G00219324

How to Make the Most of ISO/IEC 27001

Published: 9 December 2011

Analyst(s): Carsten Casper

This research explains how to gain certification with ISO/IEC 27001 (Information technology — Security techniques — Information security management systems — Requirements), published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It describes the types of use, as well as the potential benefits and best practices. Certification is becoming important for private and public companies in all industries, as well as for government organizations. This research also explains the benefits of aligning with the standard without certification.

Key Findings

- ISO/IEC 27001 is part of a series of international information security standards that's gaining in importance. For global organizations, there's no certification alternative to ISO/IEC 27001.
- According to a Gartner survey, 29% of respondents said they would support or consider ISO/IEC 27001/27002 in the IT compliance projects they undertake. In addition, 65% of those involved in information security responded that their organization is audited regularly by a third-party against accepted standards or guidelines.
- Organizations use ISO/IEC 27001 when they need to provide outside parties with evidence of their security level of effort or when they have a corporate culture based on total quality, especially ISO 9000, and are seeking the information security equivalent. If they merely want to establish an information security management system (ISMS) informally, they usually apply ISO/IEC 27002.

Recommendations

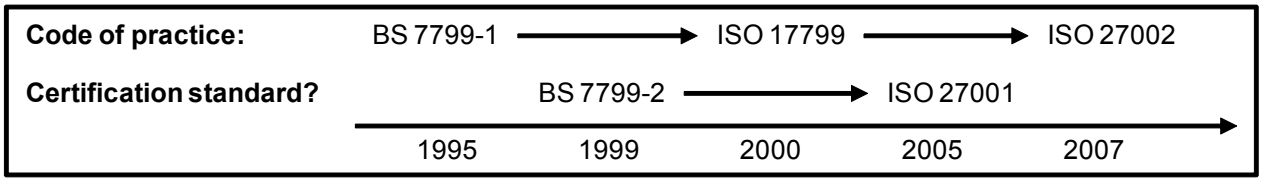
- Organizations should invest in complying with ISO/IEC 27001, but only if there's a business justification. Formal certification is justified if a business partner requires it, or if it can be leveraged to demonstrate a sufficient level of security to external stakeholders. Security process improvements, however, can be achieved by complying with the standard without a formal audit or certification.

- Organizations that want to get audited or certified, or need advice regarding ISO/IEC 27001, will find an appropriate partner in one of the certifying organizations that are accredited nationally — for example, BSI Group, Bureau Veritas Certification, Det Norske Veritas (DNV), Certification Europe, LRQA, or the TUV companies.
- Global organizations should establish an ISMS worldwide, but audit and certification are easier to handle on a per-country basis. ISMS audits can be integrated with internal audits.

Analysis

ISO/IEC 27001/27002 is a set of related consecutively numbered information security practice standards, the first of which, ISO/IEC 27001, has a formal third-party certification program. It's based on the British Standard (BS) 7799, which comes in two parts: Part 1 is a code of practice; Part 2 is a standard for the certification of an ISMS. See Figure 1 for a simplified overview of the development and Note 1 for a brief description of the history.

Figure 1. Simplified Overview of the Development of ISO/IEC 27001/27002



Source: Gartner (December 2011)

Since the BS 7799 standard was first published in 1995, the set of ISMS standards has evolved significantly, based in part on existing standards, covering areas like terminology, guidelines, metrics, certification and audits, as Figure 2 illustrates.

Figure 2. Overview of the ISO/IEC 2700 Series Standards

Publication	Content	Preceding/Related Standards	Published
ISO/IEC 27000	Vocabulary for the ISMS standards		2009
ISO/IEC 27001	Standard for ISMSs	BS 7799-2	2005
ISO/IEC 27002	Code of practice for ISMS	BS 7799-1, ISO/IEC 17799	2007
ISO/IEC 27003	ISMS implementation guide		2010
ISO/IEC 27004	ISMS measurements and metrics		2009
ISO/IEC 27005	Standard for information security risk management	ISO/IEC TR 13335-3 ISO/IEC TR 13335-4	2011
ISO/IEC 27006	Accreditation of ISMS certifiers	EA7/03, ISO 17021	2007
ISO/IEC 27007	Guideline for auditing of management system	ISO 19011	2011
ISO/IEC TR 27008	Guideline for auditing of controls		2011

Source: Gartner (December 2011)

The ISO/IEC group JTC 1/SC 27, which was responsible for ISO/IEC 27001, and related standardization bodies continue to work on ISMS standards, adjusting the concept to certain industry sectors or specific technologies (see Figure 3).

