Enabling Compliance Requirements using ISMS Framework (ISO27001)

Shankar Subramaniyan
Manager (GRC)
Wipro Consulting Services
Shankar.subramaniyan@wipro.com

OWASP

10/21/09

The OWASP Foundation

http://www.owasp.org

Key Objectives

- Overview on ISO27001 and its controls
- Implementation Approach
- Certification Process
- Common Implementation Challenges
- Synergies between ISO27001 and compliance requirements

ISO27001 Overview

- Most widely recognized security standard in the world
- More flexible
- Comprehensive in its coverage of security controls
- Process centric Information Security Management System (ISMS) Framework
- Addresses Information security across Industries

ISO27000 series

- 27000, Information Security Management System – Fundamentals and vocabulary (13335-1)
- 27001, Information Security Management System – Requirements (2005)
- 27002, Code of Practice for Information Security Management (2007)
- * 27003, Information Security Management System –
- Implementation guidelines
- * 27004, Information Security Management Measurements (metrics)
- 27005, Information Security Risk Management (13335-2) (2008)
- ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems (2007)
- * ISO/IEC 27007 Guidelines for information security management systems auditing

Source: http://www.iso27001certificates.com/
* under development

ISO 27001:2005 Standard requirements

- It has 8 clauses that represent various phases of PDCA (Plan Do Check Act) approach
- Clause 1 - Scope
- Clause 2 – Reference to ISO 17799:2005
- Clause 3 – Terms & Definitions
- Clause 4 – ISMS
  - 4.1 General Requirement
  - 4.2 Establishing and Managing ISMS
  - 4.3 Documentation Requirements

