Sri Lanka Institute of Information Technology

ISO

27001

Security

Name: Haputhanthrie J.S.

IT No: IT 13 1135 82

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

Table of Contents

1. [Introduction 3](#_Toc458330950)
2. [Benefits 3](#_Toc458330951)
3. [Cost 4](#_Toc458330952)

* [Management cost 4](#_Toc458330953)
* [Implementation cost 5](#_Toc458330954)
* [Certification cost 5](#_Toc458330955)

# Introduction

|  |  |
| --- | --- |
|  | IFS is one of the most leading IT company in Sri Lanka. Currently they are providing huge amount of job opportunities to the society. So that as an organization there is a threat for their information security in order to develop the organization.  Every company should provide data accessibility to their employees and customers according to their requirements. Information security is the key factor for any organization to maintain the stability of the organization because most valuable and privacy data must safe. In order to transfer data through network data should available within 24 hours. Additionally avoiding network issues and transferring data should be secured.  ISO 27001 Information Security Standards will help the organization to maintain control of its information, improve security of information and reduce the risk of damage to data or loosing data. Investing in developing an Information Security Management System (ISMS) a long term solution and it guarantee the security of the information. |

# Benefits

|  |  |
| --- | --- |
|  | Protecting your organizations information is critical for the successful management and smooth operation of your organization. Completing ISO/IEC 27001 information security management systems certification will aid your organization in managing and protecting your valuable data and information assets.  **1. Compliance**  It might seem odd to list this as the first benefit, but it often shows the quickest “return on investment” – if an organization must comply to various regulations regarding data protection, privacy and IT governance (particularly if it is a financial, health or government organization), then ISO 27001 can bring in the methodology which enables to do it in the most efficient way.  **2. Marketing edge**  In a market which is more and more competitive, it is sometimes very difficult to find something that will differentiate you in the eyes of your customers. ISO 27001 could be indeed a unique selling point, especially if you handle clients’ sensitive information.  **3. Lowering the expenses**  Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruption in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees.  The truth is, there is still no methodology and/or technology to calculate how much money you could save if you prevented such incidents. But it always sounds good if you bring such cases to management’s attention.  **4. Putting your business in order**  This one is probably the most underrated – if you are a company which has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain information assets, who has to authorize access to information systems etc. |

# Cost

## Management cost

|  |  |
| --- | --- |
|  | Assign suitable project management to the organization and analyze potential risk of the project management team.  Have regular meetings with the customers when preparing information security system.  Add well qualified cyber security management to the organization to reduce the cost of having troubles in the security system.  Make proper project team to handle risk in the system. |

## Implementation cost

|  |  |
| --- | --- |
|  | Identify the changes in your organization, and requires new skills. You can prepare your employees by buying various books on the subject and/or sending them to courses.  Identify information assets and assess their security risks.  Modify the current network into a secured network with modern security standards.  Firewalls for server systems should be implemented, anti-virus and anti-malware programs should be installed in the workstations and the existing programs should be updated.  Training programs for the staff to get familiar with newly introduced security system and security procedures.  Timely backups of the information should be maintained.  Security access cards for the authorized personal to access restricted areas like data stores and data warehouses. |

## Certification cost

|  |  |
| --- | --- |
|  | Consult a suitable body to ensure that the organization meets the certification requirements.  Audits and working time spent by the staff for the certification related activities |