# IT INDUSTRY COMPLIANCE AND STANDARDS



The information technology sector is of vital importance to everything we do today. IT organizations must be vigilant about the security of their systems and data, while ensuring the efficiency of service delivery and customer satisfaction in order to fend off competition in an ever growing and advancing marketplace. Security isn’t only important at the IT level; it must also permeate every level of the organization, from the CEO all the way down to the custodial staff.  
  
Implementation and registration to international quality management systems standards is an excellent way for IT organizations to handle these challenges, and to provide reassurance to their client base that their information is secure.

## IT organizations can benefit from the following ISO information security standards:

* **ISO 27001 Information Security Management Systems:** ISO 27001 establishes concrete information security standards for use by data centres and other organizations. Most recently updated in 2013, the latest revisions reflect the increased importance of cloud computing and software-as-a-service. One of the key components of ISO 27001 is the established controls and control objectives — an essential part of any risk management plan. These controls include everything from human resources policy to encryption standards. Cumulatively, they reflect a set of best practices for information security management at the organizational level.
* **ISO IEC 20000-1 Information Technology Service Management:** ISO IEC 20000-1 is a set of standards for IT service providers that outlines best practices for maintaining security, delivering consistent service, and adopting new technologies as they become available. The standard sets out system requirements, codes of practice, relationship, resolution and control processes, and more. The most recent revision was published in 2011.

## **Other top ISO standards that can be used in industry-**



# **ISO 9001**

By far the most popular family is that of ISO 9000. A family of quality management standards, there are fourteen in total. Of these, ISO 9001:2015 is the only one that can be certified to. It was first published in 1987, and has since been updated about every 7 years. The standard details how to put a Quality Management System (QMS) in place to better prepare your organization to produce quality products and services. It is customer focused, and places an emphasis on continuous improvement and top management processes that extended throughout the organization.

The standard was updated in 2015, and now places a greater emphasis on risk management. The standard is generic, and can be used in any organization in any sector.

# **ISO 27000**

This family of standards concerns information technology, with the goal of improving security and protecting company assets. Started in 2005, the two most popular standards are ISO 27001:2013 and 27002:2013. 27001 is management-based system, whereas 27002 is a technical document, focused on the individual and putting a code of conduct in place.

Organizations can choose either standard; ISO 27001 has over 22,000 certifications worldwide. It is a broad standard, and for this reason the certification can be customized to fit the needs of the organization, and is not mandatory.

# **ISO 50001**

One of the newest standards, the energy standard ISO 50001:2011 is nevertheless becoming increasingly important. Released in 2011, the standard is meant for companies to put in place an Energy Management System (EMS) dedicated to improving energy usage and efficiency. This includes reducing an organization’s energy footprint by reducing greenhouse gas emissions as well as energy cost.

# **ISO 31000**

It is very important for an organization in any field to be able to manage risk effectively. ISO 31000:2009 puts in place a risk-management system to do just that. It was created in 2009 as an attempt to create a universally recognized program to reduce risk, eliminating the need for the many standards in other industries that include risk. The standard allows a company to better identify threats before they occur, and effectively allocate and use resources for risk treatment.

# **ISO 26000**

A relatively new standard, ISO 26000 focuses on social responsibility and was released in 2010. It cannot be certified to, but rather provides guidance on how businesses can operate in a socially responsible way. It helps clarify what social responsibility is, and helps organizations put in place the methodology to take effective actions relating to global social responsibility.