SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
4th Year – 2nd Semester

Enterprise Standards for Best Practices of IT Infrastructure

IT 13 1204 12

Dharmasiri G.D.N.P

Assignment 2 – Business Case

ESBPII

ISO 27001 – Information Security Management

Introduction

Etisalat in Sri Lanka

The UAE based operator Etisalat, began its operations in Sri Lanka on 25th February 2010, after acquiring 100% stake of Tigo, a subsidiary of Millicom International Cellular. The company was previously Sri Lanka's first cellular network, then known as Celltell which inaugurated its operations in 1989, and changed its brand name to “Tigo” in 2007.

Etisalat is fully owned and operated by the Emirates Telecommunication Corporation in UAE. It has extended operations in Egypt and Saudi Arabia in the Middle East and further into Asian markets such as Pakistan, Afghanistan and Sri Lanka, recording over 167 million subscribers across 16 countries offering opportunities for synergy with Etisalat other operations in the region.

Etisalat is consistently providing not only the widest coverage and an unprecedented service, but also a host of other Value Added Services. Etisalat is dynamic and treat their customers as their own, and consider customer service as their first priority.

Many organizations like banks and other financial institutions have implemented ISO 27001 in their businesses because they had to implement very strict information security and business continuity procedures and safeguards. And this is exactly why Etisalat Company should consider adapting to ISO 27001. These are some of the potential reasons why the company might certify in ISO 27001.

1) Marketing - company can use the certificate to get some new clients (because of, e.g., tenders), or to stay in the business (e.g., all your competitors already have the certificate).

2) Compliance- In rare cases some regulations will requires to implement ISO 27001, but company may have cases where they will sign contracts with clients which oblige the company to implement information security or business continuity compliant with these standards. And instead of having to stand the auditors from each of clients who want to check whether the company complied with the contract, company can have the certification auditor do the job, and then show everyone else the ertificate.

3) Internal pressure- In some companies, these kinds of projects will never finish unless there is powerful pressure – e.g., a clear deadline. So, if the company agree with the certification body on a fixed date for the certification audit, both the management and your employees will have a much stronger sense of urgency for implementation.

4) Objective inputs- If the company wants to their business continuity to be at a really high level, it is good to call in people with high experience and who know how it can benchmark with the best in the industry. Certification auditors will be more than happy to audit someone who is trying really hard and will provide inputs on what you could improve.

Companies are implementing ISO 27001 because they understood the biggest value in the methodology this standard provides. Solid and reliable Information Security Management System (ISMS) will helps to secure information within the organization and ensure safety and reliability for customers of Etisalat.

ISMS Benefits

1. With increasing fines for personal data breaches, organizations need to ensure compliance with legislative requirements; ISO 27001 provides a framework for the management of information security risks, which ensures to take into account legal and regulatory requirements.

    - Supports compliance with relevant laws and regulations
    - Reduces likelihood of facing prosecution and fines
    - Can help to gain status as a preferred supplier

2. Potential information breach, damaging reputation are some of information security issues that companies faced, by adapting to ISO 27001 requires to identify risks to information and put in place security measures to manage or reduce them, It ensures to implement procedures to enable prompt detection of security breaches, It is based around continual improvement, and requires to regularly review the effectiveness of your information security management system (ISMS) and take action to address new and emerging security risks.

- Protects the reputation
- Provides reassurance to clients that their information is secure
- Cost savings through reduction in incidents

3. Availability of vital information at all times is another security issue that companies have to face with, how ISO 27001 helps with this issue is it ensures that authorized users have access to information when they need it. It demonstrates that information security is a priority, whilst reassuring stakeholders that a best practice system is in place and it makes sure you continually improve your information security provisions.

    - Demonstrates credibility and trust.
    - Improves the ability to recover operations and continue business as usual.

4. Lack of confidence in organizations ability to manage information security risks will reduce by certifying to ISO 27001 because this standard gives a framework for identifying risks to information security and implementing appropriate management and technical controls and it is risk based – delivering an appropriate and affordable level of information security.

    - Confidence in information security arrangements
    - Improved internal organization
    - Better visibility of risks amongst interested stakeholders

5. Difficulty in responding to rising customer expectations in relation to the security of their information is also a security issue. ISO 27001 provides a way of ensuring that a common set of policies, procedures and controls are in place to manage risks to information security It gives organizations a straightforward way for responding to tender requirements around information governance.

    - Meet customer and tender requirements
    - Reduce third party scrutiny of your information security requirements
    - Get a competitive advantage

6. No awareness of information security within the organization is one of the biggest security issue this standard ensures senior management recognize information

security as a priority and that there is clear tone from the top. It requires to implement a training and awareness program throughout the organization as well as it requires management to define ISMS roles and responsibilities and ensure individuals are competent to perform their roles

- Improved information security awareness
- Shows commitment to information security at all levels throughout your organization
- Reduces staff-related security breaches

ISO 27001 Implementation Costs.

ISMS Costs

Firstly company has to consider these things,

- The total cost of implementation will depend on the size of the organization. (Or the size of the business unit(s) that will be included in the ISO 27001 scope).
- The level of criticality of information (for instance, information in banks is considered more critical and demands a higher level of protection).
- The technology the organization is using (for instance, the data centers tend to have higher costs because of their complex systems).
- The legislation requirements (usually the financial and government sectors are heavily regulated with regards to information security).

Secondly,

Company should find out which level of protection they need, company should perform risk assessment, because such analysis will tell which security measures are required. When it gets the results of risk assessment, Company will have to take into account the following costs:

1. The cost of literature and training Implementation of ISO 27001 requires changes in the organization, and requires new skills. Company can prepare their employees by buying various books on the subject and/or sending them to courses (in-person or online).

2. The cost of external assistance Training employees is not enough. If the company doesn't have a project manager with deep experience in ISO 27001 implementation, company need someone who does have such knowledge, either

hire a consultant or get some online alternative.

3. The cost of technology Hardware and software that required for the implementation as well as how to use existing technology in a more secure way. However, company need to plan such investment if it proves to be necessary.

4. The cost of employees' time Standard should be implemented by the company itself, it can't be implemented by a consultant only (if company hire one). Employees have to spend some time figuring out where the risks are, how to improve existing procedures and policies or implement new ones, they have to take some time to train themselves for new responsibilities and for adapting to new rules.

5. The cost of certification If the company wants to obtain public proof that company have complied with ISO 27001, the certification body will have to do a certification audit, the cost will depend on the number of man days they will spend doing the job, ranging from under 10 man days for smaller companies up to a few dozen man days for larger organizations. The cost of man day depends on the local market.