CHAPTER EIGHTEEN

18 Understanding and Reviewing Compliance with ISO Standards

IN THE YEARS FOLLOWING World War II, the United States emerged as the worldwide economic and political leader. Due to this dominance, many in the United States all but ignored many commercial best practice standards developed and used elsewhere in our globally connected economy. These international best practice standards are collaborative efforts that take into account a wide range of national needs and requirements. The source of many of these standards is the International Standards Organization (ISO; www.iso.org), an international body based in Geneva, Switzerland, that has issued well-recognized standards covering a wide range of areas, such as specifications for fastener screw threads in an automobile engine, the thickness of a personal credit card, and information technology (IT) quality standards. These standards have been expanded over the years to cover many areas that are important for enterprise governance and quality.

IT auditors should have an understanding of the role of any ISO standards that are appropriate in their enterprises. The implementation of most ISO standards often brings an IT auditor out of the internal audit office and to enterprise production areas. Enterprise quality auditors, as described in Chapter 31, are usually the audit professionals most involved with ISO standards. Quality auditors often have quite different objectives and approaches from those of Institute of Internal Auditors (IIA) or Information Systems Audit and Control Association (ISACA) internal audit teams. Chapter 31 discusses the role of quality auditors following American Society for Quality (ASQ) standards, but several of ISO standards are important for all IT auditors.

The proper implementation of and compliance with relevant ISO standards are important to enterprises and to IT auditors. An enterprise may embrace many different

published standards; an IT auditor should be aware of the IT-critical standards and consider them as part of internal controls reviews.

This chapter provides an overview and introduction to several of the many ISO standards that are particularly important for IT auditors, with a focus on ISO 9001 quality standards and ISO 27001 computer security standards. The chapter also introduces several other ISO standards, including those for IT management systems, for risk management, and for quality management. Compliance with appropriate ISO standards is important worldwide today, as enterprises establish worldwide compliance benchmarks. That is, if an enterprise follows some ISO standard and if its compliance to the standard is accredited by a recognized outside reviewer, the enterprise's compliance to the standards will be recognized worldwide.

BACKGROUND AND IMPORTANCE OF ISO STANDARDS IN A WORLD OF GLOBAL COMMERCE

The ISO is responsible for developing and publishing a wide range of international standards in many business and process areas. Some of these standards are very broad, such as ISO 14001, covering effective environmental control systems, while others are very detailed and precise, such as a standard covering the size and thickness of a plastic credit card. The broad ISO standards are important because they allow all worldwide enterprises to be talking in the same language when they can claim that they have, for example, an effective ISO 14001 environmental control system. Many of the more detailed standards are also very critical in order to allow, for example, an ATM (automated teller machine) anywhere in the world to expect to receive the same size and thickness of a credit card.

ISO standards are developed through the collaborative efforts of many national standards-setting organizations, such as the American National Standards Institute or other groups throughout the world. The standards-setting process begins with a generally recognized need for a standard in some area. An example would be ISO 27001, which outlines the high-level requirements for an effective information security management system. This standard was developed through the efforts of international technical committees sponsored by the ISO in cooperation with the International Electrotechnical Commission (IEC) international standards-setting groups. The standard is not specific in its detailed requirements but contains many high-level statements along the lines of "The organization shall." In some respects, this type of guidance is built into IT audit programs discussed in many of these chapters.

Because of the numerous international governmental authorities, professional groups, and individual experts involved in the ISO standards-setting process, the building and approval of any ISO document typically is long and slow. An expert committee develops an initial draft standard covering some area; the draft then is sent out for a review and comments with a review response due date; and the ISO committee finally reviews draft comments before either issuing the new standard or sending a revised draft out for yet another round of reviews and suggested changes. Typically, after many drafts and comment periods, the ISO standard is published. Enterprises then can take the necessary steps to comply with the standard. To certify their compliance,

they must contract with a certified outside ISO auditor, with skills in that standard, to attest to their compliance.

