Sri Lanka Institute Of Information Technology

ESBPII-Case Study

Business case for ESBPII assignment.

D.S.S.Dharmachandra

IT13136734

Introduction

Toshiba Corporation is a Japanese multinational conglomerate corporation in Tokyo, Japan, which supplier of IT services, hardware and software to corporate clients and develops, sells, repairs, and supports computers and related products and services. The company is one of the largest technological corporations in the world. With the time the number of clients got increased and Toshiba needed to improve more resources and information.

Toshiba sells Laptops, data storage devices, air conditioners, televisions, DVD and Blu-ray players', air-traffic control systems, railway systems, security systems. Information is a valuable advantage that can make or break the business, so the security of information should be a high priority

ISO/IEC 27001 is an internationally recognized best practice framework for an information security management system (ISMS). It belongs to the ISO 27000 series of standards (including ISO 27002 and ISO 27005). It helps you recognize the risks to your important information and put in place the correct controls to help reduce the risk.

Benefits

- Strengthens existing information security control environment by (re-)emphasizing business information security control requirements, upgrading current information security policies, controls etc. and providing stimulus to review and where necessary improve information security controls periodically
- It ensures that authorized users have access to info when they need it, which improves ability to recover operations and continue business as usual.
- Gives confidence in information security arrangements and better visibility of risks.
- It gives organization a straight forward way for responding to tender requirements.
- Improve information security awareness and reduces staff-related security breaches.
- Increased reliability, profits better human relations and security of systems.
- Based on globally recognized and well respected security
- Formally defines specialist terms, enabling information security issues to be discussed, analyzed and addressed consistently by various people at different times
- Positions the organization as a secure, trustworthy and well-managed business partner

Costs

- Project management costs

1. Find a suitable project manager
2. Prepare an overall information security management strategy
3. Plan the implementation project
4. Allocate the resources necessary to establish the implementation project team
5. Track actual progress against the plans and circulate regular status reports/progress updates
6. Identify and deal with project risks.

- Implementation costs

1. Compile an inventory of information assets
2. Assess security risks to information assets
3. Determine how to treat information risks
4. Re-design the security architecture and security baseline
5. Conduct awareness/training regarding the ISMS
6. Such as introducing new security policies and procedures.

- Certification costs

1. Assess and select a suitable certification body
2. Pre-certification visits and certification audit by an accredited ISO/IEC 27001 certification body
3. Risk of failing to achieve certification at first application
4. Staff/management time expended during annual surveillance visits.

- Operation and maintenance costs

1. Periodic ISMS internal audits to check that ISMS procedures are being followed correctly
2. Complete preventive and corrective actions to address potential and actual issues
3. Periodic review and maintenance of information security policies, standards, procedures, guidelines, contractual terms.