Information Security Policy and Standard

Sanjiv Agarwala, CISA,CISM,CISSP,ISO27001
Director and Principal Consultant and Trainer
Oxygen Consulting Services Pvt Ltd

Agenda

- Security principles
- Types of Information security policies- Administrative and Technical
- A structure and framework of compressive security policy, policy infrastructure, policy design life cycle and design processes, PDCA model,
- Security policy standards and practices - BS7799, ISO/IEC 17799, ISO 27001. Auditing tools such as ISO 27001 ISMS TOOL KIT, NGS AUDITOR, Windows password auditor, ISO IES 27002 2005 IS AUDIT TOOL

Fundamental Principles of Security

- Confidentiality
- Integrity
- Availability

Thirteen security design principles

- 1) Secure the weakest link - security should e consistent with no weak link to provide easy access
- 2) Defend in depth - multi-layered security
- 3) Fail securely -do not reveal weaknesses while failing
- 4) Grant least privilege - avoid unintentional, unwanted, or improper uses of privilege by doling it out in a miserly fashion

Thirteen security design principles

- 5) Separate privileges - no de-facto privileges, Keep privilege sets apart
- 6) Economize mechanism - Complexity increases the risk of problems. Avoid complexity and avoid problems."
- 7) Do not share mechanisms - If you have multiple users using the same components, have your system create different instances for each user

Thirteen security design principles

- 8) Be reluctant to trust - Assume that the environment where your system operates is hostile
- 9) Assume your secrets are not safe- Assume that an attacker will find out about as much about your system as a power user, maybe more
- 10) Mediate completely - Every access and every object should be checked, every time.

Thirteen security design principles

- 11) Make security usable - Make sure that your security system is as secure as it needs to be, but no more
- 12) Promote privacy - When you design a system, think about the privacy of its ultimate users.
- 13) Use your resources - If you’re not sure whether your system design is secure, ask for help

PDCA

- PLAN Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

- DO Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

- CHECK Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences.

- ACT Request corrective actions on significant differences between actual and planned results. Determine where to apply changes that will include improvement of the process or product.

Policy

- Policy: A broad statement of principle that presents management’s position for a defined control area.
- Policies are intended to be long-term and guide the development of more specific rules to address specific situations.
- Policies are interpreted and supported by standards, baselines, procedures, and guidelines.
- Policies should be relatively few in number, should be approved and supported by executive management, and should provide overall direction to the organization.

Procedure

- Procedures define specifically how policies, standards, baselines, and guidelines will be implemented in a given situation.
- Procedures are either technology or process dependent and refer to specific platforms, applications, or processes. They are used to outline steps that must be taken by an organizational element to implement security related to these discrete systems and processes.

Standard

- A rule that specifies a particular course of action or response to a given situation.
- Standards are mandatory directives to carry out management's policies and are used to measure compliance with policies.
- Standards serve as specifications for the implementation of policies.
- Standards are designed to promote implementation of high-level organization policy rather than to create new policy in themselves.

Guideline

A guideline is a general statement used to recommend or suggest an approach to implementation of policies, standards, and baselines.

Guidelines are essentially recommendations to consider when implementing security. While they are not mandatory in nature, they are to be followed unless there is a documented and approved reason not to.

Types of Security Policy

- Administrative - policies governing overall control, management other than technical controls like personnel security, incident management policies, security awareness, change management, risk management etc
- Technical policies - Policies governing hardware, software and communication devices and systems and other technical controls

Life Cycle of Security Policy

- During its development a policy is created, reviewed, and approved.
- This is followed by an implementation phase where the policy is communicated and either complied with or given an exception.
- Then, during the maintenance phase, the policy must be kept up-to-date, awareness of it must be maintained, and compliance with it must be monitored and enforced.
- Finally, during the disposal phase, the policy is retired when it is no longer required.

Plan, Research, Document, and Coordinate the Policy

- The first step in the policy development phase is the planning for, research, and writing of the policy.
- The policy creation function includes identifying why there is a need for the policy; determining the scope and applicability of the policy; roles and responsibilities inherent in implementing the policy; and assessing the feasibility of implementing it.

Plan, Research, Document, and Coordinate the Policy

Note : This also includes conducting research to determine organizational requirements for developing policies, (i.e., approval authorities, coordination requirements, and style or formatting standards), and researching industry-standard best practices for their applicability to the current organizational policy need.

Review: Get an Independent Assessment of the Policy

- Once the policy document has been created and initial coordination has been effected, it must be submitted to an independent individual or group for assessment prior to its final approval.
- There are several benefits of an independent review: a more viable policy; broadened support for the policy; and increased policy credibility
- As part of this activity, the creator of the policy is expected to address comments and recommendations for changes to the policy, and to make all necessary adjustments and revisions resulting in a final policy ready for management approval.

Approval: Obtain Management Approval of the Policy

- The intent of this activity, is to obtain management support for the policy and endorsement of the policy by a company official in a position of authority through their signature.
- Approval permits and hopefully launches the implementation of the policy.
- Also, should the approving authority hesitate to grant full approval of the policy, the policy creator must address issues regarding interim or temporary approval as part of this activity.

