

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

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

**4th Year 2nd Semester 2016**

Name: L.A.C.Dissanayake

SLIIT ID:IT13147006

Group Number:

Practical Session: WD

Practical Number : Lab 05 ([ISO 27001 Business Case](http://courseweb.sliit.lk/mod/assign/view.php?id=42241))

Date of Submission: 1/08/2016

Date of Evaluation : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Evaluators Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Samsung PVT LTD was founded by [Lee Byung-chul](https://en.wikipedia.org/wiki/Lee_Byung-chul) in 1938 as a [trading company](https://en.wikipedia.org/wiki/Trading_company). Over the next three decades, the group diversified into areas including food processing, textiles, insurance, securities and retail. Samsung entered the [electronics industry](https://en.wikipedia.org/wiki/Electronics_industry) in the late 1960s and the construction and shipbuilding industries in the mid-1970s; these areas would drive its subsequent growth. Following Lee's death in 1987, Samsung was separated into four business groups – Samsung Group,  [Shinsegae](https://en.wikipedia.org/wiki/Shinsegae" \o "Shinsegae) Group, [CJ Group](https://en.wikipedia.org/wiki/CJ_Group) and [Hansol](https://en.wikipedia.org/wiki/Hansol" \o "Hansol) Group. Since 1990s, Samsung has increasingly globalized its activities and electronics, particularly mobile phones and semiconductors, have become its most important source of income.

Notable Samsung industrial subsidiaries include [Samsung Electronics](https://en.wikipedia.org/wiki/Samsung_Electronics) (the [world's largest information technology company](https://en.wikipedia.org/wiki/List_of_the_largest_information_technology_companies) measured by 2012 revenues, and 4th in market value),[Samsung Heavy Industries](https://en.wikipedia.org/wiki/Samsung_Heavy_Industries) (the world's 2nd-largest shipbuilder measured by 2010 revenues), and [Samsung Engineering](https://en.wikipedia.org/wiki/Samsung_Engineering) and [Samsung C&T](https://en.wikipedia.org/wiki/Samsung_C%26T) (respectively the world's 13th and 36th-largest construction companies). Other notable subsidiaries include [Samsung Life Insurance](https://en.wikipedia.org/wiki/Samsung_Life_Insurance) (the world's 14th-largest life insurance company).

Samsung sells Mobile phones, Televisions (LCD, PDP, CRT, LED), LCD monitors, Lithium-ion batteries, Digital cameras, Large-size LCD panels, Hard-disk drives, NAND flash, DRAM, Application processors, Handsets, MP3 players, Life Insurance and electronics built by other manufacturers. Samsung is in need of ISO/IEC 27001 implementation, which is an internationally recognized best practice framework for ISMS

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization’s information risk management processes. The ISO 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

**ISMS Benefits**

* Strengthens existing information security control environment by re-emphasizing business information security control requirements, upgrading current information security policies, controls *etc*. and providing stimulus to review and where necessary improve information security controls periodically.
* Provide a structured way of managing information security within an organization
* Managers and staff become increasingly familiar with information security terms, risks and controls
* Demonstrable governance using internationally-recognized good security practices
* Provides a logically consistent and reasonably comprehensive framework/structure for disparate information security controls
* ISO 27001 provides an overarching framework for information security management that encompasses a broad range of both external and internal requirements, leveraging the common elements
* Provides customers and stakeholders with confidence in how you manage risk
* Is generally applicable and hence re-usable across multiple departments, functions, business units and organizations without significant changes
* Adopting generally-acknowledged good practices provide a valid defense in case of legal/regulatory enforcement actions following information security

# ISMS Costs

* Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k.
* Hold regular project management meetings involving key stakeholders
* Compile an inventory of information assets
* Assess security risks to information assets, and prioritize them
* Assess and select a suitable certification body
* Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body
* Determine how to treat information risks
* Periodic ISMS internal audits to check that ISMS procedures are being followed correctly
* Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual terms *etc*.

**Reference**

<https://en.wikipedia.org/wiki/Samsung>

<http://www.iso.org/iso/iso27001>

<http://certificationeurope.com/benefits-of-iso-27001/>