Aprio®

Passionate for what's next®

Aprio's ISO 27001 Certification Program

CERTIFICATION MECHANICS AND EFFICIENCIES

The ISO/IEC 27001 framework is the international standard for information security management systems (ISMS). The ISO 27001 framework provides a strong foundational approach to the management of information security that allows companies to approach risk as an organization. An ISO 27001 Information Security Management Systems certification includes an optional pre-assessment, a two-stage certification audit and ongoing surveillance audits. Aprio is here to help ease an organization's transition to and implementation of this standard.

ISO 27001 can represent a cornerstone for most security audits or compliance requirements, especially SOC 2 and the HIPAA Security Rule. Aprio's ISO certification program can streamline the process for clients that are required to conduct other security audits. We minimize the need to manage multiple audit firms and help reduce the redundancies in certification requirements. Aprio's streamlined process saves you time and eliminates unnecessary duplication of fees.

Aprio delivers to our clients a unified risk management program that includes risk analysis, risk management and on-going monitoring and attestation services against such frameworks as SOC 2, PCI Data Security Standard and ISO 27001. A CPA attestation provides clients with the highest level of confidence and peace of mind, offering greater assurance than a report or certification for those clients that need the highest level of assurance available.

ISO 27001

Information Security Management Systems (ISMS) certification

About the Standard

An ISO/IEC 27001 certification will allow your company not only to be recognized for security practices on a national level, but also on an international level. By implementing this internationally-recognized security standard, organizations can effectively identify security risks and put controls in place to manage or mitigate them.

We view ISO/IEC 27001 as a strong foundational approach to the management of information security. The standard can be broken out into two main parts:

- First, there are the requirements of 27001, which are broken out into 10 sections. These sections state requirements for the management system, including elements such as planning, implementation, monitoring, review and improvement. It defines specific responsibilities for management, such as the setting of objectives, measurement and review of objectives and the system, and internal audit requirements.
- Second, there is a set list of controls contained in Annex A of ISO 27001, which align with the requirements defined in sections 1-10. These controls should be implemented at the organization, when applicable. It is up to the organization and management to perform a risk assessment and determine with controls are applicable to the organization based on identified risks, services, industry, etc.

An ISO/IEC 27001 certification will allow your company not only to be recognized for security practices on a national level, but also on an international level.

The Certification Process

The following certification activities are performed as part of the ISO 27001 Information Security Management Systems (ISMS) certification:

PRE-ASSESSMENT

Aprio performs an optional assessment of the ISMS and reviews the policies and procedures, including information system processes, to assess potential gaps in the client's ISMS. The pre-assessment/readiness phase prepares clients undergoing ISO 27001 for the first time.

CERTIFICATION AUDIT

The initial certification is conducted to evaluate the client's Management System documentation and the implementation and monitoring of the client's ISMS. The audit is conducted in two stages, Stage 1 and Stage 2.

- **Stage 1 Audit** - the first stage includes an audit of management's system documentation and an evaluation of the client's location(s) in preparation for the Stage 2 audit. The client's understanding of the standard, including the scope of the audit and resources, is also evaluated during this stage.

- **Stage 2 Audit** - the second stage of the initial certification review includes detailed testing to determine that the client has effectively implemented and is consistently monitoring its Management System in accordance with ISO 27001. This stage is performed onsite at the client's location(s).

The results of the Stage 1 and Stage 2 audits and the evidence gathered determines the audit conclusions and issuance of initial ISO 27001 certification. The initial certificate issued is valid for three years from the issuance date.

SURVEILLANCE AUDIT

Surveillance audits are performed onsite at the client's location(s). These audits are required to ensure that the client continues to conform to the requirements of the standards to which the initial certification is granted. The surveillance audits are performed at least once a year.

SHORT-NOTICE AUDITS

It may be necessary for Aprio to 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. In such cases, Aprio shall describe and make known in advance to the client the conditions (e.g. detailed description of the unplanned audit; the normative requirements for certification; documents describing the rights and duties of certified clients, including requirements, when making reference to its certification in communication of any kind; client need to comply with certification requirements and make all necessary arrangements for the conduct of the audits, including making provisions, where applicable, to accommodate the presence of observers (e.g. accreditation assessors or trainee auditor)) under which such audits will be conducted.

SCOPE CHANGE

Any changes required to the client organization's scope of certification can be processed in conjunction with the ongoing audit program. If the client organization wishes to change or add to the systems against which it already holds certification, or wishes to add more sites into the scope of certification, the scope can be changed with the assigned project manager or by contacting Dan Schroeder, partner-in-charge of Information and Assurance Services at Aprio.