Many U.S. enterprises first got involved with these international standards through the launch of ISO 9000 quality management system standards in the 1980s. Companies were faced with the high-quality design standards found in many non-U.S. products at that time, such as Japanese automobiles. Japanese enterprises had designed many high-quality products by following what became ISO 9000, and U.S. manufacturers began to modify their own processes to comply with these higher standards of product quality. Compliance with the ISO 9000 standard allowed worldwide enterprises to design their operations in accordance with a single, consistent standard and then to assert that they have a quality management system in place in accordance with the international standard.

ISO standards are much more specific and controlled than the Information Technology Infrastructure Library (ITIL) best practices guidelines discussed in Chapter 7. The standards are published and controlled by the ISO organization in Geneva following strict copyright rules. The materials cannot downloaded through a casual Web search; they must be purchased. Many of the actual ISO standards are very detailed outlines of practices to be followed. While certainly out of context, Exhibit 18.1 is an extract from a small section of the ISO 27001 information security management systems standard on the control of documents for an information security management system (ISMS). The guidance is clear and unambiguous and often points to other sections of this standard for follow-up. For example, line 5.b states that management should define the roles and responsibilities for information security. This is a prompt for appropriate levels of action. The guidance also is like a checklist of questions for IT auditor reviews. It says that the IT auditor should encourage

5 Management Responsibility
Management Commitment
Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;
b) establishing roles and responsibilities for information security;
c) ensuring roles and responsibilities for information security;
d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMA (see 5.2.1);
f) deciding the criteria for accepting risks and the acceptable levels of risk;
g) enduring that internal ISMS audit are conducted (see 6); and
h) conducting management reviews of the ISMS (see 7).

EXHIBIT 18.1 ISO Standards Example: 27001 on Management Commitment

Source: These terms and definitions, taken from ISO/IEC 27001:2005 Information Technology Security Techniques—Information security management systems—Requirements clause 5.1 a through h, are reproduced with permission of the International Organization for Standardization. This Technical Report can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

managers to define their information security roles and responsibilities in order to remain in compliance with an ISO standard.

An enterprise can follow and rely on ISO standards similar to the ITIL best practices discussed in Chapter 7, but ISO standards are much more than ITIL's recommended best practices. They represent performance measures for an enterprise and its peers. By adhering to these worldwide standards, an enterprise can verify that it is operating in accordance with a consistent international standard. ISO 13485 on quality management regulatory requirements for medical devices provides an example. This standard defines the quality requirements covering human healthcare devices. The standard calls for an enterprise manufacturing such devices to establish appropriate calibration controls. Because of the diversity of calibration approaches, the standard cannot specify just one approach; it does, however, require that enterprises have appropriate mechanisms in place.

It is one thing for an enterprise to read an ISO standard and change its processes to follow it; it is another thing to demonstrate to others that it is following the standard. This ISO certification is a process similar to an external audit of financial records performed by certified public accountants (CPAs). Financial statement audits require a licensed CPA external auditor to assess whether an enterprise's financial reports are ''fairly stated'' following good internal controls and recognized accounting standards. These are high-level words, but such a signed external audit report along with the final reported results provides a level of assurance that the financial reports are fairly stated and are based on good internal control procedures.

The ISO certification process is also similar to a CPA-led financial audit that is based on compliance with generally accepted auditing standards (GAAS) performed by a major public accounting firm. No ''Big 4'' set of major ISO auditing firms exists, but national standards-setting organizations qualify outside reviewers to perform external audits of various ISO standards. There is no ISO GAAS, however, but a wide degree of diversity in audit objectives since a reviewer for ISO 27001 on IT security management systems will be looking for different control procedures than would an ISO auditor for 13485 medical device quality management systems. In all cases, however, the qualified ISO outside auditor may identify areas for corrective actions and publish a report to management similar to an internal audit process. Once the ISO auditor's recommendations are corrected, the outside reviewer will certify that the enterprise is in compliance with that standard.

Once certified, the enterprise can advertise to the outside world that it has a process in place that meets that specific ISO standard. For example, a customer for the medical diagnostic device would want to know if a potential supplier is in compliance with ISO 13485. That same medical device manufacturer would also want to gain assurance that its prime component suppliers are ISO qualified.

