Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure

Business Case for – HP Inc.

Name – Gamage K.G.J.H

Student ID – IT13003142

1. Introduction

HP Inc. (often known now as just "HP") is an American technology company, created on November 1, 2015 as one of two successors of Hewlett-Packard, along with Enterprise. It develops and provides hardware, such as personal computers and printers. It is the legal successor of the old Hewlett-Packard. The split was structured so that Hewlett-Packard changed its name to HP Inc. and spun off Hewlett Packard Enterprise as a new publicly traded company. HP Inc. retains Hewlett-Packard's stock price history, as well as its NYSE ticker symbol of HPQ (whereas Hewlett Packard Enterprise uses a new ticker,HPE).HP is now focusing on consumers who improve their computers frequently and spend more money on games. They released the gamer-centric Omen line of laptops and desktops targeted at mid-range consumers with an Omen X line to debut later in 2016.

2. Why need an Information Security Management System (ISMS) for **HP Products** ?

HP fell from third to sixth overall this year because some really poor products brought its reviews score down to near the bottom. IN that case they must keep their clients very secure. Because most of the clients private details are store in the laptops. There for security is must. So this kind of product must want a proper kind of Security Management system. Therefor it is better to follow this ISMS.
The numerous information security controls recommended by the standard are meant to be implemented in the context of an ISMS, in order to address risks and satisfy applicable control objectives systematically. Compliance with ISO27002 implies that the organization has adopted a comprehensive, good practice approach to securing information.

3. Benefits of implementing an ISMS based on ISO/IEC 27000 series at **HP Product**

A. Benefits of (Information Security Management System) ISMS

- **For Consumers**

ISO has over 21000 standards touching almost all aspects of daily life. When products and services conform to International Standards consumers can have confidence that they are safe, reliable and of good quality. For example, ISO's standards on road safety, toy safety and secure medical packaging are just a selection of those that help make the world a safer place.

- **For business**

International Standards are strategic tools and guidelines to help companies tackle some of the most demanding challenges of modern business. They ensure that business operations are as efficient as possible, increase productivity and help companies access new markets.

ISO standards help businesses to:

- **Cut costs**, through improved systems and processes.
- Increase **customer satisfaction**, through improved safety, quality and processes
- **Access new markets**, through ensuring the compatibility of products and services
- Reduce their impact on the **environment**.

- **For government**

  ISO standards draw on international expertise and experience and are therefore a vital resource for governments when developing public policy. National governments can use ISO standards to support public policy, which has a number of benefits, including.

  - **Getting expert opinion** - By integrating an ISO standard into national regulation, governments can benefit from the opinion of experts without having to call on their services directly.
- **Opening up world trade** - ISO international standards are adopted by many governments, so integrating them into national regulation ensures that requirements for imports and exports are the same the world over, therefore facilitating the movement of goods, services and technologies from country to country.

B. Benefits of Standardization

1. 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.

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

3. 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. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees.

4. Putting your business in order

This one is probably the most underrated – if you are a company which has been growing sharply for he last few years, you 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

C. Information Security Management System (ISMS) Costs

1. The cost of certification

If you want to obtain public proof that you have 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 job, ranging from under 10 man days for smaller companies up to a few dozen man days for larger organizations. The cost of man day depends on the local market.

2. The cost of employees' time

The standard isn't going to implement itself, neither can it be implemented by a consultant only (f you hire one). Your employees have to spend some time figuring out where the risks are, how to improve existing procedures and policies or implement new ones, they have to take some time to train themselves for new responsibilities and for adapting to new rules.

3. The cost of technology

It might seem funny, but most companies I've worked with did not need a big investment in hardware, software or anything similar - all these things already existed. The biggest challenge was usually how to use existing technology in a more secure way. However, you do need to plan such investment if it proves to be necessary.