



# Protecting Information Assets Using ISO/IEC Security Standards

The ISO/IEC 27000 *Information technology – Security techniques* series of standards takes a risk management approach that will enable information professionals to contribute to an information security management system featuring the controls needed to protect information assets against external and internal threats.

## Lois Evans

Since 2005, an estimated 5,000 data breaches involving 675 million individual records have taken place worldwide, according to a November 7, 2015, article in *The Economist*, “Data Breaches in America: The Rise of the Hacker.”

In the United States, data breaches have occurred across many industry sectors, including:

- Government defense (e.g., U.S. Army, U.S. State Department, National Security Agency)
- Finance (e.g., Morgan Stanley, JP Morgan Chase, Wells Fargo)
- Retail (e.g., Target, eBay, Home Depot, Staples)
- Communications and entertainment (e.g., Yahoo, Tumblr, Sony Pictures)
- Online service providers (e.g., Dropbox, Epsilon, Evernote)
- Medical services (e.g., Anthem,

Complete Health Systems, Advocate Health and Hospitals)

While the responsibility for information security has escalated to the executive level, many executives do not understand the threats their organizations face and find it difficult to keep up-to-date on the responses and products needed. As a result, some organizations lack sufficient protection while at the same time over-spend for it, paying \$100 for every \$50 of loss prevented, according to *The Economist* article “Cyber-Crime and Business: Think of a Number and Double It,” published January 17, 2015.

### ISO/IEC 27000 Is ‘Family’ of Standards

The ISO/IEC 27000 *Information technology – Security techniques* series of standards provides the information that executives and other stakeholders need to develop and operate a customized information security management system (ISMS) that is based on clearly communicated objectives and controls and incorporates features experts believe are essential for managing information as an asset.

The series, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), includes nearly 20 standards. The first three, ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002, describe the vocabulary, requirements, and code of practice, while the balance provide general instructions for governance, security risk management, measurement, and auditing, as well as sector-specific instructions for finance, cloud services, energy utilities, and health. (See the “ISO/IEC 27000 *Information technology – Security techniques* Series” sidebar for the complete list of standards in this series.)

The series takes a risk management approach, enabling each or-

---

## Information Technology – Security Techniques

The ISO/IEC 27000 series is to information security what the ISO-9000 series is to quality assurance – a comprehensive set of standards that provides best practice recommendations for organizations of any type or size.

ISO/IEC 27000:2016	<i>Information security management systems – Overview and vocabulary</i>
ISO/IEC 27001:2013	<i>Information security management systems – Requirements</i>
ISO/IEC 27002:2013	<i>Code of practice for information security controls</i>
ISO/IEC 27003:2010	<i>Information security management system implementation guidance</i>
ISO/IEC 27004:2009	<i>Information security management – Measurement</i>
ISO/IEC 27005:2011	<i>Information security risk management</i>
ISO/IEC 27006:2015	<i>Requirements for bodies providing audit and certification of information security management systems</i>
ISO/IEC 27007:2011	<i>Guidelines for information security management systems auditing</i>
ISO/IEC 27008:2011	<i>Guidelines for auditors of information security controls</i>
ISO/IEC 27009:2016	<i>Sector-specific application of ISO/IEC 27001 – Requirements</i>
ISO/IEC 27010:2015	<i>Information security management for inter-sector and inter-organizational communications</i>
ISO/IEC 27011:2008	<i>Information security management guidelines for telecommunications organizations based on ISO/IEC 27002</i>
ISO/IEC 27013:2015	<i>Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ISO/IEC 27014:2013	<i>Governance of information security</i>
ISO/IEC 27015:2012	<i>Information security management guidelines for financial services</i>
ISO/IEC 27016:2014	<i>Information security management – Organizational economics</i>
ISO/IEC 27017:2015	<i>Code of practice for information security controls based on ISO/IEC 27002 for cloud services</i>
ISO/IEC 27018:2014	<i>Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i>
ISO/IEC 27019:2013	<i>Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry</i>
ISO/IEC 27799:2016	<i>Health informatics – Information security management in health using ISO/IEC 27002</i>

---

ganization to tailor its ISMS to its own business environment to protect a range of information assets (e.g., financial, personally identifiable, confidential, and third-party) against specific threats and vulnerabilities.

In essence, the ISO/IEC 27000 series is to information security what the ISO 9000 series is to quality assurance – a comprehensive set of standards that provides best practice recommendations for organizations

## In essence, the ISO/IEC 27000 series [of standards] is to information security what the ISO 9000 series is to quality assurance.

of any type or size. Importantly, the standards are battle tested: stemming from a 1995 British security standard (BS7799), they have been in place since 2005 and are reviewed and updated regularly.

