SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Business Case

Information Security Management System based on the ISO27001

Name: Pinnawalage H.U

SLIIT ID: IT13055486

Date of Submission: 02/09/2016

Business Case: Information Security Management System based on the ISO27001

Fortune Technologies Pvt. Ltd.

31th August 2016

1. Introduction

Fortune Technologies Pvt. Ltd is an upcoming global player in the innovative e-commerce solutions market. It was founded in May 2012 with the aim of supplying high quality software products and services to customers worldwide.

2. Why 'Fortune Technologies Pvt. Ltd.' needs an Information Security Management System (ISMS)?

Most organizations and businesses have some form of controls in place to manage information security. These controls are necessary for Fortune Technologies Pvt. Ltd. as information is one of the most valuable assets that the business owns that can make or break the business. So the security of information should be a high priority. Information security management gives the business the freedom to grow, innovate and broaden the customer relationship. Design and implementation of information Security Management System (ISMS) will also give internal business gains for the business such as better efficiency and higher productivity.

Designing and implementing ISMS will not only mean more business for the business, it will also provide a platform for protection of the most important assets as well as give Fortune Technologies Pvt. Ltd., a system that will ensure business continuity. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

ISO 27001 is the international standard for information security. ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control.

Businesses and organizations that adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard. Therefore Fortune Technologies Pvt. Ltd. can use the ISO 27001 framework to improve the business and to obtain external verification through ISO certification that can help create trust with business's potential customers.

3. Benefits of implementing an Information Security Management System based on ISO27k standards at 'Fortune Technologies Pvt. Ltd.'

a. Improves enterprise security

- Implementing and maintaining an information security management system (ISMS) certified to the internationally recognized data security standard ISO 27001 is the most effective way of reducing the risk of suffering a data breach.
- When Fortune Technologies Pvt. Ltd. uses ISO 27001 it systematically examines the information security risks, taking account of the threats, vulnerabilities and impacts that are unique to that organization.
- It provides a framework for the selection and implementation of information security controls and other forms of risk treatment to address those risks that are unacceptable to the organization.
- It ensures that the risk treatments continue to meet the organization's individual information security needs on an on-going basis.

b. Standardization

- ISO 27001 certification provides an internationally recognized, externally assured, quality mark for information security management for the organization.
- ISO 27001 is the industry yard stick that most Information Security Management activity is measured against.
- External assurance can be provided to both the customer and the Fortune Technologies Pvt. Ltd.'s management on the actual state of the organization's Information Security Management System.
- External, qualified ISO 27001 auditors impartially review and assess the organization's information security practices, policy procedures and their operation against the standard.

c. Increases customer confidence

- ISO 27001 certification gives service consumers and customers an easily recognisable security hallmark.
- Using the ISO 27001 logo on Fortune Technologies Pvt. Ltd.'s literature is a continual reminder to potential and existing customers that demonstrates commitment to information security at all levels of the organization.
- The certification demonstrates credibility and trust.

d. Build trust internally and externally

- ISO 27001 improves company culture. The Standard's holistic approach covers the whole organization, not just IT, and encompasses people, processes and technology. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.
- The Standard helps businesses become more productive by clearly setting out information risk responsibilities.

e. Satisfy audit requirements

- By providing a globally accepted indication of security effectiveness, ISO 27001 certification negates the need for repeated customer audits, reducing the number of external customer audit days. Consider how many days of detailed preparation this could save the organization and calculate the cost involved.

f. Increased legislative and regulatory compliance

- ISO 27001 is the only auditable international standard that defines the requirements of an information security management system (ISMS).
- The Standard is designed to ensure the selection of adequate and proportionate security controls that help to protect information assets of Fortune Technologies Pvt. Ltd..
- ISO 27001 supports compliance with relevant laws such as the Data Protection Act 1998 and software copyright legislation.

4. Information Security Management System (ISMS) Costs

a. Management costs

- Find a suitable project manager to implement the Information SecurityManagement System (ISMS).
- Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27000.
- Plan the implementation project.
- Obtain management approval to allocate the resources necessary to establish the implementation project team.
- Assign employees for projects and manage, direct and track various project resources.
- Hold regular project management meetings involving key stakeholders.
- Track actual progress against the plans and make regular status reports/progress updates.
- Identify and deal with project risks.

b. Implementation costs

- Compile an inventory of information assets.
- Assess security risks to information assets, and prioritize them.
- Determine how to treat information risks.
- Re-design the security architecture and security baseline.
- Review and update existing security policies and prepare new information security policies and standards.
- Conduct awareness and training regarding the ISMS.

c. Certification costs

- Assess and select a suitable certification body.
- Pre-certification visits and certification audit and inspection by an accredited ISO/IEC 27001 certification body.
- Staff and management time expended during annual surveillance visits.

d. Maintenance costs

- Periodic ISMS internal audits to check that ISMS procedures are being followed correctly.
- Complete preventive and corrective actions to address potential and actual issues.
- Periodic review and maintenance of information security policies and standards.