

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

[**Enterprise Standards and Best Practices for IT Infrastructure**](http://courseweb.sliit.lk/course/view.php?id=137)

Priyaranga G.S.C

IT13133078

Practical Session: Wednesday

Date of Submission: 2/9/2016

Date of Evaluation : 2/9/2016

**About The Company**

Softlogic Holdings PLC is a supplier of many services in Sri Lanka, hardware and software to corporate clients. With the time the number of clients got increased and Softlogic Holdings PLC needed to add more assets and information. Definitely, information is one of the most valuable assets and it has to be protected.

This company has areas of strength in relation to security, however they also have weaknesses. Understanding and mitigating these allow the organization to have more control over its activities and to put controls in place to strengthen those weaknesses.

Softlogic Holdings PLC is in need of ISO/IEC 27001 implementation, which is an internationally recognized best practice framework for an ISMS. It helps the company to identify the risks of the important information and put in place the appropriate controls to help reduce the risks.

**Benefits of having ISO27001**

1. Risk reduction.

By adopting ISO 27001 information security standards the company can strengthen its existing information security control. It will upgrade the current information security policies. The well-structured approach of this standard will identify the security threats, vulnerabilities, and impacts as soon as possible and try to secure the company from all those treats. The standardized and rational risk management approach can be used to address information security risks according to the relative priorities.

1. Reduce the cost

The company will be able to reduce the cost that it has kept for the insurance purposes. This standard will increase the ability to transfer only selective, small risks to insurers or third parties and handle main and highly cost risks by the company itself. The stakeholders or authorities may at some point insist that the organization complies with ISO27001 as a condition of a business or to satisfy privacy and other laws, whereas implementing it on our own terms and timescales is likely to be more cost-effective if we are already using the ISO27001. This standard may allow unnecessary, inappropriate or excessive controls that cost more to be removed without compromising valuable information assets.

1. Provide valid defense in case of legal enforcement actions.

Adopting this standard generally-acknowledged well practices and provide a valid defense in case of legal enforcement actions following information security incidents.

1. Increase the brand value

The company will be following a globally recognized and well respected security standard. This standard will position the organization as a secure, trustworthy and well-managed business partner. The customers and other stakeholders of Softlogic will be able to trust the company to provide their information and their loyalty will be increased.

**Costs**

1. Management costs

This will include the cost of finding a suitable project manager and train him. Also should prepare an overall information security management strategy, aligned with other business strategies, objectives, and imperatives as well as ISO27k. Need to plan the implementation project. Should allocate the resources necessary to establish the implementation project team and need to train them also. Have to hold regular project management meetings involving key stakeholders and track actual progress.

1. Implementation costs

The cost to compile an inventory of information assets. Should assess security risks to information assets, and prioritize them. The cost to determine and treat information risks. Need to design the security architecture and security baseline. Have to increase the budget to update existing information security policies and prepare new information security policies, standards, procedures, guidelines, and contractual terms. Also, should implement proper risk treatment policies. Have to conduct awareness/training regarding this standard for implement an information security management system.

1. Certification costs

The cost for assessing and select a suitable certification body. ISO27001 certification body will do a Pre-certification visits and certification inspection. So there is a risk of failing to achieve certification at first application. The company will be able to bear the cost for re applying for the standard. All these costs will all be minimized if the company achieve high quality implementation through our own efforts.