ISO 27000
A Business Critical Framework For Information Security Management

George Spalding
Executive Vice President
Pink Elephant
Agenda

- Framework or Standard?
- What is ISO?
- What is Information Security?
- ISO 27000 Series Overview
  - ISO 27000
  - ISO 27001
  - ISO 27002
  - ISO 27003
  - ISO 27004
  - ISO 27005
  - ISO 27006
- ISO 27002 in more detail
Framework or Standard?

- ITIL (IT Infrastructure Library)
- COBIT (Control Objectives for Information and related Technologies)
- eTOM (Enhanced Telecom Operations Map)
- MOF (Microsoft Operations Framework)
- ISO (International Standards Organization)
  - ISO 27001
  - ISO 27002
- CMMI (Capability Maturity Model Integrated)
International Organization for Standardization

- **www.iso.org**
- ISO is a network of the national standards institutes of 156 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.
- ISO is a non-governmental organization: its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of various industry associations.
- Over 700 Joint Technical Committees (JTC) are currently active in the ISO. These JTC’s do the actual work in developing and revising/updating the ISO standards.
ISO Member Organizations…

- **Relevant ISO Members:**
  - US – ANSI (American National Standards Institute)
  - CA – SCC (Standards Council of Canada)
  - MY – DSM (Department of Standards Malaysia)
  - SG – SPRING SG (Standards, Productivity and Innovation Board - Singapore)
  - MX – DGN (Dirección General de Normas - Mexico)
  - UK – BSI (British Standards Institution)
  - NL – NEN (Nederlands Normalisatie-instituut - Netherlands)
  - ZA – SABS (South African Bureau of Standards)
  - AU – SA (Standards Australia)
  - NZ – SNZ (Standards New Zealand)
  - ES – AENOR (Asociación Española de Normalización y Certificación – Spain)
  - SA – SASO (Saudi Standards, Metrology and Quality Organization)
  - Etc…
ISO/IEC

- ISO/IEC 20000-1:2005 (IT Service Management)
- ISO/IEC 38500:2008 (IT Governance)

- Custodian:
  - ISO, the International Organization for Standardization
  - IEC, the International Electrotechnical Commission
  - Geneva, Switzerland

- Standards evolve and change just like everything else
- In the ISO, years are used instead of version numbers and revision and document control is stringent
- A published ISO version is in place for, at least, 3 years
What is Information Security?

- Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

- Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by mail or by using electronic means, shown on films, or spoken in conversation.
What is Information Security? (2)

- Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

- Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.
The ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title "Information technology — Security techniques"

- ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2005, Information security management systems — Requirements
- ISO/IEC 27003:2010, Information security management system implementation guidance
- ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing (proposed release date 10-15-2011)
ISO/IEC 27001:2005 Overview

- This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of an ISMS should be a strategic decision for an organization. The design and implementation of an organization’s ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

- This International Standard can be used in order to assess conformance (audit standard) by interested internal and external parties.
The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

- a) understanding an organization’s information security requirements and the need to establish policy and objectives for information security;
- b) implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;
- c) monitoring and reviewing the performance and effectiveness of the ISMS; and
- d) continual improvement based on objective measurement.
ISO/IEC 27001:2005 PDCA

- This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes.

- The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002) governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.
ISO/IEC 27001:2005 PDCA (2)

PDCA model applied to ISMS processes

Source: ISO/IEC 27001:2005
ISO/IEC 27002:2005 Overview

- This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

- The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.
ISO/IEC 27003:2010 Overview

- The purpose of this International Standard is to provide practical guidance in developing the implementation plan for an Information Security Management System (ISMS) within an organization in accordance with ISO/IEC 27001:2005. The actual implementation of an ISMS is generally executed as a project. The process described within this International Standard has been designed to provide support of the implementation of ISO/IEC 27001:2005 and document:
  - a) the preparation of beginning an ISMS implementation plan in an organization, defining the organizational structure for the project, and gaining management approval,
  - b) the critical activities for the ISMS project and,
  - c) examples to achieve the requirements in ISO/IEC 27001:2005
ISO/IEC 27003:2010 Overview (2)

- By using this International Standard the organization will be able to develop a process for information security management, giving stakeholders the assurance that risks to information assets are continuously maintained within acceptable information security bounds as defined by the organization.
- This International Standard does not cover the operational activities and other ISMS activities, but covers the concepts on how to design the activities which will result after the ISMS operations begin. The concept results in the final ISMS project implementation plan. The actual execution of the organizational specific part of an ISMS project is outside the scope of this International Standard.
- The implementation of the ISMS project should be carried out using standard project management methodologies.
ISO/IEC 27004:2009 Overview

- This International Standard gives recommendations concerning the following activities as a basis for an organization to fulfill measurement requirements specified in ISO/IEC 27001:
  - a) developing measures (i.e. base measures and indicators);
  - b) implementing and operating an Information Security Measurement Program;
  - c) collecting and analyzing data;
  - d) developing measurement results;
  - e) communicating measurement results to the stakeholders;
  - f) using measurement results as contributing factors to ISMS-related decisions;
  - g) using measurement results to identify needs for improving the implemented ISMS, including all facets; and
  - h) facilitating continual improvement of the Information Security Measurement Program.
This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS. This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.
ISO/IEC 27006:2007 Overview

- ISO/IEC 17021 is an International Standard which sets out criteria for bodies operating audit and certification of organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 with the objective of auditing and certifying Information Security Management Systems (ISMS) in accordance with ISO/IEC 27001:2005, some additional requirements and guidance to ISO/IEC 17021 are necessary. These are provided by this International Standard.

