Planning for and Implementing ISO 27001

Charu Pelnekar, CISA, CISM, ACA, AICWA, BCOM, CISSP, CPA, MCSE, QSA, is a director with Professional Consultant, a consulting firm. He has skills in business and technology consulting, as well as experience with audits and risk management, process reengineering, and business management. Since 1993, he has worked in an advisory role with national and international corporations across various industries. He served as vice president, in 2007–2008, and as membership director, in 2006–2007, of the ISACA Austin (Texas, USA) Chapter. He can be contacted at *charpeln@hotmail.com.*

ISO/IEC 27001:2005 *Information Technology—Security techniques—Information security management systems—Requirements* is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).[1, 2] The potential benefits[3, 4] of implementing ISO 27001 and obtaining certification are numerous. Implementing ISO 27001 can enable enterprises to benchmark against competitors and to provide relevant information about IT security to vendors and customers, and it can enable management to demonstrate due diligence. It can foster efficient security cost management, compliance with laws and regulations, and a comfortable level of interoperability due to a common set of guidelines followed by the partner organization. It can improve IT information security system quality assurance (QA) and increase security awareness among employees, customers, vendors, etc., and it can increase IT and business alignment. It provides a process framework for IT security implementation and can also assist in determining the status of information security and the degree of compliance with security policies, directives and standards.

The goal of this article is to provide guidance on the planning and decision-making processes associated with ISO 27001 implementation, including associated costs, project length and implementation steps.

COSTS OF IMPLEMENTATION

Before implementing ISO 27001, one needs to consider the costs and project length, which are further influenced by the detailed understanding of the implementation phases. Any cost is painful in tough economic times. In today's cloud computing environment, organizations that want to reduce costs without compromising information security are looking at ISO 27001 certification as a promising means to provide knowledge about their IT security.

Implementation costs are driven by the perception of risk and how much risk an organization is prepared to accept. Four costs need to be considered when implementing this type of project:

1. **Internal resources**—The system covers a wide range of business functions including management, human resources (HR), IT, facilities and security. These resources will be required during the implementation of the ISMS.
2. **External resources**—Experienced consultants will save a huge amount of time and cost. They will also prove useful during internal audits and ensure a smooth transition toward certification.
3. **Certification**—Only a few approved certification agencies currently assess companies against ISO 27001, but fees are not much more than against other standards.
4. **Implementation**—These costs depend largely on the health of IT within the organization. If, as a result of a risk assessment or audit, a gap appears, then implementation costs are bound to go up based on the solution implemented.[5]

On average, implementation of a system such as this can take four to nine months and depends largely on the standard of conduct and quality and management support (tone at the top[6]), the size and nature of the organization, the health/maturity of IT within the organization, and existing documentation.

