman will make the certification recommendation on the basis of an evaluation of the audit findings, conclusions, and any other relevant information (e.g., public information or comments on the audit report from the client). The certification decision will be provided to the client no more than four weeks after the conclusion of Stage 2.

If Schellman is not able to verify the implementation of corrections and corrective actions of any major nonconformity within six (6) months after the last day of Stage 2, Schellman will conduct another Stage 2 audit prior to recommending certification.

Surveillance Activities & Maintenance

Once a client has received the initial certification, it remains valid for three years, a lifecycle that will include subsequent surveillance activities. At a minimum, a surveillance audit is required to be performed at least once a year, with the first taking place no more than 12 months from the certification decision date of Stage 2. Additional surveillance audits or activities can be scheduled depending upon the complexity of the client's services, changes to the scope of the management system, or due to any incidents that may occur, as well as any changes made to facilities or infrastructure (hardware, software, personnel, etc.) supporting the management system, etc.

Surveillance audits help ensure that the certified management system continues to be designed and operate effectively—an assurance largely maintained through surveillance activities, which include on-site audits assessing the certified client's management system's fulfillment of specified requirements with respect to ISO 27001, ISO 20000-1, ISO 9001, or ISO 22301 as applicable. Other surveillance activities may involve:

- Inquiries from Schellman to the certified client on aspects of certification;
- Review of any client's statements with respect to its operations (e.g., promotional materials or website);
- Requests to the client for documents and records (on paper or electronic media); and
- Other means of monitoring the certified client's performance.

Surveillance Activities & Maintenance (cont.)

Though not necessarily full system audits, surveillance audits are on-site and are planned together with the other surveillance activities so that Schellman can maintain confidence that the management system continues to fulfill requirements between certification and recertification audits. In addition to the aforementioned activities, the surveillance audit also includes, at a minimum:

- Internal audits and management review;
- Review of actions taken on nonconformities identified during the previous audit;
- Treatment of complaints;
- Evaluation of the effectiveness of the management system with regard to achieving the certified client's objectives;
- Continued progress of planned activities aimed at continual improvement;
- Ongoing operational control;
- Review of any changes; and
- Use of marks and/or any other reference to certification.

A report of the results of the surveillance audit is provided to both the client and the certification decision maker responsible for the certification decision. If a nonconformity or other situation that may lead to the suspension or withdrawal of the client's certificate occurs, the team lead is required to report the need to initiate a review by a different audit team to determine whether certification can be maintained. Schellman maintains certification based on demonstration that the client continues to satisfy the requirements of ISO 27001, ISO 20000-1, ISO 9001, or ISO 22301 as applicable.

Recertification

Schellman plans and conducts a recertification audit to evaluate the continued fulfillment of all of the requirements of ISO 27001, ISO 20000-1, ISO 9001, or ISO 22301, as applicable, for a client certificate. Recertification audits confirm the continued conformity and effectiveness of the management system as a whole, as well as its continued relevance and applicability for the scope of certification.

The recertification audit considers the performance of the management system over the period of certification and includes the review of previous surveillance audit reports. Recertification audit activities may need to include a Stage 1 audit in situations where there have been significant changes to the management system, the client, or the context in which the management system is operating (e.g., changes to legislation). In the case of multiple sites, the planning for the audit ensures adequate on-site audit coverage to provide confidence in the certification.

The recertification process includes an on-site audit that addresses the following:

- The effectiveness of the management system in its entirety in light of internal and external changes, as well as its continued relevance and applicability to the scope of certification;
- What commitment has been demonstrated to maintain the effectiveness and improvement of the management system in order to enhance overall performance; and
- Whether the operation of the certified management system contributes to the achievement of the organization's policy and objectives.

Recertification (cont.)

When instances of nonconformity or lack of evidence of conformity are identified during a recertification audit, Schellman will then define time limits for correction and corrective actions to be implemented prior to the expiration of certification.

Schellman will make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification.

When recertification activities are successfully completed prior to the expiry date of the existing certificate, the expiry date of the new certificate will be based on the expiry date of the existing certificate. The issue date on a new certificate will be on or after the recertification decision.

If Schellman has not completed the recertification audit or if Schellman is unable to verify the implementation of corrections and corrective actions for any nonconformity prior to the expiry date of the established certificate, then recertification shall not be recommended and the validity of the certificate shall not be extended. Schellman is required to communicate this, along with the consequences of certificate expiration, to the client.