Figure 3. Overview of Industry Sector or Technology-Specific ISO/IEC 2700 Series Standards

Publication	Content	Focus	Status
ISO/IEC 27010	Intersector and interorganizational communications	Sector	Planned
ISO/IEC 27011	Telecommunications	Sector	Published in 2008
ISO/IEC 27015	Financial services	Sector	Planned
ISO/IEC 27017	Information security aspects of cloud computing	Technology	Planned
ISO/IEC 27018	Privacy aspects of cloud computing	Technology	Planned
ISO/IEC 27034	Application security	Technology	Planned
ISO/IEC 27040	Storage security	Technology	Planned
ISO/IEC 27799	Health sector	Sector	Published in 2008

Source: Gartner (December 2011)

Given the market recognition and wide support that ISO/IEC 27001 enjoys, one could assume that related standards will equally gain in importance. However, this will take several years, and in the

meantime, ISO/IEC 27001 will undergo some revision. Whether ISO/IEC can hold together this increasingly complex group of related standards remains unclear.

Motivation for Adoption Is Increasing

ISO/IEC 27001 is becoming more popular among Gartner clients. Worldwide, more than 7,500 organizations are already certified (more than 3,900 alone in Japan). In a Gartner survey published in 2011, 29% of respondents said they would support or consider ISO/IEC 2700x in the IT compliance projects that they undertook. This number is fairly high compared with other IT compliance initiatives, such as Statement on Auditing Standards (SAS) 70 (20%), Control Objectives for Information and Related Technology (COBIT — 19%), and the PCI Security Standards Council's Data Security Standard (DSS — 17%). Numbers vary significantly by country and company size, as Figure 4 illustrates.

Figure 4. Adoption of ISO 27001/27002

Which of the following regulations or standards does your organization support or take into account in your organization's IT compliance projects undertaken in 2010? (n=185, selected answers)

Annual Revenue			Multiple responses allowed, color coding shows ranking (green = top, red = bottom)	Total	Country						
$500 million to less than $1 billion	$1 billion to less than $3 billion	$3 billion or more			Australia	Canada	Germany	India	Japan	U.K.	U.S.
35%	34%	41%	**Audit requirements**	37%	45%	67%	16%	46%	50%	8%	38%
37%	36%	36%	**Privacy legislation**	36%	27%	57%	26%	50%	20%	42%	30%
25%	19%	41%	**ITIL**	31%	45%	38%	21%	38%	20%	46%	24%
21%	30%	34%	**ISO 27001/27002**	29%	27%	14%	37%	42%	40%	42%	22%
13%	15%	27%	**SAS 70**	20%	36%	14%	11%	42%		8%	21%
13%	17%	24%	**COBIT**	19%	36%	24%	21%	29%	20%		18%
17%	13%	19%	**PCI DSS**	17%		10%	16%	13%	10%	17%	24%
8%	19%	20%	**Common Criteria**	16%		14%	5%	29%	30%	13%	17%

Source: Gartner (December 2011)

However, this doesn't mean that these companies intend to become ISO/IEC-27001-certified. Many simply use ISO/IEC 27001/27002 as guidance for designing and implementing an ISMS, without intending to pursue a certification audit anytime soon. Organizations look to this standard because they realize that adopting ISO/IEC 27001 can have the following benefits:

- An organization that bases its information security program on ISO/IEC 27001 can be sure that it addresses all organization-specific aspects of information security — aspects that matter to that business outfit. It is not necessarily what most organizations worldwide believe should be part of the program. For this reason, the implementation includes use of the Statement of

Applicability, where the organization can justify why it does or does not implement controls and clauses and also has the liberty to add its own controls and clauses. Many organizations treat ISO/IEC 27001 — together with ISO/IEC 27002, which is actually the more detailed and commonly used component of the 27000 series — as a checklist that covers security policy, security organization, personal security, physical and environmental security, communications and operations management, access control, acquisition/development/maintenance of information systems, incident management, business continuity management, and compliance.

