ISO 27001

Quick Start Guide

Orion
ASSESSMENT SERVICES

ISO 27001

ISO 27001 is a globally recognized standard for information security management that outlines best practices and security controls for protecting sensitive information. The standard ensures the confidentiality, integrity, and availability of information, providing organizations with a comprehensive framework for managing information security.

It is important to note that the latest version of the standard, ISO 27001:2022, has recently been released, superseding the 2013 version. Although certification bodies will not be accredited to offer certification to this new version until mid 2023, organizations can already begin to implement the updated best practices and security controls outlined in the standard.

The benefits of ISO 27001 certification include:

Improved Information Security

ISO 27001 provides a framework for implementing effective information security controls, reducing the risk of data breaches and ensuring the confidentiality, integrity, and availability of sensitive information.

Increased Business Continuity

ISO 27001 helps organizations prepare for and respond to security incidents, ensuring business continuity and reducing downtime.

Enhanced Reputation and Customer Trust

By demonstrating compliance with ISO 27001, organizations can enhance their reputation and increase customer trust, helping to build brand loyalty and win new business. ISO 27001 certification is also increasingly being viewed as a requirement for doing business with organizations in regulated industries, such as finance and healthcare.

ISO 27001 can be purchased from: www.ISO.org

Orion
ASSESSMENT SERVICES

Implementing ISO 27001

Organizations can choose to implement the ISO 27001 standard either internally or with the assistance of a consultant. If implementing internally, it is recommended to take a course on the standard to gain a comprehensive understanding of the requirements. This will help ensure that all relevant aspects of the standard are addressed. A gap assessment should be conducted to identify areas where the standard has not been met and to prioritize the implementation process.

On the other hand, if organizations choose to work with a consultant, the consultant should provide a structured implementation plan to guide the process. This plan should cover all aspects of the standard and ensure that the implementation process is efficient and effective.

Applying for ISO 27001 Certification

To apply for certification, the organization must provide information on the ISMS scope and the number of people in scope. Certification bodies use ISO 27006 as a starting point for quoting, and the quote may be adjusted based on the complexity of the management system.

The certification process is divided into two stages, Stage 1 and Stage 2.

The **Stage 1 audit** is a high-level review of the management system to ensure that it is implemented and there are no major gaps. The **Stage 2 audit** is a detailed review of all requirements to ensure they are effectively implemented. If any issues are identified during the audits, the organization must close them or have a corrective action plan in place.

After the audit, the auditor's package is reviewed by an internal team, and upon successful review, the organization will receive their certification with a three-year expiry. Annual surveillance audits are required to maintain certification.

Orion
ASSESSMENT SERVICES

The Importance of Defining the Scope of the ISMS

The scope of the Information Security Management System (ISMS) is a critical factor that affects both the implementation and certification costs. Organizations should determine the scope by identifying the information to be protected and the processes, systems, people, and departments that interact with that information.

For example, a company that designs and manufactures armored vehicles with critical intellectual property related to the targeting system might choose to focus on the design, installation, and testing of the targeting system. In this case, the scope may involve the software and hardware design teams, installers, and testers of the targeting system, while excluding the manufacturing and assembly staff who do not have access to critical information.

The scope statement for this company might look something like: "**The scope of <Organization> information security management system (ISMS) includes all people, processes, and facilities that develop, operate, and support the infrastructure that provides customer services and all underlying assets that support those business processes located in XXXXXXXX.**"

Defining the scope upfront helps organizations to accurately estimate the implementation and certification costs and to ensure a more efficient and cost-effective process.

By taking the time to define the scope of the ISMS, organizations can ensure a more efficient and cost-effective implementation and certification process. This helps to minimize any unexpected costs and ensures that the implementation and certification are aligned with the organization's goals and objectives.

Orion
ASSESSMENT SERVICES

Certification Review

It is important to note that maintaining certification status requires annual surveillance audits to ensure continued compliance with the standard. These audits provide an opportunity to review the effectiveness of the Information Security Management System (ISMS) and make any necessary updates to ensure its ongoing effectiveness.

For example, a company that has received ISO 27001 certification for its software development processes may undergo an annual surveillance audit to assess the continued effectiveness of its controls and ensure that the ISMS is aligned with any changes in the threat landscape or business objectives. By undergoing regular surveillance audits, the organization can maintain its ISO 27001 certification and demonstrate its commitment to information security.

The certification review and maintenance process is an essential aspect of ISO 27001 compliance. Organizations should take the necessary steps to undergo regular surveillance audits and maintain their certification status to ensure the ongoing effectiveness of their ISMS.

Summing Up

Orion Assessment Service can assist your organization in achieving ISO 27001 certification from the initial application request, and through to the required stages.

In conclusion, ISO 27001 is an essential standard for organizations looking to secure their sensitive information and protect against data breaches. By working with our team of experts, organizations can achieve their information security goals. Contact us today to learn more.

Canadian Office
1201 Dundas St East
Suite 209
Toronto, Ontario
M4M 1S2, Canada

info@orioncan.com
www.orioncan.com

US Office
28411 Northwestern Hwy
Suite 840
Southfield, MI
48034, United States

Orion
ASSESSMENT SERVICES

Orion
ASSESSMENT SERVICES