Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure-2016

Business Case-Lab Assignment 03

Submitted by:

Marasinghe M.M.K.B

IT13127374

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

Introduction

Union Bank established in 1995, as the 8th indigenous Bank. Union Bank is amongst the top 5 private commercial Banks in Sri Lanka in market capitalization, offering a full range of products and services to personal and commercial financial sectors. This Bank delivering a unique value proposition, backed by exceptional service, Union Bank continues to expand its reach across Sri Lanka through a robust channel strategy consisting of an island-wide branch network and alternate channels. This bank listed in the Colombo Stock Exchange and synonymous as a rapidly progressing and potential business entity that has attracted top globally and local investors.

In Year 2014, marks significance for Union Bank with TPG the US based global investment firm with $67Bn in capital under management acquiring 70% equity in the Bank. This investment marked a milestone in the financial services industry as one the largest foreign direct investments to Sri Lanka. Union Bank's growth is further augmented with its strategic diversifications and its subsidiaries include National Asset Management Limited, Sri Lanka's premier Asset Management Company and UB Finance Company Limited. Union Bank has etched for its self a solid foundation of financial stability backed with international know-how and best practices and is rapidly progressing as one of Sri Lanka's fastest growing Financial Services Groups supported by the strength of a global giant.

ISO/IEC 27001 - Information security management

The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC).

The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

The standards are the product of ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Subcommittee 27), an international body that meets in person twice a year.

Purpose

In modern days stored the amount of data electronically is overwhelming in the bank industry, and that figure is only going to increase over time. Unfortunately, with the increase in cyber data comes the increase of cyber-attacks. Hackers are a constant threat to any industry that utilizes technology. ISO 27001 is an information security management standard that provides organizations of any size and industry a framework for securing and protecting confidential and sensitive data.

The banking industry, in particular, can benefit from an ISO 27001 certification. Union Bank collect a great deal of personal information from their clients, and with the switch to electronic data storage, that information is more so at risk. It's an obvious target for cyber hackers; a one-branch to branch for information on credit, deposits, social security, and more. Because of this risk, Bank are drawn to organizations that can provide information security, and especially drawn to organizations that can prove their commitment.

An ISO 27001 is the proof organizations need to set themselves apart from the competition. It identifies and alleviates information security risks, guards confidential information, and lets clients/banks know that the value their confidentiality. In the likely event that further regulations are put on the banking industry in the future, Union Bank will be more prepared to adapt with an ISO 27001 certification.

Union Bank can gain many benefit from an ISO 27001 certification. Banking organizations can assure their clients that they care for their safety and confidentiality by taking every precaution necessary through ISO 27001.

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.

- Union Bank 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 Union Bank'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

1. The cost of literature and training

Implementation of ISO 27001 requires changes in Union Bank, and requires new skills. Bank can prepare their employees by buying various books on the subject and/or sending them to courses (in-person or online) – the duration of these courses varies from 1 to 5 days .And bank have to buy the ISO 27001 standard itself .

2. The cost of external assistance

If bank don't have a well-trained project manager with deep experience in ISO 27001 implementation, Bank will need to hire someone who does have such knowledge – bank can either hire a consultant or get some online alternative .

The greatest value of someone with experience helping bank with this kind of project is that they won't end up in dead end streets – spending months and months doing activities that are not really necessary or developing tons of documentation not required by the standard. And that really costs.

3. The cost of technology

Most of the time bank initially need a big investment in hardware, software or anything similar.. The biggest challenge was usually how to use existing technology in a more secure way.

4. The cost of employees' time

The standard isn't going to implement itself, neither can it be implemented by a consultant only. Employees have to spend some time figuring out where the risks are, how to improve existing procedures and policies or implement new ones, they have to take some time to train themselves for new responsibilities and for adapting to new rules.

5. The cost of certification

If bank want to obtain public proof that they have complied with ISO 27001, the certification body will have to do a certification audit – the cost will depend on the number of man days they will spend doing the job, ranging from under 10 man days for smaller companies up to a few dozen man days for larger organizations. The cost of man day depends on the local market.