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 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 certification services against ISO 27701, ISO 22301, ISO 9001 as well as ISO 27017 and ISO 27018 extensions in addition to ISO 27001.

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.

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 which are referred to as the management system clauses. These sections state requirements for the management system, including elements such as planning, implementation, monitoring, review, and improvement. They define 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.

Aprio

Passionate for what's next®

The Certification Process

The following certification activities are performed as part of the ISO 27001 Information Security Management Systems (ISMS) certification. This process also applies to other certifications offered by Aprio namely, ISO 27701, ISO 22301, ISO 9001. ISO 27017 and ISO 27018 are extensions that can be completed in conjunction with ISO 27001.

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 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. Areas of concern may be identified during Stage 1 which the client must address prior to Stage 2.

- **Stage 2 Audit** - the second stage of the initial certification review includes detailed testing to determine that the client has effectively implemented the Management System Clauses and the Annex A controls and is consistently monitoring its Management System in accordance with ISO27001. Non-conformities may be identified during Stage 2 which the client must address prior to certification.

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 in years two and three of the certification. These audits are required to help ensure that the client continues to conform to the requirements of the standards to which the initial certification is granted. Surveillance audits cover all of the management system clauses in each surveillance year, and the Annex A controls are split across the two surveillance audits.

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.

About Aprio

Since 1952, clients throughout the US, and across more than 50 countries have trusted Aprio for guidance on how to achieve what's next. As a premier business advisory and accounting firm, Aprio delivers advisory, audit, tax, managed 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.

For more information, contact:

Powell Jones
Partner, ISO Practice Leader,
Information Assurance Services
powell.jones@aprio.com
770-353-3157

Shipra Sharma
Senior Manager,
Information Assurance Services
shipra.sharma@aprio.com
770-353-3033