SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

ISO 27001 certification

Name: Kulathilake M.B.K.M

SLIIT ID: IT13085704

Practical Session: WE Monday

Practical Number : Lab 04

Date of submission : 2016/08/01

People's leasing and Finance

Founded in 1995, People's leasing and Finance PLC is Sri Lanka's unshakable leader in the leasing sector. In the past 14 years, People's Leasing has built an extraordinary tradition of excellence in all spheres of leasing and we are now the established market leader. Our customers range from individuals to SMEs to blue chip companies in every corner of the island. They have contributed immensely to the country's economic growth and the quality of life of millions of Sri Lankans.

The People's Leasing Group has recently diversified to include five subsidiaries, united under the PLC name. Customers can now obtain Insurance, Finance, Microfinance and Fleet Management services under one roof. Their user-friendly product range, nationwide outreach and strong foundation of talented management and staff have made the Company immensely profitable. They are now a major contributor to the success of our parent company, People's Bank. As a subsidiary of People's Bank, the group enjoys government protection along with private sector flexibility.

The PLC Philosophy

- To respond to all stakeholders with deliverable core values of:
- Economic Viability
- Social Accountability
- Environmental Responsibility.

What is ISO 27001?

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO 27001 uses a top down, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

Define a security policy.
Define the scope of the ISMS.
Conduct a risk assessment.
Manage identified risks.
Select control objectives and controls to be implemented.
Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organization.

The 27001 standard does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the accompanying code of practice, ISO/IEC 27002:2005. This second standard describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.

ISO 27002 contains 12 main sections:

1. Risk assessment

2. Security policy

3. Organization of information security

4. Asset management

5. Human resources security

6. Physical and environmental security

7. Communications and operations management

8. Access control

9. Information systems acquisition, development and maintenance

10. Information security incident management

11. Business continuity management

12. Compliance

Why People's leasing and Finance company need this 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.

What are benefit after you apply ISO 27001?

- **It improves enterprise security**

Whether the People's leasing and Finance (PLC) using ISO 27001 decides to go for full certification or not, ISO 27001 brings with it a systematic examination of the organization's information security risks, taking account of the threats, vulnerabilities and impacts that are unique to that organization. It provides a framework for the selection and implementation of a coherent suite of information security controls and/or other forms of risk treatment to address those risks that are deemed unacceptable to that individual organization. It also brings with it a continual improvement ethos to ensure that the risk treatments continue to meet the organization's individual information security needs on an on-going basis.

- **It increases customer confidence**

ISO 27001 certification gives service consumers and customers an easily recognizable security hallmark. Using the ISO 27001 logo on company literature is a continual reminder to potential and existing customers that demonstrates commitment to information security at all levels of the organization. The certification demonstrates credibility and trust.

- **It reduces customer and supply chain audit**

ISO 27001 certification reduces third party scrutiny of your Information Security Management by customers and the wider supply chain. It provides assurance to customers that their information is appropriately protected and, as such, reduces the need to undertake time consuming and costly onsite security audits reducing time and cost for both parties.

- **It provides market differentiation**

Holding an ISO 27001 certification is an increasing requirement to do business in many different verticals, especially when processing any type of personal or sensitive data. The achievement of ISO 27001 will differentiate two competing organizations in the market place, providing a valuable competitive advantage.

- **Expand into global markets.**

ISO 27001 is an international standard, which means that your global clients and customers will recognize the advantages that registration provides.

- **Information security risk assessments**

Information security management can be described as the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment. As a result, the identification, mitigation, and management of risks to information security are vital for the future sustainability of any organization.