schellman
Quality, above all.

ENS CERTIFICATION SERVICES PROCESSES

ENS

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, such as a wholly owned subsidiary of Schellman requesting certification from its parent.
- Certification shall not be considered or provided for another certification body.
- Certification activities must be undertaken impartially.
- Certification activities shall not allow commercial, financial or other pressures to compromise impartiality.
- Certification activities shall not be performed where Schellman (or any part of the same legal entity / entities under its organizational control) was / is the supplier, provider, operator, designer, developer, manufacturer, installer, distributor or maintainer of the certified product, process, or service.
- Certification shall not be considered or provided for an organization that has received ENS or product related consultancy services from Schellman 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 which has received ENS or product related consultancy or internal audits from Schellman where there is a threat of impartiality.
- Personnel who have provided ENS or product consultancy shall not be used by Schellman to take part in any audit or other ENS certification activities within two years following the end of the consultancy.
- Personnel who are or have been a supplier, provider, operator, designer, developer, manufacturer, installer, distributor, or maintainer of the certified product, process, or service shall not be used by Schellman to take part in any audit or other ENS certification activities within two years following the end of these activities.

Scope & Planning

To prepare for ENS certification, organizations must first understand the requirements of the ENS, as defined within Royal Decree 311/2022, of May 3. The process for the adaptation of ENS can be found at ens.ccn.cni.es. At a high-level, this includes the identification of scope, the categorization of systems according to the security dimensions of the services provided, the completion of a risk analysis, the definition and validation of the declaration of applicability, the assignment of roles and responsibilities, and the preparation and approval of the security policy.

Prior to establishing the audit plan, an ENS Scoping Questionnaire will be provided to each certification applicant ("client") in order to identify the following:

- Client name and address
- Client contact information
- Audit scope
    - In-scope systems
    - Relevant infrastructure / locations where in-scope data is processed
    - System security category (i.e., BASIC, MEDIUM, or HIGH)
    - Extent of data processing
- Client complexity
- Outsourcing activities and sub-service organizations, as applicable
- Information concerning the use of consultancy
- Prior report results or certificates, as applicable
- Requested audit timing / project timelines
- Other existing certifications, etc.

After reviewing this information, Schellman will determine whether to enter into a contract with the client to perform ENS certification services under Royal Decree 311/2022, ensuring that:

- The information about the client and the product is sufficient for the conduct of the certification process.
- Certification requirements are clearly defined, documented, and provided to the client.
- Any known difference in understanding between Schellman and the client is resolved, including agreement regarding standards or other normative documents.
- The scope of certification sought is defined (i.e., in-scope information systems / products, system security category, location(s), extent of data processing, and any other points influencing the certification).
- The means are available to perform all evaluation activities.
- Schellman has the competence, impartiality, and capability to perform the certification.
- Schellman will decline to undertake a specific certification if it lacks any competence or capability for the certification activities it is required to undertake.
- Where Schellman relies on certifications it has already granted to the client, or has already granted to other clients, to omit any activities, then Schellman shall reference the existing certification(s) in its records. If requested by the client, Schellman shall provide justification for omission of activities.
- Records of the justification for the decision to undertake the audit are maintained.

Scope & Planning (cont.)

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 Scoping Questionnaire to determine the timing of the audit and assign 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 ENS certification (under Royal Decree 311/2022) 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 audit plan and information request list. The audit plan will include details regarding the audit criteria, scope, objectives, assigned resources / team, and day-to-day schedule (i.e., interviews, reviews, and tests to be performed). The information request list will be tailored to the client's Declaration of Applicability and system security category. Relevant project dates and timelines will also be provided to the client.

Our ENS Certification Process

Assessment Fieldwork

After Schellman provides the client with our Audit Plan and Information Request List, the client will electronically submit the requested documentation to us, which we will review in advance of fieldwork to help ensure the planned fieldwork interviews and test plans are appropriate. Fieldwork will be initiated via a formal kickoff meeting and will include interviews, evidence and documentation review, and testing for relevant ENS Chapters and Articles and applicable Annex II security measures to determine compliance with the provisions of Royal Decree 311/2022.

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 certification.
- Determine that the aforementioned 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 information systems.
- Communicate the results of the audit to the client, as well as any deviations.

At the conclusion of fieldwork, a closing meeting will be held to formally close out fieldwork and align on next steps. In the event of any deviations, a Findings and Observations Document will be provided to the client's team.

Deviations can include the following:

- **Major Nonconformity —** Significant failure or absence related to essential Articles of the ENS (e.g. system categorization, declaration of applicability, designation of security officer, or information security policy); absence or inadequate implementation of a significant number of Annex II measures within any grouping; legal breaches or deviations that significantly affect the system's ability to perform essential functions; or a significant number of minor nonconformities associated with the same requirement.
- **Minor Nonconformity —** Partial non-compliance with any ENS Article or Annex II security measure; requirements met in an improvable way or inconsistencies between aligned requirements; does not by itself reveal a serious risk to the information system.
- **Observation —** A weakness, vulnerability, or specific situation that, while not currently compromising the information system, could in the auditor's opinion ultimately lead to a nonconformity or security problem over time.
- **Opportunity for Improvement —** An area that can be improved upon based on the auditor's professional experience and best practices.

