

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

For

**Etisalat Lanka**

(<https://mypage.etisalat.lk/>)

By Vishmi Iloka R

(IT13018924)

.

## Executive Summary

### Benefits

Information has now become a truly business critical asset. Protecting this asset through developing robust information security strategies and implementing effective information security management system (ISMS) is a key management responsibility. The benefits of implementing an ISMS will primarily result from a reduction in information security risks. Specifically, benefits realized from the adoption of the ISMS family of standards include:

- Keeps confidential information secure.
- Provides customers and stakeholders with confidence in how you manage risk.
- Allows for secure exchange of information.
- Allows you to ensure you are meeting your legal obligations.
- Helps you to comply with other regulations (e.g. SOX).
- Provide you with a competitive advantage.
- Enhanced customer satisfaction that improves client retention.
- Consistency in the delivery of your service or product.
- Manages and minimizes risk exposure.
- Builds a culture of security.
- Protects the company, assets, shareholders and directors.

### Costs

Most of the costs associated with information security would be incurred anyway since information security is a business and compliance imperative. The additional costs specifically relating to the ISMS are mainly:

- **Internal resources**—The system covers a wide range of business functions including management, human resources (HR), IT, facilities and security. These resources will be required during the implementation of the ISMS
- **External resources**—Experienced consultants will save a huge amount of time and cost. They will also prove useful during internal audits and ensure a smooth transition toward certification.
- **Certification**—Only a few approved certification agencies currently assess companies against ISO 27001, but fees are not much more than against other standards.

- **Implementation**-These costs depend largely on the health of IT within the organization. If, as a result of a risk assessment or audit, a gap appears, then implementation costs are bound to go up based on the solution implemented.<sup>5</sup>

## **Introduction, Scope and Purpose**

ISO 27001 is an international standard published by the International Standardization Organization (ISO), and it describes how to manage information security in a company. ISO 27001 can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. It was written by the world's best experts in the field of information security and provides methodology for the implementation of information security management in an organization. It also enables companies to become certified, which means that an independent certification body has confirmed that an organization has implemented information security compliant with ISO 27001.

This paper identifies and categorizes the financial implications of implementing an ISO27k ISMS as a set of typical or commonplace benefits and costs. It is of course generic since we have no knowledge of your specific information security situation or risks.

## **ISMS Benefits**

Following ways describes how ISO27001 typically benefits the organization.

### **Reduction in information security risks**