ISO/IEC 27001 Foundation: A new qualification to help you understand this information security standard

Tracey Caldwell & Steve Johnson

APMG-International
Accrediting Professionals

APMG-International ™
ISO/IEC 27001

APMG-International ™
ISO/IEC 27001

Many organizations have implemented a raft of security controls and point solutions to address the issue of information security. Too often, the IT department handles information security management, resulting in a focus on technical solutions, leaving other information sources vulnerable. There is a growing need for a co-ordinated, systemic approach.

Organizations increasingly need to demonstrate that they have a well-documented management system, not only to make sure they are meeting their own information security objectives but also to comply with regulations, legislation, industry mandates and to meet the expectations of customers and partners.

ISO/IEC 27001 is an international standard that provides a framework for establishing an Information Security Management System (ISMS). The standard is designed to help organizations of all sizes and types to select suitable and proportionate security controls for information held electronically, on paper or other media. It provides a structured approach to help organizations work through their business processes, identify their information security weaknesses and create a tailored ISMS that takes account of their business risks.

APMG's ISO/IEC 27001 Foundation training and qualification is recommended for people who are working to implement or maintain an ISMS within an organization or whose role calls for them to audit an ISMS. It satisfies the need to have a thorough, basic understanding of the standard.

This white paper provides an overview of the ISO/IEC 27001 standard for information security management systems and highlights the benefits of certification for organizations.

Business context

Information security management is a major issue worldwide.

The US Privacy Rights Clearing House reports that 543m records have been breached in the US since 2005. In 2011 alone, Verizon's Data Breach Investigations Report found that 174m records were compromised in a total of 855 data breaches in what it called an "an all-time low" for information protection. This isn't just a problem for large organizations; the same report outlined an increasing trend that sees a growing proportion of these breaches happen in small- and medium-sized businesses, year on year.

Regulatory Compliance

In Europe, the EC is working on a major overhaul of data protection rules to strengthen online privacy rights. It is looking to reflect the fact that technological progress and globalisation have changed the way data is collected, accessed and used since the EU first put in place data protection rules in 1995. The 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. The plan is that a new single law will replace all the country-specific laws.

In the UK, the Information Commissioner's Office (ICO), the body responsible for enforcing data protection law, has been coming down hard on transgressors. In September 2012, for example, it fined Scottish Borders Council £250,000 after the council employed an outside company to digitise records, but failed to seek appropriate guarantees on how the personal data would be kept secure. Former employees' pension records were found in a paper recycling bank in a supermarket car park.

In the same month the ICO published guidelines reminding organizations that they remain responsible for how personal data is looked after, even if they pass it to cloud computing service providers.

ISO/IEC 27001 provides organizations with a recognized approach to information security based upon industry best practice that will enable them to comply with the rising tide of data protection rules and regulations.

Press reports and regulatory bodies have often criticized the way that some organizations have handled data breaches as people were left wondering whether or not their personal data was affected. Late and partial disclosure of a breach does not show any organization in a good light and reputational damage is likely to lead to other consequential losses.

ISO/IEC 27001 acknowledges that there can never be a guarantee that systems will not be breached or data lost or stolen. Demonstrating the protective controls that the ISMS has put in place and initiating a prepared, controlled response following any suspected data breach or loss can reduce reputational risk and mitigate regulatory or legal action that may result.

Resilience and Continuity

Loss of business-critical information or the environment supporting business operations can, of course, have a catastrophic impact beyond simple capital and revenue losses. ISO/IEC 27001 guides the organization to assess and apply proportionate controls to mitigate these risks and support business continuity. If a disaster situation arises, the ISMS will have a prepared response that integrates with any existing initiative to ensure a managed return to service.

Information security extends beyond the protection of the personal information of customers and end-users. Adoption of an ISMS should be a strategic decision, as the design of the system will need to take account of other information of value to the organization such as company records, the intellectual property of products and designs and sensitive commercial information.

Strategic Governance

The ISMS is also moulded by the business objectives of the organization, its current and planned size and structure. The ISMS supports due diligence prior to acquisitions or mergers; it underpins controlled disposal of organizational operations and assets; it assists with impact analyses of internal organizational changes and restructuring; it enables informed decisions at the highest levels.

ISO/IEC 27001 allows organizations to manage information assets in an organized way, facilitating continual improvement and adaptation to changing goals. It is about creating and maintaining a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness. It helps to build customer, partner and shareholder confidence in the mature governance of the organization and resilience of the business.

Overview of ISO 27001

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) together form the body for worldwide standardization.

ISO/IEC 27001 was published in October 2005, replacing the old BS7799-2 standard that was first published in the 1990s to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS.

An organization needs to identify and manage many activities in order to function effectively. The standard takes a process-based approach, first enabling people to identify the processes that happen within their organizations and how the various processes overlap and interact

It adopts the Plan-Do-Check-Act (PDCA) model:

Plan
The planning starts when the organization decides to work with the standard and the first step is getting management commitment to it. The planning stage includes gaining an understanding of an organization's information security requirements by means of a risk assessment to determine the organization's risk exposure.

