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 Sony Corporation

Submitted by:

IT13010768
W.M.P.S.Wijesundara
Weekday batch

Date of submission: 17/08/2016

INTRODUCTION

Sony Corporation is commonly referred to as Sony, is a Japanese multinational conglomerate corporation headquartered in Konan Minato, Tokyo, Japan. Its diversified business includes consumer and professional electronics, gaming, entertainment and financial services. The company is one of the leading manufacturers of electronics products for the consumer and professional markets.

Sony Corporation is the electronics business unit and the parent company of the Sony Group, which is engaged in business through its four operating segments – electronics (including video games, network services and medical business), motion pictures, music and financial services. The Sony Group is Japan-based corporate group primarily focused on the Electronics (such as AV/IT products and components), Game (such as the PlayStation), Entertainment (such as motion pictures and music) and Financial Services (such as insurance and banking) sectors. The group consists of Sony Corporation (holding and electronics), Sony Interactive Entertainment (games), Sony Pictures Entertainment (motion pictures), Sony Music Entertainment (music), Sony/ATV Music Publishing (music publishing), Sony Financial Holdings (financial services) and others. Sony is among the worldwide top 20 semiconductor sales leaders and as of 2013, the fourth-largest television manufacturer in the world, after Samsung Electronics, LG Electronics and TCL.

Why Sony 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 Sony 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

- 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.