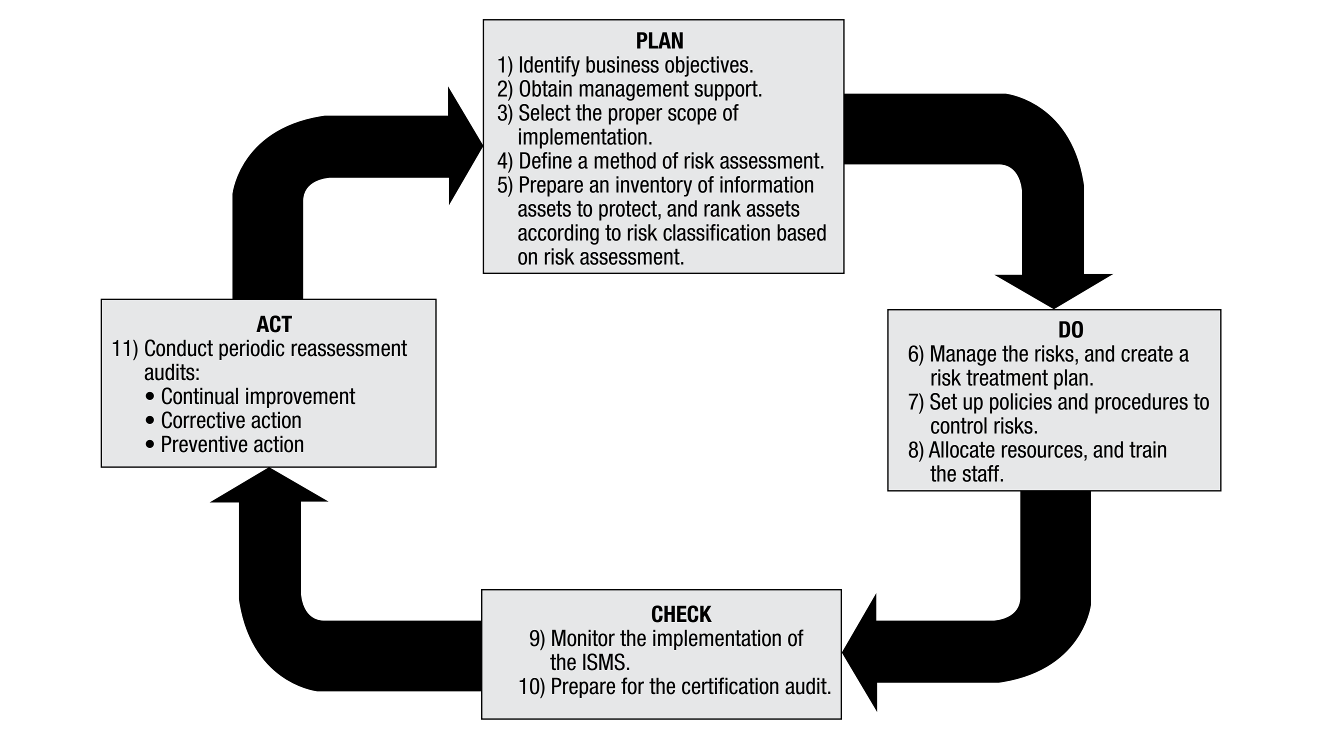
ISO 27001 requires a company to establish, implement and maintain a continuous improvement approach to manage its ISMS. As with any other ISO compliance, ISO 27001 follows the plan-do-check-act (PDCA) cycle, as shown in **figure 1**.

The cost factors mentioned earlier are directly impacted by the inventory of IT initiatives within the organization. Organizations with COBIT framework, Statement on Auditing Standards (SAS). No. 70 Type I and Type II, Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), or US Sarbanes-Oxley Act capabilities in place provide a ready inventory of set policies

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Figure 1—PDCA Cycle and Respective Implementation Phases



PLAN

1) Identify business objectives.
2) Obtain management support.
3) Select the proper scope of implementation.
4) Define a method of risk assessment.
5) Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment.

DO

6) Manage the risks, and create a risk treatment plan.
7) Set up policies and procedures to control risks.
8) Allocate resources, and train the staff.

CHECK

9) Monitor the implementation of the ISMS.
10) Prepare for the certification audit.

ACT

11) Conduct periodic reassessment audits:
    - Continual improvement
    - Corrective action
    - Preventive action

Figure 2—Time and Cost Savings on Respective PDCA Phases Associated With the IT Initiative

IT Initiative	Ready Information Inventory	Time and Cost Savings on the Following PDCA Phases
COBIT	Policies, procedures, risk assessment, control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 5—Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment. Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks. Phase 8—Allocate resources, and train the staff.
SAS 70 Type I and Type II	Policies, procedures, risk control objectives and controls	Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks.
NIST	Risk assessment, detailed control objectives and controls	Phase 2—Obtain management support. Phase 3—Select the proper scope of implementation. Phase 4—Define a method of risk assessment. Phase 6—Manage the risks, and create a risk treatment plan.
PCI DSS	Detailed control within the PCI DSS framework	Phase 6—Manage the risks, and create a risk treatment plan.

and procedures, risk assessments, control objectives, and operational controls that can often significantly reduce the time and expense needed to complete the project. Refer to **figure 2** to understand the time and cost savings on respective PDCA phases associated with different IT efforts.

