

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

**Enterprise Standards and Best Practices for IT  
Infrastructure**

**(4<sup>th</sup> Year 2<sup>nd</sup> Semester 2016)**

**Lab Assignment 6**

**Name:** Edirisinghe I.R

**ID:** IT12088560

**Batch:** Weekday

# **Business case for Central finance Company PLC for an Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k)**

## **1. Introduction**

Providing dynamic and innovative financial solutions since 1957, Central Finance Company PLC is Sri Lanka's leading financial house. With a range of diversified services including Asset Leasing, Contract Hire, Fleet Management, Insurance Broking, Micro Finance and SME lending together with a broad portfolio of Savings and Deposit products, they help their customers fulfill their diverse financial needs and aspirations.

## **2. Scope**

The company should commit to protecting its information and that of its clients. To achieve this goal the company should implement an information security management system in accordance with ISO/IEC 27001. ISMS covers the management, operation and maintenance of the information assets and information systems and associated processes that enable the processing of application and the security of the server and the company. Protection of company assets is vital success of the business. To this end the company should establish an information security management system that operates all the process required to identify the information that the company needs to protect and how to protect.

- Information should only accessible to authorizes persons from or outside the company and may be from other branches.
- Confidentiality of information is to be maintained.
- Integrity of information and maintain throughout the process.
- All personnel should be trained on information security and are informed that compliance with the policy is mandatory.

### 3. ISMS benefits & costs

These are the ways in which an ISO27k ISMS will typically benefit the company

1. Company needs to use proper security process. Because company server is packed with external and internal services.

- **Benefit:** Strengthens existing information security control environment by (re-) emphasizing business information security control requirements, upgrading current information security policies, controls etc. and providing stimulus to review and where necessary improve information security controls periodically -**Risk reduction**

(Save worker's time, reduce impact of cyber-attacks and secure important information of the company, reduce data lost.)

- **Cost:** Employ/assign, manage, direct and track various project resources.

2. Company's every office worker has admin access on their computer. This is information security threat. As a solution, only authorized persons can have administration rights.

- **Benefit:** Managers and staff become increasingly familiar with information security terms, risks and controls - **Risk Reduction**
- **Cost:** Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k.

3. Company's backup operation is not visible. To solve this, step wise plan to implements.

- **Benefit:** Increases our ability to transfer certain risks selectively to insurers or other third parties, and may facilitate negotiating reduced insurance premiums as key controls are implemented and managed -**Cost Saving**
- **Cost:** Track actual progress against the plans and circulate regular status reports/progress updates.