APMG International™
ISO/IEC 27001

# ISO/IEC 27001 Certification from APMG

## Qualifications to help you understand and apply the information security standard

Authors: Tracey Caldwell & Steve Johnson

## How secure are your IT systems?

# Introduction

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. The result is often a focus on technical solutions, leaving other information sources vulnerable. There is a growing need for a coordinated, systemic approach.

Organizations increasingly need to demonstrate that they have a well-documented management system, not only to ensure they are meeting their own information security objectives, but also to comply with regulation, legislation, industry mandates and 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.**

Our ISO/IEC 27001 Foundation and Practitioner training and qualifications are recommended for people who are working to implement or maintain an ISMS, or whose role requires them to audit an ISMS. The Foundation qualification satisfies the need to have a basic understanding of the standard and its benefits. The Practitioner qualification addresses application of ISO/IEC 27001 to business scenarios to enhance control of information.

**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.**

> "Personal data is the currency of the digital market."
>
> Viviane Reding,
> European Commissioner for Justice

That statement describes the behaviours of commercial organizations and government bodies, many of whom are seizing opportunities to analyse their records of customer and citizen personal information. Merging this with volumes of traded 'anonymized' data, these organizations aim to harvest new insights, seeking competitive advantages and efficiencies.

The same statement also resonates with the wider black market trade that includes personal account IDs and passwords, credit card details, commercial intellectual property and sensitive financial data. The value of that information is motivating theft, funding organized crime, satisfying nation state espionage and driving an evolution of globally-dispersed technical threats to challenge established operational principles and practices.

Organizations are increasingly embracing online opportunities to promote their business and consolidate their position in the marketplace through the use of mobile device applications and social networking presence. Mobile devices and 'the internet of things' have dissolved traditional organizational perimeters and are dispersing information both geographically and logically across the internet. This presents a wide exposure to diverse and sophisticated technical threats.

ISO/IEC 27001 enables the implementation of an ISMS that is flexible and adaptable to the evolving digital ecosystems of customer engagement and service delivery that are transforming business whilst also being responsive to the emerging threats that seek to exploit them.

## Business impact risks

The outdated concept of traditional perimeters was highlighted in December 2013 when US retailer Target discovered that criminals had harvested an estimated 40 million credit and debit card details from point-of-sale terminals in stores across the country.  As investigations continued, it became apparent that the names and contact details of 70 million individuals had also been disclosed.  In combination, this presents a credible risk of fraud and identity theft for those customers.

The 2013 Information Security Breaches Survey by the Department for Business, Innovation & Skills highlights the scale of information security threats in the UK. The report reveals that 14% of large businesses know that outsiders have stolen valuable or confidential data, costing up to 6% of their turnover.  This isn't just a problem for large organizations; in an increasing trend, 87% of small businesses reported breaches costing £65k on average. In many cases, the root cause was not related to technology; 36% of all reported security breaches were caused by human error (and a further 10% by deliberate misuse of information systems).

Target was fortunate in discovering their incident relatively quickly. A report by Trustwave confirms that a staggering 64% of data breaches remain undetected for more than 3 months and 19% remain undiscovered for more than a year.

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.

**14% of large businesses know that outsiders have stolen valuable or confidential data.**

**87% of small businesses reported breaches costing £65k on average.**

**64% of data breaches remain undetected for more than 3 months.**

**19% of data breaches remain undetected for more than a year.**

ISO/IEC 27001 acknowledges that there can never be a guarantee that systems will not be impacted 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.

## Regulatory Compliance

In Europe, the European Commission is working on a major overhaul of data protection rules to strengthen online privacy rights. It is looking to reflect the technological progress and globalization that has 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 implemented the 1995 rules differently, resulting in divergences in enforcement. The plan is that a new single law will replace all country-specific variants.

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 March 2014, for example, it fined the British Pregnancy Advice Service (BPAS) £200,000 after thousands of individual's details were disclosed to a malicious hacker who threatened to publish them. BPAS were apparently unaware that their web site was storing the information and vulnerabilities had enabled the hacker to gain access.

In the same month the ICO published the results of health sector data protection audits highlighting the improvements needed. These ranged from IT system access password controls to improved physical protection of records from fire and flood.

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.

## Resilience and Continuity

2013 was also characterized by tactical business disruption. Motivated by greed, political or ethical values, criminals and activists exploited technical and human vulnerabilities to deny access to services by overloading systems with internet traffic (a 'Distributed Denial of Service' attack). This tactic is used to deface public web sites to express their own views of the victim organization, and to scramble business-critical data while offering the decryption key for a high value fee (epitomized by the CryptoLocker ransom scheme).

Whether the cause is motivated or accidental, loss of business-critical information or the working 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.

## Strategic Governance

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.

The ISMS is moulded by the business objectives of the organization, its current and planned size and its structure. An effective ISMS:-

- Supports due diligence prior to acquisitions or mergers;
- Underpins controlled disposal of organizational operations and assets;
- Assists with impact analysis of internal organizational changes and restructuring;
- 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/IEC 27001

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

**Revised and re-released in 2013, ISO/IEC 27001 builds upon established foundations as the most widely recognized international standard specifically aimed at information security management.**

An organization needs to identify and manage many requirements and activities in order to function effectively. The standard takes a business-focused approach, first enabling people to identify the context in which the business operates and its aims and objectives. It guides the organization to combine this context with a risk-based strategy to define and drive the planning, operation, maintenance and improvement of an effective ISMS.

