

Enterprise Standards and Best Practices for IT Infrastructure

**Lab 5 – Business Case on Information Security Management
(ISMS) for Virtusa Corporation**

Liyanarachchi H.P - IT13119836

**Sri Lanka Institute of Information Technology
B.Sc. Special (Honors) Degree in Information Technology
Specialized in Information Technology**

Introduction

Virtusa Corporation is a global information technology services company founded in 1996 with its headquarters in Westborough, United States. The company provides IT Consulting, Business Consulting, Systems Implementation and Application Outsourcing services to large enterprises and software vendors.

The company has delivery centers in the United States, the United Kingdom, Singapore, Germany, Malaysia, the Netherlands, India, and Sri Lanka. They provide high-value IT services that enable their clients to enhance business performance, accelerate time-to-market, increase productivity and improve customer service. They serve Global 2000 companies and the leading software vendors in Banking & Financial Services, Insurance, Telecommunications, Technology and Media, Information & Education industries. They got more than 10000 employees in their company.

What is ISO27k and why is it needed to Virtusa Corporation?

ISO27k deals with the Information Security Management Systems (ISMS) and it helps to reduce the information security risk and strengthens the information security control environment by applying new policies, rules etc. As the result of the improving Information security Control Company can reduce cost and increase customer attraction toward the company.

Virtusa Corporation is a multinational company which deals with many famous and reputed companies, banks, hospitals and many more. so it contains lot of high sensitive information about each company as well as lot of employee details, so well defined manner should be use to manage these sensitive information and protect them from intruders. So those information has to be protected in well define manner. Protecting data means protecting its confidentiality, integrity, availability and durability etc. as an example, when we think about confidentiality, if company cannot protect the client data etc. It will affect to the customers of the company because those companies get help from Virtusa Corporation and most of the time share some sensitive data with Virtusa Corporation in order give some clear idea on what they expect like requirement explanation from Virtusa Corporation. If some other client competitive company got those information it can lead to high business loss if that kind of thing happens customer leave company. Consider another example, Because of data integrity failure might result in virus being planted in your server

allowing an intruder to pass your corporate secrets on to your competitors. If an integrity failure affects your accounting records, you may no longer really know your company's true financial status. To get rid of these problems have to consider about those things and have to find and plan better ways to avoid those problems associated with information security and reduce the risk of losing company data.

Benefits of implementing an Information Security Management System based on ISO/IEC 27000 series standards (ISO27k) at Virtusa Corporation

ISMS benefits

Four Key benefits of implementing ISO27k in Organization.

1. Compliance.
2. Marketing edge.
3. Lowering the expenses.
4. Putting your business in order.

There are the ways in which an ISO27k ISMS will typically benefits the organization.

- Keeps confidential information secure.
- Provides customers and stakeholders with confidence in how you manage risk.
- Allows for secure exchange of information.
- Allows you to ensure you are meeting your legal obligations.
- Provide you with a competitive advantage.
- Enhanced customer satisfaction that improves client retention.
- Consistency in the delivery of your service or product.
- Manages and minimizes risk exposure.
- Builds a culture of security.
- Protects the company, assets, shareholders and directors.

Benefits of standardization

1. Provides a security baseline, almost universally required information security controls on which to implement specific additional controls as appropriate-cost saving
2. An embodiment of good practices, avoid re-inventing the wheel-cost saving.
3. Avoids having to specify the same basic controls repeatedly in every situation-cost saving.
4. Based on globally recognized and well respected security standard-brand value.

Benefits of certification

- Build trust internally and externally –always should plan about building trust with clients as well as with the company employees because employee also valuable assets in the company. If company comes with standards employees are happy to work in the office and others who willing to join with company also increases with good attraction.
- Satisfy audit requirement - If company comes with ISO27k certification, certification negates the need for repeated customer audits, reducing the number of external customer audit days because certification is globally accepted indication for information security. Because of this company cost will decrease.
- Certification will help to improve and protect the company reputation because customer confidence will increase and their feedback will help to increase company new business projects.

ISMS Costs

ISMS implementation project management, maintenance and other costs

1. Find a suitable project manager to implement ISMS.
2. Prepare an overall information security management strategy.
3. Project implementation planning.
4. Employ/assign, manage, direct and track various project resources.
5. Hold regular project management meeting involving key stakeholders.
6. Identify and deal with project risk.
7. Compile and inventory of information assets.
8. Assess security risk to information assets.
9. (Re-) design the security architecture and security baseline.
10. Assess and select a suitable certification body.
11. Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body.
12. Staff/management time expended during annual surveillance visits.
13. Periodic ISMS internal audits to check that ISMS procedures are being followed correctly.
14. Periodic review of information security rules, standards, guidelines and etc.
15. Normally certification cost will depends on the number of employees and the regular compliance review to maintain company certification only cost normally about US \$5 and it very cost effective once after got the certification first time.