Do
The next stage will be selecting appropriate controls to manage those risks, recording the justification for each decision, implementing and operating controls to manage an organization's information security risks in the context of its business risks.

Check
This comprises the monitoring and reviewing of the performance and the effectiveness of the ISMS. Are the controls effective in reducing risks? Are the objectives being achieved?

Act
Continual improvement based on objective measurements taken during the process of monitoring and reviewing the system.

ISO/IEC 27001 is one of a number of documents in the ISO 27000 family that applies to information security. Fundamental to ISMS implementation are:

ISO/IEC 27001:2005 specifies formal requirements for an ISMS and forms the basis for certification. It is mandatory to meet all requirements in Clauses 4 – 8. Annex A contains a list of controls that must be met unless exclusion can be justified. Further controls can also be added to this list to satisfy legal, regulatory or business requirements.

ISO/IEC 27002:2005 provides implementation advice and best practice guidance in support of the controls found in Annex A of ISO/IEC 27001.

ISO/IEC 27003:2010 offers practical guidance for the successful implementation of an ISMS in accordance with ISO/IEC 27001.

ISO/IEC 27004:2009 documents guidelines on the development and use of measurements in order to assess the effectiveness of the ISMS, control objectives and controls used to implement and manage information security as specified in ISO/IEC 27001.

ISO/IEC 27005:2011 provides advice on implementing a process-oriented risk management approach to assist in implementing the requirements of information security risk management in ISO/IEC 27001.

ISO/IEC 27006:2011 specifies requirements and provides guidance for Accredited Certification Bodies (ACBs) providing audit and certification of an ISMS in accordance with ISO/IEC 27001. It supports the accreditation of certification bodies and provides those considering certification with a useful insight into how external certification auditors will expect to work with them.

Why certification?

Organizations and individuals may use the ISO/IEC 27001 standard as a framework when developing an Information Security Management System. The scheme enables independent external ACBs to audit the ISMS and certify that the requirements of the standard have been met.

Certification is not compulsory, but it is evidence of independent verification and validation of an established, embedded and effective ISMS.

The initial process of certification is normally a three-stage audit by an ACB beginning with an informal review and progressing to a detailed check that the provisions of ISO/IEC 27001 have been met. After initial certification, ACBs carry out follow-up audits at least once a year and more usually every six months for a large organization. These surveillance audits sample the ISMS to verify its continued compliance. Every three years there is a full re-certification audit to make sure the entire ISMS remains compliant.

Holistic approach

Information security is just one of a number of areas where organizations seek market differentiation and independent confirmation of mature governance and operations through certification. ISO/IEC 27001 stands alongside the ISO/IEC 9001 quality management system and ISO/IEC 14001 environmental management system standards as one of the major process-based standards to which organizations are looking to achieve certification. These standards share a structure of creating a policy-based approach supported by top management. They also share requirements for internal auditing to make sure that systems are effective and for that information to be passed to top management for review. Applied together, these standards are able to create a robust, integrated management system.

Organizations that achieve an ISO/IEC 27001 compliant system are already able to use parts of that development to inform their approach to other management systems. Already many enterprises achieve certification to both ISO/IEC 27001 and ISO/IEC 20000-1 for IT Service Management Systems (ITSMS), complementing ITIL implementation.

As the ISMS considers information assets and operational environmental controls that protect those assets, further synergies are found with BS ISO 22301:2012 which specifies the requirements for setting up and managing an effective Business Continuity Management System (BCMS).

What happens after initial certification?

It takes quite a concentrated effort to develop a system ready for audit by an external party. The certification process does not stop there, however. It is better viewed as embarking on a journey rather than reaching a destination.

The organization must review systems and processes continuously to ensure that information security remains effective with the current practices in the organization, the types of information it is holding and the way in which it is operating systems.

Businesses need be sure to update security plans to take into account the findings of monitoring and reviewing activities and record all actions and events that could have an impact on the effectiveness or performance of the ISMS.

The benefits of ISO/IEC 27001 certification

ISO/IEC 27001 provides organizations with a clear framework for ensuring the security of their information systems. Certification brings independent confirmation that this remains compliant with the standard.

Certification provides a clear competitive advantage for companies in many sectors. Those providing services and managing and holding data for clients will be only too aware of their responsibility to ensure information is held securely and the need to be able to show they are doing so.

The public sector, from central to local government and related governmental organisations, holds volumes of personal information across multiple systems and can ill afford a fine from the Information Commissioner if it fails to protect that information from disclosure.

The financial sector too, stands to lose in both monetary and reputational terms if it fails to ensure information security. Financial organizations must comply with growing legislation and regulation from bodies such as the FSA that encompass the need to employ secure information management.

The healthcare sector also holds sensitive personal data, much of it still on paper, some of it on ICT-based systems. This sector faces the challenge of sharing some of its data with other agencies.

These sectors are the frontrunners in achieving ISO/IEC 27001 certification. It is certain that many others, particularly those who partner with or supply products or services to organizations in these sectors, see the benefit of being able to show that they operate an independently-certified information security management system.

ISO/IEC 27001 certification is often a key part of the pre-tender and purchasing process as the customer in turn will be looking to demonstrate that they have carried out due diligence in selecting a supplier.

