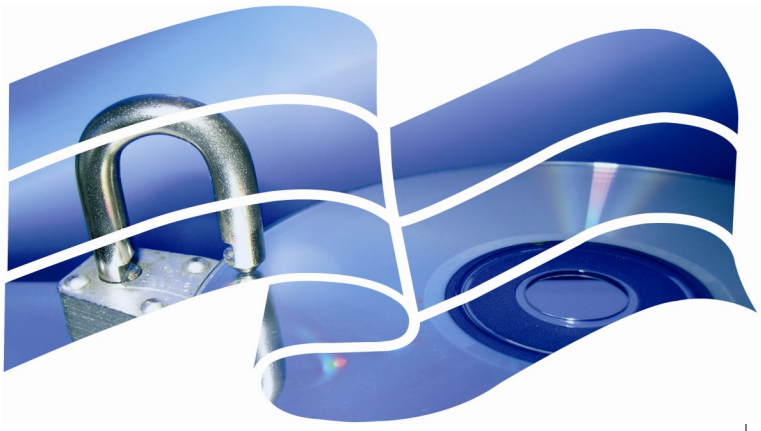

Certify Your Information Security Management System

ISO 27001:2013

Enabling Companies to Address Critical Issues

The final version of ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems*, is available, and replaces ISO/IEC 27001:2005. The Information Security Management System (ISMS) is a **systematic approach to managing sensitive company information** so that it remains secure. It encompasses **people, processes, and IT systems**. The international standard provides the framework for an organization to implement a **globally recognized system** for managing the security of their information.

With **increased usage of new technology** to store, transmit, and retrieve information, we have exposed ourselves to **increased numbers and types of threats**. The overall approach to Information Security, and integration of different security initiatives needs to be managed in order for each element to be most effective. An ISMS allows you to **coordinate your security efforts effectively**. The implementation of ISO/IEC 27001:2013 will **reassure customers and suppliers that information security is taken seriously** within your organization and defined processes are in place to deal with information security threats and issues.

The ISMS standard can be used by a **broad range of organizations** – small, medium, and large – in most of the **commercial and industrial market sectors**: technology, finance and insurance, telecommunications, healthcare, utilities, retail and manufacturing sectors, various service industries, transportation sector, government and many others. Like its predecessor, **ISO/IEC 27001:2013 specifies the processes** to enable a business to establish, implement, review and monitor, manage and maintain an **effective ISMS**.

The ISO 27001 standard integrates the **process-based approach** of ISO's management system standards, including the **Plan-Do-Check-Act** cycle and requirement for **continual improvement**. Meeting the standard assures customers and suppliers that organizations have developed and certified their information management systems to an **internationally recognized standard for security**.

The ISO 27001 Standard

ISO/IEC 27001 is intended to be used with **ISO/IEC 27002**, the **Code of Practice** for Information Security Management, which lists objectives, controls, and implementation guidelines. Organizations that implement an ISMS in accordance with **ISO/IEC 27002** are likely to also meet the requirements of ISO/IEC 27001. This ISO standard is the first in a **family of information security related standards** which are assigned numbers in the 27000 series. They include:

- **ISO/IEC 27000** – a vocabulary or glossary of terms used in the ISO 27000-series standards
- **ISO/IEC 27002** – the code of practice
- **ISO/IEC 27003** – the ISMS implementation guide
- **ISO/IEC 27004** – the standard for information security measurement and metrics
- **ISO/IEC 27005** – the standard for risk management
- **ISO/IEC 27006** – the guide to the certification process
- **ISO/IEC 27007** – the guide for information security auditing
- **ISO/IEC 27010** – the guide for inter-sector and inter-organizational communications
- **ISO/IEC 27011** – the guide for telecomms based organizations
- **ISO/IEC 27019** – the guide for process control systems in the energy utility industry
- **ISO/IEC 27799** – Healthcare informatics – Information security in healthcare organizations

Control Objectives and Controls

In addition to the clauses of the ISO/IEC 27001 standard, minimum control objectives and controls are located in the Annex (i.e. Annex A Controls). Minimally, these objectives and controls shall be a part of the ISMS. Additional objectives and controls may be necessary, depending on legal and regulatory, customer, and the organization's requirements.

Certification to ISO/IEC 27001

The ISO 27000-family of information security management standards align with other ISO management system standards, such as **ISO 9001** (quality management) and **ISO 14001** (environmental management), regarding both general structure and the nature of **integrating best practices with certification standards**. Certification of an organization to ISO/IEC 27001 is one means of providing assurance that the organization has not only implemented a system for the management of information security in line with the international standard, but also maintains and continuously improves the system.

Credibility and recognition are the primary advantages of being certified by a respected, independent third party. It provides **assurance and confidence** to management, suppliers, customers, and employees that the organization is committed to information security management and **continual improvement**. Organizations may be certified compliant with ISO 27001 by a number of accredited certification bodies worldwide.

Certification audits are led by IRCA certified ISO 27001 Lead Auditors. Certification is a **two-stage audit process**:

- **Stage 1 is a Readiness Review** – assessing the existence and completion of key documentation and preparing for the Stage 2 audit
- **Stage 2 is the on-site Certification Audit** that assesses overall conformance to the standard. It is a detailed, in-depth audit to assess the existence and effectiveness of the controls stated in the ISMS as well as their supporting documentation

Maintaining certification over a typical three-year period requires periodic **surveillance audits** to confirm that the ISMS continues to operate as required and observed in the certification audit.

SRI is a Full-Service, 27001 Accredited Registrar

As acceptance of international standards has grown, so has SRI. Established in 1991, **SRI was one of the first five registrars in the U.S.** SRI is also the first and only U.S.-based and U.S.-Wholly owned ANAB accredited ISO 27001 registrar.

SRI Auditors Make the Difference

From its leadership role, SRI has built its business by employing the best auditors in the field. Our senior auditors are seasoned professionals averaging more than 25 years of experience. They know the standards and the industry so they can step right in and add value to your audit.

We know you have a choice.

Here's why you should choose SRI:

- Accredited by ANAB, RvA, IATF, SRI offers registration to a full range of standards to meet all your business needs
- SRI's web-based e-VENTS system, integrated with our fully automated operation support, puts all your sites' audit schedules, plans, and results at your fingertips when you need it, where you need it
- SRI uses the same audit team across audit events for greater consistency and effectiveness
- We offer Pre-Assessments and two-stage Registration and Renewal audits that give you one-on-one time with a lead auditor and an early look at your system, which leads to a smoother registration audit
- SRI's no-surprises, practical, open-book approach builds strong, long-lasting relationships
- We are one of the top five U.S. owned and operated registrars, and among the first to be QS-9000 and ISO/TS 16949 qualified. Decisions regarding your business and registration are made right here by us
- SRI's membership in key QMS and EMS technical advisory groups, and participation in industry standards development and oversight, ensure you are among the first to know about changes that will affect your business
- Training conducted publicly by our lead auditors on standards and requirements gives you the practical, hands-on knowledge you need to succeed
- Our organization is the right size to provide responsive, one-on-one service to every client. We are ready when you need us

SRI Information Security Registrar

ISO 27001 Certification

a division of SRI Quality System Registrar

Headquarters
300 Northpointe Circle
Suite 304
Seven Fields, PA 16046
TEL 724.934.9000
FAX 724.935.6825

ISO 9001
ISO/TS 16949
AS9100/9120
ISO 27001
ISO 20000
ISO 14001
RC14001/RCMS
ISO 13485
OHSAS 18001/Z10