ISO 27001: Information Security Management System

An overview and understanding of the need for an information security management system framework

For more information related to products and services please contact The Strategic Consulting Group www.myscg.ca.

THE Strategic Consulting Group

THE
Strategic Consulting Group

INTRODUCTION

According to Wikipedia, Industry 4.0 is a name for the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing. In other words, big data and lots of information will be driving the future of manufacturing. However big data and information are not just limited to manufacturing we now see it in our day to day lives, from healthcare to streaming entertainment into our homes. The increase in information is also driving an increase in cloud computing and cloud storage needs as well. As an example, the cloud storage market is projected to increase with a compound annual growth rate of 30% from 2017 to 2022 to reach market size of US $92.48 billion.

So, what you may say, cloud services or big data won't impact my organization, well that may not be the case. Along with the increase in cloud services is the increased need for cyber security for all sizes of organizations. Small and Medium Enterprises (SMEs) have become easy targets for cyber criminals with and estimated loss of US $75 billion per year due to ransomware alone. If for some reason, you think that investing in new firewall technology will ensure your information is secure you run the risk of being one of the SME statistics. What organizations need is a framework for an Information Security Management System (ISMS) and ISO 27001 is just that framework. This white paper examines the reasons why an organization should use ISO 27001 as a tool for implementing a robust ISMS.

A Brief History of ISO 27001 Standard

Originally adopted in the UK in 1992 under a different name and use the standard has evolved to be what we know it as today:

- In 1992 The Department of Trade and Industry (DTI), which is part of the UK Government, publishes a 'Code of Practice for Information Security Management';
- In 1995 the Code of Practice is amended and re-published by the British Standards Institute (BSI) as BS7799;
- In 2000, BS7799 is re-published, this time as a fast-tracked ISO standard to become ISO/IEC 17799;
- In 2002 a second part to the standard is published: BS7799-2. This is an Information Security Management Specification, rather than a code of practice. It begins the process of alignment with other management standards such as ISO 9000;
- In 2005 ISO 27001 is published, replacing BS7799-2, which is withdrawn. This is a specification for an ISMS, which aligns with ISO 17799 and is compatible with ISO 9001 and ISO 14001; and
- In 2013 the newest release of ISO 27001 is updated and published and is also referred to as ISO 27001:2013.

The 2013 revision includes the High Level Structure (HLS) that is identical to several other ISO standards. HLS not only provides standard alignment it also provides management with more autonomy and flexibility with their individual interpretation and adoption of the standard. Further HLS removes the prescriptive lists of past standards and replaces it with a descriptive framework that can be integrated into the organization's Business Management System (BMS).

Why Adopt ISO 27001

An information threat storm is brewing in the cybersphere, small and large organizations need to be prepared.

A storm is brewing in the cybersphere while the demand for cloud computing services, storage, big data and information increases so does the cyber threat landscape which has become more hostile with denial of services, ransomware and increasing data breaches. In the midst of this storm, organizations, small and large are facing the growing threat of cyber-attacks that can impact them in more ways than one, including:

- Loss of information or the access to information, thus paralyzing their operations from hours to days;
- The release of customer data and a requirement to disclose the loss, that can result in a loss of trust and legal fees;
- A slower uptake of customers to open accounts or to use the organization's cloud based services resulting in material financial damage to the bottom line; and
- Although early adopters looked at the risks of the brewing storm, they also had to meet information security requirements by customers or governments agencies and departments that purchased cloud based services.

Today cyber risks are increasing daily and customer demands for information security is increasing at the same rate. Organizations both small and large private and public need a framework for ISMS and the ISO 27001 standard is an excellent framework for anyone who has information assets that needs protection. Along with protecting information assets, the framework can be used help improve the performance of the organization. Finally obtaining external verification through the ISO registration process ensures that the organization has adopted and implemented best practices.