In addition to the previously mentioned cost savings, the organization that wants to have a step-by-step approach to ISO compliance can adopt a corporate scheme, which envisages that the scope of compliance can be restricted to a specific division, business unit, and type of service or physical location. The adoption of a corporate scheme will save time and allow the organization to realize the benefit of ISO 27001 certification. In addition, once successful compliance has been achieved for a limited, but relevant, scope, the corporate scheme can be expanded to other divisions or locations.

ISMS—PLANNING FOR ISO

ISO/IEC 27001 and its supporting document, ISO/IEC 27002 (ISO/IEC 17799), detail 133 security measures, which are organized into 11 sections and 39 control objectives. These sections specify the best practices for:

- Business continuity planning
- System access control
- System acquisition, development and maintenance
- Physical and environmental security
- Compliance
- Information security incident management
- Personnel security
- Security organization
- Communication and operations management
- Asset classification and control
- Security policies

The ISMS may be certified as compliant with ISO/IEC 27001 by a number of accredited registrars worldwide. The ISO/IEC 27001 certification, like other ISO management system certifications, usually involves a three-stage audit process:

- **Stage 1**—Informal review of the ISMS that includes checking the existence and completeness of key documents such as the:
  - Organization's security policy
  - Risk treatment plan (RTP)
  - Statement of applicability (SOA)
- **Stage 2**—Independent tests of the ISMS against the requirements specified in ISO/IEC 27001. Certification audits are usually conducted by ISO/IEC 27001 lead auditors.
- **Stage 3**—Follow-up reviews or periodic audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic reassessment audits to confirm that the ISMS continues to operate as specified and intended.

Independent assessment necessarily brings some rigor and formality to the implementation process, and it must be approved by management. ISO/IEC 27001 certification should help assure most business partners of the organization's status regarding information security without the business partners having to conduct their own security reviews.

Planning

As in all compliance and certification initiatives, consideration of the organization's size, the nature of its business, the maturity of the process in implementing ISO 27001 and commitment of senior management are essential. The most important departments and activities that will be vital to the success of the project include:

- **Internal audit**—During the initial planning phase, the input from internal audit will be useful in developing an implementation strategy, and early involvement of internal auditors will be useful during the later stages of certification that require review by management.
- **IT**—The IT department will have to dedicate resources and time to the activities associated with the ISO 27001 initiatives. An inventory of existing IT compliance initiatives, procedures and policies, and the maturity of existing IT processes and controls will be useful to gain an understanding of how the existing processes align with ISO 27001 requirements.

Although implementation of policies and procedures is largely perceived as an IT activity, other departments play an important role in the implementation. For example, facilities management is largely responsible for physical security and access controls.

Decision Making

The decision of when and how to implement the standard may be influenced by a number of factors, including:

- Business objectives and priorities
- Existing IT maturity levels
- User acceptability and awareness
- Internal audit capability
- Contractual obligations
- Customer requirements
- The enterprise's ability to adapt to change
- Adherence to internal processes
- Existing compliance efforts and legal requirements
- Existing training programs

IMPLEMENTATION PHASES

Various IT initiatives that can save time and cost on implementation phases are illustrated in **figure 2**. As explained earlier, an organization also needs to have the detailed understanding of PDCA implementation phases to manage the costs of the project. The cycle of PDCA is consistent with all auditable international standards: ISO 18001, 9001 and 14001. ISO/IEC 27001:2005 dictates the following PDCA steps for an organization to follow:

- Define an ISMS policy.
- Define the scope of the ISMS.
- Perform a security risk assessment.
- Manage the identified risk.
- Select controls to be implemented and applied.
- Prepare an SOA.

These suggested PDCA steps are further simplified and mapped (**figures 1, 3** and **4**) to the implementation phases developed for easy understanding and implementation—with the end objective of time and cost savings in mind. The following steps take into account the IT maturity within the organization and the review/registration process (see **figure 4** for the details of review and registration steps).

