**IT No : IT13040772**

**Batch : Week Day - IT**

**INTRODUCTION**

Samsung is a South Korean multinational conglomerate company headquartered in Samsung Town, Seoul. It comprises numerous subsidiaries and affiliated businesses, most of them united under the Samsung brand, and is the largest South Korean chaebol. Samsung was founded by Lee Byung-chul in 1938 as a 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 in the late 1960s and the construction and shipbuilding industries in the mid-1970s; these areas would drive its subsequent growth.

Samsung Electronics is a multinational electronics and information technology company headquartered in Suwon and the flagship company of the Samsung Group. Its products include air conditioners, computers, digital televisions, liquid crystal displays (including thin film transistors (TFTs) and active-matrix organic light-emitting diodes (AMOLEDs)), mobile phones, monitors, printers, refrigerators, semiconductors and telecommunications networking equipment. It is the world's largest mobile phone maker by unit sales in the first quarter of 2012, with a global market share of 25.4%. It is also the world's second-largest semiconductor maker by 2011 revenues (after Intel).

**Why Samsung need an Information Security Management System?**

In a connected world main approaches to security have fallen short. No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program by information security professionals. The process of creating a security program will make you think holistically about your organization’s security. A security program provides the framework for keeping Samsung at a desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you keep the program and their practices up to date.

The key asset that a security program helps to protect is your data and the value of Samsung’s is in its data. You already know Samsung is one of many whose data management is dictated by governmental and other regulations, for example, how you manage customer credit card data. If your data management practices are not already covered by regulations, consider the value of the following:

* Product information, including designs, plans, patent applications, source code, and drawings.
* Financial information, including market assessments and Samsungs’s own financial records
* Customer information, including confidential information you hold on behalf of customers or clients

Protecting your data means protecting its confidentiality, integrity, and availability as illustrated by the C-I-A triangle. The consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company

* Failure to protect data’s confidentiality might result in customer credit card numbers being stolen, with legal consequences and a loss of goodwill. Lose your clients’ confidential information and you may have fewer of them in the future.
* A data integrity failure might result in a Trojan horse being planted in your software, allowing an intruder to pass your corporate secrets on to your competitors. If an integrity failure affects your accounting records, you may no longer really know true financial status.

**ISMS benefits**

ISMS is a system that helps to prevent and counteract interruptions to business activities. It protects critical business processes from the effects of information security incidents, disasters and major failures of information systems and ensures the timely resumption of normal operations.

It is relevant to all organizations, regardless of whether they use stand-alone computers or complex heterogenic network systems. It is applicable to all sectors of industry and business, and not limited to information that is handled by electronic media. It is relevant to any type of information protection, whether in printed format or written on paper, stored electronically, transmitted by post or e-mail, or spoken in conversation.

* Credibility, trust and confidence of your customer
* Greater awareness of security
* Compliance with legislation
* Securing confidentiality, integrity and availability
* Prevention of confidentiality breaches
* Prevention of unauthorized alteration of critical information
* Prompt detection of data leakage and fast reaction
* Competitive advantage - deciding differentiator in contract negotiations
* Meeting international benchmarks of security

**Benefits of standardizations**

Dell knows security should be managed differently. Their Security software solutions give you the power to protect the organization from endpoint to datacenter to cloud, achieve your most stringent compliance requirements, and transform security to a function of enablement through rapid adoption of new technologies such as cloud, BYOD and etc.

**ISMS Cost**

These are the main costs associated with the management system elements

* Find a suitable project manager (usually but not necessarily the person who will ultimately become the CISO or Information Security Manager)
* Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27k
* Plan the implementation project
* Obtain management approval to allocate the resources necessary to establish the implementation project team
* Employ/assign, manage, direct and track various project resources
* Hold regular project management meetings involving key stakeholders
* Track actual progress against the plans and circulate regular status reports/progress updates
* Identify and deal with project risks, preferably in advance
* Liaise as necessary with various other interested parties, parallel projects, managers, business partners *etc*.

## **Other ISMS implementation costs**

* Compile an inventory of information assets
* Assess security risks to information assets, and prioritize them
* Determine how to treat information (Re-)design the security architecture and security baseline
* Review/update/re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual terms *etc*.
* Rationalize, implement additional, upgrade, supplement or retire existing security controls and other risk treatments as appropriate
* Conduct awareness/training regarding the ISMS, such as introducing new security policies and procedures[[1]](#footnote-2)
* May need to ‘let people go’ or apply other sanctions for non-compliance.

1. [↑](#footnote-ref-2)