ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements *(second edition)*

Introduction

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called 'information security risks' in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (*e.g.* commercial enterprises, government agencies, non-profits), all sizes (from micro-businesses to huge multinationals), and all industries or markets (*e.g.* retail, banking, defense, healthcare, education and government). This is clearly a very wide brief.

ISO/IEC 27001 does *not* formally mandate specific information security controls since the controls that are required vary markedly across the wide range of organizations adopting the standard. The information security controls from ISO/IEC 27002 are noted in annex A to ISO/IEC 27001, rather like a menu. Organizations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information risks, drawing on those listed in the menu and potentially supplementing them with other *a la carte* options (sometimes known as extended control sets). As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organization's information risks, which is one vital part of the ISMS.

Furthermore, management may elect to avoid, transfer or accept information risks rather than mitigate them through controls - a risk treatment decision within the risk management process.

History

ISO/IEC 27001 is derived from BS 7799 Part 2, first published as such in **1999**.

BS 7799 Part 2 was revised by BSI in **2002**, explicitly incorporating the Plan-Do-Check-Act cyclic process.

BS 7799 part 2 was adopted as ISO/IEC 27001 in **2005**, with various changes to reflect its new custodians.

The standard was extensively revised in **2013**, bringing it into line with the other ISO certified management systems standards and dropping explicit reference to PDCA. See the timeline page for more.

Structure of the standard

ISO/IEC 27001:2013 has the following sections:

0 Introduction - the standard uses a process approach.

1 Scope - it specifies generic ISMS requirements suitable for organizations of any type, size or nature.

2 Normative references - only ISO/IEC 27000 is considered absolutely essential to users of '27001: the remaining ISO27k standards are optional.

3 Terms and definitions - a brief, formalized glossary, soon to be superseded by ISO/IEC 27000.

4 Context of the organization - understanding the organizational context, the needs and expectations of 'interested parties', and defining the scope of the

ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" a compliant ISMS.

5 Leadership - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.

6 Planning - outlines the process to identify, analyze and plan to treat information risks, and clarify the *objectives* of information security.

7 Support - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.

8 Operation - a bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).

9 Performance evaluation - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system in order to make systematic improvements where appropriate.

10 Improvement - address the findings of audits and reviews (*e.g.* nonconformities and corrective actions), make continual refinements to the ISMS

Annex A Reference control objectives and controls - little more in fact than a list of titles of the control sections in ISO/IEC 27002. The annex is 'normative', implying that certified organizations are expected to use it, but they are free to deviate from or supplement it in order to address their particular information risks.

Bibliography - points readers to five related standards, plus part 1 of the ISO/IEC directives, for more information. In addition, ISO/IEC 27000 is identified

in the body of the standard as a normative (*i.e.* essential) standard and there are several references to ISO 31000 on risk management.

Mandatory requirements for certification

ISO/IEC 27001 is a formalized specification for an ISMS with two distinct purposes:

1. It lays out, at a fairly high level, what an organization can do in order to implement an ISMS;
2. It can (optionally) be used as the basis for formal compliance assessment by accredited certification auditors in order to certify an organization.

The following mandatory documentation (or rather "documented information" in the curiously stilted language of the standard) is explicitly required for certification:

1. ISMS scope (as per clause 4.3)
2. Information security policy (clause 5.2)
3. Information risk assessment *process* (clause 6.1.2)
4. Information risk treatment *process* (clause 6.1.3)
5. Information security objectives (clause 6.2)
6. Evidence of the competence of the people working in information security (clause 7.2)
7. Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
8. Operational planning and control documents (clause 8.1)
9. The *results* of the risk assessments (clause 8.2)
10. The *decisions* regarding risk treatment (clause 8.3)
11. Evidence of the monitoring and measurement of information security (clause 9.1)
12. The ISMS internal audit program and the results of audits conducted (clause 9.2)
13. Evidence of top management reviews of the ISMS (clause 9.3)

14. Evidence of nonconformities identified and corrective actions arising (clause 10.1)
15. Various others: Annex A, which is normative, mentions but does not fully specify further documentation including the rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, information security incident response procedures, relevant laws, regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

Certification auditors will almost certainly check that these fifteen types of documentation are (a) present, and (b) fit for purpose. The standard does not specify precisely what form the documentation should take, but section 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a fairly formal ISO 9000-style approach. Electronic documentation (such as intranet pages) are just as good as paper documents, in fact better in the sense that they are easier to control.