How To Make it More Than a Framework

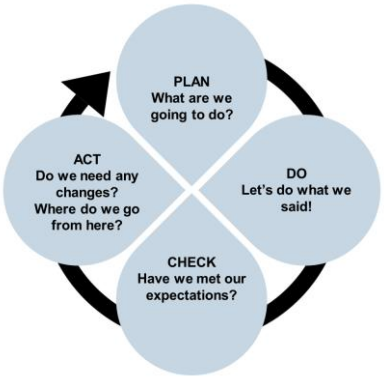
The International Organization for Standardization has stated that *"ISO was founded with the idea of answering a fundamental question: what's the best way of doing this?"*

In the case of ISMS, ISO 217001 is regarded as the best internationally recognized framework for securing information assets. Along with the framework ISO 27001 can be used as a change management agent to establish an organizational culture that empowers employees to take action to protect information. An ISMS framework, is a systematic approach to managing information so that it remains secure and includes four major elements: ***People, Risk Management, Processes and IT Systems.***

It all starts with the executive branch of the organization with a commitment to being involved in the adoption of the information security culture by leading through day to day examples. The process takes time and effort and is more than just a list of requirements that you tick off one at a time until you reach the bottom. The adoption process involves:

- An Initial Site Survey;
- A Comprehensive Change Management Plan;
- A Detailed Implementation Project Plan;
- Awareness Training for Management;
- Awareness Training for Employees;
- Information Flow Diagrams;
- Reviews of Existing Documents, Policies, Processes and Procedures;
- Updates or The Creation of New Documents;
- A Detail Risk Management Site Assessment;
- The Creation of Risk Management Plan
- The Creation and Implementation of a Risk Register;
- The Integration of the ISMS into the BMS;
- Ongoing Internal Audits, Corrective Actions and Updates;
- Management Review of Findings; and
- The Initial and Ongoing Registration Audits.

Like other ISO standards ISO 27001 follows the PDCA model.



Regardless of the size of the organization adopting ISO 27001 is a process that takes time that can last up to a year to reach your first registration audit. From that point forward if you've integrated the ISO 27001 framework into the organizations' BMS culture future audits will only reaffirm the organizations commitment.

Integrating Information Security principles in your Business Management System (BMS) will provide the organization the confidence it will continually meet its clients growing information protection expectations as the cyber threat landscape changes. By going the extra mile and getting ISO registration of your ISMS the organization is:

- Providing verifiable evidence that its taking appropriate control measures to protect confidential and privileged information;
- Following recognized and accepted best practices to mitigate cyber threats and has cyber incident response and management processes to respond to a potential cyber-attacks; and
- Using a formal information risk management process that is integrated into its Information Security Risk Management System.

Conclusion

In the past executives, may have been willing to accept the risk of ignoring cyber threats or information security breaches, however that time has passed. Information threats can no longer be assumed as a binary adoption process of yes or no "if we adopt" issue or simply reduced to technical risk that can be mitigated by a better firewall

policy. Instead today's executives and Boards of Directors must take into consideration the changing landscape of information threats along with the costs of information loss and ensure that their organization has instilled a culture that manages those risks effectively and efficiently.

About The Strategic Consulting Group

The Strategic Consulting Group's consultants have the hands-on experience and in-depth knowledge of ISO standards to help your organization reach its transition or registration goal. Our team provides strategic and practical solutions to help overcome CHALLENGES. We work with a range of private and not for profit organizations across Canada and the USA. Our approach is to develop strategies by using Predictive Analytics, Strategic Visual Harvesting and Cognitive Diversity. Integrating the three, hyper focuses a team, eliminates social influences, inherent biases, and delivers highly predictable and accurate ISO strategic solutions.

From one on one coaching, workshops, retreats and consulting mandates our services are realistic with measurable results, geared to your schedule, needs and challenges.

For additional information please contact:
The Strategic Consulting Group
Email: Info@myscg.ca
Tel: 613-604-9600

THE Strategic Consulting Group