

Information Security Management and IT Audit

By Vernon Poole

Why the emerging ISO 27000 series are vital for business resilience

Background

Many readers will remember the early days of BS7799 when efforts were made to establish a UK code of practice on information security management. From 1989 onwards, attempts were made to convert this standard into an international standard (ISO 17799) and it soon became obvious that, as information security threats and vulnerabilities grew, an acceptable global standard ISO 27001 would emerge.

ISO 27001 was the first move by the ISO community to align information security management with the quality management standard (ISO 9001).

There is now an ISO 27000 series of standards that IT auditors need to be aware of and this article outlines their emergence and progress, and how they will be valuable tools for IT auditors to adopt.

ISO 27000 series – Introduction

The initial family of ISO 27000 series covered the following seven areas (see overleaf):



Including:

Forthcoming Audit Events **p5**
CIPFA Audit Panel Vacancies **p6**

AT THE HEART OF
PUBLIC SERVICES



- **ISO 27000** – Fundamentals and Vocabulary (under development)
- **ISO 27001** – ISMS Requirements (BS7799 – Part 2) from 2005
- **ISO 27002** – (ISO/IEC 17799:2005) from July 2007
- **ISO 27003** – ISMS Implementation Guidance (under development)
- **ISO 27004** – ISMS Metrics and Measurement (under development)
- **ISO 27005** – ISMS Risk Management (under development)
- **ISO 27006** – Guidelines on ISMS accreditation for certifiers from January 2007.

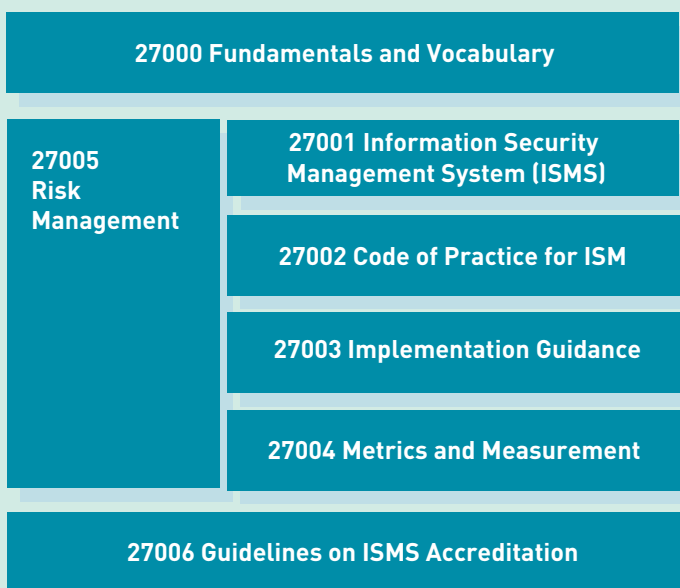
The initial aspect for IT auditors to understand is that:

- ISO 27001 is the certification process to gain compliance or certification
- ISO 27002 is the Code of Practice (11 guiding principles; 133 detailed controls).

The other 27000 standards are additional pieces of guidance and advice to assist organisations to establish a consistent framework on information security management: the emphasis is on information security (IS) **not** IT because of the wider governance requirements. There are now developments on auditing (ISO 27007) and other guidance will be added over time. A key issue will be the emergence of sector-specific guides.

These seven areas can be viewed pictorially:

Structure of 27000 Series



ISO 27000 series – in detail

1. ISO 27000 Fundamentals and Vocabulary

Once finalised, this standard will:

- explain the terminology for all the 27000 series family of standards
- address global concerns on definitions that vary from country to country to establish consistency.

The clarity that ISO 27000 will bring should not be underestimated. Its principles will impact on other standards like COBIT (IT Processes) and ITIL (IT Service Delivery) and will try to avoid confusion. Debate and arguments regularly take place between organisations (especially in an outsourced environment) or professional bodies on various terms like network security or risk assessment; ISO 27000 should bring about clarity.

The publication date for this standard is scheduled for 2009.

