ESBPII Assignment

ISO 27001 security Business case for SANASA Development Bank

IT13008642

P.W.J.B Polkotuwa

Weekday

1. Introduction

Globally, Banking institutions depend on Information Technology to help them to achieve their vision, and strategy. So good practice in data security is regarded as a pre-requisite of affective and successful banking business. Also confidentiality of customer bank account details is seen as fundamental activity of banking. So it is important to avoid loss of customer account details or their acquisition by unauthorized third parties. So there must be standards to mitigate those risks.ISO 27000 is an internationally recognized standard for implementing information security. It was chosen by most banks, because it covers virtually all aspects of data security.so good data security is an integral part of customer's confidence in a banking business is at the heart of banking.

2. Why they select ISO 27001 security standards?

The amount of data stored electronically today is overwhelming, and that figure is only going to increase over time. Unfortunately, with the increase in cyber data comes the increase of cyber-attacks. Hackers are a constant threat to any industry that utilizes technology. ISO 27001 is an information security management standard that provides organizations of any size and industry a framework for securing and protecting confidential and sensitive data.

The banking industry, in particular, can benefit from an ISO 27001 certification. Banks collect a great deal of personal information from their clients, and with the switch to electronic data storage, that information is more so at risk. It's an obvious target for cyber hackers; a one-stop shop for information on credit, social security, and more. Because of this risk, clients are drawn to organizations that can provide information security, and especially drawn to organizations that can prove their commitment.

An ISO 27001 is the proof organizations need to set themselves apart from the competition. It identifies and alleviates information security risks, guards confidential information, and lets your clients know that you value their confidentiality. In the likely event that further

regulations are put on the banking industry in the future banking organizations can assure their clients that they care for their safety and confidentiality by taking every precaution necessary through ISO 27001.

3. Advantages.

- To assure clients of creditability and reliability.
- To demonstrate commitment to quality of the bank.
- To fulfill corporative mission of transparency and excellent customer service.
- To provide competitive edge and helping to spread banks investments in any other areas.
- To helps to govern the protection of information.
- Improves efficiencies and increase profits.
- To bring flexibility and resilience in banking service.
- To boost the working environment of the bank.
- To helps to develop and manage interactions with other organizations.
- To have a good security policy for the bank.
- For information asset management.
- For HR security.
- For physical and informational security.
- For communication and operations management.
- For Access control.
- For information systems acquisition, development and maintenance.
- For information security incident management.
- For compliance and audit in the bank.
- For Automation of user-provisioning.
- For outsourced employee screening process.
- For effective data disposal procedure.

- For have a good incident response procedures in place.

4. Cost for having an ISO27001 security system.

- Cost for suitable staff including good, experienced project manager for managing ISMS in a bank.
- Cost for prepare an information security management strategy.
- Cost for implementing the ISMS.
- Cost for hold regular project management meetings involving key stakeholders.
- Cost to identify and deal with project risks.
- Cost to design the security architecture and security baseline.
- Cost to upgrade and other risk treatments as appropriate.
- Cost to conduct awareness training regarding the ISMS such as introducing new security policies and procedures.
- Cost to assess and select a suitable certification body.
- Cost to Pre-classification visits and certification audit/inspection by ISO/IEC certification body.
- Cost to manage staff who maintain ISMS.
- Cost for annual surveillance visits.
- Cost to buy new security hardware.