



SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

Lab Assignment

Business Case study for implementing an ISMS to Union Bank

R.G.H.K.Wijewickrama

IT13033538

Weekday – IT

Introduction

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. 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.

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. Supported by the strength of a global giant, 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.

Their vision is to be the innovator of banking solutions to the wider corporate, SME and Retail segments and to be their Bank of choice, through professional and empowered people. Since they are mainly concerned on achieving their targets they also need to think of how to secure the information which they are maintaining and how to manage them. So to accomplish that ultimately they need to implement ISMS within the bank.

Why Union bank needs an Information Security Management (ISMS)..?

Information is a valuable asset that can make or break your business, so the security of information (infosec) should be a high priority. Union bank is a large organization which has many branches all around the country and have countless methods of internal and external communication, each of which can lead to a breach in confidentiality and even more importantly, a leak of crucial information to competitors and the outside world. Hence information has to be properly managed and it allows you to operate with confidence. Finally Information security management gives you the freedom to grow, innovate and broaden your customer-base in the knowledge that all your confidential information will remain that way.

For an example imagine that your or your business partner's network is down for a couple of hours, that the data stored in your computer is lost, or that your competitor(s) have obtained your customer lists and business plans? How much will this cost you? Can your company bear such costs? Considering the consequences, the importance of setting up a comprehensive information security management system immediately becomes apparent.

Information which are managing by the union bank is very sensitive since most of the details contain of their customers. They need to be highly secured and properly managed. That is the place where ISMS is going to play its role.

Benefits of implementing an Information Security Management System (ISMS) based on ISO/IEC 27000 series standards (ISO27k) at Union Bank

- Quality assurance - With a suitable ISO 27001 implementation the management can be assured they have a recognized framework for dealing with the information security.
- Confidentiality, integrity and availability of assets - As the ISMS is a system mainly designed for the information security it regulates and helps to provide the confidentiality, integrity and availability of assets.
- Better risk planning - The information security strategy can be integrated with the overall organizational risk strategy leading to a comprehensive platform on which risk planning decisions can be made.
- Better employee relations – Clear policies and guidelines makes things easier for staff. This will increase employee satisfaction and may help reducing staff turnover. Better security awareness programs, trainings and clear disciplinary procedures will also induce increased professionalism among the employees as well.
- Increased profits – Since customers are satisfied because when they realized the organization is embedded with an ISMS they tend to come to the same place and it even makes a positive image within the other customers too. This would drive higher customer satisfaction, new customers and increased profitability. This can even be leveraged as a competitive advantage over the rival organizations.
- Security awareness – Since the ISO 27001 implementation and its practice is a continuous process that will engage organizational personal in various security related aspects it will raise the overall employee awareness about the security aspects.
- Management commitment to the information security - The ISMS makes the management pay more attention to the information security risks and issues.
- Public recognition of its security benchmark - Organizations can benchmark their achievement in ISMS and gain public recognition.
- Compliance with regulatory requirements - Establishing the ISMS, especially when following the requirements of security standards, organizations more likely become compliant to regulatory requirements, because the regulators itself follow these standards.

Costs of implementing an Information Security Management System (ISMS) based on ISO/IEC 27000 series standards (ISO27k) at Union Bank

- Need to manage or upgrade the Information Security Management System with ISO standards periodically (ex: year by year).
- Should identify what are the risks to be maintained and what are the information need to be secured.
- Management staffs of every department of the bank need to be trained to familiar with the ISMS. And also there is a cost for the trainers.
- Cost of external assistance - A suitable person has to be found to implement ISMS. Unfortunately, training your employees is not enough. If you don't have a project manager with deep experience in ISO 27001 implementation, you'll need someone who does have such knowledge.
- Cost of technology – Determine how to use Software, Hardware in a more secure way and should be taken to the organization.
- 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.
- Cost of certification - If you want to obtain public proof that you 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.