SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Name: Gunasinghe S.U

SLIIT ID: IT13022570

Practical Session: WD Friday

Practical Number: Lab 5

Introduction

OrangeIT is a leading Software company in Sri Lanka. They offer wide variety of business solutions in software, mobile and web designing and development. They have so many important information stores. So they are dealing with huge scale of important details. So it is so important to have a standard system to make sure the data and information are secured.

Every organization must have an Information security management system (ISMS). Because when the company is depend on the information, they have to concern about the risk that might be occurs in there information systems.

When there are huge numbers of information to handle with, several treats can be occur. As Information technology firm OrangeIT has much digital information. So those can be copy, modify or steal. Also information can be corrupted.

Also physical losses can be happened. Like natural disasters. Though these are digital information, there can be disk failures, power failures, modifying data, unauthorized access by unauthorized people also can be happen.

For reduce these risks and treats they need to have a proper system. They need a standard system to secure the information. ISO 27001 is the internationally accepted and recognized standard for ISMSs. ISO 27001 is intended to provide guidance on how to manage information security for an organization. To expand on this, the ISO standard is focused on an company as a whole, including all information types, systems, people, policies, processes, and technologies. It is very suitable for a Software firm like OrangeIT.

Benefits of having ISO27001

Holding an ISO 27001 certification is widely accepted proof of a reliable, defensible, standards-based information security posture. It confirms to both management and clients that the company is proactively managing its security control responsibilities.

ISO 27001, with its process-based and risk-driven approach, provides a mechanism to integrate information security into the company's overall risk management strategy. By making information security decisions on the defensible basis of risk management, the information security practitioner and business manager can employ a common terminology.

In addition, the information security function becomes more integrated with the company as a whole. Management gains a clear window into the results of its security investment, and better insight info which security processes are working well and which need improvement. And also it Keep confidential information secure. It protects the company, assets, shareholders and directors. This is protecting company’s reputation. This may increase the trust in customer trust towards the company.

Costs

As an IT company, Investing in IT security early on will reduce the costs to both the company's finances and reputation if a breach were to occur. Mitigation strategy: Educate and encourage members of management who understand the need to protect systems and are able to communicate that need throughout the company. To educate and encourage employees about the information security system may high costly. According to the company's assets that are available and size of the company may change the amount of the cost. But if once use this ISO27001 ISMS, they have to keep their standard without decreasing. Because if that standard decreases it will be a huge loses to the company. So they have to bear a high cost on keeping the standard still.

They have to train the company management and the employees to the ISO27001 standard. These training programs may be cost high. Sometimes they have to keep special systems to keep the standard still. So that may cost high because they have to educate the staff about the new system. And project managers also have to be knowledgeable about the ISO27001.

If they need a public recognition as they 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 task.

.