Enterprise Standards and Best Practices for IT Infrastructure

Lab Report

Lab 04 - ISO 27001 Report

IT 12067916 – N.C Rathnavibushana

WEEKEND IT

Sri Lanka Institute of Information Technology B.Sc.

Special (Honors) Degree in Information Technology

Specialized in Information Technology

Risk Treatment Plan for GSS Company

ISO 27001 Security
By Global System Solution International (Pvt.) Ltd.

Business Case

Executive Summary

Global System Solution (GSS) is IT Company under the GSS group of companies. To effectively manage and coordinate the entire Global Solution System (GSS) and Enhance statistical production and utilization at the head office and the regional Offices, GSS has an objective of streamlining its information security management Systems by implementing ISO 27001 International Standard and consequently seeking certification by a Certification Body (CB) on the same standard.

This case study concerns the IT security methods and process should implement for GSS international (Pvt.) Ltd. Company will gain significant improvement after implementing this ISO 27001 and increased the customer relations in Super market Background with that. This case study reveals some important facts to implement. Benefits of implementing this certification are customer base is increased, Customer satisfaction increased, Employee salary details are protected, Better working environment, Buying patterns are protected, predictions are protected. Costs have been incurred relating to the process improvement and resource improvements.

Introduction, scope and purpose

Purpose of this document is to address the audience of Hila (CEO) and some higher management to provide some guide lines to explain methodology to follow the process. Scope of the project is to cover implementation of the ISO 27001 in the company by using resources and the train employees to handle the new process and Market productions. **GSS** is a supermarket goods brand checking chain that implemented in 12 distinct district company has acquired its growth by acquisition and dedication.

GSS Ltd Business Background

Networking service industry is a highly competitive environment. Applications are complex process server creation, cloud environments, company network handling, trouble shooting and deal with costly brand names, those applications customized to international standards chain. Many network companies have used legacy systems since they are focusing on market strategies. Still low priority is given to IT related process and low information security. GSS services developed over time and was independent of one another. As a result it utilizes various database management systems with super market goods. Including oracle, Apache server E-business suite. Main product is introducing correct branded super market goods to the Market.

Benefits of implementing ISO 27001

Direct Benefits

Highly Secured Applications

Front of Store application is developed from purchasing now – defunct company, Currently GSS has signed with retired programmers from the previous company to develop the system which is in the sense they can access company DB and other application environment . So the security risk is there. Network system purchased from Trevor Inc. has security holes since old version is still using in the company were root access permission are simply given to any person in the company. Most of the time HR staff will access this system and user level authorization are poorly maintained there for even normal HR employee also can access the system and its salary details at any time. General Ledger is also an old system has heritage too old to track .By adapting to ISO 27001standereds help to gain constant information security by implementing policies where necessary , employee compliance with the policies followed by enforceable disciplinary process.

Risk reduction cost saving and brand value

- Formal confirmation by an independent, competent assessor that the organization's GSS fulfills the requirements of ISO/IEC 27001 **– risk reduction**
- Provides assurance regarding an organization's information security management capabilities (and, by implication, its information security status) for employees, owners, business partners, suppliers, regulators, auditors and other stakeholders, without requiring numerous individual evaluations, assessments or audits, or having to rely purely on management assertions and assumptions **- cost saving and risk reduction**
- Positions the organization as a secure, trustworthy and well-managed business partner (similar to the ISO 9000 stamp for quality assurance) **– brand value**

- Demonstrates management's clear commitment to information security for corporate governance, compliance or due diligence purposes **– cost saving and risk reduction**

Increase Reliability and maintainability in the DB systems

Starting from maintain several networks through remote server support system there is huge risk and problems happen through the systems. It cost lot to maintain this system since there is no direct support for the developer's perspective. There for better to migrate to a new technology.

DB system should be migrated to a new technology which is supported by the development company. It will reduce maintain cost.

Structured approach

- Provides a logically consistent and reasonably comprehensive framework/structure for disparate information security controls **– cost saving**
- Provides the impetus to review systems, data and information flows with potential to reduce overhead of duplicated and other unnecessary systems/data/processes and improve the quality of information (business process re-engineering) **– cost saving**
- Provides a mechanism for measuring performance and incrementally raising the information security status over the long term **– cost saving and risk reduction**
- Builds a coherent set of information security policies, procedures and guidelines, tailored to the organization and formally approved by management **– long term benefits**

High Profits

When server system is will implemented according to ISO 27001it will help to manage waste effectively and food system will predict buying strategies correctly with more user interaction and followed by the constant ISO 27001 audits. This will help higher management to make correct decision on correct time and to manage stock and reduce waste of food items and gain more profits.

Indirect Benefits

Better human relations

When highly secured system is available only authorized employees will access confidential information. This will reduce conflicts among other employees like getting to know other salary details etc. By improving coding standard according to ISO27001 and with more usability feature can improve employee interaction with these systems and get the maximum benefits out of it. Following ISO 27001 will help to arrange training according to standard procedure and will increase employee knowledge for better competitive point.

Improvement Risk management and contingency planning

Through ISO 27001 certification process it identifies vulnerabilities and threats to the system which are explained above and will help to reduce those and will help higher management to take necessary action to business continuity.

Enhanced supplier confidence

Network goods and sever maintain industry contains highly confidential supplier information's which suppliers share with only their trusted customers like discount rate provided, new products there are planning to release etc. ISO 27001 provides certification to ensure information confidentiality. This is bold statement and will make out network services from others and will help to attract more customers.

ISO 27001 Cost

Find a suitable project manager (usually but not necessarily the person who will ultimately become the 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. Employee/assign, manage, direct and track various project resources. Hold regular project management meetings involving key stakeholders. Track actual 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*. Cost of implementing ISO 27001 is modest. So we need a cultural change. We have to set our employee mind set to adapt to the change. May be we have to let go some employees who are not willing to adapt to the process. Constant training for the Retails staff is needed.

Organizing technical workshops to brush up knowledge and to tech about ISO 27001 is needed. Data base server migration to the new technology and initial cost will be somewhat high but the benefits out of it more than that since security and audits saves money and time.

Scope

The Information Security Management System (ISMS) applies to the provision of trusted and managed information security services to internal and external customers of "Netware Ltd" in accordance with the ISMS Statement of Applicability revision 01.