SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

# Enterprise Standards and Best Practices for IT Infrastructure

**4th Year 1nd Semester 2016 (June Intake)**

Name: N.D.U.Gamage

SLIIT ID: IT13113100

Group Number: -

Practical Session: WD

Practical Number : Lab 5

Date of Submission: 29/08/2016

Date of Evaluation : ______________________

Evaluators Signature : ______________________

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

## Introduction of Commercial Bank

Commercial bank of Ceylon PLC is a prominent financial bank in Sri Lanka which has 250 and 625 ATMs. Not only in Sri Lanka in is also spread in Bangladesh. Commercial bank rated as best bank in Sri Lanka by “Global Finance” for the 14th consecutive year and also won “Bank of the year” by The Banker Magazine on seven occasions.

## Need of information security

Island wide network of branches leads to occupied IT systems to provide more accurate, quick service to customers with high efficiency. Due to commercial Bank has noble business value, it is important to protect information to provide good service via connected networks. Confidentiality, Integrity and Availability are the key requirements to satisfy to maintain high information security inside the bank. Since thousands of transactions happens via internet it required high integrity and availability. Commercial bank account details, customer details and staff details should only be accessed by authorized people to protect confidentiality. And the system always should be available for online transaction as well as ATM transactions. Therefore to provide a valuable service it is suggesting to use ISO 27001 (ISMS) security standards.

## What is ISO 27001 security standard

ISO 27000 is a standard that helps to keep organization assets secure such as financial information, account details, employee details and intellectual property. Once ISO 27000 initiates in an organization it will manage information security using the governance and management processes comprising the management system. Also ISO 27000 will lead an organization to increase several benefits over costs

## ISMS Benefits

1. Easy access to all possible threats before they occurs at unexpected time by preparing proper approach to identify all assets with their vulnerabilities, threats and impact on the Commercial bank.
2. Provide strong information security control by introducing new security policies, controls and procedures.
3. Increase the information and communication consistency by following standardized, rational

risk management approach.

4. Enhance the awareness of staff on information security and risks

5. Provide suitable security baseline to implement additional controls when required.

6. Avoid reinventing same source codes/products as well as repeating of basic controls in Common situations.

7. Allow commercial bank to focus on important resource and effort on security requirements to protect information assets like database, servers and disk drives.

8. Increase reusability of standards with slight changes among different departments, business units and functions which leads to time and cost saving

9. Provide reasonable, consist framework for different information security controls.

10. Commercial bank will be able to acquire formal confirmation by ISO/IEC 27001 which ensures bank as secure, well-organized trustworthy banking partner

**ISMS costs**

1. Selecting experienced manager for establish ISMS inside Commercial bank

2. Prepare Information Security Management Strategy for which associated with all the department policies, procedures and functionalities.

3. Plan an effective establishment process and assign suitable talented employees for the ISMS Team with the approval of higher management

4. Conduct regular meetings trainings to track the progress time to time against establishment plan.

5. Conduct awareness programs to update staff on newly introduced policies and procedures.

6. Selecting suitable certification body to Pre-certify the progress of ISMS establishment

7. Having risk of failure to obtain Pre- certification and ISMS certification

8. Increase wages for project managers and ISMS members.

9. Tri- annual re-certification cost

10. More time required for planning and implementation process.