Business Case for an Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k)

For

Millennium Information Technologies

(http://www.millenniumit.com/)

By Abeysinghe A.M.S

IT13030490

Executive Summary

Benefits

ISMS is a set of policies concerned with information security management or IT related risks. The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. The benefits of implementing an ISMS will primarily result from a reduction in information security risks.

- Business managers of the organizations will make informed decisions regarding potential risk and should be able demonstrate compliance with standards and regulations.
- minimize the impact from these external threats of various cybercrime.
- Implement technical, management, administrative and operational controls, which is the most cost effective way of reducing risk. Highest priority risks are tackled first to attain best ROI in information security.
- Responsible for protecting information assets and more specifically business manager. The business manager may delegate their responsibility.
- Organization will improve credibility and trust among internal stakeholder and external vendors. The credibility and trust are the key factors to win a business.
- ISMS raises awareness throughout the business for information security risks, involve all employees throughout an organization and therefore lower the overall risk to the organization.
- Keep Confidential Information Secure.
- Allow for secure information exchange.
- Build culture of security.

Costs

The additional costs specifically relating to the ISMS

- The cost of literature and training - Implementation of ISO 27001 requires changes in your organization, and requires new skills. You can prepare your employees by buying various books on the subject and/or sending them to courses
- The cost of external assistance – cost of hire a consultant or get some online alternative
- The cost of Technology – need a big investment in hardware, software or anything similar – all these things already existed. The biggest challenge was usually how to use existing technology in a more secure way.
- The cost of Employees' time - The standard isn't going to implement itself, neither can it be implemented by a consultant only (f you hire one). Your employees have to spend some time figuring out where the risks are, how to improve existing procedures and policies or implement new ones, they have to take some time to train themselves for new responsibilities and for adapting to new rules.
- The Cost od Certification - the certification body will have to do a certification audit – the cost will depend on the number of man days they will spend doing the job, ranging from under 10 man days for smaller companies up to a few dozen man days for larger organizations. The cost of man day depends on the local market.