ISO STANDARDS OVERVIEW

Compliance with appropriate ISO standards is not the same type of a requirement for an enterprise as the types of appropriate internal controls that must be implemented in order to certify for an audited financial statement. Because of SEC financial reporting

rules, the lack of an audited financial report or a report with an unfavorable auditor's opinion can be very damaging for a publicly traded enterprise. Virtually all publicly traded enterprises are expected to have audited financial statements, but the rules are not the same regarding compliance with ISO standards. In most instances, compliance with an ISO standard is voluntary only but still often essential. We have cited the ISO standard covering the thickness and size of a personal credit card as an example. An enterprise that manufactured cards or card readers that were not in compliance with such a standard would soon fail in the marketplace.

ISO standards covering quality management systems are a bit different. An enterprise can all but ignore a standard such as ISO 9000 calling for a quality management process and still succeed within a national marketplace. For example, in the United States, some senior managers historically looked at this standard as ''too much paperwork'' and made only minimal efforts to achieve compliance. However, as we move to a more worldwide business-trading environment, many enterprises request such certifications today from their suppliers. What was once just nice to have has become almost mandatory in the United States for manufacturing and many other enterprises.

IT auditors should attempt to learn more about the status of ISO standards compliance within their enterprises. Some ISO standards, such as the thread pattern on a bolt or the thickness of a credit card, would have to become mandatory, or the internal auditor's enterprise would not be in business manufacturing non-compliant products. Quality standards, such as our one-paragraph Exhibit 18.1 extract, require that improved processes be established and monitored. If an enterprise has a separate quality audit function, as described in Chapter 31, IT audit should develop an understanding of levels of activity and compliance with appropriate ISO quality standards. Although there are a wide range of ISO standards, the next sections discuss several that are important for IT auditors in today's world of heightened internal controls and governance.

ISO 9001 Quality Management Systems

ISO 9000 has a heritage dating back to World War II, when both sides of the conflict required strong product uniformity while operating at extremely high levels of production volume. Even if the products produced were bullets and bombs, they still had to work correctly, and there was a need for strict product quality control. On the western Allies' side, some strong quality assurance standard procedures and the professions of industrial engineers and production quality control specialists arose. After the war, ISO was established as part of the General Agreement on Trade and Tariffs, one of the international agreements to bring the world to more of a peacetime environment. ISO 9000 on quality management systems was one of these earlier ISO standards. It first received most attention in the newly recovering European countries.

Japan was another rebuilding and recovering postwar country that strongly embraced quality management systems. In the 1950s and 1960s, the Japanese invited a series of U.S.-based quality systems experts, such as W. Edwards Deming and others, to

help at many of their plants. While these quality systems experts had been all but ignored in the United States, their philosophies and techniques were heavily embraced by Japanese industry, and by the mid-1970s, Japanese electronic and automobile manufacturers began to make deep inroads into U.S. markets due to the quality and value of their products. Many in the United States began to recognize that these Japanese-manufactured products were superior in many respects to their own. ISO 9000 quality standards became an increasingly important factor to measure and assess the quality of products worldwide.

ISO 9000 is a family of standards for quality management systems. Maintained by ISO, these standards include requirements for such matters as:

- Monitoring processes to ensure they are effective
- Keeping adequate records
- Checking output for defects, with appropriate corrective action where necessary
- Regularly reviewing individual processes and the quality system for effectiveness
- Facilitating continual improvement

Each of these items refers to processes, not specific actions. However, for an enterprise to assert that it is in compliance with ISO 9000 (actually 9001), for example—that it is monitoring key processes to be effective—often it must make significant changes to management procedures and supporting documentation. Compliance with an ISO standard also creates a required level of expectations. Any enterprise, on a worldwide scope, that holds to such standards is stating that it has effective quality systems in place. An enterprise that has been independently audited and certified to be in conformance with ISO 9001, for example, may publicly state that it is ''ISO 9001 certified'' or ''ISO 9001 registered.'' Certification to an ISO 9000 standard does not guarantee the compliance (and therefore the quality) of end products and services; rather, it certifies that consistent business and production processes are being applied.

The actual certification is achieved through a review by a registered ISO auditor certified for the particular ISO standard. As discussed, this process is similar to the CPA's review and certified audit of an enterprise's financial statements. Regulated by their national standards organizations, ISO auditors are authorized to register an enterprise's compliance with unique ISO standards.

