SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

Name: Wickramasinghe H.E.

SLIIT ID: IT13072384

Practical Session: WE Monday

Practical Number: Lab 6

Date of Submission: 02/09/2016

Date of Evaluation : ______________________

Evaluators Signature : ______________________

Introduction

MSI (Micro-Star International Co., Ltd, Chinese is a Taiwanese multinational information technology corporation headquartered in New Taipei City, Taiwan. It designs, develops and provides computer hardware, related products and services, including laptops, motherboards, graphics cards, All-in-One PCs, servers, industrial computers, PC peripherals, car infotainment products, etc.

The company has a primary listing on the Taiwan Stock Exchange and was established in August 1986 by 5 founders – Hsu Xiang (a.k.a. Joseph Hsu), Huang Jinqing (a.k.a. Jeans Huang), Lin Wentong (a.k.a. Frank Lin), Yu Xian'neng (a.k.a. Kenny Yu), and Lu Qilong (a.k.a. Henry Lu). First starting its business in New Taipei City, Taiwan, MSI later expanded into Mainland China, setting up its Baoan Plant in Shenzhen in 2000 and establishing research and development facilities in Kunshan in 2001. It also provides global warranty service in North America, Central/South America, Asia, Australia and Europe.

The company has been a sponsor for a number of eSports teams and is also the host of the international gaming event MSI Masters Gaming Arena (formerly known as MSI Beat IT). The earliest Beat IT tournament can be traced back to 2010, featuring Evil Geniuses winning the championship.

Why MSI needs an Information Security Management System?

MSI is a multinational computer technology company which holds large amount of information. MSI provides some services because of that it has severs. So that information should have been protected by well define manner. As a business company needs a legal obligation under the Data Protection Act.

The ISO 27001 standard is designed to ensure that adequate and proportionate security controls are put in place to ensure Data Protection and protect sensitive company information and data in order to comply with Data Protection laws and also to gain customer confidence.

Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k)

ISMS benefits

- Compliance with legislation.
- Securing confidentiality, integrity and availability.
- Prevention of confidentiality breaches.
- Prevention of unauthorized alteration of critical information.
- Prompt detection of data leakage and fast reaction.
- Meeting international benchmarks of security.

Benefits of standardization

- Risk based approach to help plan and implement an Information Security Management System.
- ISO 27001 ensures the right people, processes, procedures and technologies are in place to protect information assets.
- ISO 27001 protects information and ensures its confidentiality, integrity and availability are maintained.

ISMS costs

- Project implementation planning.
- Employ assign, manage, direct and track various project resources.
- Hold regular project management meeting involving key stakeholders.
- Identify and deal with project risk.
- Compile and inventory of information assets.
- Assess security risk to information assets.
- Redesign the security architecture and security baseline.
- Assess and select a suitable certification body.