ISO/IEC 27001
Information Security Management System

Presented by Daminda Perera
26/07/2008

Agenda

- Overview of ISMS Family of Standards
- ISO/IEC 27001
- Implementation
- Certification
- Benefits of Compliance
- Summary
Overview of ISMS Family of Standards

• The ISMS standards specify a framework for organisations to manage information security aspects of their business, and if necessary to demonstrate to other parties (e.g. business partners, auditors, customers, suppliers) their ability to manage information security.

• Published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).

• It specifies a risk-based security management system that is designed to ensure that organisations select and operate adequate and proportionate (i.e. cost effective) security controls to protect information assets.

• It uses the ‘plan-do-check-act (improve)’ model.
Overview of ISMS Family of Standards (cont’d)

ISO/IEC 27000 - ISMS fundamentals and vocabulary
ISO/IEC 27001 -
- Establishing, implementing, operating, maintaining and improving an ISMS
- Documentation requirements
- Management responsibilities
- Internal audits and management reviews

ISO/IEC 27003 - ISMS implementation Guide
ISO/IEC 27004 – Measurement and metrics
ISO/IEC 27005 – Risk management
ISO/IEC 27006 – Requirements for the accreditation of bodies providing certification of ISMS
Overview of ISMS Family of Standards (cont’d)

- ISO 27000 Family
  - ISO 27001
  - ISO 27002
  - ISO 27003
  - ISO 27004
  - ISO 27005
  - ISO 27006

- New name of ISO 17799
- ISMS requirements (2005)
- Fundamentals and vocabulary
- Guidelines for the use of ISO 17799 in health sector
- ISMS implementation guidelines
- ISMS measurement
- Information security risk management
- Requirements for bodies providing audit and certification of an ISMS.
ISO/IEC 27001

• ISO/IEC 27001: ‘Information Security Management Systems - Requirements’ is the foundational standard; it is applicable to all types of organization and all sectors of the economy.

• The goal of ISO 27001 is to:
  - Provide the standard for Information Security Management Systems
    Consists of 11 control sections, 39 control objectives, and 133 controls
  - Provide the base for third-party recognition
    ISO 27001 Registrations/Certifications demonstrate conformance to the standard

• Specifies requirements for establishing, implementing and documenting information security management systems (ISMS).

• An internationally recognized structured methodology dedicated to information security

• A management process to evaluate, implement and maintain an Information Security Management System (ISMS)

• Prepared to provide a model for: establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)
ISO/IEC 27001 (Cont’d)

- A comprehensive set of controls comprised of best practices in information security applicable to all industry sectors emphasis on prevention
- A management system should balance physical, technical, procedural, and personnel security
- Emphasis that the information security is a management process, not a technological process
- Adoption of an ISMS should be a strategic decision.
- The design and implementation is influenced by the organization’s needs and objectives, security requirements, the processes employed and the size and structure of the organization
- Scale the system in accordance with your needs, which may well change (simple situation=simple ISMS solution; complex situation=complex ISMS solution)
Information Security

• “Information”
  • ‘An asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected.’
    – Source: ISO/IEC 17999:2005 Section 0.1

• “Asset”
  • “anything that has value to the organization”
    – Source: ISO/IEC 27001:2005, 3.1

• “Information Security”
  • “preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved”
    – Source: ISO/IEC 27001:2005
## Information Security (Cont’d)

<table>
<thead>
<tr>
<th><strong>Confidentiality</strong></th>
<th>Ensuring that information is accessible only to those authorized to have access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clause 3.3 of ISO/IEC 27001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Integrity</strong></th>
<th>Safeguarding the accuracy and completeness of information and process methods.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clause 3.8 of ISO/IEC 27001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Availability</strong></th>
<th>Ensuring that authorized users have access to information and associated assets when required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clause 3.2 of ISO/IEC 27001</td>
<td></td>
</tr>
</tbody>
</table>
What is an ISMS?

• Information Security Management System
• Strategic decision of an organization
  • Design and implementation
    – Needs and objectives
    – Security requirements
    – Processes employed
    – Size and structure of the organization
• Scaled with ‘needs’ – *simple situation requires a simple ISMS solution*
**PDCA**

- **Plan, Do, Check, Act** is to be applied to structure all ISMS processes.
- Figure 1 illustrates how an ISMS takes the information security requirements and expectations of the interested parties and, through the necessary actions and processes, produces information security outcomes that meet those requirements and expectations.