ISO 9000 and other ISO standards impose heavy documentation requirements on an enterprise. It is not sufficient for an enterprise just to claim some process has been once documented. There must be an ongoing process to keep that documentation current over time. In past years, many enterprises went through one-time efforts to create documentation and failed to keep it current. Many IT auditors have faced this kind of situation where they frequently ask if some system or process they are reviewing is documented. If the documentation is out of date or nonexistent, this lack of documentation often would become an audit report finding but would result in little definitive corrective action. ISO 9000 compliance raises documentation requirements for quality processes to a whole new level. An outside reviewer must certify that the enterprise is in compliance in order for the enterprise to advertise to the outside world that it is in compliance with the ISO standard.

As a clarification, what is commonly referred to as just ISO 9000 is not one standard but really a series of "certifiable" standards and guidelines:

ISO 9001. Certifiable standard dealing with design
ISO 9002. Certifiable standard dealing with manufacturing
ISO 9003. Certifiable standard dealing with manufacturing and assembly
ISO 9004. Guideline defining a quality system

These standards are updated periodically with the current year appended to the standard number. To add to the complexity, an enterprise can claim compliance only with an earlier version, such as ISO 9000:1994. A QS 9000 series of standards is similar but pertains just to the automotive industry. A *certifiable standard* is subject to review by an outside auditor, as discussed. The current version of the ISO quality standard 9001 is ISO 9001:2008, although it includes only a few new definitions from the more recognized ISO 9001:2000. For purposes of this discussion, we just use the more generic term of ISO 9000 to refer to all of these quality management system standards.

ISO 9000 is a set of standards for a continual improvement-driven quality system, no matter whether a manufactured component or a service process. Exhibit 18.2 shows such a quality management system process that is driven by internal procedures for continual improvements as well as customer requests. In this continual process, existing processes should be monitored, actions planned for improvements, and the action items implemented for subsequent monitoring and further improvements. For many, the

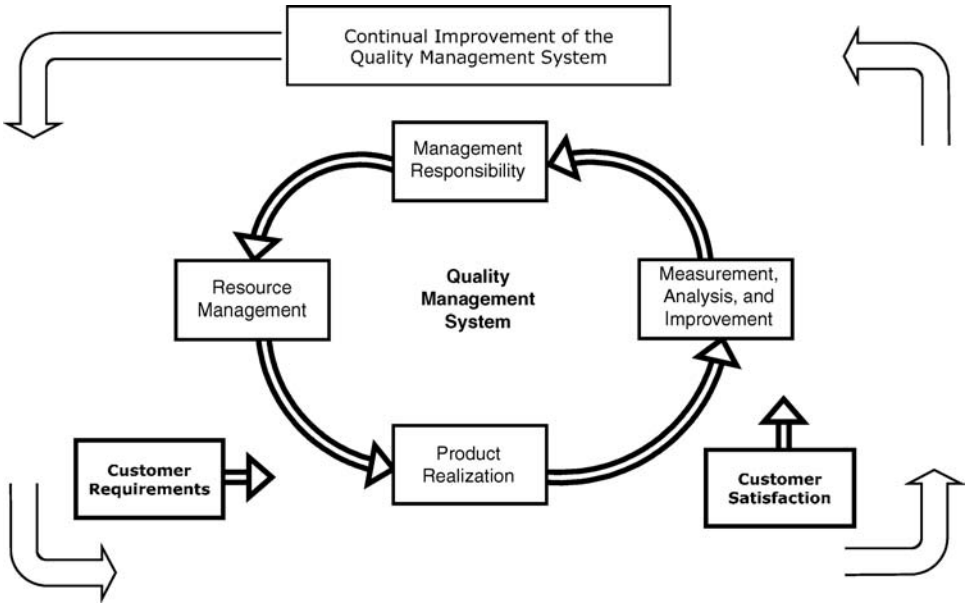

EXHIBIT 18.2 Quality Management System Process

continual improvement quality process is nothing new. IT auditors and systems development professionals have used essentially the same set of general processes since the early days of IT systems development, in what was called the systems development life cycle (SDLC), a process to develop new IT systems discussed in Chapter 10. However, many SDLC-developed applications called for a great deal of documentation, which often was not prepared. Many of today's IT applications are developed through more informal and iterative rapid application development processes.

