Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure

Business Case for – Sony Mobile Communication Inc.

Name – Madhumali D.P.P.K

Student ID – IT13003210

1. Introduction

Sony is a multinational mobile phone manufacturing company in Japan, and is a fully owned subsidiary of Sony Corporation. It was founded on October 1st, 2001 as a joint venture between Sony and Swedish telecommunications equipment company Ericsson, under the name **Sony Ericsson.** Sony acquired Ericsson's share in the venture on February 16, 2012.

Sony mobile Communication and development facilities in many countries. This is the fourth largest smartphone manufacture by market share in the fourth quarter of 2012 with 9.8 million units shipped.

The current flagship device of Sony is the Sony Xperia Z5, a smartphone that is water and dust proof with an IP68 rating, Qualcomm Snapdragon 810 Chipset, Android 5.1 OS, and a 23-megapixel 4K camera that has a G Lens, Exmor RS, and BIONZ image processor.

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

Sony product is most famous in lot of countries. So they have a big client connection all over the world. In that case they must keep their clients very secure. Because most of the clients private details are store in the smart phone. There for security is must.Management should actively support information security by giving clear direction (*e.g.* policies), demonstrating the organization's commitment, plus explicitly assigning information security responsibilities to suitable people.
So this kind of product must want a proper kind of Security Management system. Therefor it is better to follow this ISMS.

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

A. Benefits of (Information Security Management System) ISMS

i. High awareness of security within and outside the company.
ii. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.
iii. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).
iv. Proper risk assessment and treatment according to priorities.

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.

C. Information Security Management System (ISMS) Costs

1. The cost of literature and training

Implementation of ISO 27001 requires changes in your organization, and requires new skills. You can prepare your employees by buying various books on the subject and/or sending them to courses (in-person or online) - the duration of these courses varies from 1 to 5 days. And don't forget to buy the ISO 27001 standard itself - too often I run across companies implementing the standard without actually seeing it.

2. The cost of external assistance

Unfortunately, training your employees is not enough. If you don't have a project manager with deep experience in ISO 27001 implementation, you'll need someone who does have such knowledge - you can either hire a consultant or get some online alternative The greatest value of someone with experience helping you with this kind of project is that you won't end up in dead end streets - spending months and months doing activities that are not really necessary or developing tons of documentation not required by the standard. And that really costs.

However, be careful here - do not expect the consultant to do the whole implementation for you - ISO 27001 can be implemented by your employees only.

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.