SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

(ESBPII)

4th Year 2nd Semester 2016

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

For

DFCC Bank PLC

(http://www.dfcc.lk/en/)

Name: K.G.C.C Kulasekara

SLIIT ID: IT13133146

Date of Submission: 08/27/2016

Table of Content

1 Introduction

Development Finance Corporation of Ceylon (DFCC Bank) is a private development and commercial bank in Sri Lanka. It was Established in 1955 with a mandate to spearhead development financing in a newly independent nation, DFCC Bank PLC has over the past 60 years grown, evolved and diversified to meet the changing needs and aspirations of an emerging economy. It is Involved in leasing, lending, investing banking, deposits, cash management, fund management and unit trusts, venture capital and industrial estates. A career at DFCC Bank promises opportunities for development, a variety of benefits and a culture that values professionalism, teamwork, openness, diversity, respect for individual values and recognition. Whether you are looking for a job or internship opportunity, at DFCC you are free to shape your own path, working with professionals who are focused on sustainable business growth.

2 Why they select ISO 27001 security standards?

Information Security Management System (ISMS) is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career. DFCC Bank uses almost 40 different technologies. Various services, infrastructure and applications are built around these technologies. As described under the processes enabler, each of these services is mapped to the information security maturity level. A continuous updating of the maturity level against attributes such as automation, effectiveness, incident management and measurement ensures that these services are monitored very closely. All projects for improvement of the services are based on the maturity level aimed at the particular service.

2.1 Compliance

It might seem odd to list this as the first benefit, but it often shows the quickest “return on investment” – if an organization must comply to various regulations regarding data protection, privacy and IT governance (particularly if it is a financial, health or government organization), then ISO 27001 can bring in the methodology which enables to do it in the most efficient way.

2.2 Marketing edge

In a market which is more and more competitive, it is sometimes very difficult to find something that will differentiate you in the eyes of your customers. ISO 27001 could be indeed a unique selling point, especially if you handle clients’ sensitive information.

2.3 Lowering the expenses

Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees.

The truth is, there is still no methodology and/or technology to calculate how much money you could save if you prevented such incidents. But it always sounds good if you bring such cases to management’s attention.

2.4 Putting your business in order

This one is probably the most underrated – if you are a company which has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain information assets, who has to authorize access to information systems etc.

ISO 27001 is particularly good in sorting these things out – it will force you to define very precisely both the responsibilities and duties, and therefore strengthen your internal organization.

To conclude – ISO 27001 could bring in many benefits besides being just another certificate on your wall. In most cases, if you present those benefits in a clear way, the management will start listening to you.

3 Advantages

The ISMS will bring information security under firm management control, allowing direction and improvement where needed. Better information security will reduce the risk (probability of occurrence and/or adverse impacts) of incidents, cutting incident-related losses and costs.

- To assure clients of creditability and reliability.
- To demonstrate commitment to quality of the bank.
- To fulfill corporative mission of transparency and excellent customer service.
- To provide competitive edge and helping to spread banks investments in any other areas.
- To helps to govern the protection of information.
- Improves efficiencies and increase profits.
- To bring flexibility and resilience in banking service.
- To boost the working environment of the bank.
- To helps to develop and manage interactions with other organizations.
- To have a good security policy for the bank.
- For information asset management.
- For HR security.
- For physical and informational security.
- For communication and operations management.
- For Access control.
- For information systems acquisition, development and maintenance.
- For information security incident management.
- For compliance and audit in the bank.
- For Automation of user-provisioning.
- For outsourced employee screening process.
- For effective data disposal procedure.
- For have a good incident response procedure in place.

4 Cost for having an ISO27001 security system

4.1 Information security movie

A 20-minute movie was created and presented with all the trappings of a real movie theatre experience (e.g., tickets, popcorn). The movie has proven extremely popular, and so far 40,000 employees have seen it. Every training program begins with this movie.

4.2 Information security cartoon strip

A cartoon strip was created with two characters, one named Sloppy and the other Sly. Their exploits entertain the readers and also carry a very powerful security message. This cartoon strip is now planned to be printed in a calendar format.

4.3 Email and picture campaign

Regular emails are sent cautioning everyone about being alert, e.g., a reminder about avoiding phishing emails is sent after any successful.

4.4 Ten security commandments

The user policy document has been summarized into key information security rules that are easy to read and remember.

4.5 Security First course

All employees have to undertake this one-hour course every two years. Taking the examination and obtaining passing marks is mandatory. A certificate is issued to all successful candidates. The certificate acts as an official recognition. Apart from the certificate, the star performers are also recognized through global mailers sent to all the bank’s employees as well as monetary rewards.

4.6 One-day workshop

A one-day workshop is conducted periodically for senior management at which the CISO explains the importance of information security for the bank and the specific measures deployed for its implementation.

5 Github Link

Github Link – (https://github.com/CharithaKulasekara/ESBPII-IT13133146/tree/master/ESBPII-LAB5)