SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

# Enterprise Standards and Best Practices for IT Infrastructure

**4th Year 2nd Semester 2016**

Name: Madhushi Pabasara K.

SLIIT ID: IT13061180

Practical Session: WD Friday

Practical Number: Lab 5

## Business case for an organization:

Introduction.

Millennium Information Technologies (MIT) is a leading software company in Sri Lanka. There are many branches available all over the country. Around 500 employees are working on this software firm. This is an Information Technology service provider for the financial and telecom industries. Millennium IT also offers information technology infrastructure and consulting services.

With the improvement of the technology, organizations are become dependent on the information systems. There are threats associated with these information in different ways. So need to concern about how to secure the information assets of the organization without getting any risk.

When the amount of digital data/information is getting increasing, the severity of information is getting increase. Information is become a very significant asset to the organization. There are two types of assets. Tangible (physical assets) and Intangible (Assets that cannot touch). And there are inherent threats/risks to digital information such as, coping data, modifying data, stealing data, etc.

For more threats, Physical loss of data, The Company can lost data due to several reasons. Flooding, power failure, disk failure etc. Unauthorized access to the employees' data or clients' data, when sending data between two companies there can be intercepting, data corruption can be happen due to modifying data by someone else.

Basically all the data/information is vulnerable. Along with the vulnerabilities there is an associated threat. That threat will redirect to certain level of risk.

If we want to reduce risks, at least for a certain level we have to reduce threats. But threats can't be mitigated. But we can reduce vulnerabilities that can happen to a certain asset. To secure the organization's information before getting vulnerable, we should have an Information Security Management System (ISMS) going on our organization.

Benefits of having ISO 27001

Using this standard, our organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to us by third parties. ISO 27001 is providing requirements for an ISMS. An ISMS is a systematic approach to managing sensitive company information security. It includes people, processes and IT systems by applying a risk management process.

Some of the benefits from this standard are, keeps confidential information secure, allows for secure information exchange, and provides customers and stakeholders to stick with the

company by doing risk management, builds a security framework to the company, minimize the risk exposure, protecting the organization's reputation, improving trust in customer relationships, providing greater reliance on interactions with trading partners.

Costs.

If we use this standard for our organization, there will be certain set of costs we have to bear as an organization. Amount of costs will be changed due to several things. Company size, assets that are available, information criticality etc. There are mainly several kind of costs available. Implementation costs, management costs, certification costs and etc.

When we have significant technologies in organization, such as data centers, that costs are very high because of their complex systems. Even though the resources are available the employees don't know how to use those resources using existing technologies.

The company can start a security awareness programs to train the employees in the organization. From that employees can get lessons how to avoid certain security threats. For the training program it will cost some. But it is very important having such a program.

Find suitable project manager is very essential to the company. Project manager should have the deep knowledge about the ISO 27000 certification. Or we can hire a consultant to get advices to improve the process of the organization.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.

By implementing a standard to particular company/ organization, we can mitigate the certain threats to the assets (tangible /intangible) in the organization and it will reduce the costs associated with those assets. Because the impact with the threats that can happen without ISO 27001 can be higher than the accompanying the standard in an organization. If the organization doesn't have a security standard (ISO 27001), it will reduce the company's reputation and finances of the company.