Business case for an Information security Management System based on the ISO/IEC27000 series standards for HSBC

IT13032852
R.M.M.D Gunathialake
weekday

Introduction

HSBC is one of the world's largest banking and financial services organizations. they serve more than 47 million customers through four global businesses: Retail Banking and Wealth Management, Commercial Banking, Global Banking and Markets, and Global Private Banking. Our network covers 71 countries and territories in Europe, Asia, the Middle East and Africa, North America and Latin America.

Their objective is to be the world's leading and most respected international bank. they help small and large companies grow domestically and internationally, and are developing wealth management services and investing in retail banking in markets where they can achieve profitable scale.

Why HSBC need Information Security Management System (ISMS) ?

Banks face a difficult challenges in the area of security management. With a growing population of internal and external users accessing an increasing number of applications, the need has brown exponentially for banks to develop a new generation of security tolls that can help them better comply with regulations, control access to confidential data and limit identity theft. At the same time, banks are challenged to institute security measures that satisfy users who are demanding both stronger security and ease of use and control often competing priorities.

Every asset in every organization must be protected and information is an asset which must be protected as well. During the evolution of human race the value of information is growing constantly. The higher the value of information the more effectively it must be protected. There are a lot of schemes and mechanisms for information protection. One of the most popular systems that helps organizations to establish information security is the ISMS defined by ISO 27000 standards. The benefits of implementing an ISMS in this case seem obvious.

ISO/IEC 27000 certification enforces most stringent controls to ensure ample security measures are implemented to protect the Bank's information assets. ISMS provides a framework for

- establishing information security policies
- risk assessment and risk treatment
- management of information assets
- human resources security
- operational security

- physical and environmental security
- communication and operational security
- acquisition and maintenance of information systems
- information security incident management
- vulnerability management
- security in supplier management and business continuity and disaster recovery.

The benefits of implementing an ISMS

The ISMS is a system which drives the management of Information, regulates the information flows and builds an environment for information protection. The ISMS is not a single document or even a single process, it is a set of well-organized processes and documents. All the benefits of implementing an ISMS derive from those well organized processes and documentation.

The ISMS is a system which drives the management of Information, regulates the information flows and builds an environment for information protection. The ISMS is not a single document or even a single process, it is a set of well-organized processes and documents. All the benefits of implementing an ISMS derive from those well organized processes and documentation. Well organized ISMS helps organizations to identify the assets subject to risks, evaluate and manage these risks in a proper manner, monitor the implemented controls. The phases of risk management methodology of ISMS are similar to other standards: Risk Identification, Risk assessment and Risk treatment.

The main objective of using ISMS is,

Three basic security concepts regarding the information on the internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation.

By implementing ISMS the organization can gain,

- A trust, confidence and credibility of its clients
- Greater awareness of its security.
- Compliance with regulatory requirements
- Confidentiality, integrity and availability of assets
- Prevention of security breaches
- Prevention of unauthorized access of critical information
- Competitiveness
- Management commitment to the information security
- Public recognition of its security benchmark

ISMS Cost

- Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k
- Obtain management approval to allocate the resources necessary to establish the implementation project team .
- Employ/assign, manage, direct and track various project resources.
- Identify and deal with project risks, preferably in advance.
- Track actual progress against the plans and circulate regular status reports/progress updates.
- Hold regular project management meetings involving key stakeholders.
- Upgrading the ISMS .

Other ISMS implementation costs

- Assess security risks to information assets, and prioritize them
- Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual terms *etc*.
- Conduct awareness/training regarding the ISMS, such as introducing new security policies and procedures[1]
- Determine how to treat information (Re-)design the security architecture and security baseline

Certification costs

- Assess and select a suitable certification body.
- Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body.
- Staff/management time expended during annual surveillance visits.