- Following the standard makes an organization's ISMS auditable and comparable with industry peers and/or previous years. It encourages an organization to define a scope for its ISMS (see Note 2 for a list of typical ISMS scopes), to follow a "plan, do, check, act" process cycle (a four-step model for carrying out change), and to decide which controls it believes the organization should implement. There's an increasing pool of skilled people who can tell an organization how well it's executing on its plan to follow the standard, and how the organization's efforts compare with the efforts of its industry peers.
- A successful ISO/IEC 27001 audit or certificate helps organizations demonstrate a level of due diligence that may satisfy regulatory requirements. Although no law explicitly requires ISO/IEC 27001 certification, some laws demand that organizations address risk management, and require them to follow best practices and apply due care. Following ISO/IEC 27001 is evidence of an organization's compliance efforts, especially since it became a widely recognized standard. For example, the government of India has come out with four notifications for its Information Technology (Amendment) Act, 2008 (see "Learn the Implications of IT Laws in India"). One of them states: "*The body corporate or a person on its behalf who has implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government.*"
- An implementation of ISO/IEC 27001 links different pieces together. An organization that decides to adopt the standard also will find support from various tools (especially tools that document, enforce and automate security controls), as well as assistance to map this information security standard to other IT and industry standards (such as ITIL, PCI DSS and COBIT) to facilitate the demonstration of compliance. As other standards of the ISO/IEC 27000 series evolve, and as an organization considers using them, it will find that ISO/IEC 27001 is at the heart of, and the basis for, much of this development.

Getting It Done — From Consulting Projects to Ongoing Certification Audits

Gartner has written a body of research for the creation and maintenance of an information security program (see Recommended Reading). Such a program is independent from any particular information security standard; it includes a security architecture, a governance structure, security policies and controls, measuring and reporting mechanisms, and a security awareness program. Within such a security program, organizations can use standards and technical reports for information security technologies — for example, ISO/IEC 21827:2002 (Systems Security

Engineering — Capability Maturity Model [SSE-CMM]), ISO/IEC TR 19791:2006 (security assessment of operational systems) or ISO/IEC 15408 (evaluation criteria for IT security [also known as Common Criteria]). Moreover, organizations can use a standard for an ISMS: ISO/IEC 27001.

Organizations that use ISO/IEC 27001 do so in a variety of ways. In many cases, they start with a consulting project, and later continue with a formal audit and certification.

1. Design information security based on ISO/IEC 27001: Organizations hire consultants or dedicate internal resources to:

- Establish an ISMS (for example, define scope and boundaries, define a policy that describes the organization and sets objectives, decide how to approach risk assessments and select controls).
- Implement and operate the ISMS (for example, implement controls and training programs, and manage resources).
- Monitor and review the ISMS (for example, measure effectiveness and review risk assessments).
- Improve and maintain the ISMS.

Note that there's a difference between standards compliance and certification. Many consulting firms say that they will implement security that's compliant with ISO/IEC 27001. However, this doesn't mean that the company will pass certification. The level of compliance is subjective, based on the view of the consulting firm, and will differ from what another consulting firm (or an auditor) would say.

Resources needed: The Big 4 auditing firms and many IT security consulting boutiques can help with general ISO/IEC 27001 guidance. Initial projects may take only a few months to complete. Special ISO/IEC 27001 training for the consultants is optional because general information security experience may be sufficient. Standard consulting charges apply.

