Enterprise Standards and Best Practices for IT Infrastructure

Business case for ‘ASUSTeK Computer Inc.’

Rajapakse S. I.

IT13021344

1. Introduction

ASUSTeK Computer Inc. is a Taiwanese multinational computer hardware and electronics company. It was founded in Taipei, Taiwan in 1989 and currently it is the world's 4th largest PC vendor by 2015. The name 'ASUS' comes from the last four letters of 'Pegasus'.

Asus' products include laptops, desktops, tablets, mobile phones, servers, workstations, motherboards, networking equipment, graphic cards, monitors, cooling systems and other computer components.

Asus manufactures their products in Taiwan, China, Mexico and the Czech Republic and currently it operates around 50 service sites across 32 countries and has over 400 service partners worldwide.

2. Why 'ASUSTeK Computer Inc.' needs an Information Security Management System (ISMS)?

ASUSTeK Computer Inc. serves their services worldwide. Their main services include online purchases, product registrations, driver downloads, the customer help center and some more. So the company has to protect their clients' details and information completely. Because the users provide their personal details, credit/debit card information, confidential data when getting above mentioned services. So the company must protect confidentiality, integrity, availability and durability of those data to keep customers and users without going away from the company. As an example the confidentiality of details like payment information must be highly secured. If the company fails to do that it will harm the company reputation and it will discourage their customers to continue.

So a proper security mechanism or a security management system should be implemented to secure key factors like confidentiality and integrity of the company and users.

3. Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k) at 'ASUSTeK Computer Inc.'

a. Benefits of (Information Security Management System) ISMS

i. Reduces the probability of risk occurrence or adverse impacts
ii. Cuts incident-related losses and costs (risk reduction and cost saving)
iii. Credibility and trust to/of customers
iv. Proper risk assessment and treatment according to priorities
v. High confidentiality, integrity, availability and durability of data and information
vi. Meets an internationally recognized security standard and other security best practices
vii. High awareness of security within and outside the company

b. Benefits of Standardization

i. Provides a security baseline, almost universally required information security controls on which to implement specific additional controls as appropriate – Cost saving
ii. An embodiment of good practices, avoid re-inventing the wheel – Cost saving
iii. Avoids having to specify the same basic controls repeatedly in every situation – Cost saving
iv. Is generally applicable and hence reusable across multiple department, function, business units and organization without significant changes – Cost saving
v. Based on globally recognized and well respected security standard – Brand value
vi. ISO27000 standards suite is being actively developed and maintained by the standards bodies, reflecting new security challenges. – Brand value
vii. Allows unnecessary, inappropriate or excessive controls to be relaxed or removed without unduly compromising valuable information assets – Cost saving

viii. Being risk-based, the ISO27000 approach is flexible enough to suit any organization, as opposed to more rigid and prescriptive standards such as PCI-DSS – Cost saving

c. Information Security Management System (ISMS) Costs

i. Find a suitable project manager to implement the Information Security Management System (ISMS)
ii. Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27000.
iii. Plan the project implementation
iv. Employ/assign, manage, direct and track various project resources.
v. Hold regular project management meetings involving key stakeholders.
vi. Identify and deal with project risks
vii. Compile an inventory of information assets
viii. Assess security risks to information assets and prioritize them
ix. Assess and select a suitable certification body
x. Staff/management time expended during annual surveillance visits.