Sri Lanka Institute of Information Technology

Enterprise Standards and Best Practices for IT Infrastructure

ISO/IEC 27000 series standards (ISO27k) – Information Security Management System (ISMS) Business case for hp Corporation

Submitted by:

H.M.P.Madukapriya
IT13026462
Weekday batch

Date of submission: 03/09/2016

INTRODUCTION

HP(Hewlett-Packard Company**)** American multinational information Technology Company headquartered in Palo Alto, California. It developed and provided a wide variety of hardware components as well as software and related services to consumers, small- and medium-sized businesses (SMBs) and large enterprises, including customers in the government, health and education sectors.

The company was founded in a one-car garage in Palo Alto by William "Bill" Remington Hewlett and David "Dave" Packard, and initially produced a line of electronic test equipment. HP was the world's leading PC manufacturer from 2007 to Q2 2013, after which Lenovo remained ranked ahead of HP. It specialized in developing and manufacturing computing, data storage, and networking hardware, designing software and delivering services. Major product lines included personal computing devices, enterprise and industry standard servers, related storage devices, networking products, software and a diverse range of printers and other imaging products. HP marketed its products to households, small- to medium-sized businesses and enterprises directly as well as via online distribution, consumer-electronics and office-supply retailers, software partners and major technology vendors. HP also had services and consulting business around its products and partner products.

Hewlett-Packard company events included the spin-off of its electronic and bio-analytical measurement instruments part of its business as Agilent Technologies in 1999, its merger with Compaq in 2002, and the acquisition of EDS in 2008, which led to combined revenues of $118.4 billion in 2008 and a Fortune 500 ranking of 9 in 2009. In November 2009, HP announced the acquisition of 3Com, with the deal closing on April 12, 2010. On April 28, 2010, HP announced the buyout of Palm, Inc. for $1.2 billion. On September 2, 2010, HP won its bidding war for 3PAR with a $33 a share offer ($2.07 billion), which Dell declined to match.

On October 6, 2014, Hewlett-Packard announced plans to split the PC and printers business from its enterprise products and services business. The split closed on November 1, 2015, and resulted in two publicly traded companies: HP Inc. and Hewlett Packard Enterprise.

Why HP Corporation need an Information Security Management System?

The establishment, maintenance and continuous update of and ISMS provide a strong indication that a Sony is using a systematic approach for the identification, assessment and management of information security risks. Critical factors are Confidentiality (protecting information from unauthorized parties), Integrity (protecting information from modification by unauthorized users) and Availability (making the information available to authorized users). If hp will be capable of successfully addressing information confidentiality, integrity and availability(CIA) requirements which in turn have implications are minimization of damages and losses, competitive edge,

profitability and cash-flow, legal compliance, respected organization image and business continuity.

These are the key facts that security experts said,

- Security depends on people more than on technology.
- Employees are a far greater threat to information security than outsiders.
- Security is like a chain. It is only as strong as its weakest link.
- The degree of security depends on three factors,
    - The risk you are willing to take.
    - The functionality of the system.
    - Costs you are prepared to pay.
- Security is not a status or a snapshot, but a running process.
- Information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects, remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness.

BENEFITS OF ISMS

- Comprehensive, well-structured approach increases the likelihood that all relevant information security threats, vulnerabilities and impacts will be identified, assessed and treated rationally **–** risk reduction
- Managers and staff become increasingly familiar with information security terms, risks and controls – risk reduction
- Formal confirmation by an independent, competent assessor that the organization's ISMS fulfills the requirements of ISO/IEC 27001 – risk reduction
- Comprehensive, well-structured approach increases the likelihood that all relevant information security threats, vulnerabilities and impacts will be identified, assessed and treated rationally – risk reduction.
- An embodiment of good practices, avoids 're-inventing the wheel – cost saving

- Is generally applicable and hence re-usable across multiple departments, functions, business units and organizations without significant changes – cost saving
- Avoids having to specify the same basic controls repeatedly in every situation – cost saving
- Allows the organization to concentrate effort and resources on specific additional security requirements necessary to protect particular information assets – cost saving
- Provides a mechanism for measuring performance and incrementally raising the information security status over the long term – cost saving and risk reduction
- Based on globally recognized and well respected security standards – brand value
- Positions the organizations as a secure, trustworthy and well-managed business partner (similar to the ISO 9000 stamp for quality assurance) – brand value
- Builds a coherent set of information security policies, procedures and guidelines, tailored to the organization and formally approved by management – long term benefits

COSTS OF ISMS

ISMS implementation project management costs

- 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 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 risks. (i.e. mitigate them using suitable security controls, avoid them, transfer them or accept them)
- (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.
- May need to 'let people go' or apply other sanctions for non-compliance.

Certification costs

- Assess and select a suitable certification body.
- Pre-certification visits and certification audit/inspections by an accredited ISO/IEC 27001 certification body.
- Risk of failing to achieve certification at first application. (any items that caused failure would themselves represent unacceptable information security risks – delayed certification more likely than complete failure)
- Staff/management time expanded during annual surveillance visits.