Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure-2016

Business Case-Lab Assignment 03

Submitted by:

IT13038656

P.H.A.S.Rajapaksha

Business case for Hatton National Bank for an Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k)

Introduction

Hatton National Bank PLC is a leading private bank in Sri Lanka with 256 branches and 452 ATMs spread across the island. It has eight representative offices in the UAE, Bahrain, Italy, Oman, and Qatar. In 1888 the hill station of Hatton saw the genesis of a bank, aptly named Hatton Bank. HNB has been internationally recognized by the Asian Banker Magazine as the “Best Retail Bank in Sri Lanka” on eight occasions from 2007 to 2012 and in 2015. This bank is actively involved in retail banking, corporate banking; international banking, treasury and project financing. HNB has gained certification to international standard including ISO 9001 (Quality Management) to provide professional service.

ISO/IEC 27001 - Information security management

ISO 27001, has been developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.". It’s was developed and supported by the member nations of the International Organization of Standardization (ISO), an organization chartered by the United Nations. The ISO 27000 series of standards evolved from the British Standard BS 7799. Originally published in 1995, Part One of BS 7799, the Code of Practice (aka the implementation guide), is now the basis for ISO 27002 (formerly known as ISO 17799). Part Two of BS 7799, first published in 1998 is the auditable ISMS set of specifications, now embodied in ISO 27001. The ISMS presents a systematic approach to keep sensitive information secure. It manages people, processes and IT systems through

applying risk management processes. The ISMS suits not only large organizations but also small and medium businesses.

Purpose

The bank industry is subject to increasingly intense regulatory scrutiny island wide, and HNB's clients also come from a number of highly regulated industry sectors including Garment, Constructions and Productions. HNB provides different facilities including saving accounts, current accounts, loans, cards, remittance, leasing, online banking and internet banking etc. Not only that most of the customers' deposits are high range amount of money and withdrawing money in a frequent manner and they expect high privacy between money transactions. Therefore, HNB is facing increased security challenges of managing sensitive company information such as customers' financial information, transaction details as well as employees' information.

Information security is fundamental to the success of HNB services with much of its work involving receiving, analyzing and storing sensitive consumers and bank employees' information. It is vital that the bank has appropriate controls in place to protect its systems from hackers, and prevent personal information on its systems falling into the wrong hands as there is a real risk it could be used by criminals to commit identity fraud. It is therefore imperative that HNB can assure its customers and the general public that it takes the security of their personal information seriously.

The bank is regularly audited by interested parties such as Audit Department of Sri Lanka and HNB anticipate that moving forward, this third party scrutiny will only increase. As such, it is HNB's aspiration to get on the front foot by becoming the most compliant bank in its industry.

Benefits

- The ability to stand apart from competition. Attaining ISO 27001 will give a highly effective market differentiator for the bank. The bank's competitors are most likely already looking at or moving toward ISO 27001 certification. Then the certificate will provide bank with a competitive advantage and it shows consistency in the delivery of bank services.
- HNB can deployed ISO/IEC 27001 to protect the confidentiality of both its own and its partners' and customers' financial and transaction information. Clients and the general public can have total confidence in HNB's information security practices and the way their personal information is managed. Therefore, enhance customer satisfaction as well as that improves client retention and help to increase profits.
- Information security of the bank's sensitive data is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, minimize cyber-attacks/cyber-crimes and maximize business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware. Implementation of ISO/IEC 27001 will satisfy above facts continuously.
- Banks are audited for various reasons by the Audit department in Sri Lanka. ISO/IEC 27001 allows the bank to meet a level which satisfies these audits.
- Core requirements of ISO/IEC 27001 is to ensure an organization manages key assets in a way that is appropriate to the business. Therefore, the bank can identify their key assets and how best to protect them and this provides a framework for managing the assets of the bank.

Costs

- The time and internal resources required to implement a system. Developing policies, procedures and ensuring end-user training and awareness all taken time even when using internal resources and cost will also depend on size of the organization, the risk assessment, the level of protection you need, technology, legislation, etc. HNB is a large scale financial organization in Sri Lanka. Therefore, ISMS implementation project management cost will get high.
- External consultancy support can help shortcut many issues, but at the end of the day the bank has to spend time developing and using its information security system, and this all come with a cost.
- The other typical costs are project management, technology, training, employee time and certification.
    - Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body.
    - Staff/Management time of the bank expended during annual surveillance visits.
- Costs for periodic review and maintenance of information security policies, standards, procedures, guidelines, contractual terms etc.