ISMS scope, and Statement of Applicability (SoA)

Whereas the standard is *intended* to drive the implementation of an enterprise-wide ISMS, ensuring that all parts of the organization benefit by addressing their information risks in an appropriate and systematically-managed manner, organizations can scope their ISMS as broadly or as narrowly as they wish - indeed scoping is a crucial decision for senior management (clause 4.3). A documented ISMS **scope** is one of the *mandatory* requirements for certification.

Although the "Statement of Applicability" (**SoA**) is not explicitly defined, it is a mandatory requirement of section 6.1.3. This commonplace term refers to the output from the information risk assessments and, in particular, the decisions around treating those risks. The SoA may, for instance, take the form of a matrix identifying various types of information risks on one axis, and risk treatment options on the other,

showing how the risks are to be treated in the body, and perhaps who is accountable for them. It usually references the relevant controls from ISO/IEC 27002, but the organization may use a different framework such as NIST SP800-55, the ISF standard, BMIS and/or COBIT or a custom approach. The information security control objectives and controls from ISO/IEC 27002 are provided as a checklist at Annex A in order to avoid 'overlooking necessary controls'.

The ISMS scope and SoA are crucial if a third party intends to attach any reliance to an organization's ISO/IEC 27001 compliance certificate. If an organization's ISO/IEC 27001 scope only notes "Acme Ltd. Department X", for example, the associated certificate says absolutely nothing about the state of information security in "Acme Ltd. Department Y" or indeed "Acme Ltd." as a whole. Similarly, if for some reason management decides to accept malware risks without implementing conventional antivirus controls, the certification auditors may well challenge such a bold assertion but, *provided* the associated analyses and decisions were sound, that alone would not be justification to refuse to certify the organization since antivirus controls are not in fact mandatory.

Metrics

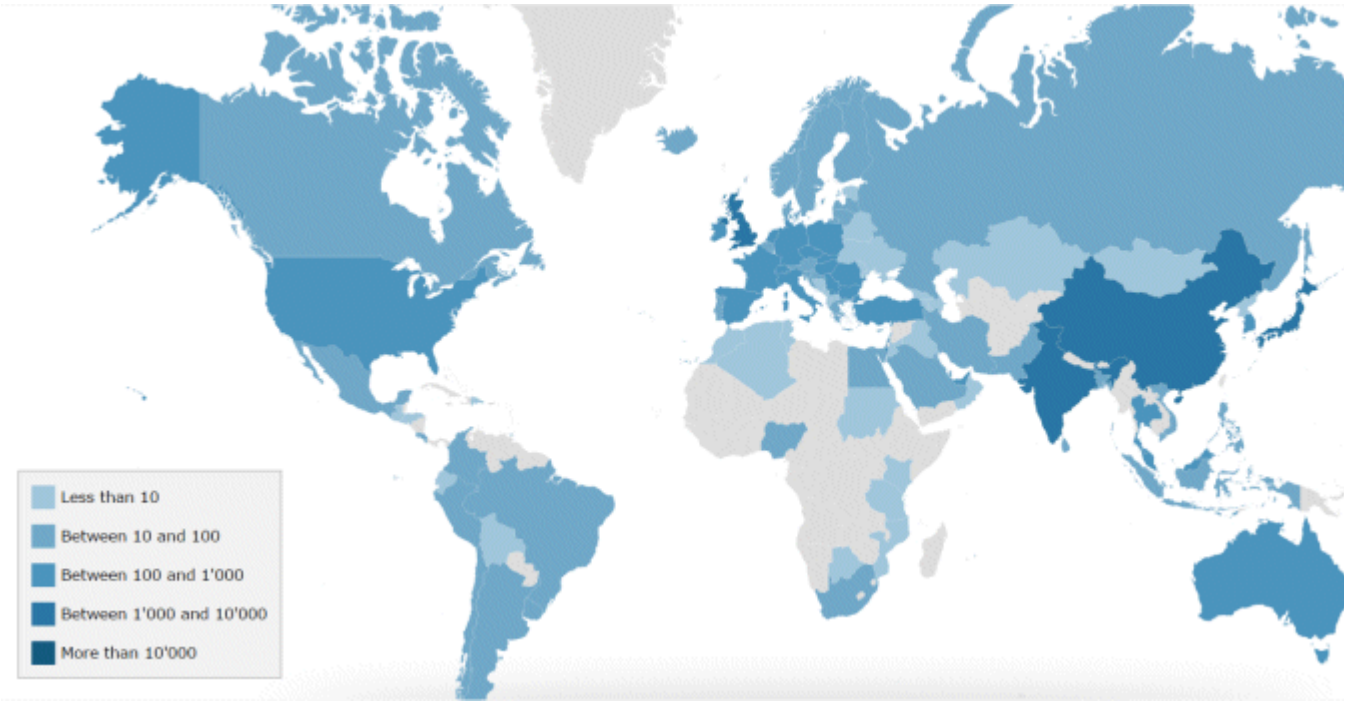
In effect (without actually using the term "metrics"), the 2013 edition of the standard requires the use of metrics on the performance and effectiveness of the organization's ISMS and information security controls. Section 9, "Performance evaluation", requires the organization to determine and implement suitable security metrics ... but gives only high level requirements.