Solid and accurate documentation is extremely important for an enterprise seeking to claim ISO registration, ISO registration a global requirement. When ISO 9001:2000 Section 4.2.3 states, among other provisions, that "[a] documented procedure should be established to define the controls needed" along with such subsections as "a) to approve documents for adequacy of issue," an enterprise or process documentation control system is needed to demonstrate compliance with that standard. ISO best practices call for a hierarchy of documentation in any area starting with top-level manuals to explain the whys and then down to instructions describing the hows of the practice. Exhibit 18.3 shows this documentation hierarchy with Documentation and Forms on the bottom part of triangle providing proof. This documentation is essential to support a quality management system and certainly is required by ISO external certification auditors.

This section has provided a very high-level description of the ISO 9000 quality management process. Compliance with these ISO 9000 processes are important for all types of enterprises to assert to their own internal management and to the outside world that the enterprise is focused on quality. In 1995, the American Institute of Certified Public Accountants became the first major worldwide professional organization to become ISO 9001 certified.[1] Neither ISACA nor the IIA has been certified. Organizations of all levels should consider adopting ISO 9000 processes.

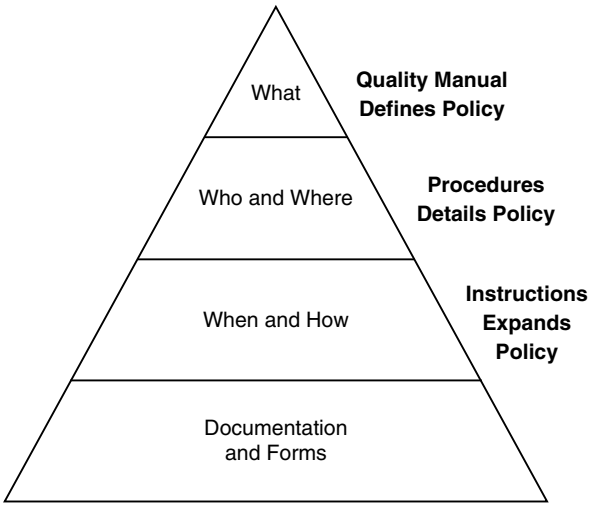

EXHIBIT 18.3 ISO Documentation Hierarchy

ISO IT Security Standards: ISO 27001 and 27002

There two ISMS standards, ISO 127001 and ISO 27002. ISO 27002 represents an important IT-related security standard designed to help any enterprise that needs to establish a comprehensive information security management program or improve its current information security practices.

ISO 27002 is a standard concerning both a wide range of information sources and information security in a general sense. Because such information can exist in many forms, the standard takes a very broad approach and includes a wide range of standards covering security regarding:

- Data and software electronic files
- All formats of paper documents, including printed materials, handwritten notes, and photographs
- Video and audio recordings
- Telephone conversations as well as e-mail, fax, video, and other forms of messages

The idea here is that all forms of information, not just IT, have value and need to be protected, just like any other corporate asset. Many enterprises today do not even consider security standards in these broad areas, but the ISO standard suggests they should be covered when appropriate. In addition, the infrastructure that supports this information, including networks, systems, and functions, also must be protected from a wide range of threats, including everything from human error and equipment failure to theft, fraud, vandalism, sabotage, fire, flood, and even terrorism.

Similar to all other ISO standards, this published standard does not really prescribe *what* is specifically required but outlines areas where security-related standards are required. Exhibit 18.4 outlines some ISO 27002 topics. The standard does not contain detailed requirements for each of these areas—a thorough and consistent international standard would require a huge, extensive text that would not be all inclusive and would soon be out of date. Rather, as an example, line 4.2 calls for security standards covering third-party access policies. ISO calls for the enterprise to have a documented and approved processes covering third-party access policies. An enterprise should develop its own more detailed standards and procedures in this area. Their type and extent can depend on many factors, but an ISO 27002–compliant enterprise should address this issue along with the other topic areas in the standard.