- Not applicable to practitioner organizations.
SO
NOW
WHAT?
History of ISO 27002

- ISO 27002 is a direct descendant of ISO 17799 which in turn is a direct descendant of the British Standard Institute (BSI) Information Security Management standard BS 7799-1 first released in 1995. In the late 1990’s, in response to industry demands, several updates and releases of BS 7799 occurred in 1998, 1999, 2000, and finally again in 2002. By this time, information security had become a serious concern to computer users worldwide. While some organizations still utilized the BS 7799 standard (UK), demand grew for an internationally recognized information security standard under the auspices of an internationally recognized body, such as the ISO. This demand led to the “fast tracking” of BS 7799-1 by the BSI, culminating in its first release by ISO as ISO/IEC 17799:2000 in December 2000. To maintain consistency with the new nomenclature of the ISO27000 series of standards, ISO17799 was slightly updated and re-released as ISO 27002 in June of 2005.
ITILv2 1999
<table>
<thead>
<tr>
<th>ISO 27001</th>
<th>ISO 27002</th>
</tr>
</thead>
<tbody>
<tr>
<td>An auditable standard based on auditable <em>requirements</em></td>
<td>An implementation guide based on best practice <em>suggestions</em></td>
</tr>
<tr>
<td>A list of management controls that an organization <em>shall</em> address</td>
<td>A list of operational controls an organization <em>should</em> consider</td>
</tr>
<tr>
<td>Used as a means to <em>audit</em> and <em>certify</em> an organization’s Information Security Management System (ISMS)</td>
<td>Used as a means to <em>assess</em> the comprehensiveness of an organization’s Information Security Program</td>
</tr>
</tbody>
</table>
ISO 27002 Control Areas (Clauses)

- ISO 27002 has identified 11 control areas, 39 control objectives, and 133 specific controls.
  - a) Security Policy (1);
  - b) Organizing Information Security (2);
  - c) Asset Management (2);
  - d) Human Resources Security (3);
  - e) Physical and Environmental Security (2);
  - f) Communications and Operations Management (10);
  - g) Access Control (7);
  - h) Information Systems Acquisition, Development and Maintenance (6);
  - i) Information Security Incident Management (2);
  - j) Business Continuity Management (1);
  - k) Compliance (3).
Security Policy (27002)

- The security policy control area addresses management direction and support for information security in accordance with business requirements and relevant laws and regulations, including:

  - **Information security policy document** – an approved and published document demonstrating management commitment and outlining the organizations approach to information security. Information security policy statements may be part of an overall organizational corporate policy document.

  - **Review of the information security policy** – ongoing relevance and commitment to information security is established by assigning an ownership and review schedule for the information security policy document.
Organizing Information Security (27002)

- The organization of information security control addresses the ability to manage information security within an organization, including:
  - Management commitment to information security – unlike the information security policy in the previous control area, the focus here is on leadership through clear direction, authorization, and accountability.
  - Information security coordination – this is some form of “multi-disciplinary forum” within which to disseminate information security concerns throughout the organization. This does not require a distinct working group, but may be an agenda item in an existing organizational forum.
  - Allocation of information security responsibilities – individual information security responsibilities that are unambiguously allocated and detailed such as within job descriptions.
Organizing Information Security (27002) (2)

- **Authorization processes for information processing facilities** – security considerations are evaluated and approvals obtained for new and modified information processing systems.
- **Confidentiality agreements** – to maintain information security in situations where information is beyond the organization’s control.
- **Contact with authorities** – relationships with external incident management partners and local law-enforcement personnel.
- **Contact with special interest groups** – relationships with external information sources.
- **Independent review of information security** – relationships with external assessors and auditors.
- **Identification of risks related to external parties** – external risk assessment and governance.
- **Addressing security when dealing with customers** – disclaimers.
- **Addressing security in third party agreements** – information security service level agreements.
Asset Management (27002)

- The Asset Management area addresses the ability of the security infrastructure to protect organizational assets, including:
  - **Accountability and inventory** – mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets.
  - **Classification** – mechanisms to classify assets based on business impact.
  - **Labeling** – labeling standards that clearly brand assets to their classification.
  - **Handling** – handling standards; including introduction, transfer, removal, and disposal of all assets; based upon asset classification.
Human Resources Security (27002)

- The Human Resources Security control area addresses an organization’s ability to mitigate risk inherent in human interactions, including:

  - **Personnel screening** – policies within local legal and cultural frameworks ascertain the qualification and suitability of all personnel with access to organizational assets. This framework may be based on job descriptions and/or asset classification.

