SMITH+
HOWARD

A Guide to the ISO 27001 Certification Process

SMITH-HOWARD.COM

Pre-Certification Activities
Application
Remote Audit
Obtaining Verifying Information
Certification Decision
Suspension Policy
Appeals Process
Impartiality
Complaints
Certification Marketing Guidelines

Pre-Certification Activities

Enterprise Risk Security "ERS" Management ensures all process requirements are followed as defined within ISO/IEC 17021-1 and in accordance with ISO/IEC 27006, with defined applicable supporting documents, for pre-certification activities, conducting audits, and certifications. The use of existing and evaluation of new information and communication technology for auditing and certification purposes will undergo analysis for effectiveness, and associated risk and ensure meets IAF MD 4, ISO 27006, and ISO 17021-1 applicable requirements.

Application

Smith + Howard should conduct the application review. Smith + Howard ensures that:

1. The information about the applicant organization and its management system is sufficient to develop an audit program.
2. Smith + Howard has the competence and ability to perform the certification activity.
3. Any known difference in understanding between the certification body and the applicant organization is resolved.
4. The scope of certification sought, the site(s) of the applicant organization's operations, the time required to complete audits, and any other points influencing the certification activity are considered (language, safety conditions, threats to impartiality, etc.).
5. Safeguards are implemented to protect impartiality.
6. The size and number of sites, their geographical locations, and multi-site risk considerations reflect the appropriate scope.
7. Applicants provide details of previous certification engagements or transfers.

Applications will be considered by Smith + Howard only if they contain the following information/declarations:

1. Legal name, legal status, address, and legal representative of the applicant.
2. List of all offices and branches of the applicant.

Application, Cont'd

Accreditation can be applied according to one of, a combination of, or all of the following scopes:

1. Maintain an on-premises information Security Management System (ISMS).
2. Maintain data center storage unit.
3. Maintain a SaaS-based application/service.
4. Maintain business unit or function within the organization.

Remote Audit

Smith + Howard will determine at the time of the client's application if a remote audit is needed. The audit team will conduct complete and systemic inspections using remote technology, including virtual walkthroughs, video conferences, and the exchange of soft copies of documents and records. This approach may facilitate the use of new technology and may improve the flow of information between auditors and clients when two parties are not physically in the same location. Remote audits and inspections may be used to replace site audits. At least one week prior to the remote audit, Smith + Howard will send an audit agenda to the client. During remote audits, Smith + Howard will assess compliance with the certification principles within the ISO 27001 certification.

Obtaining Verifiable Information

During the audit, the information should be obtained by using appropriate sampling and verified prior to becoming audit evidence. Stage 1 includes the review of documentation and records. Methods used in Stage 2 include onsite interviews with the client's subject matter experts while observing processes and activities.

Stage 1 Audit Activities:

The objective of the Stage 1 Audit is to determine an organization's readiness for their Stage 2 certification audit. The certification body will review the scope of the management system and obtain information on the process and operations. Smith + Howard will review the client's management system documented information, evaluate specific site conditions, and make sure that objective and key performance indicators are in place and are understood. The overall level of implementation of the client's management system will be assessed to determine if the organization is ready to move forward with the Stage 2 certification audit. The client will be given a major concern or minor concern.

Stage 2 Audit Activities:

The objective of Stage 2 is to evaluate the implementation and effectiveness of the client's organization management system(s). Smith + Howard will determine the degree of compliance with the standard's requirement and report any minor non-conformities or major non-conformities that the organization will have to correct before issuing the ISO 27001 certification.

Smith + Howard will provide a written report for each audit to the client. The audit team may identify opportunities for improvement but should not recommend specific solutions. Ownership of the audit report should be maintained by the certification body.

Surveillance Audit and Recertification:

Smith + Howard certifications are issued subject to the maintenance and continual conformance of the documented Information Security systems to the certification standards. Surveillance audits should be conducted at periodic interactions at least once a year during the three-year term of validity of the certificate followed by a re-assessment of the information security management systems for renewal of the certification prior to its expiry. The frequency of surveillance audits has to be at least once in 12 months from the date of the closing of the certification audit (i.e., two surveillance audits to be conducted during the three years of validity at annual interaction).

Certification Decision

Smith + Howard ERS team should ensure that the persons or committees that make the decisions for granting or refusing certification, expanding, or reducing the scope of certification, suspending, or restoring certification, withdrawing certification, or renewing certification are different from those who carried out the audits.

Upon request, our ERS team should provide the following information, after ensuring the pertaining client has not limited certain information as defined within a documented exception:

1. Geographical areas in which it operates.
2. Status of a given certification.
3. Name, related normative document, scope, and geographical location (city and country) for a specific certified client.

Suspension Policy

Example cases leading to suspension:

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

During the suspension, the client's certification must be listed as temporarily invalid. Suspended certifications will be restored once the issue that caused the suspension is resolved. If the client fails to resolve the issue within the allotted 6-month time (can be expanded under special exceptions/ extenuating circumstances) provided by Smith + Howard, the certification should be withdrawn, or the scope of certification should be reduced to exclude the parts not meeting the requirements in line with the certification.

Appeals Process

Smith + Howard clients may appeal a certification decision or audit reporting results. Smith + Howard should acknowledge receipt of the appeal and should provide the appellant with progress reports and the result of the appeal with a final notice. Smith + Howard persons receiving, validating, and investigating the appeal, and for deciding what actions need to be taken, are different from those who carried out the audits and made the certification decisions. The appeal reviewer will not participate or be a part of the audit or certification process.

