Business Case for an Information Security Management System (ISMS)

ISO 27001 Security

CENTER FOR DIABETES ENDOCRINOLOGY AND CARDIOLOGY-METABOLISM (PVT)LTD.

DIT : IT 120 800 90
Name : K.D.C.Piyamal

Introduction of ISO 27001

ISO 27001 formally known as ISO/IEC 27001:2005 Is an international standard specification for an information security management system (ISMS) publish by the international standrational organization (ISO) .It helps to the organizations keep their information assets secure and ISO 27001 can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large. This ISMS is a framework it provide all the policies and procedures that include all legal, physical and technical controls involved in an organization's information risk management processes. The focus of ISO 27001 is to protect the confidentiality, integrity and availability of the information in a company. ISO 27001 certification is the international benchmark for Information Security Management. In order to achieve this accreditation, a company must show it has a systematic and ongoing approach to managing and protecting the assets and sensitive company as well as customer information. This ISO 27001is helps to implement a system to manage information within an organization to protect information resources to ensure continuity of business even after any injure or loss occur.

And also Using this ISO 27001 standards will help your organization manage the security of assets such as financial information, property, intellectual information employee details or entrusted to you by third parties.

Scope

This paper identifies and categorizes the financial implications of implementing an ISO27k ISMS as a set of typical or commonplace benefits and costs. It is of course generic since we have no knowledge of your specific information security situation or risks. In this paper cover all the valuable assets and their risk. Mainly this document is not focused about the size of the limitation. And include enough information to determine what is covered by the processes of this ISO 2700k standard.

Purpose

Formation is a valuable asset that can make or break your business. 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. Feel free to use this paper both as a source of inspiration for your own business case, budget request or project proposal to management, and as a framework for measuring and optimizing the net value of your ISMS over the long term (*e.g.* using ISACA's Val IT approach with PRAGMATIC metrics).This document is not a project plan , the Project plan will be developed once the project is formally approved.

Why ISO 2700 important for you CDEM hospital?

Hospital/ Health care industry is becoming competitive and emerging day by day. The Quality of Service provided to the end-users/ patients has become the primary focus. It is really important to measure and improve the Quality of Service for them continuously. One of the best quality tool which help in this are the ISO certifications. The implementation of ISO certification (whether ISO 9000, ISO 14000, ISO 27000 etc.) has its own benefits:

In CDEM hospital deals with most no of patients (customers) day by day. Hospital needs to Deal with the patients' health condition which should be 100% sure and accurate it is very risky and should has done with more responsibilities .Doctors suggest medicine and treatments by depending on that data Like patient data, test reports data, scan reports ,etc. .

To give a more accurate and 100% correct data ,CDEM hospital use soft wear, systems, equipment's, Likes robotic machines(these machines are unique for the Sri Lnaka),"sukraa" hospital management ERP system (this is the main system which use for patients managements, hospital management and HR management),"Tail" soft wear (used for finance purposes). CDEM hospital uses e-channeling service to give better and quick service. To run those software, systems and equipment CDEM hospital has established servers, LAN networks

Most organization's now rely on information systems to support all of their critical business processes. This dependency has led to an evolving risk from electronic security threats such as hacking, data loss, breach of confidentiality and even terrorism. These increasingly sophisticated attacks can come from individuals, private organization's or even clandestine foreign intelligence agencies. When these attacks result in loss of information, theft of confidential data or damage to critical systems and documents, organizations can suffer severe consequences including financial repercussions and reputational risk.

If some day someone has log into this server, system illegally and change or delete data for some reason, hospital has to face major problems as above say because those data are used to treat patient and to manage employee also there will be critical problems day by day likes pc breakdown ,server break down ,IP issues, etc. .These are the ways which can damage providing quality service and relationship between hospital and the customers' .To reduce these kind of risks by finding the reasons for those illegal logins, having solution for those critical problems and giving these system and servers an international guiding and cover, it is better to have an international standard like ISO 27001K

How to achieve target

To implement this ISO 27001K standard, hospital must full fill following 16 steps. After gaining this standard hospital can cover all the related, non-related, risky and valuable assets in proper way. There will be a great cost after following these steps, as well as there will be major benefits for CDEM hospital.