Communication: Disseminate the Policy

- The policy must be initially disseminated to organization employees or others who are affected by the policy (e.g., contractors, partners, customers, etc.).
- This also entails determining the extent and the method of the initial distribution of the policy, addressing issues of geography, language, and culture; prevention of unauthorized disclosure;

Compliance: Implement the Policy

- Compliance encompasses activities related to the initial execution of the policy to comply with its requirements.
- This includes working with organizational personnel and staff to interpret how the policy can best be implemented in various situations and organizational elements; ensuring that the policy is understood by those required to implement, monitor, and enforce the policy; monitoring, tracking, and reporting on the pace, extent, and effectiveness of implementation activities; and measuring the policy's immediate impact on operations.

Exceptions: Manage Situations where Implementation Is Not Possible

- Because of timing, personnel shortages, and other operational requirements, not every policy can be complied with as originally intended.
- Therefore, exceptions to the policy will probably need to be granted to organizational elements that cannot fully meet the requirements of the policy.
- There must be a process in place to ensure that requests for exception are recorded, tracked, evaluated, submitted for approval/disapproval to the appropriate authority, documented, and monitored throughout the approved period of noncompliance.

Awareness: Assure Continued Policy Awareness

- The awareness function of the maintenance phase comprises continuing efforts to ensure that personnel are aware of the policy in order to facilitate their compliance with its requirements.
- This is done by defining the awareness needs of various audience groups within the organization; determining the most effective awareness methods for each audience group and developing and disseminating awareness materials regarding the need for adherence to the policy.

Monitoring: Track and Report Policy Compliance

- The monitoring function is performed to track and report on the effectiveness of efforts to comply with the policy (eg. IS audits, observations etc)
- This function includes continuing activities to monitor compliance or noncompliance with the policy through both formal and informal methods, and the reporting of these deficiencies to appropriate management authorities for action.

Enforcement: Deal with Policy Violations

- The enforcement function comprises management’s response to acts or omissions that result in violations of the policy with the purpose of preventing or deterring their recurrence.
- This means that once a violation is identified, appropriate corrective action must be determined and applied
-

Maintenance: Ensure the Policy Is Current

- Maintenance addresses the process of ensuring the currency and integrity of the policy.
- This function also ensures the continued availability of the policy to all parties affected by it, as well as maintaining the integrity of the policy through effective version control.
- When changes to the policy are required, several previously performed functions need to be revisited—review, approval, communication, and compliance in particular.

Retirement: Dispense with the Policy when No Longer Needed

- After the policy has served its useful purpose (e.g., the company no longer uses the technology for which it applies, or it has been superseded by another policy), then it must be retired.
- The retirement function makes up the disposal phase of the life cycle, and is the final function in the policy development life cycle.
- This function entails removing a superfluous policy from the inventory of active policies to avoid confusion, archiving it for future reference, and documenting information about the decision to retire the policy (i.e., justification, authority, date, etc.).

Policy Life-Cycle Model

- To ensure that all functions in the policy life cycle are appropriately performed and that responsibilities for their execution are adequately assigned for each function, organizations should establish a framework that facilitates ready understanding, promotes consistent application, establishes a hierarchical structure of mutually supporting policy levels, and effectively accommodates frequent technological and organizational change.

Security policy standards and practices – BS7799

- BS 7799 was a standard originally published by BSI Group (BSI)[1] in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and consisted of several parts.

- **The first part, containing the best practices for Information Security Management, was revised in 1998; after a lengthy discussion in the worldwide standards bodies, was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000. ISO/IEC 17799 was then revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007.**

BS7799 continued

- The second part to BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use.“
- BS 7799-2 focused on how to implement an information security management system (ISMS), referring to the information security management structure and controls identified in BS 7799-2, which later became ISO/IEC 27001.
- The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA) (Deming quality assurance model), aligning it with quality standards such as ISO 9000.
- BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.

ISO27001

- ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC).
- Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. As of July 2013, a new version is in draft: ISO/IEC 27001:2013. ISO 27001:2013 has been available in its release form since 25 September 2013.
- ISO/IEC 27001:2005 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard (more below).

ISO27001:2005 – 11 domains

- **Security policy - management direction**
- **Organization of information security - governance of information security**
- **Asset management - inventory and classification of information assets**
- **Human resources security - security aspects for employees joining, moving and leaving an organization**
- **Physical and environmental security - protection of the computer facilities**
- **Communications and operations management - management of technical security controls in systems and networks**
- **Access control - restriction of access rights to networks, systems, applications, functions and data**
- **Information systems acquisition, development and maintenance - building security into applications**
- **Information security incident management - anticipating and responding appropriately to information security breaches**
- **Business continuity management - protecting, maintaining and recovering business-critical processes and systems**
- **Compliance - ensuring conformance with information security policies, standards, laws and regulations**

ISO27001 and ISMS

- ISO/IEC 27001 requires that management:
- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Other standards and best practices, frameworks

- NIST
- COBIT 5 for Information Security
- Information Security Forum (ISF)
- PCI DSS (on payment cards)
- Industry specific standards (Gov, healthcare, Banking etc)

Auditing Tools

- ISO 27001 ISMS TOOL KIT
- NGS AUDITOR
- Windows password auditor
- ISO IES 27002 2005 IS AUDIT TOOL

References

- Information systems control and Audit by Ron Weber, Pearson Pub.
- IS control journals from ISACA
- Information security Management Hand book- 5th Edition-HAROLD F. TIPTON
- Wikipedia
- www.searchsecurity.techtarget.com
- www.secure-byte.com
- www.security-internal-audit.com
- www.ngssecure.com/services

Information Security Policy and Standard

Sanjiv Agarwala, CISA,CISM,CISSP,ISO27001
Director and Principal Consultant and Trainer
Oxygen Consulting Services Pvt Ltd