Clause 5 – Management Responsibility

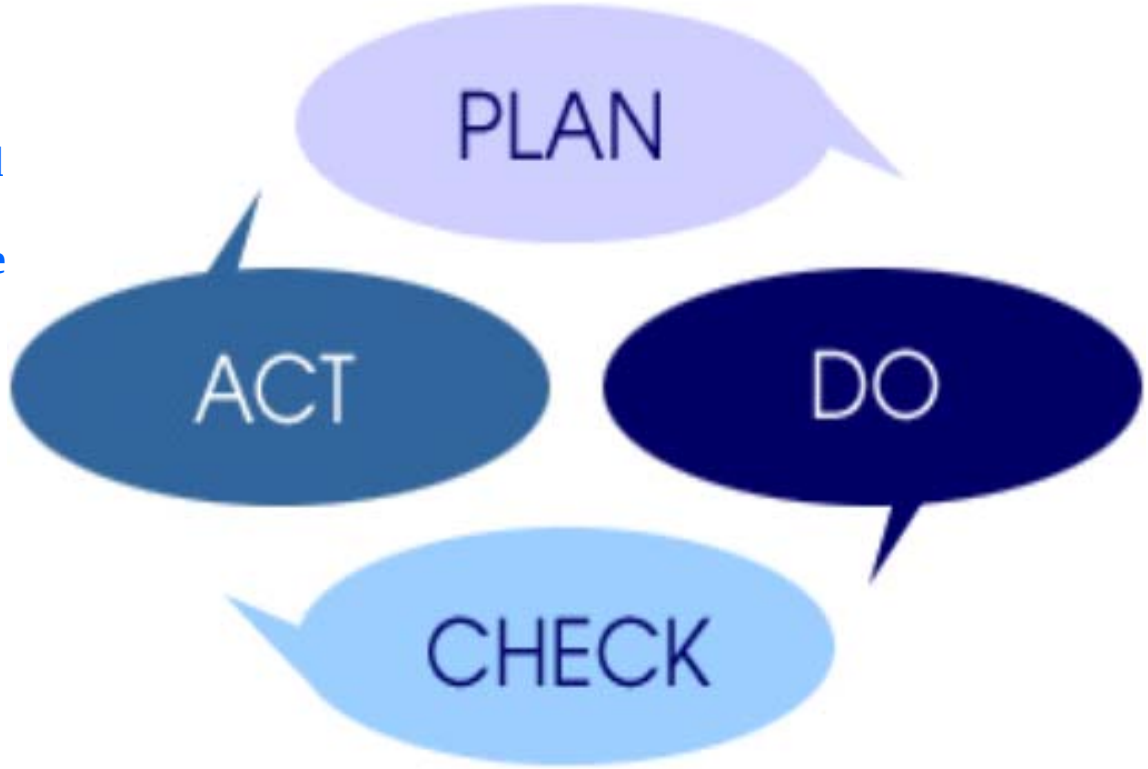
Clause 6 – Internal ISMS Audits

Clause 7 – Management Review of ISMS

Clause 8 – ISMS Improvement

ISMS PDCA Model

Define Security Policies and Procedures



Implement and manage Security controls/process

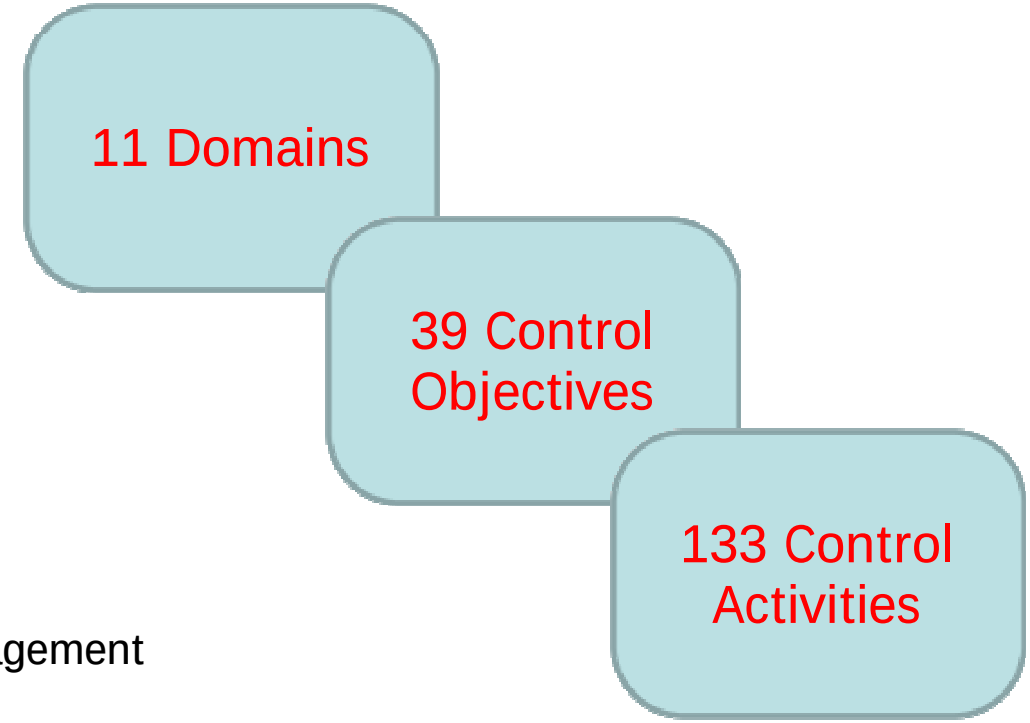
Review/ audit security management and controls

Implement identified improvements, corrective/preventive actions

Domains

Annexure A

- Security Policy
- Organization of Information Security
- Assets Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information system acquisition, development and maintenance
- Information Security Incident Management
- Business Continuity Planning
- Compliance



Implementation Approach

Phase I Baseline Information Security Assessment

- Identify the scope and coverage of Information Security
- Assess the Current Environment
- Prepare baseline information security assessment report

Phase II – Design of Information Security Policy & Procedures

- Establish Security Policy, Organization & Governance
- Asset Profiling
- Risk Assessment
- Risk treatment (Identification of ISO27001 Controls& Additional Controls)
- Formulate Information Security Policy & Procedures
- Prepare Statement of Accountability