### ISO/IEC 27001 Is Series' Foundation

The key to the ISO/IEC 27000 series is ISO/IEC 27001:2013 *Information security management systems – Requirements*. At 23 pages, ISO/IEC 27001 can be read through in one sitting, yet contains enough information to direct a months-long project. The first half consists of 10 narrative sections outlining the general requirements for an ISMS, while the second half consists of an annex listing the 14 key control objectives required for ISO/IEC 27001 compliance.

An easy way to approach the document is to skim through the narrative sections, read the annex to get a sense of the extent of an ISMS, and then return to the first section for a more in-depth read. Orienting to the controls listed in the annex provides a better sense of the effort required.

### Narrative Sections Summarized

The ISO/IEC 27001 narrative sections include the following:

**Scope:** ISO/IEC 27001 specifies the requirements for an ISMS, based on assessing and treating information security risks specific to an organization.

**Normative Reference:** ISO/IEC 27000 *Information security management systems – Overview and vocabulary* is the normative reference for

ISO/IEC 27001. ISO/IEC 27000 provides an overview of principles, processes, administration, and benefits of an ISMS, as well as an explanation of how the standards in the ISO/IEC 27000 “family” are related.

**Terms and Definitions:** The 80-plus security terms and definitions found in ISO/IEC 27000 apply to ISO/IEC 27001.

**Context of the Organization:** Each organization faces unique external and internal issues that affect its ability to achieve information security. Identifying these issues ensures that the needs and expectations of interested parties are met and that the scope of the ISMS is appropriate.

**Leadership:** Top management must ensure that information security objectives align with organizational objectives, that information security is integrated into business processes, that the appropriate level of resources is assigned, and that roles, responsibilities, and authorities are clear. Management must also establish an information security policy and ensure communication of and conformance with the policy.

**Planning:** Using a risk management approach, an organization must determine the risks and opportunities it faces, analyze and evaluate the risks, and define treatments.

**Support:** All persons working under an organization’s control must be competent, aware of the security policy and their responsibilities, and understand what aspects of the ISMS may or may not be communicated. Documentation for the ISMS must be maintained, updated, and controlled.

**Operations:** Information security processes must be identified, implemented, and documented per the security objectives identified through risk assessment. Risk treatments must be implemented and documented.

**Performance Evaluation:** Organizations must determine what should be monitored and measured and when and how results should be analyzed and evaluated. Internal audits and management reviews are required at planned intervals.

**Improvement:** An ISMS must exist in an atmosphere of continual improvement. Non-conformity must be evaluated, corrected, and documented, with a focus on eliminating the cause so it does not recur.

### ISMSs Require Collaboration

An ISMS depends on information governance (IG), which extends across both information security and records and information management (RIM). Importantly, the two disciplines share many priorities.

For example, the overall objectives of information security are most commonly expressed as preserving confidentiality, integrity, and availability (often referred to as CIA). According to ISO/IEC 27000, these objectives can extend to involve authenticity, accountability, non-repudiation, and reliability.

These objectives mirror the Generally Accepted Recordkeeping Principles® (Principles) of protection, integrity, and availability, and overlap

with the remaining Principles: transparency, compliance, accountability, retention, and disposition. In fact, RIM professionals and information security managers are partners in meeting IG objectives and can benefit the organization by fully understanding and supporting their colleagues' programs.

From this perspective, ISO/IEC 27001 provides RIM professionals with a starting point and vocabulary for considering and acting on areas of overlap between the organization's RIM system and the ISMS. Governance is an important issue in most collaborative efforts, where different teams often represent varying perspectives and priorities. ISO/IEC 27014:2013 *Information technology – Security techniques – Governance of information security* provides further guidance for those looking to collaborate across business units successfully.

## ISMSs Focus on Risk Management

Another takeaway from the ISO/IEC 27000 series is the focus on risk. A RIM system typically includes elements of risk management, but not all RIM professionals have participated in the type of exercise required for defining or updating an ISMS. While ISO/IEC 27001 does list the basic elements of a risk management exercise, ISO/IEC 27005: 2011 *Information technology – Security techniques – Information security risk management* provides additional direction.

Risk management involves risk identification, analysis, evaluation, and treatment, based on a thorough consideration of an organization's context, the specific threats and vulnerabilities faced, the level of risk tolerance, and the availability and affordability of treatments. If properly conducted, these activities cannot be completed overnight. Risk identification alone takes significant effort, leveraging a range of activities such as brainstorming, interviews, checklists,

scenario analysis, and/or business impact analysis.

