SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

ISO_27001_Business_Case (Lab05) Assignment

Name: H.A.E.Piumali

SLIIT ID: IT13056612

Practical Session: WD Friday

Practical Number: Lab 05

Date of Submission: 3rd of September 2016

Date of Evaluation :
Evaluators Signature :

Our Organization: Healthcare Information Solutions Team

Care stream recently received ISO 27001 Certification in Europe. We are happy to share that this is an important accomplishment for our Healthcare Information Solutions team, as it is a vital benefit to the customers we serve.

Even if ISO Certification is something you may not hear about often in the IT space, it plays a crucial role in assuring cloud customers that their data are safe, secure and accessible. In the following paragraphs, I will explain what ISO 27001 certification is, why it is important for cloud vendors to obtain it and most importantly, what it means for customers to work with ISO certified vendors.

Figure 01

What are the important business value considerations facilities should be aware of?

- This is our commitment to information security management for interested parties verified by BSI, a founding member of the International Organization for Standardization (ISO).
- It protects our business against information security threats and vulnerabilities.
- ISO 27001 is becoming a customer requirement in many countries.
- It therefore provides added value to the enterprise and its interested parties.

- It provides a framework for the management of information security risks, which ensures our take into account our legal and regulatory requirements.
- It requires us to identify risks to our information and put in place security measures to manage or reduce them.
- It ensures our implement procedures to enable prompt detection of security breaches.
- It is based around continual improvement, and requires us to regularly review the effectiveness of our information security management system (ISMS) and take action to address new and emerging security risks.
- It ensures that authorized users have access to information when they need it.
- It demonstrates that information security is a priority, whilst reassuring stakeholders that a best practice system is in place.
- It makes sure us continually improve our information security provisions.
- It provides a way of ensuring that a common set of policies, procedures and controls are in place to manage risks to information security.
- It gives organizations a straightforward way for responding to tender requirements around information governance.

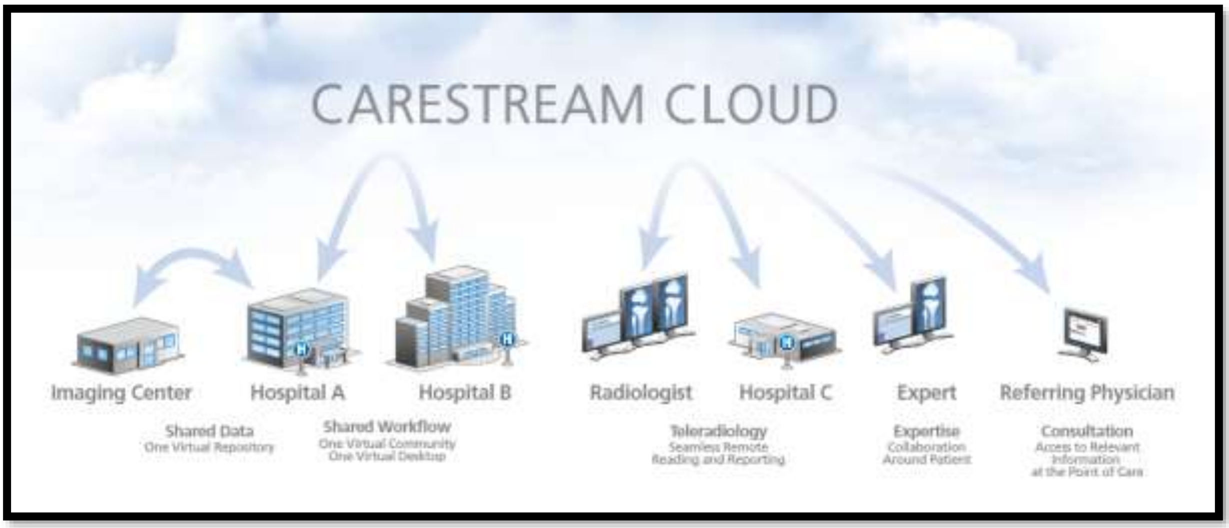

Figure 02

What are the benefits of ISO 27001 certification for our organization?

- Security risks are appropriately prioritized and cost effectively managed.
- It increases confidence in our Organization as it shows we care for our customer business, and we are committed to protect patient data they entrust to us.
- It demonstrates commitment to Information Security Management to third parties and stakeholders and will give them greater confidence to interact with us.
- It provides a framework to ensure fulfillment of our commercial, contractual and legal responsibilities.
- Supports compliance with relevant laws and regulations.
- Reduces likelihood of facing prosecution and fines.
- Can help us gain status as a preferred supplier.
- Protects our reputation.
- Provides reassurance to clients that their information is secure.
- Cost savings through reduction in incidents.
- Demonstrates credibility and trust.
- Improves our ability to recover our operations and continue business as usual.
- Confidence in our information security arrangements.
- Improved internal organization.
- Better visibility of risks amongst interested stakeholders.

How to effect Costs

These are the main costs associated with the management system elements of an ISO27001.

ISMS implementation our Management Costs

- Find a suitable manager (CISO or Information Security Manager).
- Prepare an overall information security management strategy, aligned with other business strategies, objectives and imperatives as well as ISO27001.
- Plan the implementation project.
- Obtain management approval to allocate the resources necessary to establish the implementation project team.
- Employ or 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.

Certification costs

- Assess and select a suitable certification body.
- Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body.
- Risk of failing to achieve certification at first.
- All these costs will all be minimized if we achieve high quality implementation through our own efforts.

Ongoing ISMS operation and Maintenance Costs

- Periodic ISMS internal audits to check that ISMS procedures are being followed correctly.
- Complete preventive and corrective actions to address potential and actual issues.

Conclusion

1) ISO 27001 gives us a best practice management framework for implementing and maintaining security. It also gives us a baseline against which to work - either to show compliance or for external certification against the standard.

2) However, compliance or external certification to ISO 27001 does not mean we are secure - it means that we are managing security in line with the standard, and to the level we think is appropriate to the organization.

3) If our risk assessment is flawed, we don't have sufficient security and risk assessment expertise, or we do not have the management and organizational commitment to implement security then it is perfectly possible to be fully compliant with the standard, but be insecure.

4)Implementing ISO 27001 is the right way forward to ensure the security of an organization. However, to actually be secure, it is necessary to develop a culture of valuing information and protecting it, through:

- A strong management commitment to information security.
- Individual ownership and responsibility for information security and
- Effective information security education and awareness.