SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

4th Year 2nd Semester 2016

ISO_27001_Business_Case

Name: Dinushi Madurangi G.G.

ID: IT13049096

WD

Introduction

The race is on for organizations to connect a world of people, devices and applications in ways that open new revenue streams, create advanced business models, and build rewarding relationships with customers. And in this increasingly connected world no other company can help you meet the new phase of technology and business innovation, like WSO2.

Comprehensive and Open Platform for Digital Enterprise is 100% open source middleware platform enables organizations to build a complete modern enterprise architecture and become a better digital business. Its componentized architecture enables enterprises to deploy only what they need when they need it to automatically adapt business activity in response to market events.

Rapid, Expert Support of WSO2's financial business model is based upon providing the best support in the industry. From project evaluation and inception to development and going into production, we strive for a support experience that customer's value and renew.

Leading enterprises rely on WSO2 for their mission-critical applications. Today, their customers span across healthcare, finance, retail, manufacturing, telecoms and other industries worldwide. And this company help them build competitor-eclipsing, company-advancing capabilities in record time.

Why WSO2 need Information Security Management System (ISMS)?

WSO2 offers a complete open source product stack to cater to all needs of a connected business. With their single code base structure, WSO2 products have weaved together to solve many enterprise-level complex identity management and security problems. By believing in open standards and supporting most of the industry leading protocols, WSO2 is capable of providing seamless integration with a wide array of vendors in the identity management domain. The WSO2 security platform also has the ability to extend its architecture to fit into multiple heterogeneous systems that don't support open standards.

Security is as strong as its weakest link and in many cases that link is either human or encryption based. Although security is a subjective topic, almost everyone will agree that using a hardware security module (HSM) to safeguard and manage digital keys is a huge improvement over software based management.

APIs are everywhere, and with their rapid expansion, a whole new level of security concerns is raised. However, a set of security protocols and mechanisms do exist to mitigate these issues. With a combination of these protocols and an integrated structure, WSO2 platform's comprehensive set of security features is ideal for solving the modern challenges of API security

Attacks against information systems is on the rise making enterprise security a major concern. It's important to identify and address security needs such as confidentiality, integrity, availability and auditability of information. Enterprise security patterns facilitate balanced and informed decisions about security needs, as well as provide a rationale for the evolution of security needs over time. Anti-patterns, which are fostered by misapplications of concepts and misunderstandings of security concerns, should be avoided. Enterprise security patterns and anti-patterns solve these security concerns by addressing recurrent problems and challenges. These security patterns facilitate balanced and informed decisions about security needs, avoid the misapplication of concepts and misunderstanding of security concerns and provide a rationale for evolution of security needs over time.

All enterprises today need to securely share critical business functionality with the outside world. However organizations often struggle to identify and isolate the tradeoffs among the many security options available today. With WSO2 Identity Server's extension model, organizations have the ability to tailor-make their deployment based on their requirements while enforcing multi-factor authentication.

One of the most popular systems that helps organizations to establish information security is the ISMS defined by ISO 27000 standards. The benefits of implementing an ISMS in this case seem obvious. ISO/IEC 27000 certification enforces most stringent controls to ensure ample security measures are implemented to protect the WSO2's information assets. ISMS provides a framework for

- Establishing information security policies.
- Multiple heterogeneous systems security.
- Hardware and software based management.
- API security
- Multi-factor authentication security.

- Information systems security.
- Management of information assets.
- Human resources security.
- Operational security.
- Acquisition and maintenance of information systems.
- Security in business continuity and disaster recovery.

The benefits of implementing an ISMS

The ISO 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).

- Security risks are appropriately prioritized and cost effectively managed
- It increases confidence in Organization as it shows company care for their customer business, and committed to protect patient data they entrust to company.
- It demonstrates commitment to Information Security Management to third parties and stakeholders and will give them greater confidence to interact with company
- It provides a framework to ensure fulfilment of our commercial, contractual and legal responsibilities
- External Audit Requirements
- Control risk within the organisation
- Understand the weaknesses of the business
- Maintain existing business
- Competitive Advantage or Catch Up
- Implement consistent control and process
- Understand the key assets of the business
- Reduce third party scrutiny of your information security requirements
- Improved information security awareness
- Shows commitment to information security at all levels throughout your organization
- Provides reassurance to clients that their information is secure

- Supports compliance with relevant laws and regulations
- Best framework for complying with information security legal, regulatory and contractual requirements.
- Better organizational image because of the certificate issued by a certification body
- Proves that senior management are committed to the security of the organization, including customer's information
- Focused on reducing the risks for information that is valuable for the organization
- Provides a common goal
- Optimized operations within the organization because of clearly defined responsibilities and business processes
- Builds a culture of security.

ISMS Cost

- Find a suitable project 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 meeting involving key stakeholders.
- Identify and deal with project risk, preferably in advance.
- Liaise as necessary with various other interested parties, parallel projects, managers business partners etc.

Other ISMS implementation costs

- The cost of literature and training
- The cost of external assistance
- The cost of technology
- Cost of employee's time
- Compile an inventory of information
- Assess security risks to information assets, and prioritize them

- Determine how to treat information risks
- Redesign/ design the security architecture and security baseline
- Review/ update/ re-issue existing and prepare/issue new information security policies, standards, procedures, guidelines, contractual, etc.

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 archive certification at first application
- Staff/ management time expended during annual surveillance visits.