Phase 1—Identify Business Objectives

Stakeholders must buy in; identifying and prioritizing objectives is the step that will gain management support. Primary objectives can be derived from the company's mission, strategic plan and IT goals. The objectives can be:

- Increased marketing potential
- Assurance to the business partners of the organization's status with respect to information security
- Assurance to customers and partners about the organization's commitment to information security, privacy and data protection
- Increased revenue and profitability by providing the highest level of security for customers' sensitive data
- Identification of information assets and effective risk assessments
- Preservation of the organization's reputation and standing among industry leaders
- Compliance with industry regulations

Figure 3—Mapping ISO/IEC 27001 Suggested Steps to Implementation Phases

ISO/IEC 27001:2005 Suggested Steps	Implementation Phases
Define an ISMS policy.	Phase 1—Identify business objectives. Phase 2—Obtain management support.
Define the scope of the ISMS.	Phase 3—Select the proper scope of implementation.
Perform a security risk assessment.	Phase 4—Define a method of risk assessment.
Manage the identified risk.	Phase 5—Prepare an inventory of information assets to protect, and rank assets according to risk classification based on risk assessment.
Select controls to be implemented and applied.	Phase 6—Manage the risks, and create a risk treatment plan. Phase 7—Set up policies and procedures to control risks. Phase 8—Allocate resources, and train the staff.
Prepare an SOA.	

Figure 4—Mapping Implementation Phases to Review and Registration Steps

Review and Registration Steps	Implementation Phases
Management review and internal audit	Phase 9—Monitor the implementation of the ISMS.
Registration and certification	Phase 10—Prepare for the certification audit.
ISMS improvement	Phase 11—Conduct periodic reassessment audits: • Continual improvement • Corrective action • Preventive action

Phase 2—Obtain Management Support

Management must make a commitment to the establishment, planning, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. Commitment must include activities such as ensuring that the proper resources are available to work on the ISMS and that all employees affected by the ISMS have the proper training, awareness and competency. The following activities/initiatives show management support:

- An information security policy
- Information security objectives and plans
- Roles and responsibilities for information security or a segregation of duties (SoD) matrix that shows the list of the roles related to information security
- An announcement or communication to the organization about the importance of adhering to the information security policy
- Sufficient resources to manage, develop, maintain and implement the ISMS
- Determination of the acceptable level of risk
- Management reviews of the ISMS at planned intervals
- Assurance that personnel affected by the ISMS are provided with training
- Appointment of competent people for the roles and responsibilities that they are assigned to fulfill

Phase 3—Select the Proper Scope of Implementation

ISO 27001 states that any scope of implementation may cover all or part of an organization. According to section B.2.3, Scope of the ISMS, only the processes, business units, and external vendors or contractors falling within the scope of implementation must be specified for certification to occur.

The standard also requires companies to list any scope exclusions and the reasons why they were excluded. Identifying the scope of implementation can save the organization time and money. The following points should be considered:

- The selected scope helps to achieve the identified business objectives.
- The organization's overall scale of operations is an integral parameter needed to determine the compliance process's complexity level.
- To find out the appropriate scale of operations, organizations need to consider the number of employees, business processes, work locations, and products or services offered.
- What areas, locations, assets and technologies of the organization will be controlled by the ISMS?
- Will suppliers be required to abide by the ISMS?
- Are there dependencies on other organizations? Should they be considered?
- Any regulatory or legislative standards that apply to the areas covered by the ISMS should be identified. Such standards may come from the industry in which the organization works; from state, local or federal governments; or from international regulatory bodies.

The scope should be kept manageable, and it may be advisable to include only parts of the organization, such as a logical or physical grouping within the organization.

