SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2014

Name: Denipitiya N.S

SLIIT ID: IT13103064

Group Number:

Practical Session: WD Friday

Practical: ISO 27001 Business Case

Date of Submission: 02/09/2016

1. 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 Market Data (multi-market market data dissemination) Millennium Surveillance™ (market surveillance and regulatory compliance), Millennium Post Trade (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.

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).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. It can help small, medium and large businesses in any sector keep information assets secure.

2. Benefits of having ISO27001

Implementing an information security management system will provide a system that will help to eliminate or minimize the risk of a security breach that could have legal or business continuity implications.
An effective ISO 27001 information security management system (ISMS) provides a management framework of policies and procedures that will keep your information secure, whatever the format. Following a series of high profile cases, it has proven to be very damaging to an organization if information gets into the wrong hands or into the public domain. By establishing and maintaining a documented system of controls and management, risks can be identified and reduce. There are

huge number of benefits of having ISO20071 certification in an organization. Here are some summarized benefits,

Marketing Edge - ISO27001 Certification enhances the company's standing within the market & gives potential clients the assurance that your business has a managed, professional approach to protecting client data. This opens new opportunities & is especially attractive to clients who manage sensitive information.

Commercial Advantage - More Public & Private Sector clients are now insisting that suppliers can demonstrate ISO27001 Certification as a minimum requirement in their commercial tenders. A sharp rise in the number of UK businesses achieving ISO27001 Certification means non-certified businesses are increasingly at a disadvantage.

Meeting Regulatory Compliance - ISO27001 Certification is far reaching in all aspects of IT Governance, Information Handling, Data Protection and Privacy, creating a manageable, efficient methodology based approach to ensure regulatory compliance in these areas. ISO27001 also forms the basis of G-Cloud & PSN Accreditation.

Business Improvement - ISO27001 is a living accreditation, audited annually, & encourages awareness of risk across the business. It drives clear definitions of individual roles & responsibilities for information assets & decision making – resulting in a stronger internal organization & enhanced control over business assets.

Best Practice / Protected Reputation - By implementing ISO27001 policies & controls, your business will be operating to recognized information security best practice – giving you peace of mind & protecting your business (and client data) from security incidents / data breaches that could destroy your reputation in a matter of minutes.

3. Costs

3.1 Cost of Management

The company management and the employees have to be trained for the ISO27001 standard. These training programs may be cost high. Sometimes they have to keep special systems to keep the standards. So that may cost high because they have to educate the staff about the new system. And project managers also have to be knowledgeable about the ISO27001. Therefore the management of the company has to invest more money on the ISO27001.

3.2 Cost of Implementation

Before implementing ISO 27001, the company needs to consider the costs and project length, which are further influenced by the detailed understanding of the implementation phases. Any cost is painful in tough economic times. In today's cloud computing environment, organizations that want to reduce costs without compromising information security are looking at ISO 27001 certification as a promising means to provide knowledge about their IT security.

Implementation costs are driven by the perception of risk and how much risk an organization is prepared to accept. Four costs need to be considered when implementing this type of project:

1. **Internal resource -** The system covers a wide range of business functions including management, human resources (HR), IT, facilities and security. These resources will be required during the implementation of the ISMS.
2. **External resource -** Experienced consultants will save a huge amount of time and cost. They will also prove useful during internal audits and ensure a smooth transition toward certification.
3. **Certification** - Only a few approved certification agencies currently assess companies against ISO 27001, but fees are not much more than against other standards.
4. **Implementation –** These costs depend largely on the health of IT within the organization. If, as a result of a risk assessment or audit, a gap appears, then implementation costs are bound to go up based on the solution implemented.

On average, implementation of a system such as this can take four to nine months and depends largely on the standard of conduct and quality and management support, the size and nature of the organization, the health/ maturity of IT within the organization, and existing documentation.

3.3 Cost of Certification

If the company want to obtain public proof that the company has 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, ranging from under 10 man days for smaller companies up to a few dozen man days for larger organizations. The cost of man day depends on the local market.

The company has to be very careful not to underestimate the true cost of ISO 27001 project – if company does, management of the company will start looking at your project in a negative light. On the other hand, forecasting all costs correctly will show the level of professionalism; and don’t forget to present both the cost and the benefits – read four key benefits of ISO 27001 implementation.