

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

ESBII

**4th Year 2nd Semester 2016**

Aaqil MFM

IT No: IT13000554

CSN 13

**INTRODUCTION**

HNB is one of the leading banks in Sri Lanka. It is a premier private sector commercial bank operating with 249 branches across the island. The bank has been internationally recognized by the Asian banker magazine as the “best retail bank in Sri Lanka” on eight occasions from 2007 to 2012 and 2015. The bank is actively involved in retail banking, corporate banking, international banking, treasury and project financing

**WHY HNB NEEDS AN INFORMATION SECURITY MANAGEMENT SYSTEM?**

Since it is a bank there will be huge amount of transactions happening every second and the bank has to maintain all the user data and record all the transaction happening. So all the data should be properly maintained and protected in a server, in a way that it can assure the availability, integrity, and confidentiality.

So the ISO 27001 can be implemented to ensure the data protection and protect sensitive information about the company 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

ISMS benefits

1. An ISMS is a defensive mechanism to any advanced persistent threat (APT) to minimize the impact from the external threats.
2. Informed information security decisions will be made based on risk assessment  to implement technical, management, administrative and operational controls, which is the most cost effective way of reducing risk
3. Organization will improve credibility and trust among internal stakeholder and external vendors. Credibility and trust are the important elements for a successful business.
4. Business managers of the organizations will make informed decisions regarding potential risk and should be able demonstrate compliance with standards and regulations such as SOX, GLBA, HIPAA, DPA to their critical information on regular basis.
5. ISMS raises awareness throughout the business for information security risks, involve all employees throughout an organization and therefore lower the overall risk to the organization

Benefits of standardization

1. Improve the design and management
2. Common framework for business to follow.
3. Facilitate the exportation and marketing of products
4. Establish quality, environmental and safety policies
5. Simplify the production of legal text.
6. Simplify the purchasing management
7. risk based approach to help, plan and to implement an ISMS
8. ISO 27001 protects information and ensures its confidentiality, integrity and availability are maintained

ISMS costs

1. Prepare an overall information security management strategy.
2. Project implementation planning
3. Find a suitable project manager to implement ISMS
4. Identify and deal with project risk
5. Compile and inventory of information assets.
6. Assess security risk to information assets
7. Hold regular project management meeting involving key stakeholders
8. Employ or assign manage, direct and track various project resources.
9. Assesses and select a suitable certification body
10. Re design the security architecture and security baseline.