Phase III – Implementation of Information Security Policy

- Implementation of Controls
- Security Awareness training

Phase IV- Pre Certification Audit

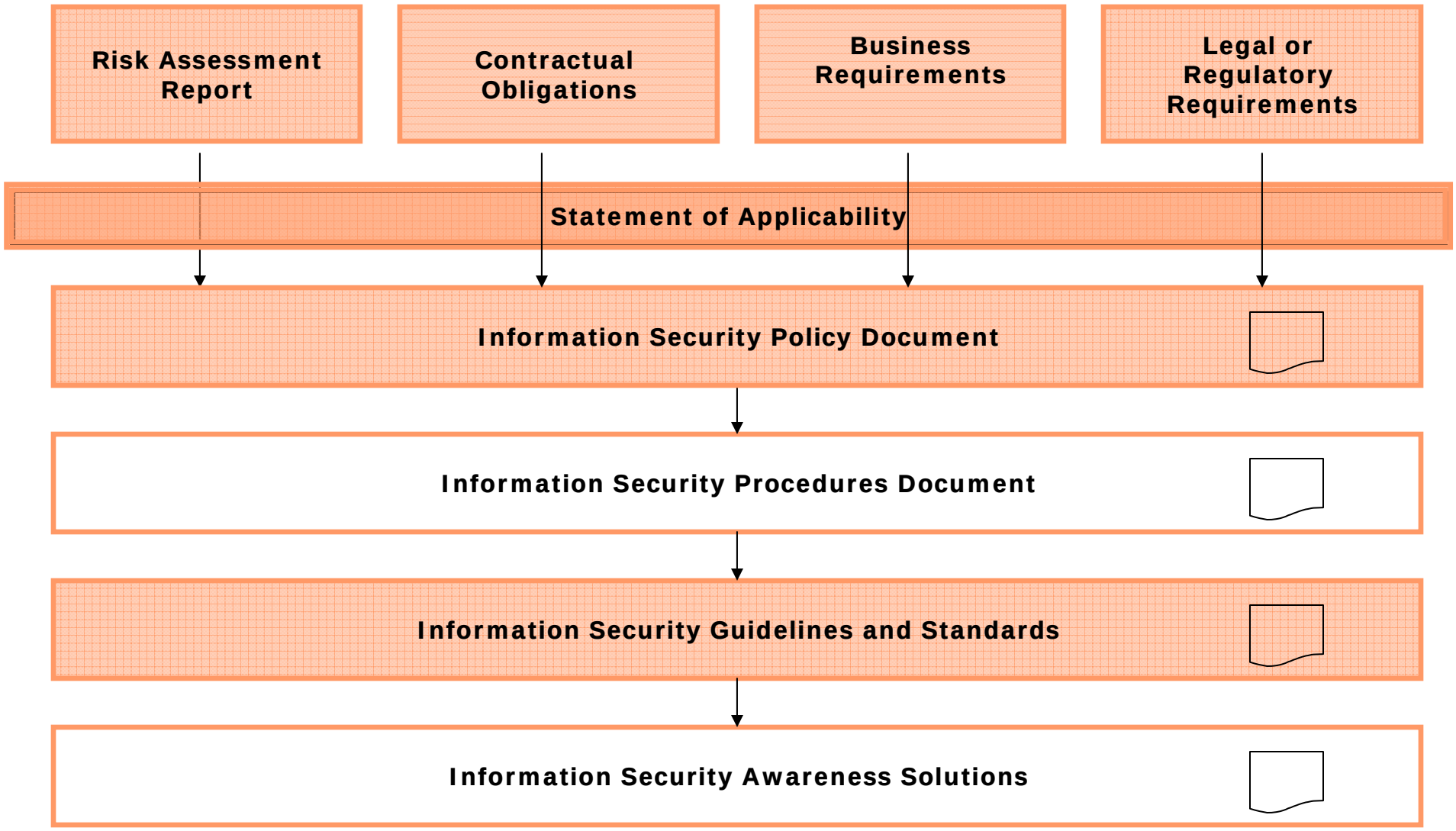
- Review by Internal team

Asset Profiling

- “Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected.”
- **Information Asset,** is any information, in any format, used to operate and manage business . It includes electronic information, Paper based assets, hardware assets (servers, desktops, other IT equipments) software assets, Equipments and People .
- Asset Profiling involves identifying and maintaining an inventory of all information assets and valuation and categorizing of information assets by evaluating level of risk of an information asset for each security objective i.e. Confidentiality, Integrity and Availability