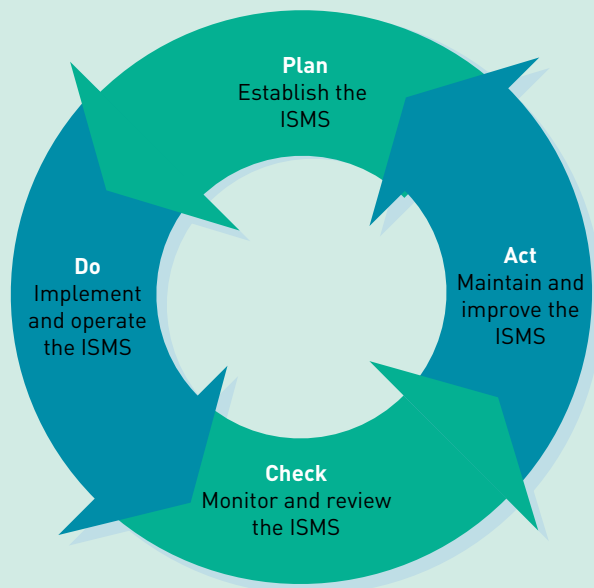
2. ISO 27001 Information Security Management System (November 2005)

This standard allowed for certification to the Code of Practice on Information Security Management (ISO 27002) with effect from 30 January 2006. Clearly, for many public sector bodies, compliance is as far as most organisations are proceeding at present. There is however an emerging scheme under which organisations can seek 'advanced compliance' when the ISMS framework is reviewed annually by a third party.

The standard clarifies and improves on PDCA process requirements, namely:

- ISMS scope
- approach to risk assessment
- selection of controls
- statement of applicability
- reviewing risks
- management commitment
- ISMS internal audits
- results of effectiveness and measurements
- update risk treatment plans/procedures and controls.

PDCA Model



The demand for ISO certification is currently growing at the rate of 150 organisations per month: there are now 4,000 certifications with over 1,000 new certifications in the last 12 months (previous certifications were up to BS7799-2 status though many have been upgraded consequently). This growth can be attributed to many factors but the overriding reason is that organisations are making this standard a contractual, regulatory (eg the e-gov directive) or service level agreement requirement – leading to a major driver for its take-up. This take-up is across both private and public sectors. Therefore, IT auditors need to monitor the ISO certification website www.iso27001certification.com and be aware of which organisations are becoming certified in their sector.

3. ISO 27002 Code of Practice for Information Security Management (July 2007)

This standard replaces ISO/IEC 17799:2005 and includes:

- 11 sections specifying 39 control objectives to protect information assets.
- 133 best practice controls adoptable on a risk assessment process. Organisations are also free to select controls not listed in the standard, which allows for great flexibility in implementation (but can be challenging for certification bodies).

The standard is updated every three years, the most recent changes covering:

- security of external service delivery and provisioning of outsourcing

- patch management
- security prior to, during and at termination of employment (HR controls)
- guidance on risk management
- a section on incident management
- mobile, remote and distributed communications.

ISO 27002 is now deployed as the **global de facto standard**. IT auditors need to understand it in detail and utilise its guidance in all their assignments.

4. ISO 27003 Implementation Guidance

This standard will utilise the appendix that was attached to the former BS7799-2 and which contains:

- an overview
- management responsibilities
- governance and regulatory compliance
- personal security and human resources
- asset management
- availability/continuity of business processes
- handling information incidents
- access control
- risk management case studies.

The publication date for this standard is scheduled for 2009.

5. ISO 27004 Metrics and Measurement

This standard is aimed at addressing how to measure the effectiveness of ISMS implementations (processes and controls) and will include:

- performance targets
- what to measure
- how to measure
- when to measure.

The measurement programme objectives are to:

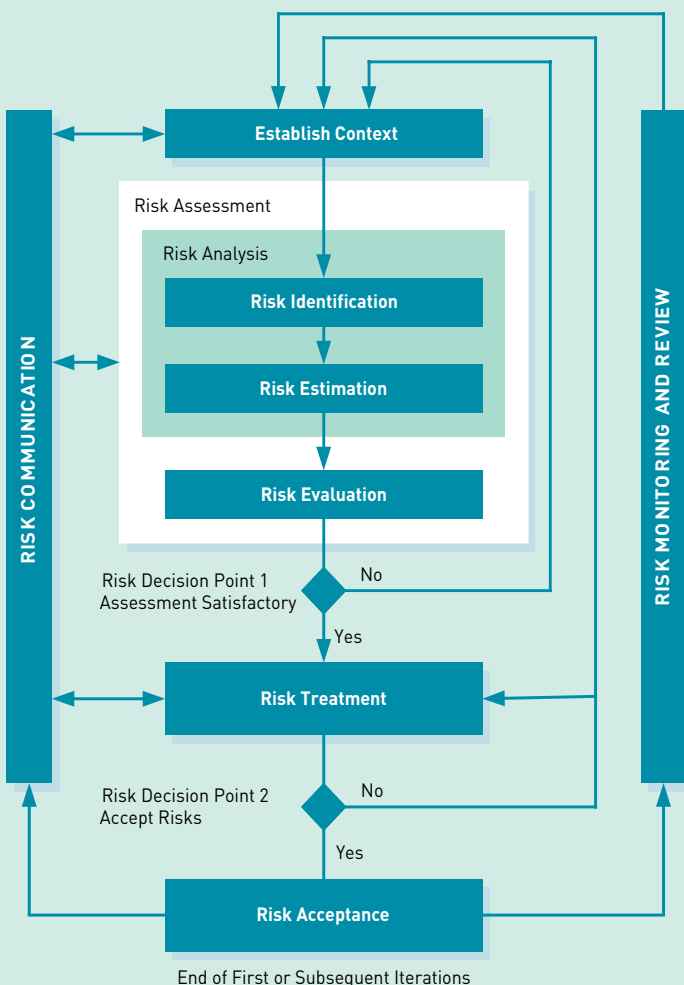
- evaluate the effectiveness of security controls and control objectives
- evaluate the effectiveness of the ISMS including continual improvement
- provide security indicators to assist management review
- facilitate improvement of information security
- provide input for security audits

- communicate the effectiveness of ISM to the organisation
- serve as an input into the risk management process
- provide output for internal comparison and benchmarking of effectiveness.

The publication date for this standard is scheduled for 2008.

6. ISO 27005 Risk Management

This is a new standard on information security risk management. This requirement has caused difficulties for many organisations who have been trying to achieve ISO 27001 certification, because for most organisations, information security risk management is either very poor or not recognised from a corporate risk register perspective. Therefore, this standard is eagerly awaited; the following outline explains how it will be developed:



- IS Risk Assessment
 - Risk analysis
 - Identification of assets

- Identification of threats
- Identification of vulnerabilities

- Information Security Risk Treatment
- Annex A – Scope
- Annex B – Identification/valuation of assets
- Annex C – Common vulnerabilities.

The publication date for this standard is scheduled for 2009.

7. ISO 27006 Guidelines on ISMS Accreditation (January 2007)

The international ISO 27000 community realised that the guidance to certification and registration bodies (EA7/03) was now outdated. There was a need for increased rigour and evidence from certifying bodies that the organisations seeking certification are 'fit for purpose,' ie that a robust ISMS framework is not only well established and meeting business needs, but also well communicated and is working in practice.

These guidelines became operational from January 2007 as launched at 'ISO 27000 Business goes Global' in London.

The new standard covers:

- general requirements – including guidance on 'impartiality'
- organisational structure – ISO/IEC 17021:2006 will apply, as it contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems
- resource requirements – ie guidance on management competence (for example, subcontracting)
- information requirements – including guidance on certification issues
- process requirements – guidance on ISMS audits.

There are three new main annexes:

- A1: Analysis of Complexity (of ISMS)
- A2: Example Areas of Auditor Competence (over different controls)
- A3: Audit Time (calculations).

Plus A4: Guidance on Reviewing Annex A controls.

8. Additional ISO 27000 Series Standards Being Discussed

ISO 27007 Guidelines for ISMS Auditing: This standard will provide guidance for audit and accredited certification bodies auditing ISMS – it will draw heavily on ISO 19011:2002 (the ISO standard for auditing quality and environmental management systems).

The publication date for this standard will not be until 2009 (currently not scheduled).

ISO 27011 ISM Guidelines for Telecommunications: The publication date for this standard will probably be 2010.

ISO 27031 ICT Readiness for Business Continuity

ISO 27032 Guidelines for Cybersecurity

ISO 27033 IT Network Security

ISO 27034 Guidelines for Application Security

There are, as yet, no publication dates for these particular guides.

ISO 27799 Security Management in Health using ISO 27002 (draft): This standard is currently being discussed because of its alignment issue.

NB There are other sector-specific guides being considered for the lottery, automotive and finance sectors.

Conclusion

IT auditors can see that there is a wealth of valuable guidance being prepared which is gaining global acceptance for a consistent approach to information security management issues. This guidance will assist you in helping your organisation to adopt best practice or identify the benefits and obstacles to implementing them.

