
Sri Lanka Institute of Information Technology

**Business case for ESBPII assignment.**

**Jayathissa K.P.S.P**

**IT 13110680**

**Weekend (Monday Lab)**

## Introduction

Dell Inc. (stylized as DELL) is an American privately owned multinational computer technology company based in Round Rock, Texas, United States, which develops, sells, repairs, and supports computers and related products and services. Named after its founder, Michael Dell, the company is one of the largest technological corporations in the world, employing more than 103,300 people worldwide.

Dell sells personal computers (PCs), servers, data storage devices, network switches, software, computer peripherals, HDTVs, cameras, printers, MP3 players, and electronics built by other manufacturers. The company is well known for its innovations in supply and electronic commerce, particularly its direct-sales model and its "build-to-order" or "configure to order" approach to manufacturing, delivering individual PCs configured to customer specifications. Dell was a pure hardware vendor for much of its existence, but with the acquisition in 2009 of Perot Systems, Dell entered the market for IT services. The company has since made additional acquisitions in storage and networking systems, with the aim of expanding their portfolio from offering computers only to delivering complete solutions for enterprise customers.

Information is a valuable asset that can make or break the business, so the security of information (InfoSec) should be a high priority. When properly managed it allows you to operate with confidence. Information security management gives you the freedom to grow, innovate and broaden your customer-base in the knowledge that all your confidential information will remain that way.

ISO/IEC 27001 is an internationally recognized best practice framework for an information security management system (ISMS). It belongs to the ISO 27000 series of standards (including ISO 27002 and ISO 27005). It helps you identify the risks to your important information and put in place the appropriate controls to help reduce the risk.

## Why do we need ISMS?

Organizations and their information systems and networks are exposed with security threats such as fraud, espionage, fire, flood and sabotage from a wide range of sources. The increasing number of security breaches has led to increasing information security concerns among organizations worldwide. Achieving information security is a huge challenge for organization as it cannot be achieved through technological means alone, and should never be implemented in a way that is either out of line with the organization’s approach to risk or which undermines or creates difficulties for its business operations. Thus there is a need to look at information security from a holistic perspective, and to have an information security management methodology to protect information systematically. This is where the need for ISMS comes in.

**ISO/IEC 27001:2005**

ISO/IEC 27001:2005 is the Requirements for Information Security Management Systems. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. The ISMS processes are based on the following Plan-Do-Check-Act model:

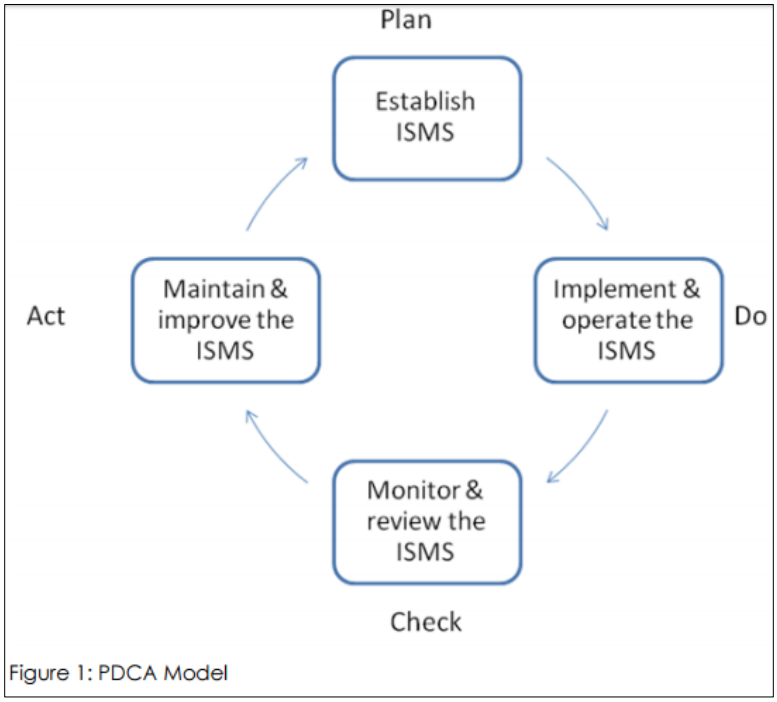

Figure 1: PDCA Model

**Advantages if Dell Company is ISMS certified**

Certification of ISMS brings several advantages;

- Provide a structured way of managing information security within an organization
- Provide an independent assessment of an organization’s conformity to the best practices agreed by a community of experts for ISMS.
- Provide evidence and assurance that an organization has complied with the standards requirement.
- Enhance information security governance within the organization.
- Enhance the organization’s global positioning and reputation.
- Increase the level of information security in the organization.

| Information security issue | How ISO/IEC 27001 helps | Benefits |
|---|---|---|
| With increasing fines for personal data breaches, organizations need to ensure compliance with legislative requirements, such as the UK Data Protection Act | • It provides a framework for the management of information security risks, which ensures you take into account your legal and regulatory requirements | • Supports compliance with relevant laws and regulations<br>• Reduces likelihood of facing prosecution and fines<br>• Can help you gain status as a preferred supplier |
| Potential information breach, damaging your reputation | • It requires you to identify risks to your information and put in place security measures to manage or reduce them<br>• It ensures you implement procedures to enable prompt detection of security breaches<br>• It is based around continual improvement, and requires you to regularly review the effectiveness of your information security management system (ISMS) and take action to address new and emerging security risks | • Protects your reputation<br>• Provides reassurance to clients that their information is secure<br>• Cost savings through reduction in incidents |
| Availability of vital information at all times | • It ensures that authorized users have access to information when they need it<br>• It demonstrates that information security is a priority, whilst reassuring stakeholders that a best practice system is in place<br>• It makes sure you continually improve your information security provisions | • Demonstrates credibility and trust<br>• Improves your ability to recover your operations and continue business as usual |
| Lack of confidence in your organizations ability to manage information security risks | • Gives you a framework for identifying risks to information security and implementing appropriate management and technical controls<br>• Is risk based – delivering an appropriate and affordable level of information security | • Confidence in your information security arrangements<br>• Improved internal organization<br>• Better visibility of risks amongst interested stakeholders |
| Difficulty in responding to rising customer expectations in relation to the security of their information | • It provides a way of ensuring that a common set of policies, procedures and controls are in place to manage risks to information security | • Meet customer and tender requirements<br>• Reduce third party scrutiny of your information security requirements<br>• Get a competitive advantage |

| | | |
|---|---|---|
| | • It gives organizations a straightforward way for responding to tender requirements around information governance | |
| No awareness of information security within your organization | • It ensures senior management recognize information security as a priority and that there is clear tone from the top<br>• It requires you to implement a training and awareness program throughout your organization<br>• It requires management to define ISMS roles and responsibilities and ensure individuals are competent to perform their roles | • Improved information security awareness<br>• Shows commitment to information security at all levels throughout your organization<br>• Reduces staff-related security breaches |