Sampling Guidelines

Product Specific Sampling

Schellman applies a risk-based approach based upon the in-scope information system(s) / product(s) and the degree of shared vs unique configurations across these systems to ensure the audit team can gain reasonable assurance that each security measure meets (or does not meet) the respective requirements.

Location / Multi-Site Sampling

The minimum number of sites to be visited per audit is:

- **Initial audit:** the sample size should be the square root of the number of sites: ($y = \sqrt{yx}$), rounded up to the next highest integer, where y = number of sites to be sampled and yx = the total number of sites.
- **Renewal or subsequent audits:** the sample size should be the same as in an initial audit. However, when the system has proven effective during a certification cycle and at the discretion of the EC/OAT Technical Manager, based on an analysis of the circumstances, the sample size could be reduced to a $y = 0.8\sqrt{yx}$ rounded up to the nearest whole number. This criterion will apply provided there have been no changes to the scope of certification and the category.

Reporting & Certification

Following the ENS certification review, Schellman will issue a Certification Report, which can result in the following opinions:

- **Favorable —** No deviations (i.e., major nonconformity, minor nonconformity) are evident.
- **Favorable with Nonconformities —** Deviations are evident and the audited organization is required to submit a corrective action plan for evaluation by the lead auditor within 30 days.
- **Unfavorable —** A significant number of major and minor nonconformities exist whose resolution, in the opinion of the lead auditor, cannot be evidenced through a corrective action plan and requires verification via extraordinary audit (within a period of no less than six months and limited to the deviations found).

The audit report is submitted to the certification decision maker / file reviewer who will concur or reject the audit team's recommendation. If Schellman determines that the client conforms to the requirements of the ENS (Favorable Opinion), the ENS certification and mark will be issued. The certificate is valid for a two-year period. In the event of nonconformities, Schellman will provide corrective action plans to be completed and submitted within 30 days. Corrective action plans include corrective action, root cause analysis, the creation of a remediation timeline, and evidence of remediation. Schellman will be unable to issue the ENS certification and mark without the receipt of acceptable corrective action plans and evidence of correction for noted nonconformities.

Once issued, the ENS certification is valid for a two-year period, at which time, a subsequent certification review will be performed (sometimes referred to as a renewal. Schellman will verify, at least semi-annually, that ENS Conformity Marks issued to clients are properly displayed in accordance with the relevant Technical Instruction. Failure to properly display the mark is classified as a Major Nonconformity under Article 38 of Royal Decree 311/2022.

Other Types of Reviews

Certification Renewals

Once issued, the ENS certification is valid for a two-year period, at which time, a subsequent certification review is performed (sometimes referred to as a renewal. Renewals should be planned and scheduled in advance of this expiration date to avoid a gap in certification. Additionally, planning calls will be held to determine any changes to scope and their impact on fieldwork. Renewals generally follow the same standard process as certifications.

Special Audits / Scope Expansions

There are occasions when a client requests to change the scope or security category of a certified information system. Under these circumstances, Schellman will undertake a review of the application and determine any audit activities necessary. In the event of changes to scope or security category, the special audit / scope expansion will be limited to applied modifications, provided the evaluation is carried out within six (6) months of the prior certification. In the event of a special audit / scope expansion request post-six months, a complete audit must be completed. It is important to note that the date of the previous certification must be maintained, meaning the new certificate's validity period coincides with that of the previous certification.

Extraordinary Audit

An extraordinary audit is conducted in the event of an Unfavorable Opinion (i.e., there is a significant amount of major and minor nonconformities, whose solution, in the opinion of the chief auditor, cannot be evidenced through a corrective action plan and requires verification of correction via extraordinary audit. Extraordinary audits must be carried out in a period less than six months and will be limited to such deviations found).

Suspending, Withdrawing, or Reducing the Scope of Certification

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

Certification shall be suspended in cases when, for example:

- The client's certified information system has persistently or seriously failed to meet certification requirements
- The certified client does not allow a renewal certification audit to be conducted at the required two-year frequency
- Schellman cannot verify appropriate corrective action of nonconformities noted during renewal reviews for certified clients
- The certified client purposely does not adhere to marketing guidelines, makes incorrect references to the certification status or, makes misleading use of certification documents, Marks, or audit reports.
- The certified client has voluntarily requested a suspension

The certified client, upon suspension, withdrawal, or termination of its certification, will discontinue its use of all advertising matter that contains a reference to certification or includes the Mark. Under suspension, the client's certification is temporarily invalid. Included within the job arrangement letter are the enforceable arrangements regarding suspension, ensuring that in such cases the client refrains from further promotion of its certified status. Schellman is required to make the suspended status publicly accessible.

Appeals

Any appeal submitted by the client is required to be formally submitted to 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.

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 result not be agreed upon by the client and Schellman, the client then has the right to appeal. 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 the 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 information system's security controls and the client's ENS compliance. Any complaint about a certified client will also be referred to the certified client in question by Schellman at an appropriate time.

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 complaint is received, the compliance team is required to contact the individual who made the submission in order to confirm the complaint 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 complaint.
- All documentation and evidence gathered during the complaint 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 complaint.
- The complaint, once closed, is filed, and will include all supporting documentation and evidence utilized in making the decision.

A confirmation of receipt of the complaint 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 complaint handling process to the complainant. The complaint handling process is available on the Schellman website.

Financial / Fees

A description of the means by which the certification body obtains financial support and general information on the fees charged to applicants and to clients will be provided upon request.

schellman
Quality, above all.

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