*Figure 1 — PDCA model applied to ISMS processes*
ISO 27001:2005 Structure

Five Mandatory requirements of the standard

- **Information Security Management System**
  - General requirements
  - Establishing and managing the ISMS (e.g. Risk Assessment)
  - Documentation Requirements
- **Management Responsibility**
  - Management Commitment
  - Resource Management (e.g. Training, Awareness)
- **Internal ISMS Audits**
- **Management Review of the ISMS**
  - Review Input (e.g. Audits, Measurement, Recommendations)
  - Review Output (e.g. Update Risk Treatment Plan, New Recourses)
- **ISMS Improvement**
  - Continual Improvement
  - Corrective Action
  - Preventive Action
ISO 27001:2005 Structure (Cont’d)

Overall the standard can be put in

a) Domain Areas -11 (Annex A :11 Domains of Information Management)
   A. 5  Security policy
   A. 6  Organization of information security
   A. 7  Asset management
   A. 8  Human resources security
   A. 9  Physical and environmental security
   A.10 Communications and operations management
   A.11 Access control
   A.12 Information systems acquisition, development and maintenance
   A.13 Information security incident management
   A.14 Business continuity management
   A.15 Compliance

b) Control Objectives – 39

c) Controls - 133
Implementation

1. Establish the ISMS
   - Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.

2. Implement and operate the ISMS
   - Implement and operate the security policy, controls, processes and procedures.

3. Monitor and review the ISMS
   - Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

4. Maintain and improve the ISMS
   - Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.
Implementation (Cont’d)

- Scope
  - Policy
- Risk Assessment (RA)
- Risk Treatment Plan (RTP)
- Statement of Applicability (SOA)
- Operate Controls
- Awareness Training
- Manage Resources
- Prompt Detection and Response to Incidents

The Deming Cycle

- Plan
  - ISMS Improvements
- Preventive Action
- Corrective Action
- Management Review
- Internal ISMS Audit

- Do
- Check

- Act
Implementation (Cont’d)

How to implement - 11 Domains of Information Management

A. 5 Security policy
A. 6 Organization of information security
A. 7 Asset management
A. 8 Human resources security
A. 9 Physical and environmental security
A.10 Communications and operations management
A.11 Access control
A.12 Information systems acquisition, development and maintenance
A.13 Information security incident management
A.14 Business continuity management
A.15 Compliance
Implementation (Cont’d)
Certification

- Implementation of ISMS
- Internal audit and review of ISMS
- Choose a registrar

- Pre-assessment (optional)
- Phase 1 Document review
- Phase 2 On-site audit

- Registration confirmed
- Continual assessment

Internal
External
- Continuing (every 6 months)
- Re-assessment (every 3 years)
International Take-up

ISMS Registrations by Continent

5 November 2006
Benefits

• Improved effectiveness of Information Security
• Market Differentiation
• Provides confidence to trading partners, stakeholders, and customers (certification demonstrates 'due diligence')
• The only standard with global acceptance
• Potential lower rates on insurance premiums
• Compliance with mandates and laws (e.g., Data Protection Act, Communications Protection Act)
• Reduced liability due to un-implemented or enforced policies and procedures
• Senior Management takes ownership of Information Security
• Standard covers IT as well as organization, personnel, and facilities
Benefits (Cont’d)

• Focused staff responsibilities
• Independent review of the Information Security Management System
• Better awareness of security
• Combined resources with other Management Systems (eg. QMS)
• Mechanism for measuring the success of the security controls
• Provides the means for information security corporate governance and legal compliance
• Focus of staff responsibilities and create security awareness
• Enforcement of policies and procedures
Summary

- Comprehensive standard for information security
- Management standard (Plan-Do-Check-Act)
- Allows controls to adapt to changing circumstances (policy getting in the way of the business? – change the policy)
- Comprehensive IT-platform focused AIL
- Increases awareness – better security – better business

ISO27001 can be
- Without genuine support from the top – a failure
- Without proper implementation – a burden
- With full support, proper implementation and ongoing commitment – a major benefit
References