Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure

LAB 05

IT 130 699 64
Subhani K.G.D.
Weekday IT
27th August 2016

Introduction

Samsung is a South Korean multinational conglomerate company headquartered in Samsung Town. It comprises numerous subsidiaries and affiliated businesses most of them united under the Samsung brand, and is the largest South Korean business conglomerate. Its diversified products and services include information technology and communications equipment and systems, electronic components and materials, power systems, industrial and social infrastructure systems, consumer electronics, household appliances, medical equipment, office equipment, lighting and logistics.

Samsung has a powerful influence on South Korea's economic development, politics, media and culture and has been a major driving force. Its affiliate companies and produce around a fifth of South Korea's total exports Samsung's revenue was equal to 17% of South Korea's $1,082 billion GDP.

Why SAMSUNG needs an Information Security Management System?

Information is an asset which, like other important business assets, has a value to an organization and consequently needs to be suitably protected. This standard will help the company coordinate all your security efforts both electronically and physically, coherently, cost effectively and with consistency and prove to potential customers that the company take the security of their personal / business information seriously.

Samsung is a multinational Computer technology company which holds large amount of information. Samsung provides some services because of that it has severs. So those information should have been protected by well define manner. As a business company needs a legal obligation under the Data Protection Act. The system promotes efficient management of sensitive corporate information, highlighting vulnerabilities to ensure it is adequately protected against potential threats. It encompasses people, process and IT systems.

An ISO 27001 certification can be achieved by any business of any size, in any given sector, which is looking to increase and enhance the company’s security of its data.

The ISO 27001 standard is designed to ensure that adequate and proportionate security controls are put in place to ensure Data Protection and protect sensitive company information and data in order to comply with Data Protection laws and also to gain customer confidence.

Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k)

ISMS benefits

- Cost reductions due to avoiding incidents
- Smoother running operations as responsibilities and processes are clearly defined
- Improved business image in the marketplace – customers have peace of mind that the company is trustworthy
- Working with a trustworthy provider maintains the company’s own integrity to the safeguarding of its data
- Installs confidence further down the supply chain resulting in stronger customers / supplier relationships
- Having appropriate access controls in place lowers the risk of accidental exposure to employees of confidential/sensitive information
- Reassurance that their employer is meeting data handling security guidelines
- Defines clearly and precisely roles and responsibilities therefore job satisfaction and productivity is increased
- Securing confidentiality, integrity and availability
- Prevention of confidentiality breaches.
- Prevention of unauthorized alteration of critical information.
- Prompt detection of data leakage and fast reaction.
- Meeting international benchmarks of security.

Benefits of standardization

- Common framework for businesses to follow.
- Risk based approach to help plan and implement an Information Security Management System.
- ISO 27001 ensures the right people, processes, procedures and technologies are in place to protect information assets.
- ISO 27001 protects information and ensures its confidentiality, integrity and availability are maintained.

ISMS costs

- Find a suitable project manager to implement ISMS.
- Prepare an overall information security management strategy.
- Project implementation planning.
- Employ/assign, manage, direct and track various project resources.
- Hold regular project management meeting involving key stakeholders.
- Identify and deal with project risk.
- Compile and inventory of information assets.
- Assess security risk to information assets.
- (Re-)design the security architecture and security baseline.
- Assess and select a suitable certification body.