**Sri Lanka Institute of Information Technology**

**4th Year – 2nd Semester**

**ESBII - 2016**

**Lab – 05**

**BUSINESS CASE for Sri Lanka Telecom for Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards**

**Submitted By: IT13025854**

**Mahimani P T**

**Company Name: Sri Lanka Telecom**

Sri Lanka Telecom PLC is a telecommunications services provider in Sri Lanka and one of the country’s largest companies with an annual turnover in excess of Rs 40 billion

SLT's Intelligent Solutions are aimed at equipping local businesses with the full range of ICT solutions to help succeed in the global arena. Speed, connectivity and security are key demands businesses make and SLT’s wide portfolio of services is perfectly poised to meet and exceed these expectations. Our comprehensive array of services is helping organisations to blaze ahead with stronger convergence capabilities, extended reliability, improved scalability, flexibility and cost effective implementation.

SLT’s industry specific tailor-made ‘Intelligent Solutions’ released for the investors and business professionals during the CHOGM 2013 Business Forum in Colombo. This sector-wise communication solutions approaches the 10 main economic sectors including.

**What is ISO 27001?**

ISO/IEC 27001 - Information security management

The ISO 27000 family of standards helps organizations keep information assets secure.

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.

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS)

Certification to ISO 27001

Like other ISO management system standards, certification to ISO/IEC 27001 is possible but not obligatory. Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed. ISO does not perform certification.

**What is ISMS?**

An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

**What is the purpose of having ISO 27001?**

Protecting the organizations information is critical for the successful management and smooth operation of the organization. Completing ISO/IEC 27001 information security management systems certification will helps to the organization in managing and protecting valuable data and information assets.

**What are the benefits Sri Lanka Telecom will gain by implementing the ISO 27001?**

## 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.

The truth is, there is still no methodology and/or technology to calculate how much money you could save if you prevented such incidents. But it always sounds good if you bring such cases to management’s attention.

## 4. Putting your business in order

This one is probably the most underrated – if you are a company which has been growing sharply for the 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.

ISO 27001 is particularly good in sorting these things out – it will force you to define very precisely both the responsibilities and duties, and therefore strengthen your internal organization.

To conclude – ISO 27001 could bring in many benefits besides being just another certificate on your wall. In most cases, if you present those benefits in a clear way, the management will start listening to you.

* Keeps confidential information secure.

Because lots of people engage with the organization it is a must to keeps confidential information secure.

* Allows for secure exchange of information.

Sri Lanka Telecome engage in lots of business sectors. For example Peo TV,telephone line,broad band etc. When the organization engaging with these business sectors there were thousands of data exchange through the servers. In that case the process of exchanging data should be secure.

**What are the costs John Keells will gain by implementing the ISO 27001?**

**ISMS Operation and Maintenance costs**

* Periodic ISMS internal audits to checks that ISMS procedures are being followed.
* Periodic review and maintenance of information security policies, standards, procedures, guidelines etc.

**ISMS Certification costs**

* Assess and select a suitable certification body.

Risk of failing to achieve certification at first application