1. Obtain management support.
2. Treat it as a project.
3. Define the scope.
4. Write an ISMS Policy.
5. Define the Risk Assessment methodology.
6. Perform the risk assessment & risk treatment.
7. Write the Statement of Applicability.
8. Write the Risk Treatment Plan.
9. Define how to measure the effectiveness of controls.
10. Implement the controls & mandatory procedures.
11. Implement training and awareness programs.

12. Operate the ISMS.
13. Monitor the ISMS.
14. Internal audit.
15. Management review.
16. Corrective and preventive actions.

ISMS benefits.

After CDEM hospital gained this ISO 27001 standard there will be more benefits such as, providing ways to secure hospital's existing systematic information and business information, establishing policies to protect useful informations.

- Identify what are the risky information and what are the security threats, after that give a value for the information and categorized-**Cover all IT related risks and threats**.

- Divide those threats and risks under using the time of impureness and availability of that information.

- if Information leaked-after implement ISO 2700k- **prevent going your organization's valuable informations to other 3rd party hand.**

- Give your information a 3rd party coverage (protect your informations in any insurance company or etc. They transfer your risk to them. And protect informations.)Purpose for transferring risk is -**minimize your risk and get very secure surety for your information**.

- Give proper training to all the employees and management staff, how to work with risks and how to reduce it and control it.

- Add big valuable to your organization globally.

- Avoid disturbances and provide very high quality and smooth process.

- Increase productivity and maximize the utilization of resources.

- Facilitate minimize internal and external threats and risk.

- enhance international competitiveness of products and services.

- **Protect your confidential informations** – from the threat of hacking, data loss, breach of confidentiality and ensure you can recover faster from such attacks.

- **Establish business continuity plans** – that ensure your operations will continue in the event of man-made and natural disasters.

- Maintain confidential information protected.

- Enable confidence to customers and stakeholders with your risk management system.

- Permit for safe exchange of information.

ISMS costs

These are the main costs associated with the management system elements of an ISO27k ISMS. The cost of developing and certifying an ISO 27001 Information Security Management System (ISMS) depends upon four key factors: ISMS scope, ISMS Gap, your organizational capacity to close that gap, and your "desired certification timeframe". Mainly identify what are cost related for this implementation .Actually your organization will spend this cost, in future you can earn lot of using this implementation.

IN CDEM organization we identify cost it goes under 4 main phrases.

1. Cost relating to organizational change (initial cost).

2. Design & development costs

3. Implementation costs
4. Certification costs
5. Ongoing maintenance costs.

Costs relating to organizational change (initial cost)

This is a very basic cost your organization will spend for the ISO 2700k implementation .because they will change your normal business procedures and processors to proper manner.in this stage your costs may vary notably.

- Find a suitable project manager (usually but not necessarily the person who will ultimately become the CISO or Information Security Manager).
- Assets identification, auditing and categorized.
- Need to raise organizational (staff & management) awareness.
- Ongoing operation & maintenance.
- Change some staff rights and their job role.
- Plan the implementation project.

- Prepare an overall information security management strategy.

Design & development costs

- Establish suitable standards, guidelines, procedures etc.
- Review/update of existing information security standards, guidelines, procedures *etc*.
- Preparation of (some) new information security standards, guidelines, procedures *etc*.
- (Re-) design of controls architecture.

Implementation costs

- Compile an inventory of information assets.
- One-off costs to upgrade and/or supplement various existing controls to meet the standard.
- Staff and management staff Awareness & training costs.
- After the risk identification, remove unnecessary assets and add proper standard, powerful assets.
- Establish new security services and policies.

Certification costs

- Initial pre-certification & certification visits by accredited ISO/IEC 27001 certification body (a few $k).
- 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 expended during annual surveillance visits.
- Tri-annual re-certification (more thorough review & hence wider impact, but still relatively minor).
- All these costs will all be minimized if we achieve high quality implementation through our own efforts.

Ongoing maintenance costs

- Annual review/maintenance of information security policies, guidelines, procedures *etc*. to maintain compliance with standard
- Minor costs to maintain registration – May perhaps be reduced by combining ISO/IEC 27001 with ISO 9000 certification.

Conclusion

The International Standards ideally suited to meet the needs of information security governance — a key aspect of corporate governance that protects an organization's information assets

Accredited certification to ISO/IEC 27001 demonstrates to existing and potential customers that an organization has defined and put in place best-practice information security processes. This document outlines the benefits of ISO 27001 certification.

Therefor it's better to have these kind of international information standard in your organization.