REDUCTION IN SCOPE OF CERTIFICATION

When an organization's scope of certification is reduced, Aprio shall issue revised certificates and scopes of certification as appropriate and the certified organization shall:

(a) Return all superseded certificates;

(b) Ensure that use of the certification mark is adjusted to reflect the reduced scope of certification;

(c) Ensure that all advertising and promotional activities and materials are adjusted to reflect the reduced scope of certification; and

(d) Pay any fees that are applicable for the facilitation of this activity.

CERTIFICATION DECISION

Following confirmation that any necessary corrective actions have been appropriately addressed (which may involve a chargeable follow-up visit by the Aprio auditor/audit team), the findings and recommendations made in the Audit Report are subject to an internal review process prior to certification being granted.

Once the client organization has met the requirements for Aprio certification for compliance with the relevant standard(s), the client organization will be issued with the appropriate certificate(s) and/or scopes of certification. Details of the certification may be made publicly available.

SUSPENSION OR REFUSAL OF CERTIFICATION

In the event that an applicant organization fails to comply with the requirements of the relevant standard/audit requirements, or in the event that a certified organization fails to comply with these conditions of certification (including prompt payment of fees) or is unable to maintain compliance with the relevant certification standard, Aprio may:

(a) Refuse certification;

(b) Suspend certification;

(c) Reduce the scope of certification; or

(d) Withdraw certification and related services.

Such decisions and the grounds for them will be communicated to the organization in writing. When an organization's certification is suspended or refused, the organization shall, for the period of suspension or refusal:

i. Withdraw and cease to use any advertising or promotional material that promotes or advertises the fact that the organization is certified;

ii. Ensure that all copies of certificates and scopes of certification are removed from areas of public display; and

iii. Cease to use the certification mark on stationery and other documents including media and packaging that are circulated to existing and potential clients, or in the public domain.

ISO 27001

Information Security Management Systems (ISMS) certification

About Aprio

Since 1952, clients throughout the U.S. and across more than 40 countries have trusted Aprio for guidance on how to achieve what's next. As a premier, CPA-led professional services firm, Aprio delivers advisory, assurance, tax and private client services to build value, drive growth, manage risk and protect wealth. With proven expertise and genuine care, Aprio serves individuals and businesses, from promising startups to market leaders alike.

Aprio.com

The organization shall advise Aprio, in writing, of actions taken with respect to the requirements as listed above. Aprio shall likewise advise the organization, in writing, of the certification processes that will need to be completed to restore certification. Please be aware that during the period of suspension the organization is required to continue to pay all fees levied by Aprio.

APPEALS AND COMPLAINTS

Appeals against certification decisions made by Aprio, and complaints against the service provided by Aprio, may be raised with Dan Schroeder, partner-in-charge of Information Assurance Services at Aprio.

USE OF CERTIFICATION MARKS

After an organization is granted certification by Aprio, it may become eligible to use appropriate Aprio and other specified certification marks to promote the fact that the organization is certified. Certified organizations may use the Aprio certification marks or other marks that it facilitates subject to compliance with the following conditions:

(a) The certification marks or other marks that it facilitates may be used on correspondence, advertising and promotional material in conjunction with the certified organization's name or emblem, and shall not be used in connection with goods, services, activities or locations not covered by the scope of certification;

(b) Certification marks shall not be applied to laboratory test, calibration or inspection reports, as such reports are deemed to be products in this context;

(c) The certification marks or other marks that it facilitates shall only be reproduced in the approved style and colors;

(d) The certification marks or other marks that it facilitates shall not be used in any manner that implies approval of a product or service;

(e) On notification in writing, the certified organization shall discontinue any use of the mark that is unacceptable to the PIC IAS (and/or its nominee) and any form of statement used in conjunction with the mark that may be misleading. The certified organization shall also undertake any other action requested by the PIC IAS (and/or its nominee) with regard to unacceptable use of the mark; and

(f) Upon termination of certification, the certified organization undertakes to immediately discontinue use of the mark/s. Use of the marks is not to be reinitiated unless certification is fully reinstated.

Getting Started

The Aprio Information Assurance Team is here to help ease an organization's transition to this standard and answer any questions you may have regarding the standard or process involved in attaining accreditation.

ISO 27001

Information Security
Management Systems
(ISMS) certification

For more information, contact:

Dan Schroeder
Partner-in-Charge,
Information Assurance Services
dan.schroeder@aprio.com
770.353.8379

Morison KSi
Independent member