I will review this article next year to keep you up to date with developments.

This article was submitted by Vernon Poole – CIPFA Audit Panel representative on IT Audit.

The views expressed in this article are based on the author's experience in deploying these standards over 17 years. The author is willing to receive comments or provide further information via vernon.poole@sapphire.net

Forthcoming Audit Events

Good Governance and Leadership – Is the Chief Executive Ready for the Mandatory Statement? 22 November 2007, Central London

Following last year's successful *Delivering Good Governance* event, CIPFA is delighted to present this year's local government corporate governance conference. The event will once again bring together an impressive line-up of speakers, each having had significant involvement in the consultation and development of the revised CIPFA/SOLACE *Delivering Good Governance in Local Government* framework and guidance (2007).

It will complement and add depth to proposals presented in the framework and guidance and will provide an opportunity for delegates to pose questions and gauge practical solutions to common governance challenges.

Aimed at practitioners working within local, fire and police authorities, this conference will benefit attendees by highlighting good practice approaches to governance and will enable delegates to identify the areas most pertinent to their organisation.

Chaired by John Whiteoak, Chairman of the CIPFA *Delivering Good Governance in Local Government* working group, topics covered will include:

- The New Governance Statements
- Links with CPA and KLOEs
- Leadership and Engagement
- Local Area Agreements
- 'Joined-up' Working with Health and Police
- Assurances and Compliance
- Reporting
- Audit Commission Diagnostics
- Case Studies and National Pilots.



This event is ideal for: senior managers involved in policy, law and finance, monitoring officers, directors of finance and treasurers, scrutiny and democratic service managers, partners and managers from private sector firms, heads of audit and legal departments, and corporate risk managers from local authorities throughout the UK including fire and police authorities.

For further information, including pricing, visit www.cipfa.org.uk/shop

CIPFA Technical Audit Update, 13 December 2007, Central London

Carefully tailored to provide a comprehensive insight into the current issues and developments driving internal audit and governance, this event will equip delegates with a firm grasp of the challenges that will face organisations in the coming months.

The day's objective is to highlight recent developments and to provide an insight into key practices that enable greater effectiveness across the management of the audit function.

Our esteemed speakers, whose expertise covers the scope of audit issues and governance, will draw on practitioner and policy-making experience to bring you the latest update on the issues of the day, and provide guidance on the range of tools and approaches that are instrumental in the development and management of systems. In addition, delegates will receive an update on the recent changes in good governance recommendations and the implications for internal audit. Other topics will include:

- Comprehensive Spending Review 2007
- The CIPFA/SOLACE Governance Framework
- Contract and procurement audit
- Implementing IFRS
- Resourcing the audit and assurance function
- IT audit and security.

This event is ideal for: practitioners working across the internal audit function in the public sector.

For further information, including pricing, please contact Claire Howard on 020 7543 5628, email claire.howard@cipfa.org or visit www.cipfa.org.uk/shop

CIPFA Audit Panel Member Vacancies

The Panel is looking to find a new member in the further and higher education sector and is keen to receive expressions of interest from practitioners in this sector from anywhere in the UK. If you are interested in joining the Panel, or would like to find out more about what membership would entail, please contact keeley.lund@cipfa.org

Both CIPFA and non-CIPFA members are welcome to apply. Expressions of interest in membership will be considered at the next Panel meeting. We look forward to hearing from you.

@ If you want to stay informed about all of CIPFA's forthcoming and recently published titles, as well as upcoming events, subscribe to CIPFA's free bimonthly courses, conferences and publications e-newsletter at www.cipfa.org.uk/shop_subscribe.cfm

© *Audit Viewpoint* is brought to you by the Audit Panel of CIPFA (The Chartered Institute of Public Finance and Accountancy)
Tel: 020 7543 5600

Audit Viewpoint is edited by Keeley Lund.
Any submissions should be mailed to:

Keeley Lund
(Technical Manager) Professional Standards and Guidance
CIPFA, 3 Robert Street, London WC2N 6RL

Tel: 020 7543 5600
Fax: 020 7543 5695
E-mail: keeley.lund@cipfa.org

Registered with the Charity Commissioners of England and Wales, Number 231060.



INVESTOR IN PEOPLE



Designed and typeset by
Ministry of Design
(www.ministryofdesign.co.uk)