In these challenging times businesses are often open to merger or acquisition. ISO/IEC 27001 accreditation provides a clear view of the business' information security processes allowing for efficient business change such as mergers with other businesses, interdepartmental mergers or partnership working.

Of course, while ISO/IEC 27001 certification is highly valuable for businesses wishing to demonstrate solid information security to any interested parties, just as importantly it creates a strong foundation for the business to grow and develop. Companies can introduce new products and services confident that a strong framework of information security supports them.

The ISO/IEC 27001 Foundation Qualification from APMG: Fast track your knowledge of the standard and how to apply it in practice

APMG's ISO/IEC 27001 Foundation Qualification takes you through the fundamentals of the standard. Passing the exam provides proof that you understand the standard and are able to apply it in practice.

The Foundation level exam assesses knowledge of the contents and high level requirements of the standard. It is a multiple-choice examination consisting of 50 questions to be completed in 40 minutes. Candidates must achieve 25 correct answers (50%) to pass.

Taking the qualification provides you with confidence to work effectively with best practice guidelines in the sensitive area of information security. The ISO/IEC 27001 Foundation qualification gives them much sought after, demonstrable skills in information security management.

Approved training is available via an international network of APMG-International Accredited Training Organizations (ATOs). Full details are available on our web site.

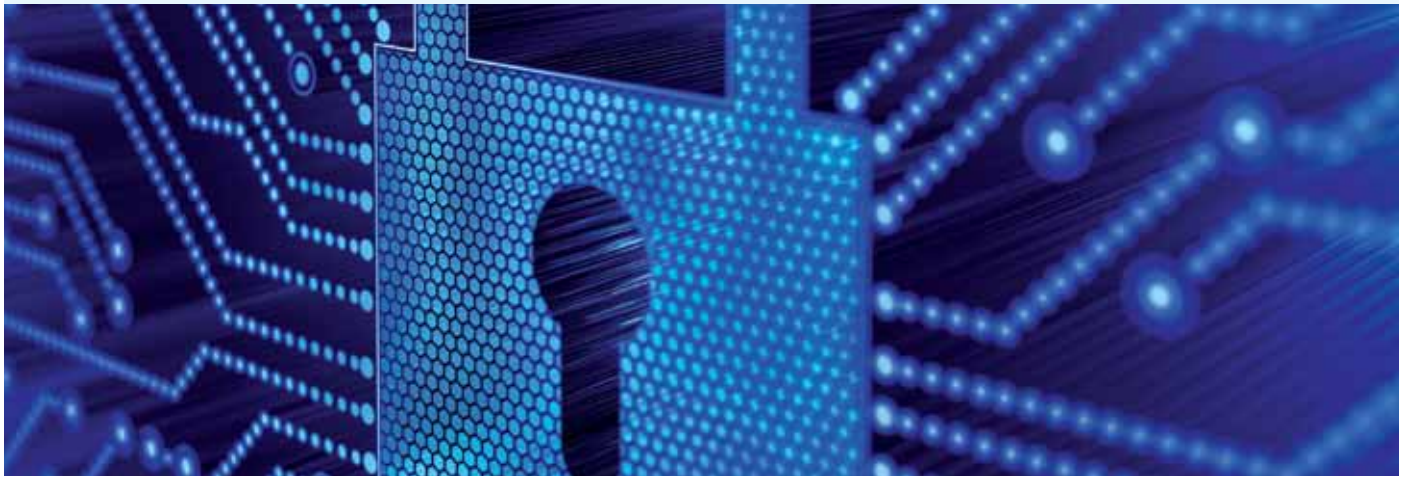
Conclusion

If information security is breached, the repercussions can range from heavy penalties to legal action that could threaten the viability of the business or have a major impact on the funds available to deliver services.

There is a pressing need to recognise that a holistic approach is needed to organization-wide information security management systems. ISO/IEC 27001 offers a framework within which organizations can approach information security management in a systemic way.

Thousands of organizations globally have recognised the value of certification to ISO/IEC 27001. The certification process provides an expert independent validation that all the parts of the standard have been addressed and complied with. Certification is not a one-off achievement. Much of its value lies in the on-going audits and continual improvement that follow certification.

As information systems change and evolve, individuals holding ISO/IEC 27001 qualification are best placed to ensure that their information security systems evolve in tandem and that their organization complies with the standard.



Written by Tracey Caldwell & Steve Johnson

Tracey Caldwell *is a freelance business technology writer. She writes regularly on information security, including certification and training issues.*

Steve Johnson *is an independent information security practitioner and trainer. He provides integrated management system support to public, private and not-for-profit clients.*

About APMG-International

APMG-International is a leading Examination Institute. We accredit professional training and consulting organizations and manage certification schemes for knowledge-based workers. We have a global reach, with regional offices located around the world.

APMG-International
Accrediting Professionals

APMG-International Head Office Sword House
Totteridge Road, High Wycombe, Buckinghamshire UK HP13 6DG

Tel: +44 (0) 1494 452 450
Fax: +44 (0) 1494 531 952
Email: servicedesk@apmg-international.com
Web: www.apmg-international.com