When the revised version is released, ISO/IEC 27004 will offer advice on what and how to measure in order to satisfy the requirement. Meanwhile, we recommend the approach described in **PRAGMATIC** Security Metrics!

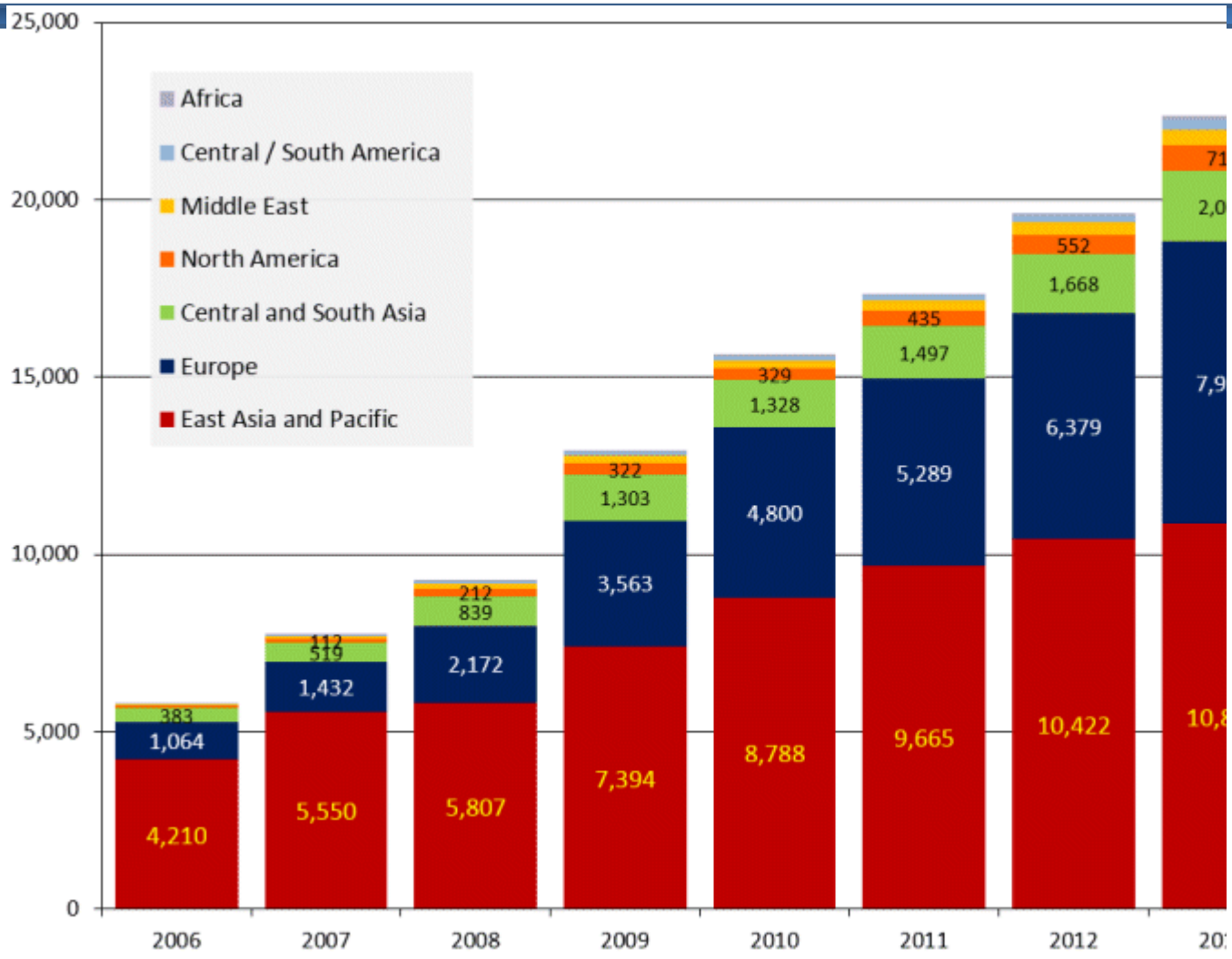
Certification

Certified compliance with ISO/IEC 27001 by an accredited and respected certification body is entirely optional but is increasingly being demanded from suppliers and business partners by organizations that are (quite rightly!) concerned about the security of their information, and about information security throughout the supply chain or network.

According to the ISO survey for 2014, there were just under 24,000 ISO/IEC 27001 certificates worldwide:



The number of ISO/IEC 27001 certificates is growing steadily year-on-year:



Certification brings a number of benefits above and beyond mere compliance, in much the same way that an ISO 9000-series certificate says more than just "We are a quality organization". Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires senior management approval (which is an advantage in security awareness terms, at least!).

The certificate has marketing potential and demonstrates that the organization takes information security management seriously. However, as noted above, the assurance value of the certificate is highly dependent on the ISMS scope and SoA - in other words, **don't put too much faith in an organization's ISO/IEC 27001 compliance certificate if you are highly dependent on its information security.** In just the same