In orienting to risk management processes, RIM professionals will appreciate the risk register approach typically used. In a *risk register*, each risk is entered as a line item in a spreadsheet, and data is entered as each item is analyzed, categorized, evaluated, prioritized, and considered for possible treatments. Risk registers can be used to create a risk table that visually depicts risk priorities and form the basis of the formal risk plan provided to top management to clarify and confirm security objectives, resourcing, responsibilities, timing, and prioritization.

## Annex Provides Security Controls

The control objectives and controls listed in the ISO/IEC 27001 annex are aligned with those listed in the 90-page ISO/IEC 27002: 2013 *Information technology – Security techniques – Code of practice for information security management* and are numbered using the same schema.

According to ISO/IEC 27000, *controls* are the means of managing risk, such as organizational structures, policies, procedures, guidelines, and practices, while a *control objective* is a statement describing what is to be

achieved as a result of implementing controls.

ISO/IEC 27001 and ISO/IEC 27002 examine 14 control categories, 35 control objectives, and 114 controls: ISO/IEC 27001 briefly introduces all items in tabular form, and ISO/IEC 27002 provides guidance for implementing each control. (See page 32).

As shown below, the ISO/IEC 27001 *control category* “8 Asset Management” lists three *control objectives*: Responsibility for Assets, Information Classification, and Media Handling.

Drilling down a level, the *control objective* for “Information Classification” is “To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.” This objective is achieved through three *controls*: Classification of Information, Labelling of Information, and Handling of Assets.

Drilling down another level, the *control* “Classification of Information” states: “Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.”

The complementary implementing guidance provided by ISO/IEC 27002 discusses the “Classification of Information” control in terms of the business needs and legal requirements for sharing and restricting information,

### Control Category: 8 Asset Management Control Objectives:

1. *Responsibility for Assets*
2. *Information Classification*: “To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.”

#### Controls:

1. *Classification of Information*: “Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.”
  2. *Labeling of Information*
  3. *Handling of Assets*
- ### 3. Media Handling

## ISO/IEC 27000 Series Controls and Objectives

Control	Name	Objectives
5	Information security policies	Provide management direction and support in accordance with business requirements and relevant laws and regulations.
6	Organization of information security	Establish a management framework; ensure the security of teleworking and mobile devices.
7	Human resource security	Ensure that employees and contractors understand their responsibilities and are suitable for their roles prior to, during, and upon termination or change of employment.
8	Asset management	Identify organizational assets and assign protection responsibilities based on information classification and appropriate handling of media.
9	Access control	Limit access to information and information processing facilities, manage user access, and ensure users safeguard their authentication information, to prevent unauthorized access.
10	Cryptography	Ensure proper and effective use of cryptography to protect information.
11	Physical and environmental security	Prevent unauthorized physical access, damage and interference to information and information processing facilities and equipment.
12	Operations security	Ensure correct and secure operations, including: documenting operating procedures, protecting against malware and data loss; logging and monitoring to record events and generate evidence; preventing technical vulnerability; and minimizing the impact of audit activities.
13	Communications security	Ensure the protection of information in networks and in transfers.
14	Systems acquisition, development and maintenance	Ensure that security is integrated in all information systems, across their lifecycle.
15	Supplier relationships	Ensure protection of assets accessed by suppliers in line with supplier agreements.
16	Information security incident management	Ensure a consistent and effective approach is taken to incidents, including appropriate communication of events and weaknesses.
17	Information security aspects of business continuity management	Embed information security into the business continuity management system, including redundancy of information processing facilities.
18	Compliance	Avoid breaches of legal, statutory, regulatory, or contractual obligations and ensure information security reviews take place in accordance with organizational policies and procedures.

as well as the responsibilities of owners for classification of information assets in terms of confidentiality, integrity and availability. Importantly, with respect to the ISMS, information classification refers to the organization's access control policy rather than its retention and disposition policy.

While information security and records classification are not the same thing, there are potential overlaps that could be exploited. As an example, ISO/IEC 27002 states that classification "should be included in the organization's processes and be consistent and coherent across the organization," and, in particular, sensitive information must be protected from disclosure, but not to the extent that public information is not made available.

Many records schedules include details about records that contain personal or confidential information; optimally, an organization's record and security classifications could be combined within the same schedules, resulting in increased compliance and accessibility.

### Series Can Help Build Partnerships

The ISO/IEC 27000 series represents an expansive body of knowledge designed to support information security professionals in their work. While RIM professionals do not require the same in-depth knowledge, they can benefit from knowing information security objectives and controls.

Identifying areas of overlap where collaboration can occur between the two business areas will encourage a culture of mutual support and understanding. To this end, ISO/IEC 27001 acts as a "CliffsNotes" / "Coles Notes" introduction to information security practice and a great way to orient to this challenging but increasingly important information domain. **END**

*Lois Evans can be contacted at levans18@mail.ubc.ca. See her bio on page 47.*