**SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY**

# Enterprise Standards and Best Practices for IT Infrastructure (ESBPII)

**4th Year 2nd Semester 2016**

## Assignment 5

http://www.millenniumit.com/about-us

Business case for an Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k)

H.K. Peiris

IT13116002

2/9/2016

# Introduction

MillenniumIT is a leading innovative trading technology business. MillenniumIT's systems are used by exchange businesses around the world including, London Stock Exchange, Borsa Italiana, Oslo Børs, Turquoise, the London Metal Exchange, Johannesburg Stock Exchange and a series of emerging market exchanges. MillenniumIT's suite of capital markets products include Millennium Exchange™ (trading platform), Millennium SOR™ (smart order router), Millennium MarketData™ (multi-market market data dissemination) Millennium Surveillance™ (market surveillance and regulatory compliance), Millennium PostTrade™ (clearing and settlement) and Millennium Gateway (single trading interface). These products cater to trading multiple asset classes including equities, derivatives, debt, commodities, forex, structured products and exchange-traded funds.

The systems integration business of MillenniumIT, is a leading Sri Lankan information technology solutions provider, specializing in IT solutions for the financial and telecom industries. MillenniumIT also offers information technology infrastructure and consulting services. Founded in 1996, and headquartered in Colombo, Sri Lanka, MillenniumIT was acquired by the international diversified exchange business London Stock Exchange Group in October 2009.

## What is ISMS?

Information Security Management System (ISMS) is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone to an IT security career. The customers of the MillenniumIT, i.e. Clients, and Employees, require continuous access to services, up to 100% up-time of systems, security for personal information and access controls to information.

## Why select ISO 27001k?

MillenniumIT helps organizations achieve the right balance with security solutions that integrate people, processes, and technology to cover the entire lifecycle of policy, planning, implementation and optimization. Data Security Solutions - to protect your critical data from sabotage and theft.

- Network Security Solutions - to protect your organization from the connected world, be it the Internet, Intranet or Extranets.
- Application Security Solutions - to protect your web presence, e-commerce applications and your mission critical databases from both internal and external threats.
- Mobile Security Solutions- to leverage on the advantages of mobility with safety.
- Cloud Security Solutions - to protect your sensitive information while at rest or during transit.
- Security Management and Monitoring solutions - to keep your organization at bay, proactively.
- Governance, Risk, and Compliance solutions - to address your voluntary or mandatory regulatory requirements.

### 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 with 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.

### 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.

## Lowering the expenses

Information security is usually considered as a cost with no obvious financial gain. However, there is a financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Alternatively, 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. However, it always sounds good if you bring such cases to management's attention.

## 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.

## Advantages

- A structured, coherent and professional approach to the management of information security, aligned with other ISO management systems.
- Increase the confidence of customers and Customer satisfaction.
- Certification can ensure an advantage over competitors.
- Supply a framework demonstrates legal and regulatory requirements, no law breaking means no penalties.
- Reduction in incidents and support costs.
- Ensure Continuous access to service.
- Ensure net available all the time – "Medical grade network."
- To fulfill the corporative mission of transparency and excellent customer service.
- To helps to govern the protection of information.
- Improves efficiencies and increase profits.
- To helps to develop and manage interactions with other organizations.
- To have a good security policy
- For information asset management.
- For HR security.
- For physical and informational security.
- For communication and operations management.
- For Access control.
- For information systems acquisition, development and maintenance.
- For information security incident management.
- For Automation of user-provisioning.
- For outsourced employee screening process.
- For effective data disposal procedure.

## Cost for having an ISO27001 security system

• **Information security movie**—A 20-minute movie was created and presented with all the trappings of a real movie theater experience (e.g., tickets, popcorn). The movie has proven extremely popular, and so far 40,000 employees have seen it. Every training program begins with this movie.

• **Information security cartoon strip**—A cartoon strip was created with two characters, one named Sloppy and the other Sly. Their exploits entertain the readers and also carry a very powerful security message. This cartoon strip is now planned to be printed in a calendar format.

• **Email and picture campaign**—Regular emails are sent cautioning everyone about being alert, e.g., a reminder about avoiding phishing emails is sent after any successful

• **Ten security commandments**—The user policy document has been summarized into key information security rules that are easy to read and remember

• **Security First course**—All employees have to undertake this one-hour course every two years. Taking the examination and obtaining passing marks is mandatory. A certificate is issued to
all successful candidates. The certificate acts as an official recognition. Apart from the certificate, the star performers are also recognized through global mailers sent to all the bank's employees as well as monetary rewards.

• **One-day workshop**—A one-day workshop is conducted periodically for senior management at which the CISO explains the importance of information security for the bank and the specific measures deployed for its implementation.