As a first step to implementing ISO 27002, an enterprise should identify its own information security needs and requirements. Doing this requires performing an information security risk assessment along the lines of the Committee of Sponsoring Organizations enterprise risk management (COSO ERM) processes discussed in Chapter 4. Such an assessment should focus on the identification of major security threats and vulnerabilities as well as an assessment of how likely it is that each will cause a security incident. This process should help to pinpoint an enterprise's unique information security needs and requirements.

As part of getting ready for the ISO 27002 information security standards-setting process, an enterprise should identify and understand all of the legal, statutory,

1. Scope: A high level description of the application of this standard
2. Terms and definitions: Consistent with other ISO standards, all major terms are defined (e.g. Definition of what is meant by ''Confidentiality'')
3. The standards or need for a high level information security policy
4. Requirements for an enterprise security organization:
   - 4.1 Information security infrastructure
   - 4.2 Security and third party access policies
   - 4.3 Outsourcing considerations
5. Asset classification and control standards:
   - 5.1 Accountability for assets
   - 5.2 Information classifications
6. Personnel security
   - 6.1 Security considerations in job definitions and resources
   - 6.2 User training for personnel security
   - 6.3 Standards for responding to security incidents and malfunctions
7. Physical and environmental security including requirements for:
   - 7.1 Secure areas
   - 7.2 Equipment security
   - 7.3 General controls
8. Communications and operations management
   - 8.1 Operational procedures and responsibility
   - 8.2 System planning and acceptance
   - 8.3 Protections against malicious software
   - 8.4 Housekeeping
   - 8.5 Network management requirements
   - 8.6 Media handling and security
   - 8.7 Exchanges of information and software
9. Access control
   - 9.1 Business requirements for access control
   - 9.2 User access management
   - 9.3 User responsibilities for security standards
   - 9.4 Network access control
   - 9.5 Operating system access control
   - 9.6 Application access management
   - 9.7 Monitoring standards for systems access and use
   - 9.8 Mobile computing and related networking
10. System development and maintenance standards
    - 10.1 Security requirements hardware and software systems
    - 10.2 Application systems security
    - 10.3 Cryptographic controls
    - 10.4 Security of system files
    - 10.5 Security in development and support processes
11. Business continuity management standards
12. Security standards covering compliance issues
    - 12.1 Compliance with legal requirements
    - 12.2 Reviews of security policy and technical compliance
    - 12.3 Systems audit considerations

EXHIBIT 18.4 ISO 27002 Standards Topics Areas

regulatory, and contractual requirements that it, its trading partners, contractors, and its service providers must meet. Doing this requires an understanding and identification of an enterprise's unique legal information security needs and requirements.

ISO 27002 is the first of a series of international standards meant for any enterprise that uses internal or external computer systems, possesses confidential data, depends on IT to carry out its business activities, or simply wishes to adopt a higher level of security by complying with a standard. The standard is relatively new and not in common application in the United States. Just as ISO 9000 has become a guarantee of quality, compliance with ISO 27002 enables partners to be confident in an enterprise's overall security. Compliance should promote an increased level of mutual confidence between partners, where each can attest that it has established security in compliance with a recognized set of standards. In addition, as ISO 27002 compliance becomes more common, it may result in lower premiums for computer risk insurance but certainly will yield better protection of confidential data and improved privacy practices and compliance with privacy laws. ISO 27002 is a structured and internationally recognized methodology that should help an enterprise to develop better management of information security on a continuing basis. The standard also supports the ISMS requirements of the related security standard, ISO 27001.

IT Security Technique Requirements: ISO 27001

ISO 27002 is a high-level code of practice covering security controls. ISO 27001 is what ISO defines as the "specification" for an ISMS. That is, this standard is designed to measure, monitor, and control security management from a top-down perspective. The standard essentially explains how to apply ISO 27002, and it defines the implementation of this standard as a six-part process:

1. **Define a security policy.** A fundamental component of any standard is the need for a formal policy statement approved by senior management. All other compliance aspects of the standard will be measured against this policy statement.
2. **Define the scope of the ISMS.** ISO 27002 defines security in rather broad terms that may not be appropriate or needed for all enterprises. Having defined a high-level security policy, an enterprise needs to define the scope of its ISMS that will be implemented. For example, ISO 27002 defines an element of security requirements as video and audio recordings. This may not be necessary for a given organization; in that case, it would be specifically excluded for its ISMS scope.
3. **Undertake a risk assessment.** The enterprise should identify a risk assessment methodology that is suited to its ISMS environment and then both develop criteria for accepting risks and define what constitutes acceptable levels of risk.
4. **Manage the risk.** This is a major process that includes formal risk identification, risk analysis, and options for the treatment of those risks. The latter can include applying appropriate risk avoidance controls, accepting risks, taking other steps to avoid them, or transferring the risks to other parties such as insurers or suppliers.
5. **Select control objectives and controls to be implemented.** This is the same IT audit and control process discussed in Chapter 5 on planning and performing

effective IT audits. For each defined control objective, the enterprise should define an appropriate controls procedure.

6. **Prepare a statement of applicability.** This is the formal documentation that is necessary to wrap up the ISMS documentation process. Such documentation matches up control objectives with procedures to manage and implement the ISMS.

As can be seen from these six steps, risk analysis and security policies are fundamental to this standard. Setting up these practices is not an internal audit attest function, but IT audit can provide strong help to management by offering to serve as an internal consultant and to help in performing adequate risk assessment procedures.

Because of strict ISO copyright rules, we have not included extracts of ISO 27001 in this chapter. The actual ISO standards are presented in tight and unambiguous text. Little specific detail is provided, but there is enough to allow an enterprise to implement its ISMS. Each formal standard concludes with an appendix section listing control procedures for each of the objective details in the standard. However, ISO 27001 should not be considered as a comprehensive set of control procedures that will change as technology changes; rather, it is an outline for the framework of an ISMS that should be continually implemented, monitored, and maintained.

ISO 27002 and ISO 27001 are already global standards, with established compliance, and certification schemes in place, particularly in the United Kingdom and the European Union. Both standards will continue to evolve, to track technology, and will expand with even wider changes. Although these standards have only been discussion topics in ISACA publications at present, we can expect the Control Objectives for Information related Technology (CobiT) framework, discussed in Chapter 2, to tie in much more closely with ISO 27002 standards in future years. There can be little doubt that these ISO standards will continue to grow in influence and that adoption will continue to expand.

IT auditors should monitor the status of this standard that calls for appropriate ISMS within their IT function. Such an enterprise IT department can delay fully implementing ISO 27002 and an ISMS, but a vendor or other major stakeholder may demand evidence of compliance. IT auditors can be of help with such matters.

Service Quality Management: ISO 20000

Many professionals will agree that we live in a world with too many standards—many of which are similar to others with objectives that are not closely connected to each other. ISO 2000 on service quality management introduces some of this much-needed standards convergence. This is an international standard for IT Service management, and it introduces many of the ITIL service management best practices that were discussed in Chapter 7. ISO 2000 consists of a Part 1 on implementing service management and a following Part 2 section describing best practices for service management. The Part 1 standard specifies the need for a series of service management documented processes, such as defining requirements for implementing such a management system, new or changed service requirements, and documented relationship, control, resolution, and release processes. Quite correctly, the standard takes the best practices approach of ITIL and calls for formal documented processes to support them.

ISO 2000 calls for an enterprise to adopt and be certified that it has adopted the ITIL best practices discussed in Chapter 7. Formally, this standard "promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirements." ISO 2000 is the first global standard for IT service management, and is fully compatible and supportive of the ITIL framework. It will undoubtedly have a significant impact on the use and acceptance of ITIL best practices and the whole IT Service Management landscape.

In future years, IT auditors should see an increasing level of recognition on the importance of ISO service related standards. In our increasingly global economy, no matter what national restrictions may be imposed across borders from time to time, internal standards are needed to define common practices and to better facilitate communication. When an enterprise or service organization—anywhere in the world—has achieved ISO 9000 quality management certification, customers and users can expect a certain minimum level of documentation and process standards. The ISO 27001 IT security standards should soon reach a similar level of importance and recognition. With our comments on ISO 2000 on ITIL and ISO 9000's similarities with the Sarbanes-Oxley Act (SOx), we should see increasing convergence trends between ISO and standards in other areas. Internal and IT auditors at all levels should understand and embrace these important ISO standards.

