

## ISO 27001 Compliance

### What is ISO?

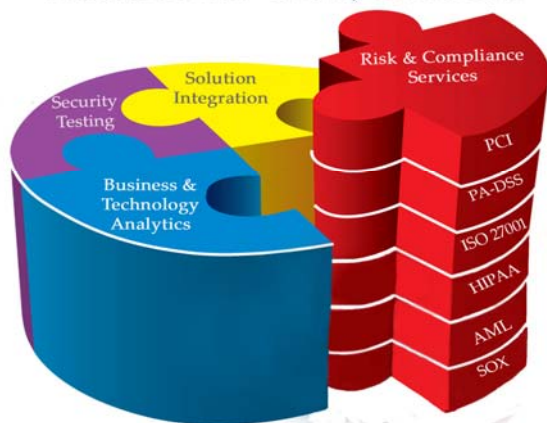
The International Organization for Standardization is an organization made up of member nations that develop standards for everything from electronics to management systems.

There are various ISO standards that cover every aspect of business operation. In the critical area of information security management, ISO promotes the development of an international security standard, and provides best practice recommendations for its deployment by those who are responsible for initiating, implementing or maintaining IT security.

Commonly referred to as ISO 27k, the ISO/IEC 27001:2005 (ISO 27001), published in October 2005, is an Information Security Management System (ISMS) standard. An ISMS consists of documented security objectives and measures including security policies, procedures, resources, and structures that effectively manage accessibility, confidentiality, and integrity of information assets and minimize information security risks. The ISO 27001 standard sets the requirements for an ISMS certification.

### Risk & Compliance Services

- Part of the Tevora™ Security Services Suite



The standard is comprised of two parts – The first covers a code of practice detailing what is necessary to establish, execute and sustain an Information Security Management System. The second covers a set of standard controls tailored to an organization's needs. ISO 27001 has increasingly become accepted as the single, overarching standard to assure that companies achieve compliance with numerous information-related security and compliance requirements.

### Who Should Comply?

The ISO Standards apply to nearly every type of company in nearly every area of business around the world. For ISO/IEC 27001:2005, each organization is expected to undertake a structured information security risk assessment process to determine its specific requirements, before selecting controls that are appropriate to its particular circumstances.

Organizations need only implement the security controls relevant to their business, and do not need to implement every single control identified in the standard. An external consultant with experience in ISO legislation can provide an array of services to help companies manage compliance, while reducing redundancies and cutting costs.

A systematic approach to maintaining the confidentiality and integrity of corporate information can pay significant dividends in dealing with both customers and vendors, thus helping to build a trusting relationship. The standard also provides an excellent method of implementing good governance regarding information security.

An ISO certificate also ensures that a company is in compliance with a full range of information-related legislation, including HIPAA, GLBA, SB 1386 and other State breach laws, PIPEDA, FISMA and EU Safe Harbor regulations.

Other practical reasons for implementing ISO standards is a systematic approach to maintaining the confidentiality and integrity of corporate information has far reaching benefits such as:

- ◆ Reducing the risk of an information breach
- ◆ Preserving consumer confidence
- ◆ Creating a safer, more resilient infrastructure

## **ISO Compliance: Tevora's Approach**

Assistance with achieving and demonstrating ISO compliance should be obtained through an experienced enterprise solutions provider that specializes in security and compliance; one that can perform an ISO 27001 Audit by a certified ISO 27001 Lead Auditor.

The objective is to analyze, remediate, and assess adherence to the ISO standard in a cost effective manner. An end-to-end compliance management solution helps identify vulnerabilities, define internal and external policies and manage changes and enforcement.

Tactical and precise, the road to ISO compliance can be as simple as the following three- step process:

### **Step 1: Gap Analysis**

A Tactical Gap Analysis and documentation review will go a long way in outlining strategies for a cost effective road to compliance. In this phase the lead auditor will request certain documents for review in order to ensure that proper documentation of the Information Security Management System (ISMS) exists. In addition to this, the lead auditor will interview key stakeholders and staff in order to determine that validity of the ISMS. Along with covering the general requirements of ISO/IEC 27001:2005, control validations should be made early on so remediation efforts can be direct and focused.

### **Step 2: Report of Recommendation**

This report demonstrates the existence of a best-practice based information security infrastructure.

### **Step 3: Remediation**

Whether it is writing security policies or implementing the recommended security controls; working hand in hand with a qualified lead auditor ensures direct and efficient ROI, and helps a company focus on the continuous improvement of its information security processes.

Following this process, a company should receive a certified assessment of compliance to all appropriate ISO security standards.

## **About Tevora**

Tevora Business Solutions is a leading international consulting firm specializing in information assurance, governance and compliance. With a distinctive combination of proven services, Tevora aids enterprises in protecting their most important assets from external and internal threats. We base our practice on the need for clarity, objectivity and expertise and utilize proven methodologies and industry best practices. In a world where enterprises are facing increasingly complex information security challenges, Tevora's expertise assures its clients skilled solutions. Tevora was founded in 2003 and is based in Lake Forest, California.

Please contact us for more information:  
e: [info@tevora.com](mailto:info@tevora.com)  
t: (949) 250 3290  
f.: (949) 250-9993

[www.tevora.com](http://www.tevora.com)