2. Internal audit for alignment with ISO/IEC 27001: When an ISMS is in place — ideally, one that's considered compatible with the ISO/IEC 27001 standard — an internal audit of that ISMS can be used to prove compliance (or alignment with ISO/IEC 27001) to company management. This audit should happen at planned intervals, and confirm that the controls and processes of the ISMS are effectively implemented and maintained. An internal audit does nothing to contribute to the certification process, but helps get an objective view.

Resources needed: ISO/IEC 27001 isn't simply a detailed checklist, and an audit requires some experience. The auditor (such as an external consultant or someone from the internal audit department) should have a formal education (for example, "BSI Lead Auditor" or some other ISO/IEC-17024-approved training), and, ideally, would be accredited by the International Register of Certificated Auditors (IRCA — see www.irca.org/about/links.html to find a directory of auditors). However, to demonstrate standards conformance to internal management, it may not be mandatory to use a certified auditor.

3. Get an ISO/IEC 27001 compliance certificate: When an organization is confident that its ISMS conforms with the ISO/IEC 27001 standard, it may want to prove this compliance to an external party. This could be a business partner or a regulator, or the organization could use the ISO/IEC 27001 certificate to publicly market the organization's adherence to information security best practices. According to a Gartner survey, 65% of organizations are regularly audited by a third-party against accepted standards or guidelines — and ISO 27001 is one of them (see Evidence section). Note that a minimum set of documents must be produced to become certified, such as the Statement of Applicability, a risk assessment, and the statement of scope and boundaries to explain and justify which controls have been implemented and which have been excluded.

Resources needed: Organizations that can issue ISO/IEC 27001 certificates follow the standard for conformity assessments (ISO/IEC 27006, based on ISO/IEC 17021), which contains principles and requirements for the competence, consistency and impartiality of the audit and the certification of management systems. Such organizations must be accredited by a national accreditation body (see Note 3). Every accreditation body maintains a list of accredited national certifiers. There's no international register. As soon as a certifier has conducted a third-party audit and provided an ISO/IEC 27001 certificate, expect an assessment to occur every six to nine months. The certificate is valid for three years, after which the ISMS needs to be recertified. Fees for ISO/IEC 27001 certification are similar to ISO 9001:2000 or ISO 14001:2004 certification fees.

The types of audits listed above apply to organizations that want to be certified against ISO/IEC 27001. In addition, some organizations may want other organizations to comply with ISO/IEC 27001 — for example, their business partners, and, in particular, providers of managed security services. To verify compliance, an organization could audit the provider (assuming that internal skills exist) or (more likely) ask an external party to audit the provider for ISO/IEC 27001 compliance. Ideally, this would result in an ISO/IEC 27001 certification (see No. 3 above).

Organizations that want to audit their ISMSs and potentially get a certificate have three options to find an appropriate auditor or certifier:

- They can look for an accredited auditor (see No. 2 above).
- They can search a country's register of accredited certifiers (see Note 2).
- They can browse the unofficial register of certified organizations (see www.iso27001certificates.com), which is maintained by the ISMS International User Group and lists most certifiers (in addition to the certified organization and the country).

Names that appear in several countries are BSI Group, Bureau Veritas Certification, Det Norske Veritas (DNV), Certification Europe, LRQA and the TUV companies.

Best Practices for ISO/IEC 27001 Certification

- Audits and certifications cost time and money. Business owners are more inclined to invest in ISO/IEC 27001 certification if the benefit is apparent. This is the case if a business partner asks for the certificate. Then, ideally, the requester would give some guarantee that the supplier will get the deal if it passes the audit, to ensure that the investment pays off.