Impartiality

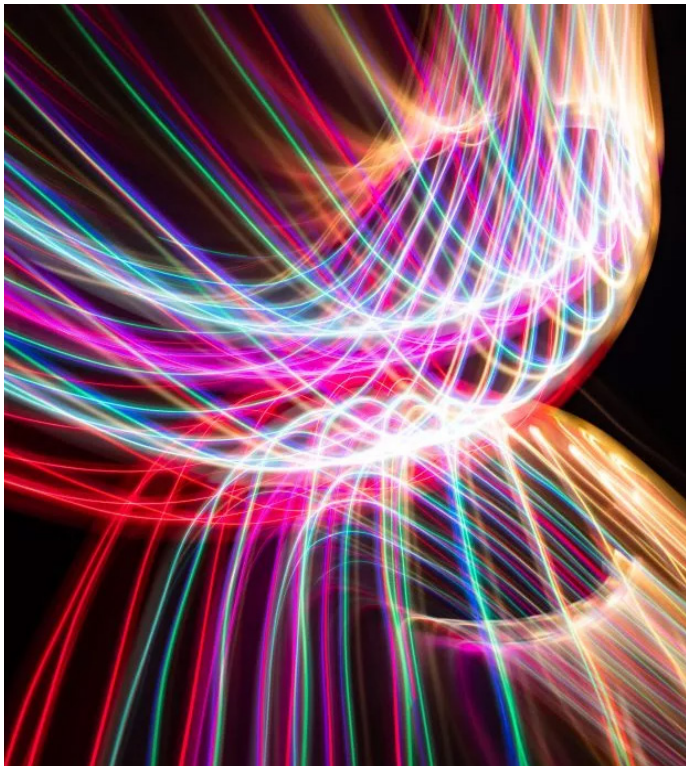
Smith + Howard management and staff are committed to the importance of impartiality, by identifying and managing conflicts of interest and by ensuring the objectivity of information security management system audit and certification activities.

The impartiality committee should:

1. assist the certifying body (i.e. Smith + Howard) in developing the policies relating to the impartiality of its certification activities,
2. counteract any tendency on the part of a certification body to allow commercial or other considerations to prevent the consistent objective provision of certification activities,
3. advise on matters affecting confidence in certification, including openness and public perception,
4. conduct a review, at least once annually, of the impartiality of the audit, certification, and decision-making processes of the certification body, and
5. approve the conflict-of-interest analysis and the mitigation measures.

Complaints

Individuals and organizations may submit a complaint against Smith + Howard or a client of Smith + Howard's. Smith + Howard should acknowledge receipt of the appeal and should provide the complainant with progress reports and the result of the complaint with a final notice. Smith + Howard team members receiving, validating and investigating the complaint, and deciding what actions need to be taken, are different from those who were previously involved in the subject of the complaint.



Certification Marketing Guidelines

The certification marketing guidelines apply to organizations who have obtained ISO 27001 certification of their information security management system ("Registrant") from Smith + Howard and have been provided Smith + Howard's ISO 27001 certification mark ("Mark"). These requirements were agreed to by the Registrant as a condition of Smith + Howard's acceptance of an ISO 27001 engagement leading to certification.

1. The Registrant should conform to the reasonable and mutually agreed requirements of Smith + Howard when referring to its certification status in communication media such as the Internet, brochures, advertising, or other documents. The reference must include identification of the certified client, including the type of management system and the applicable standard and the certification body (Smith + Howard) issuing the certificate.
2. The Registrant should not make or permit any misleading statements regarding its certification. Furthermore, the Registrant should not use or permit the use of a certification document, or any part thereof, in a misleading manner.
3. The Registrant should, upon suspension or withdrawal of its certification, discontinue its use of all advertising matters that contain a reference to ISO 27001 certification and/or includes a Mark.
4. The Registrant should amend all relevant advertising material when the scope of certification has been modified.
5. The Registrant should not allow reference to its information security management system certification to be used in such a way as to imply that Smith + Howard certifies a product, service or process.
6. The Registrant should not imply that the certification applies to activities that are outside the scope of registration.
7. The Registrant should not use its certification in such a manner that would bring Smith + Howard and/or the certification system into disrepute or cause loss of public trust.
8. The Registrant should use the Mark only in reference to the information security management system certified by Smith + Howard.
9. The Registrant should not use the certification in such a manner to be applied to laboratory tests, calibration or inspection reports.
10. The Registrant acknowledges that Smith + Howard has the right to suspend or withdraw certification if it finds that the Registrant has purposefully made incorrect references to the certification status or misleading use of certification documents, marks or audit reports

Certification Marketing Guidelines, Cont'd

11. The Mark is a service mark of Smith + Howard. The Mark should only be used during periods of active certification. The Mark may not be used in connection with any product or service that was not within the scope of the certification review, in any manner that is likely to confuse customers, or in any manner that disparages or discredits Smith + Howard.
12. The Mark will be provided in an approved form. The Registrant may use any approved version of the Mark during periods of active certification. However, the Registrant should not modify the form or color of any Mark provided by Smith + Howard.

Meet the Team

Marvin H. Willis
CPA/CITP, CHQP, CGMA
404-874-6244
mwillis@smith-howard.com
PARTNER
SMITH + HOWARD PC
SMITH + HOWARD ADVISORY LLC

Oliver Villacorta
CISSP, HCISPP, CCSP
404-879-3228
ovillacorta@smith-howard.com
SENIOR MANAGER
SMITH + HOWARD ADVISORY LLC