  - **Security responsibilities** – personnel should be clearly informed of their information security responsibilities, including codes of conduct and non-disclosure agreements.

  - **Terms and conditions of employment** – personnel should be clearly informed of their information security responsibilities as a condition of employment.

  - **Training** – a mandatory information security awareness training program is conducted for all employees.

  - **Recourse** – a formal process to deal with violation of information security policies.
Physical and Environmental Security control addresses risk inherent to organizational premises, including:

- **Location** – organizational premises should be analyzed for environmental hazards.

- **Physical security perimeter** – the premises security perimeter should be clearly defined and physically sound. A given premises may have multiple zones based on classification level or other organizational requirements.

- **Access control** – breaches in the physical security perimeter should have appropriate entry/exit controls commensurate with their classification level.

- **Equipment** – equipment should be sited within the premises to ensure physical and environmental integrity and availability.

- **Asset transfer** – mechanisms to track entry and exit of assets through the security perimeter.

- **General** – policies and standards, should exist to govern operational security within the workspace.
Communication and Operations Management control addresses an organization’s ability to ensure correct and secure operation of its assets, including:

- **Operational procedures** – comprehensive set of procedures, in support of organizational standards and policies.
- **Change control** – process to manage change and configuration control, including change management of the Information Security Management System.
- **Incident management** – mechanism to ensure timely and effective response to any security incidents.
- **Segregation of duties** – segregation and rotation of duties minimize the potential for collusion and uncontrolled exposure.
- **Capacity planning** – mechanism to monitor and project organizational capacity to ensure uninterrupted availability.
Communication & Operations (27002)

- **System acceptance** – methodology to evaluate system changes to ensure continued confidentiality, integrity, and availability.

- **Malicious code** - controls to mitigate risk from introduction of malicious code of any kind.

- **Housekeeping** – policies, standards, guidelines, and procedures to address routine housekeeping activities such as backup schedules and logging.

- **Network management** - controls to govern the secure operation of the networking infrastructure.

- **Media handling** – controls to govern secure handling and disposal of information storage media and documentation.

- **Information exchange** – controls to govern information exchange including end user agreements, user agreements, and information transport mechanisms.
Access Control (27002)

- Access Control addresses an organization’s ability to control access to assets based on business and security requirements, including:
  - **Business requirements** – policy controlling access to organizational assets based on business requirements and “need to know.”
  - **User management** – mechanisms to register and deregister users, control and review access and privileges, and manage passwords
  - **User responsibilities** – informing users of their access control responsibilities, including password stewardship and unattended equipment.
Access Control (27002) (2)

- **Network access control** – policy on usage of network services, including mechanisms (when appropriate) to authenticate nodes, authenticate external users, define routing, control network device security, maintain network segmentation, control network connections, and maintain the security of network services.

- **Host access control** – mechanisms to automatically identify terminals, securely log-on, authenticate users, manage passwords, secure system utilities, furnish user duress capability, enable terminal, user, or connection timeouts.

- **Application access control** – limits access to applications based on user or application authorization levels.

- **Access monitoring** – mechanisms to monitor system access and system use to detect unauthorized activities.

- **Mobile computing** – policies and standards to address asset protection, secure access, and user responsibilities.
System Development (27002)

- Information System Development and Maintenance control addresses an organization’s ability to ensure that appropriate information system security controls are both incorporated and maintained, including:
  - **System security requirements** – incorporates information security considerations in the specifications of any system development or procurement.
  - **Application security requirements** – incorporates information security considerations in the specification of any application development or procurement.
  - **Cryptography** – policies, standards, and procedures governing the usage and maintenance of cryptographic controls.
  - **System Integrity** – mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.
  - **Development security** – integrates change control and technical reviews into development process.
Information Security Incident Management

- To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

- Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.
Business Continuity Management (27002)

- Business Continuity Management control addresses an organization’s ability to counteract interruptions to normal operations, including:
  - **Business continuity planning** – business continuity strategy based on a business impact analysis.
  - **Business continuity testing** – testing and documentation of business continuity strategy.
  - **Business continuity maintenance** – identifies ownership of business continuity strategy as well as ongoing re-assessment and maintenance.
Compliance (27002)

- Compliance control addresses an organization’s ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including:

- **Legal requirements** – awareness of:
  - Relevant legislation
  - Intellectual property rights
  - Safeguarding of organizational records
  - Data privacy
  - Prevention of misuse
  - Regulation of cryptography
  - Collection of evidence

- **Technical requirements** – mechanism to verify execution of security policies and implementations.

- **System audits** – auditing controls to maximize effectiveness, minimize disruption, and protect audit tools.
Conclusion

- ISO 27002 is the implementer’s guide, suggesting what *should* be done based upon internationally recognized best practice. It serves as an excellent basis to build an enterprise Information Security Program.

- An Information Security Program oversees the organization’s information protection initiative, and may have responsibility over multiple operational areas.

- ISO 27001 is the auditor’s guide specifying what *shall* be done based upon Quality Management principles inherent to a management system.
Thank You!

g.spalding@pinkelephant.com
www.pinkelephant.com