Phase 4—Define a Method of Risk Assessment

To meet the requirements of ISO/IEC 27001, companies need to define and document a method of risk assessment. The ISO/IEC 27001 standard does not specify the risk assessment method to be used. The following points should be considered:

- The method to be used to assess the risk to identified information assets
- Which risks are intolerable and, therefore, need to be mitigated
- Managing the residual risks through carefully considered policies, procedures and controls

Choosing a risk assessment method is one of the most important parts of establishing the ISMS. Use of the following will be helpful:

- NIST Special Publication (SP) 800-30 *Risk Management Guide for Information Technology Systems*
- Sarbanes-Oxley IT risk assessment
- Asset classification and data classification documents (determined by the organization)

ISO 27001 needs risk evaluations based on levels of confidentiality, integrity and availability (CIA):

- **Confidentiality**—Clause 3.3: Ensuring that information is accessible only to those authorized to have access
- **Integrity**—Clause 3.8: Safeguarding the accuracy and completeness of information and processing methods
- **Availability**—Clause 3.9: Ensuring that authorized users have access to information and associated assets when required

Phase 5—Prepare an Inventory of Information Assets to Protect, and Rank Assets According to Risk Classification Based on Risk Assessment

The company needs to create a list of information assets to be protected. The risk associated with assets, along with the owners, location, criticality and replacement value of assets, should be identified. Information regarding the grouping of assets, data classification documents and assets inventory documents will be useful. Following are suggested steps:

- For assets, identify the CIA impact levels: high, medium and low.
- Identify risks, and classify them according to their severity and vulnerability.
- After identifying the risks and the levels of CIA, assign values to the risks.
- Based on risk values, determine whether the risk is tolerable and whether to implement a control to eliminate or reduce the risk. The risk assessment methodology will guide in establishing risk levels for assets.

Once the assessment is completed, the information assets that have intolerable risk and, therefore, require controls will be identified. At that time, a document (sometimes referred to as a risk assessment report) that indicates the risk value for each asset is created.

Phase 6—Manage the Risks, and Create a Risk Treatment Plan

To control the impact associated with risk, the organization must accept, avoid, transfer or reduce the risk to an acceptable level using risk mitigating controls. The next stage is performing the gap analysis with the controls provided in the standard (refer to Annex A of ISO/IEC 27001 or to ISO/IEC 27002) to create an RTP and an SOA. It is important to obtain management approval of the proposed residual risks.

The RTP (**figure 5**) provides:

- Acceptable risk treatment (accept, transfer, reduce, avoid)
- Identification of operational controls and additional proposed controls, with the help of gap analysis
- A proposed control implementation schedule

Figure 5—Risk Treatment Plan

	Explanations of Risk Treatment Categories			
Risk	**Reduce**	**Avoid**	**Accept**	**Transfer**
Information security risk	Reduce or mitigate the risk; refer to the 133 controls to identify and implement suitable information security controls or the other initiatives in the organization, e.g., ITIL, COBIT.	Avoid the situation that creates the risk by proactive planning, redesigning or reengineering.	Management should acknowledge the residual risk if there is no cost-effective solution.	Is it possible to transfer some or all of the risk to a third party (insurer)?
Risk and Risk Treatment Example With Applicable Controls				
Inappropriately configured firewall rule sets increasing the risk of unauthorized access to critical and/or privileged network resources	Management performs and reviews vulnerability assessments on an annual basis.	Management has defined perimeter security controls, including firewalls and intrusion detection systems.		

Figure 6—Example SOA for Applicable Controls

Control Objective	Control From Annex A of ISO/IEC 270001	Adopted or Not Adopted	Justification	Organization Procedures and Reference
Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process.	10.5.1 Information Backup	Adopted	Management has implemented a strategy for cyclical backup of data and programs.	XXX—Information security policy XXX—Information backup and media protection procedure

Figure 7—Referenced Policies and Procedures to Control Risks Example

ISO 27001:2005 Controls			Existing Controls	Excluded Controls	Justification	Reference Policies and Procedures
Clause	Section	Control/Control Objective				
Information systems acquisition, development and maintenance	12.4	Security of system files	Yes		Best practices	Systems acquisition/ development policy
	12.4.1	Control of operational software				
	12.4.2	Protection of system test data				

The SOA documents the control objectives (**figure 6**), the controls selected from Annex A, and the justification for adopting or not adopting the control.

Phase 7—Set Up Policies and Procedures to Control Risks

For the controls adopted, as shown in the SOA, the organization will need statements of policy or a detailed procedure and responsibility document (**figure 7**) to identify user roles for consistent and effective implementation of policies and procedures.