way that certified PCI-DSS compliance does *not* mean "We guarantee to secure credit card data and other personal information", certified ISO/IEC 27001 compliance is a positive sign but *not* a cast-iron guarantee about an organization's information security. It says "We have a compliant ISMS in place", not "We are secure". That's an important distinction.

Status of the standard

ISO/IEC 27001 was completely rewritten and re-issued in **September 2013**. This was far more than just tweaking the content of the 2005 edition since ISO/IEC JTC1 insisted on substantial changes to align this standard with other management systems standards covering quality assurance, environmental protection *etc.* The idea is that managers who are familiar with any of the ISO management systems will understand the basic principles underpinning an ISMS. Concepts such as certification, policy, nonconformance, document control, internal audits and management reviews are common to all the management systems standards, and in fact the processes can, to a large extent, be standardized within the organization.

ISO/IEC 27001:2013 is available now from the usual outlets.

ISO/IEC 27002 was extensively revised and re-issued at the same time, hence Annex A to ISO/IEC 27001 was completely updated too: see the ISO/IEC 27002 page for more.

A **technical corrigendum** published in October 2014 clarified that *information* is, after all, an asset.

A further **technical corrigendum** was published in December 2015, clarifying that organizations are formally required to identify the implementation status of their information security controls in the SoA.