SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Name: Fernando W.W.S.D

SLIIT ID: IT13032616

Practical Session: WD Friday

Practical Number: Lab - 5

Date of Submission: 02.09.2016

Business Case

Introduction

Virtusa is a global information technology (IT) services company. The company proves IT consulting, business consulting, technology implementation and application outsourcing services. Virtusa provides cost-effective services that enable its clients to use IT to enhance business performance, accelerate time-to-market, increase productivity and improve customer service. Over 9800 employees are working on this IT Company. Vertusa serve Global 2000 companies and the leading software vendors in Banking & Financial Services, Insurance, Telecommunications, Technology and Media, Information & Education industries.

Now a days organizations are depend on the information systems. So need to have a security program because it help to maintain IT security. And also it can use to identify and stay in compliance with the regulations that affect how you manage your data. Protecting data means protecting its confidentiality, integrity, and availability. Having a security program means mitigate the risk of losing data in any one of a variety of ways, and have defined a life cycle for managing the security of information and technology within the organization. The value of company is in its data. So need to have a plan to ensure the security of information assets in the organization without getting any risk. To ensure the company is secure, have to use better standards. ISO 27001, is the most effective way of reducing the risk of suffering a data branch.

Why you need to go with ISO 27001

The ISO 27001 Information Security standard provides companies with a structured and proven way to implement and manage an Information Security Management System. And provide management and the business with confidence in the security measures that are in place. An Information Security Management System is a systematic approach to managing a security of sensitive information and is designed to identify, manage and reduce the range of threats to which information is regularly subjected.

Information is a valuable asset that can make, or break organization, so the security of information should be a high priority. Protecting its information assets through defining, achieving, maintaining and improving security levels is essential for an organization to meet its objectives and strengthen its legal compliance and image. The coordinated activities needed to direct the implementation of suitable controls and mitigate unacceptable information security risks are part of information security management. So ISO 27001 certification helps you to demonstrate good security practices, thereby improving working relationships and retaining existing clients.

Benefits of having an ISO 27001

Protecting organizations information is critical for the successful management and smooth operation of the organization. Completing ISO 27001 information security management systems certification will aid our organization in managing and protecting valuable data and information assets.

Some of the benefits of ISO 27001 are leading international standard for information security management, protect the confidentiality, integrity and availability of information, provides customers and stakeholders with confidence in how organization manage risk, focus on all business process and business assets, focus on reducing the risks for information that for the organization, help to comply with other regulations, provide a competitive advantage, enhanced customer satisfaction, reduce third party investigation of information security requirements that improves client retention, Better visibility of risks amongst interested stakeholders, shows commitment to information security at all levels throughout organization, Improved information security awareness.

Costs

If we use ISO 27001 standard for our organization, most of the cost associated with information security. The foundation for ISO 27001 is organization risk assessment and then organization statement of applicability and risk treatment plan. This is where organization decide what controls organization need to put in place. Depending on this there might be controls that are already in place (zero cost) and there might be controls that needs to be designed and implemented. There is a cost associated with this but until organization has decided on the control and how to mitigate the risk organization is not able to budget for the cost.

To be successful with ISO 27001 design and implementation, ISO 27001 should be treated as a project and cost associated with this such as a project manager. Perhaps someone in the organization that has ISO 27001 experience as well as project management experience. In whatever case there is a cost, either internal employee time or external consulting assistance. So that's why ISO 27001 provide an overarching framework for information security management that encompasses a broad range of both external and internal requirements.

ISO 27001 is however not just done by having a project manager and a consultant. Involvement of employees is also a must. So this means cost in employee time doing training, risk assessment, writing documentation, reviewing documentation, etc. Sometimes cost depends on the certification body and the size of the organization and scope of the ISMS and number of man days.