Sl.no	Asset	Location	Owner	Custodian	User	Asset Number

Information Security Policy Management Documents

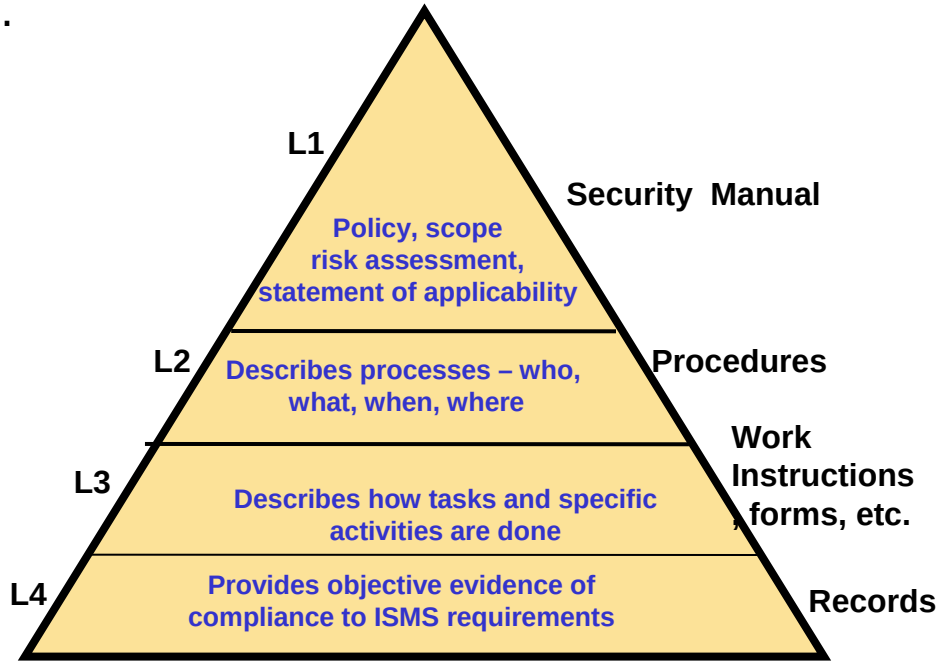


Certification Process

Stage 1 Audit (Desktop Review)

- Desktop Review (Stage 1 Audit) enables the certifying body to gain an understanding of the ISMS in the context of the organization's security policy and objectives and approach to risk management. It provides a focus for planning out the Stage 2 audit and is an opportunity to check the preparedness of the organization for implementation.

- It includes a documents review:
  - Security Policy and Procedures
  - Risk Assessment Report
  - Risk Treatment Plan
  - Statement of applicability



Certification Process … (Continued)

Stage 2 Audit (Implementation)

- Based on Stage 1 Audit Findings the Certification Body produces Stage 2 Audit Plan
- It takes place at the site of the organization
- The Stage 2 audit covers:
  - Confirmation that the organization is acting in accordance with its own policies, objectives and procedures
  - Confirmation that the ISMS conforms with all the requirements of the ISO 27001:2005 standard and is achieving the organization's policy objectives

Certification Process … (Continued)

Stage 3 - Surveillance and Recertification

- The certificate that is awarded will last for three years after which the ISMS needs to be re-certified.
- During this period there will be a surveillance audit (e.g. every 6-9 months)
- After 3 Years one needs to go for recertification.

