



SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

Name: Gamage Y.M.K

IT No: IT13087616

Practical Session: Weekday

Practical Number : 05

Introduction

David Pieris Information Technologies Ltd (DPITL) is a wholly owned subsidiary of David Pieris Motor Company, a large business conglomerate in Sri Lanka, with diversified interests in automotive products, financial services and Information Technology. The progressive expansion of the IT operations of group of Companies, logically evolved into David Pieris Information Technologies Ltd. which was founded in 1997 under the name DPMC Electronics (Pvt) Ltd. Today it is an industry leader in Distributing ICT Equipment & services in Sri Lanka with a comprehensive island wide coverage and service offerings in several countries with the financial stability and back up of David Pieris group of companies - with over SLR 23.7 billion (217.6 Million US\$) of annual turnover. DPIT's recognition and popularity could be attributed to its prompt availability of products for networking solutions and high level of service standards maintained by the company. With highly committed and qualified staff DPIT works closely with many local and global partners in order to deliver products that provide a competitive edge.

Why DPIT needs an Information Security Management System?

DPIT is a multinational Computer technology company which holds large amount of information. DPIT provides some services because of that it has servers. So those information should have been protected by well define manner. As a business company needs a legal obligation under the Data Protection Act.

The ISO 27001 standard is designed to ensure that adequate and proportionate security controls are put in place to ensure Data Protection and protect sensitive company information and data in order to comply with Data Protection laws and also to gain customer confidence

Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k)

ISMS benefits

- Credibility, trust and confidence of your customer.
- Great awareness of security.
- Compliance with legislation.
- Securing confidentiality, integrity and availability.

- Prevention of confidentiality breaches.
- Prevention of unauthorized alteration of critical information.
- Prompt detection of data leakage and fast reaction.
- Meeting international benchmarks of security.

Benefits of standardization

- Common framework for businesses to follow.
- Risk based approach to help plan and implement an Information Security Management System.
- ISO 27001 ensures the right people, processes, procedures and technologies are in place to protect information assets.
- ISO 27001 protects information and ensures its confidentiality, integrity and availability are maintained.

ISMS costs

- Find a suitable project manager to implement ISMS.
- Prepare an overall information security management strategy.
- Project implementation planning.
- Employ/assign, manage, direct and track various project resources.
- Hold regular project management meeting involving key stakeholders.
- Identify and deal with project risk.
- Compile and inventory of information assets.
- Assess security risk to information assets.
- (Re-) design the security architecture and security baseline.
- Assess and select a suitable certification body.