Documentation of policies and procedures is a requirement of ISO/IEC 27001. The list of applicable policies and procedures depends on the organization's structure, locations and assets.

Phase 8—Allocate Resources, and Train the Staff

The ISMS process highlights one of the important commitments for management: sufficient resources to manage, develop, maintain and implement the ISMS. It is essential to document the training for audit.

Phase 9—Monitor the Implementation of the ISMS

The periodic internal audit is a must for monitoring and review. Internal audit review consists of testing of controls and identifying corrective/preventive actions. To complete the PDCA cycle, the gaps identified in the internal audit must be addressed by identifying the corrective and preventive controls needed and the company's compliance based on a gap analysis.

To be effective, the ISMS needs to be reviewed by management at periodic, planned intervals. The review follows changes/improvements to policies, procedures, controls and staffing decisions. This important step in the process is project management review. The results of audits and periodic reviews are documented and maintained.

Phase 10—Prepare for the Certification Audit

In order for the organization to be certified, it is essential that it conduct a full cycle of internal audits, management reviews and activities in the PDCA process, and that it retains evidence of the responses taken as a result of those reviews and audits. ISMS management should review risk assessments, the RTP, the SOA, and policies and procedures at least annually.

An external auditor will first examine the ISMS documents to determine the scope and content of the ISMS. The objective of the review and audit is to have sufficient evidence and review/audit documents sent to an auditor for review. The evidence and documents will demonstrate the efficiency and effectiveness of the implemented ISMS in the organization and its business units.

Phase 11—Conduct Periodic Reassessment Audits

Follow-up reviews or periodic audits confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic reassessment audits to confirm that the ISMS continues to operate as specified and intended. As with any other ISO standard, ISO 27001 follows the PDCA cycle and assists ISMS management in knowing how far and how well the enterprise has progressed along this cycle. This directly influences the time and cost estimates related to achieving compliance.

CONCLUSION

The true success of ISO 27001 is its alignment with the business objectives and effectiveness in realizing those objectives. IT and other departments play an important role in implementing ISO 27001. Implementing ISO 27001 is an exercise toward better understanding an existing inventory of IT initiatives, information availability and ISMS implementation phases. An organization also needs to have the detailed understanding of PDCA implementation phases.

Without a well-defined and well-developed ISO 27001 project plan, implementing ISO 27001 would be a time- and cost-consuming exercise. To achieve the planned return on investment (ROI), the implementation plan has to be developed with an end goal in mind. Training and internal audit are major parts of ISO 27001 implementation.

ISO 27001 certification should help assure most business partners of an organization's status with respect to information security without the necessity of conducting their own security reviews. An organization would choose to be certified against the ISO 27001 standard to provide confidence to their customer base and partners.

AUTHOR'S NOTE

This article contains general information only, and Professional Consultant and the author are not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. Before making any decision or taking any action that may affect the business, consult a qualified professional advisor. Professional Consultant, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this article.

The author would like to thank Mary Holloway for her assistance.

ENDNOTES

[1] The ISO 27000 Directory, "The ISO 27001 Certification Process," *www.27000.org/ismsprocess.htm*

[2] The ISO 27000 Directory, "Introduction to ISO 27002," *www.27000.org/iso-27002.htm*

[3] ISO 27001 Security, "ISO/IEC 27001," *www.iso27001security.com/html/27001.html*

[4] Perera, Daminda, "ISO/IEC 27001 Information Security Management System," 26 July 2008, *www.daminda.com/downloads/ISO27001.pdf*

[5] Activa Consulting, "ISO 27001—Likely Costs," *www.iso-27001.co.uk/iso_27001_project_costs.htm*

[6] Schwartz, Mark S.; Thomas W. Dunfee; Michael J. Kline; "Tone at the Top: An Ethics Code for Directors?," *Journal of Business Ethics*, vol. 58, 2005, *http://lgst.wharton.upenn.edu/dunfeet/Documents/Articles/Tone%20At%20the%20TopJBE.pdf*