Following the expiration of a certificate post a recertification audit, Schellman can restore the certificate within six (6) months provided that the outstanding recertification activities are completed; otherwise, at least a Stage 2 will need to be performed to achieve restoration. The effective date on the certificate is required to be on or after the recertification decision date and the expiry date is required to be based on the prior certification cycle.

Special Audits / Scope Expansions

There are occasions when a client requests to change the scope of a certified management system. Under these circumstances, Schellman will undertake a review of the application and determine any audit activities necessary to perform a scope modification audit. This may be conducted in conjunction with a surveillance audit.

In a similar vein, a client may also request that Schellman perform an audit on short notice—as a result of complaints or in response to changes, for example. Schellman will then describe and make known in advance to the certified client the conditions under which these short notice activities are to be conducted. Schellman will also exercise additional care in the assignment of the relevant audit team in these cases, as the lack of time will translate to a lack of opportunity for the client to object to audit team members.

Unannounced / Short-Notice Audits

There are occasions when Schellman must conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow-up on suspended clients. When Schellman determines to perform an unannounced or short-notice audit, Schellman will describe and make known in advance to the certified client the conditions under which these short notice visits are to be conducted.

All required planning documents will be produced for an unannounced or short notice audit, and the audit will be required to conform to Schellman's current methodology.

The unannounced or short notice audit will not be performed in lieu of the regular audit schedule but will be considered to be an out-of-schedule audit for a specific purpose. It will be considered an additional project for the client and will be performed and tracked as such internally.

Transfer of Certification

The transfer of certification is defined as the recognition of an existing and valid management system certification, initially granted by one accredited certification body, (hereinafter referred to as the “issuing certification body”), then accepted by another accredited certification body, (hereinafter referred to as the “accepting certification body”) for the purpose of issuing its own certification.

When considering the transfer of a certification, Schellman will first have to confirm that the existing certificate by the issuing certification body is covered by an accreditation of an IAF MLA signatory.

A pre-transfer review is then performed by the team lead to confirm / discuss / understand the following aspects:

- That the client’s certified activities fall within the accredited scope of the accepting certification body.
- The reasons for seeking a transfer.
- That the site or sites wishing to transfer certification hold an accredited certification that is valid in terms of authenticity, duration, and scope of activities covered by the management system certification. If practical, the validity of certification and the status of outstanding nonconformities will be verified with the issuing certification body unless it has ceased trading. Where it is not possible to communicate with the issuing certification body, the accepting certification body will record the reasons why.

Transfer of Certification (cont.)

- The last certification or recertification audit reports, subsequent surveillance reports, and any outstanding nonconformities that may arise from them. This will also include any other available, relevant documentation regarding the certification process, i.e., handwritten notes or checklists. If the last certification, recertification, or subsequent surveillance audit reports are not made available or if the surveillance audit is overdue, then the organization shall be treated as a new client.
- Any open nonconformities and actions taken to address them. Any open major nonconformities should be closed out prior to accepting the transfer.
- The established audit cycle and the plan to continue the cycle from the current certification body. Any adjustments must be recorded and communicated in the transfer report (and meet the requirements of the relevant standards).
- Complaints received and action taken.
- The stage in the current certification cycle.
- Any current engagement by the organization with regulatory bodies in respect of legal compliance.

The pre-transfer review will also include a documentation review and, if necessary, an on-site visit. Everything will be fully documented and a decision to accept the certification transfer will be made.

If the certification cannot be transferred (i.e. invalid certification, certification expired, etc.), Schellman will opt to treat the management system as a new client and will require all necessary steps and processes to be performed as such.

Suspending, Withdrawing, or Reducing the Scope of Certification

Schellman has the authority to suspend, withdraw, or reduce the scope of a certification under just cause and as a result of reasonable evidence.

Certification shall be suspended in cases when, for example:

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

Under suspension, the client's management system certification is temporarily invalid. Included within the job arrangement letter will be the enforceable arrangements regarding suspension of the certification to help ensure that in such cases, the client refrains from further promotion of its certification. Schellman is required to make the suspended status of the certification publicly accessible.

Suspending, Withdrawing, or Reducing the Scope of Certification (cont.)

The amount of time that a certification is suspended will be determined by the certification decision maker responsible for the certificate decision. During that time, the client may correct the reason for suspension and petition back to Schellman for reinstatement of the certificate. At such a point, Schellman will then perform a “surveillance-type” audit to determine if the certificate should be reinstated. The results and the audit team’s recommendation will be communicated to the client and certification decision maker, respectively.