- There's a difference in complexity between designing an ISMS and gathering evidence for the audit. Organizations with operations in several countries should design an ISMS worldwide, such as with a global policy book and a global information security organization, albeit with local variations — according to legislation and business practices — and roles, respectively. However, gathering evidence for an audit and obtaining a certificate also can be conducted on a country-by-country basis, using a nationally accredited certifier.
- There's some similarity with other management system certifications — for example, a quality-management-system certification is an advantage, and ISO/IEC 27001 is explicitly compatible with ISO 9001. This experience should be leveraged, rather than starting an ISMS certification project wholly from scratch.
- Some companies have integrated ISMS auditing with internal auditing. For example, if internal auditing covers 40% of the organization every year, and ISMS auditing happens at the same time, then every business unit also would be ISMS-certified after two-and-a-half years. However, this depends on the ISO/IEC 27001 audit's scope.
- The scope of an ISO/IEC 27001 audit can be a particular system, process or application. Many organizations focus their first audit on a particular data center. They start with that data center, gather experience and then repeat the audit for their other data centers.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Q&A: 12 Characteristics of a World-Class Information Security Program"

"The Structure and Scope of an Effective Information Security Program"

"ITScore for Information Security"

"Survey Analysis: Information Security Governance, 2011"

"Information Security and Risk Governance: Functions and Processes"

"Building an Effective Sensitive Data Classification and Handling Policy"

"What Is a Risk Register, and Why Do You Need One?"

"Information Security Organization Dynamics"

"Controlling Staff Behavior Takes More Than Technology"

"Introducing the Gartner Information Security Governance Model"

"Learn the Implications of IT Laws in India"

Evidence

Various Gartner surveys covered ISO 27001/27002 acceptance in the market:

"Survey Analysis: Information Security Governance, 2011"

- Does your organization regularly audit external service providers against accepted standards or guidelines (e.g., ISO 27001/2, COBIT)?
  - Yes = 55% (n = 158)
- Is your organization regularly audited by a third party against accepted standards or guidelines (e.g., ISO 27001/2)?
  - Yes = 65% (n = 158)

"Survey Reveals Security and Compliance Emerging Practices for Cloud Infrastructure Services"

- For your organization's current/planned infrastructure utility service (IUS) contract, what kind of security or compliance features has your organization got in place in its deal?
  - Provider's ISO/IEC 27001 certification in current IUS contract (n = 101): 17%
  - Provider's ISO/IEC 27001 certification in planned IUS contract (n = 57): 42%
- For your organization's current/planned infrastructure as a service (IaaS) contract, what kind of security or compliance features has your organization got in place in its deal?
  - Provider's ISO/IEC 27001 certification in current IaaS contract (n = 65): 15%
  - Provider's ISO/IEC 27001 certification in planned IaaS contract (n = 50): 35%

Note 1 History of ISMS Standards

Before the British Standard BS 7799 became an international standard, some countries published their own ISMS standards that were similar to the British Standard (for example, UNE 71502 in Spain, DS 484 in Denmark and SS 62 77 99 in Sweden). Some people also refer to the ISMS standard as "BS 7799-1/-2" or "ISO/IEC 17799," although, strictly speaking, one must differentiate the British version from the international version, as well as the code of practice from the standard against which companies can get certified. One also could say that ISO/IEC 27001 (certification standard) is more the "what," whereas ISO/IEC 27002 (code of practice) contains more of the "how," and, therefore, practical implementation guidance.

Note 2 Typical ISMS Scopes

The International Register of ISMS Certificates at www.iso27001certificates.com shows the scope of about 5,000 certified organizations worldwide. Click on "Certificate Register." Then in the "Register Search," click on "ISMS Certificates." Finally, click the third and last "Search Query" button. You must use Internet Explorer.

Note 3 Accreditation of ISO/IEC 27001 Certifiers

Organizations that can issue ISO/IEC 27001 certificates must be accredited by a national body, such as:

- In the U.K., the United Kingdom Accreditation Service (UKAS)
- In the U.S., the American National Standards Institute-American Society for Quality National Accreditation Board (ANAB)
- In Germany, Deutscher Akkreditierungs Rat (DAR)/Tragergemeinschaft fur Akkreditierung (TGA)
- In Switzerland, the State Secretariat for Economic Affairs, Swiss Accreditation Service (SECO-SAS)

For other countries, see the member list of the International Accreditation Forum (IAF) at www.iaf.nu.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600