SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Name: Dedigamuwa D.A.T.D

SLIIT ID: IT13103378

Group Number:

Practical Session: WD Friday

Practical: ISO 27001 Business Case

Date of Submission: 02/09/2016

Introduction

IFS is a globally recognized leader in developing and delivering enterprise software for enterprise resource planning (ERP), enterprise asset management (EAM) and enterprise service management (ESM). IFS brings customers in targeted sectors closer to their business, helps them be more agile and prepare for what's next in their industry. IFS is a public company (XSTO: IFS) founded in 1983 and currently has over 2,800 employees. IFS supports more than 1 million users worldwide from its network of local offices and through a growing ecosystem of partners.

The main reasons we think about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons. All of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Benefits of having ISO27001

Fight cybercrime - Introducing the ISO 27001 information security management system will help protect business from the threat of organized crime.

Combat cyber-terror - Terrorist organizations now work with computers as well as explosives. Introducing an information security management system makes it easier to defend the company from a destructive cyber-attack.

Improve your corporate governance - Reducing Company's financial exposure to the risk of losses resulting from IT system failure is now a corporate governance requirement. ISO 27001 will help to comply.

Recover from accidents - With ISO 27001, can minimize the risk that company information will be lost or corrupted as a result of human error.

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**.**

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 the customers. ISO 27001 could be indeed a unique selling point, especially if you handle clients' sensitive information.

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. Company probably has 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 the company could save if company prevented such incidents. But it always sounds good if company bring such cases to management's attention.

Putting your business in order - This one is probably the most underrated; if the company which has been growing sharply for the last few years, it 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 an internal organization.

Costs

The costs of internal resources to produce the relevant policies and procedures. Getting guidance from external consultants need to be also factored in. External consultancy support can help shortcut many issues, but at the end of the day the company has to spend time developing and using its information security system, and this all comes with a cost. As part of our start up plan it was identified that ISO27001 certification was an organizational objective so this was considered in all business and strategic plans. Having this vision allowed us full visibility of the costs, which were primarily resourcing and infrastructure related.

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.