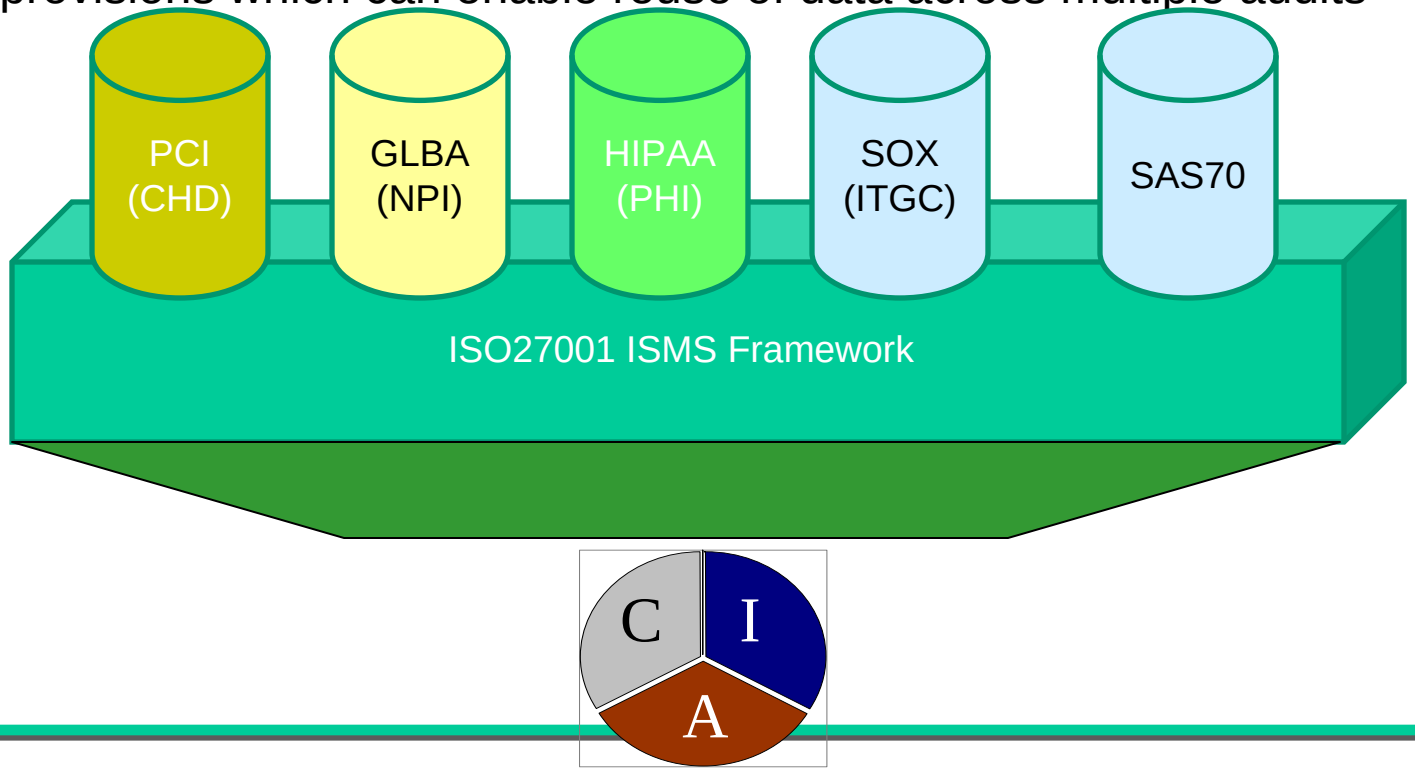
Common Implementation Challenges

- Flexible Security Framework
- Business Alignment
- Allocation of Security Responsibilities
- Process and People focus
- Resistance to Audit
- Communication and delivery of policies
- Consistent Corporate wide deployment

Synergy

• Eliminating duplicative efforts and documentation and yet fully complying to all security mandates in a cost effective manner and reduce the cost of compliance is the goal.

• There is a sufficient overlap in all these compliance requirements' security related provisions which can enable reuse of data across multiple audits



Synergy (Continued..)

- ISO27001 is process based framework. It doesn't provide specific technical controls. It provides guidance to an organization in implementing and managing an information security management system, whereas compliance or regulatory requirements focus on specific components of the implementation and status of 'applicable' controls.

- ISO27001 compliance may not lead you automatically achieve compliance to PCI etc. But if controls are properly selected and implemented and If a properly developed and implemented ISMS is in place with full documentation and working processes, it can result in a comprehensive security management approach and will give visibility to the fact that the controls are in place and are being managed and measured.

- ISMS framework would be the appropriate methodology to meet all the relevant regulatory and legal requirements and prepare any organization for future compliance and regulatory challenges

Benefits

- ISO27001 is a culture one has to build in the organization which would help to:
  - Increase security awareness within the organization
  - Identify critical assets via the Business Risk Assessment
  - Provide a framework for continuous improvement
  - Bring confidence internally as well as to external business partners
  - Enhance the knowledge and importance of security-related issues at the management level
  - Enable future security demands from clients, stockholders and partners to be met

Q&A

Thank You…