ISO 19011 QUALITY MANAGEMENT SYSTEMS AUDITING

Every ISO standard discussed here contains references on the need to audit that particular quality system. The published standard offers resources for an enterprise to "save time, effort and money" in its management systems auditing processes. ISO 19011 very much relates to the ASQ quality audit standards discussed in Chapter 31, and it outlines four critical decision/support resources for the efficient planning, conduct, and evaluation of quality and/or environmental audits:

1. The need for a clear explanation of the principles of management systems auditing
2. Guidance on the management of audit programs
3. Guidance on the conduct of internal or external audits
4. Advice on the competence and evaluation of auditors

These are topics discussed in other chapters of this book. The reader may wonder about the need for an ISO international standard here, but it is directed at quality auditors worldwide, including many who have not had exposure to IT auditing or the IIA and ISACA auditing standards discussed in Chapters 3.

This ISO standard also outlines five principles of auditing that are very similar to other principles that we have discussed for other IT auditing topics:

1. **Ethical conduct.** Auditors performing ISO 19011 audits should be honest and do the right thing.
2. **Fair presentation.** Auditors should be evenhanded when reporting results.

3. **Exercise due professional care.** Auditors should do what is reasonable and normally expected.
4. **Independence.** Auditors should avoid conflicts of interest to ensure their integrity.
5. **Evidence-based approaches.** Investigate first and then report the facts.

The ISO 19011 standard contains a detailed set of the principles of auditing from an ISO, quality audit perspective. Exhibit 18.5 is a high-level outline of topic areas in this standard. There are some duplicate titles in the subheadings, as the standard places some topics, such as the Audit Report, under multiple audit principles. This is a very comprehensive overview of internal auditing from a quality audit perspective. While space does not allow a detailed summary of this standard, virtually all of those related to internal auditing principles are described in other chapters in this book.

IT audit professionals will soon see a greater recognition of ISO standards, with an emphasis on ISO 19011 describing auditing standards. As an example, the IIA sent out a survey in August 2008 over its GAIN network, mentioned in Chapter 3, to assess IIA internal auditor involvement with ISO 19011. About 1,500 queries were sent out but only about 150 replies were received. Questions were along the lines of "Does your

Ethical Conduct
- Audit Team
- Audit Plan
- Work Documents
- Opening Meeting
- Audit Report
- Report Distribution
- Personal Attributes

Fair Presentation
- Findings
- Audit Report
- Personal Attributes
- Outcomes

Due Professional Care
- Audit Report
- Auditor Judgment
- Findings
- Conclusions

Independence
- Selecting Auditors
- Assigning Work
- Follow-Up Activities

Evidence-Based Approach
- Collecting Evidence
- Findings
- Conclusion
- Audit Report

EXHIBIT 18.5 ISO 19011 IT Audit Standards Outline

internal audit activity have any input or review role related to the annual quality management system (QMS) audit program?'' The results generally showed that IIA internal auditors have little involvement with the quality auditors (described in Chapter 31) who would be responsible for implementing this ISO standard.[2] Based on survey results, generally 70% of the responses showed no involvement with ISO 19011 in their enterprises.

ISO STANDARDS AND IT AUDITORS

As we become more and more of a global commerce world with many interconnections and relationships, the ISO standards become more important for all enterprises. Although standards describing component dimensions—such as the tread pattern and size of a bolt—are essential for commerce, the ''softer'' quality system standards, such as ISO 9000, are equally important. Enterprises in one location will refuse to do business with enterprises elsewhere unless they can certify their compliance to some ISO standard.

Although many IT auditors have not been familiar with ISO standards in the past, we expect this to change. CobiT will almost certainly become more closely aligned with ISO 27002, and the IIA's GAIN survey regarding the level internal auditor involvement with ISO 19011 shows that the IIA is at least thinking about this new international standard. When appropriate, IT auditors should try to incorporate appropriate IS standards in their IT internal controls audits.

NOTES

1. www.qualitydigest.com/june99/html/body_iso_9000.html.
2. The Institute of Internal Auditors GAIN Network, ''International Organization for Standardization (ISO) 9001:2000 Quality Management System Type: Executive Summary Report,'' April 10, 2008.