SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Name: Dissanayake D.M.L.N

SLIIT ID: IT13057220

Practical Session: Business case for ISO 27001K

Company name: DFCC bank

Date of Submission: 02.09.2016

1. Introduction

DFCC Bank was established in 1955 with a mandate to spearhead development financing in a newly independent nation. Currently it has a nationwide network of 137 branches and 257 ATM`s. They covers 50 towns and cities. DFCC Bank operates in a highly automated environment in terms of IT and communication systems. All of the bank's branches have online connectivity, which enables the bank to offer speedy funds transfer facilities to its customers. Multi-branch access is also provided to retail customers through the branch network and ATMs. The bank has prioritized its engagement in technology and the Internet as one of its key goals and has made significant progress in web-enabling its core businesses. In each of its businesses, the bank has succeeded in leveraging its market position, expertise and technology to create a competitive advantage and to build market share.

2. Why they select ISO 27001 security standards?

DFCC Bank uses almost 35 different technologies. Infrastructure, various services and applications are built around these technologies. As described under the processes enabler, each of these services is connected 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.

Marketing edge

When in marketing background, 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.

Lowering the expenses

For a company it is highly recognize to reduce cost of expenses. There for in security section, 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.

Compliance

When considering to a company, 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.

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.

- To assure clients of creditability and reliability.
- To helps to govern the protection of information.
- To bring flexibility and resilience in banking service.
- To boost the working environment of the bank.
- 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.
- 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 information asset management.
- For HR security.
- For physical and informational security.
- For communication and operations management.
- For Access control.
- For outsourced employee screening process.
- For have a good incident response procedures in place.
- To helps to develop and manage interactions with other organizations.
- To have a good security policy for the bank.

4. Cost for having an ISO27001 security system.

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