



**SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY**

**Enterprise Standards and Best Practices**  
**for IT Infrastructure**

Name: M. I. Ismail

IT No: IT13029364

Practical: ISO 27001 Business Case

**4<sup>th</sup> Year 2<sup>nd</sup> Semester 2016**

# Introduction - Microsoft

Microsoft is an American multinational technology company which is involved in developing, manufacturing, licensing and selling computer software. Microsoft Corporation is well known for its most popular Windows operating systems. It is considered as the world's largest software maker by revenue and one of the most valuable companies in the world.

Featured products by Microsoft:

1. Windows Operating Systems and Servers
2. Microsoft Office Package
3. Cloud and Online Services

## Information Security Management System for Microsoft.

*Information Security Management System (ISMS) is a systematic and structured approach which is used to manage information in a secure manner. ISMS consist of policies, processes, procedures, organizational structures and software and hardware functions. The ISMS implementation should be directly influenced by the organization's objectives, security requirements, processes employed, size and structure.*

*ISMS is based on two international standards.*

1. ISO/ IEC 27001:2005
2. ISO/ IEC 27002:2005

Information systems are vulnerable with security threats such as fraud, espionage, fire, natural disasters and sabotage from a wide range of sources. The increasing number of security breaches has led to increasing information security concerns among organizations worldwide. Achieving information security is a huge challenge for organization as it cannot be achieved completely. An ISMS might not be able protect all systems in an organization, but If an ISMS is not implemented in organizations such as Microsoft will result in losing confidential information which has greater impact on the company.

## **Benefits of ISMS.**

- Credibility, trust and confidence of your customer.
- Great awareness of security.
- 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.

## **What should be completed before implementation?**

- Preparation of the information security policy
- Project implementation plan and approvals from the senior management.
- Assessing information assets and identifying risks.
- Selecting the suitable certification body.
- Find a suitable project manager to implement ISMS.