Factors relevant to the recommendation include failure to resolve the issues that have resulted in the suspension in the time established by Schellman, which may result in withdrawal or reduction of the scope of certification. A reduction in the scope of the certification could occur to exclude the parts not meeting the requirements when the client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction shall be in line with the requirements of ISO 27001, ISO 20000-1, ISO 9001, ISO 22301, as applicable.

However, if the determination is to withdraw the certification entirely, Schellman, as included in the job arrangement letter, will have enforceable arrangements with the certified client concerning conditions of withdrawal, ensuring upon notice of withdrawal of certification that the client discontinues its use of all advertising matter that contains any reference to a certified status.

Upon request by any party, Schellman will correctly state the status of certification of a client's management system as being suspended, withdrawn, or reduced.

Appeals

Any appeal submitted by the client is required to be formally submitted to the Schellman's compliance team, via e-mail, mail, or through the Schellman website. The submission should include the reason for appeal, the date of the appeal, and any supporting evidence. Schellman's compliance team will ensure that the persons engaged in the appeals handling process are different from those who carried out the audits and made the certification decisions. Submissions, investigations, and decisions on appeals do not result in any discriminatory actions against the appellant.

During the appeal process, the following steps are required to be followed, at a minimum:

- The compliance team will log the appeal and record the date received, by whom it was received, and who the appellant is.
- Once the appeal is received, the compliance team is required to contact the appellant to confirm the appeal and direct the appellant to the publicly accessible appeals handling process.
- The Schellman compliance team will oversee the due diligence process to validate or dismiss the appeal.
- All documentation and evidence gathered during the appeal handling process will be provided to the compliance team, independent from the audit team and certification decision maker. This team will be responsible for deciding what actions should be taken in response to the appeal.
- The appeal, once closed, is filed, and will include all supporting documentation and evidence utilized in making the decision.

Appeals (cont.)

A confirmation of receipt of the appeal must be provided to the appellant within five business days. However, appeals may not be actually resolved within five business days due to the extent of appeal, any required due diligence, and the formality of the necessary response. Still, a progress update is to be provided to the appellant once per month at a minimum. The final decision communicated to the appellant will be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the appeal. Additionally, Schellman will provide formal notice of the end of the appeals handling process to the appellant.

Should an appeal results not be agreed upon by the client and Schellman, the client then has the right to appeal to Schellman's respective accreditation body.

The appeals handling process is available on the Schellman website.

Complaints

Any complaint by the client is required to be formally submitted to the Schellman compliance team, either via e-mail, mail, or through the Schellman website. The submission should include the reason for complaint, the date of the complaint, and any supporting evidence. The Schellman compliance team will ensure that the persons engaged in the complaint handling process are different from those who carried out the audits and made the certification decisions. Submissions, investigations, and decisions on complaints do not result in any discriminatory actions against the complainant.

If the complaint relates to a certified client, the examination of the complaint will consider the effectiveness of the certified management system. Any complaint about a certified client will also be referred to the certified client in question by Schellman at an appropriate time.

Complaints (cont.)

When resolving a complaint, the following steps are required to be followed, at a minimum:

- The compliance team will log the complaint and record the date received, by whom it was received, and who made the complaint.
- Once the compliant is received, the compliance team is required to contact the individual who made the submission in order to confirm the compliant before then directing said individual to the publicly accessible complaint handling process.
- The compliance team will oversee the due diligence process to validate or dismiss the compliant.
- All documentation and evidence gathered during the compliant handling process will be provided to the Schellman compliance team, independent of the audit team and certification decision maker. This team will be responsible for deciding what actions should be taken in response to the compliant.

- The compliant, once closed, is filed, and will include all supporting documentation and evidence utilized in making the decision.

A confirmation of receipt of the compliant must be provided to the complainant within five business days. However, the time necessary to resolve a complaint may vary due to the extent of the complaint, any required due diligence, and the formality of the necessary response. Still, a progress update is to be provided to the complainant once per month at a minimum. The final decision communicated to the complainant will be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the complaint. Additionally, Schellman will provide formal notice of the end of the compliant handling process to the complainant.

The compliant handling process is available on the Schellman website.



www.schellman.com

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607

1.866.254.0000

Outside of the United States, please dial: +1.813.288.8833