In contrast to previous editions of the standard, the 2013 edition supplements the business-focussed approach with a greater emphasis on demonstrating clear management leadership and support of the ISMS, the application of robust and repeatable risk management and the evaluation and improvement of ISMS effectiveness.

## 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 27001:2013** specifies formal requirements for an ISMS and forms the basis for certification. Annex A contains a list of controls that must be considered in the ISMS with inclusions or exclusions justified. Additional or alternative controls can supplement this list to satisfy legal, regulatory or industry requirements.

**ISO/IEC 27002:2013** 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 Certification Bodies (CBs) 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.

Reflecting the business criticality of information security in today's global economy, the ISO/IEC 27000 family of standards continues to grow with sector-specific standards.

Examples of these include:-

- **ISO/IEC 27011** for telecommunications and
- **ISO/IEC 27015** for financial services

These additions supplement ISO/IEC 27001 and provide additional best practice guidance in these sectors.

## 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 9001 quality management system and ISO 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.

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

Organizations that achieve an ISO/IEC 27001 compliant system are already able to use that development to inform their approach to other sector-specific management systems standards. ISO/IEC 27001 readily integrates with the Energy Management Systems standard BS EN ISO 50001 in the oil and gas industry. And many enterprises already achieve certification to both ISO/IEC 27001 and ISO/IEC 20000-1 for IT Service Management Systems (ITSMS), complementing ITIL® implementation (ISO/IEC 27013 provides additional guidance for this particular integration model).

## 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 certification bodies (CBs) 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. This can be a valuable differentiator in a competitive market, providing reassurance to sponsors, shareholders and customers alike.

The initial process of certification is normally a three-stage audit by a CB beginning with an informal review and progressing to a detailed check that the provisions of ISO/IEC 27001 have been met. After initial certification, CBs carry out follow-up audits at least once a year and more frequently (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 and effective.

## 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 organizations, holds volumes of personal information across multiple systems and can ill afford a fine from the relevant authorities 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 Financial Conduct Authority in the UK) that encompass the need to employ secure information management.

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

**Service and infrastructure** industries such as transport and utility sectors are also facing increased scrutiny and demands for improved resilience and security both directly and in their supply chains.

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 ISMS.

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 mergers or acquisitions. ISO/IEC 27001 accreditation provides a clear view of the business' information security processes allowing for efficient business change.

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.

## APMG International ISO/IEC 27001 Foundation Qualification:

### *Fast track your knowledge of the standard.*

Our 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 recognize and advise its requirements.

The Foundation 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 marks (50%) to pass.

### APMG International ISO/IEC 27001 Practitioner Qualification:

*Take your knowledge to the next level.*

Our ISO/IEC 27001 Practitioner qualification enables you to leverage the fundamental ISO/IEC 27001 requirements for an ISMS to apply these to business scenarios and address the need to continually improve.  Achieving the qualification provides recognition of consolidated, demonstrable skills in business information security management.

The Practitioner exam assesses applied knowledge of the contents and detailed requirements of the standard through an objective-testing examination consisting of 4 questions (20 marks per question) to be completed in 2½ hours. Candidates must achieve 40 marks (50%) to pass.

Taking the qualifications provides you with confidence to work effectively with best practice guidelines in the sensitive area of information security.

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

**www.APMG-International.com/AccreditedProviders.**

# Conclusion

**If information security is breached, the repercussions can range from heavy penalties to legal action and reputational damage 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 recognize 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 systematic way.**

**Thousands of organizations globally have recognized the value of certification to ISO/IEC 27001. The certification process provides an expert, independent validation that all 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, continual improvements that follow certification.**

**As information systems change and evolve, individuals holding ISO/IEC 27001 qualifications are best placed to ensure that their security systems evolve in tandem to ensure continued protection, resilience and controlled recovery from unplanned incidents.**

**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 and is a Deputy Chief Examiner for APMG's ISO/IEC 27001 qualifications.

**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 Head Office**

Sword House, Totteridge Road,
High Wycombe, Buckinghamshire
HP13 6DG, UK

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

# APMG International Regional Offices

## GLOBAL HEADQUARTERS

## UNITED KINGDOM

Tel: +44 (0)1494 452450
Email: servicedesk@apmg-international.com
Web: www.apmg-international.com

## EMEA

### BENELUX OFFICE

Tel: +31 (0)35 52 31 845
Email: admin@apmg-benelux.com

### FRANCE OFFICE

Tel: +33 (0)1 56 95 19 32
Email: info@apmg-france.com

### GERMANY OFFICE

Tel: +49 (0)2133 53 1667
Email: admin@apmg-deutschland.com

### ITALY OFFICE

Tel: +39 (0)333 326 6294
Email: info@apmg-italia.com

### SOUTH AFRICA OFFICE

Tel: +27 (0)21 0033623
Email: nigel.mercer@apmg-international.com

### SPAIN OFFICE

Tel: +34 (0)911 829933
Email: info@apmg-espania.com

### UK OFFICE

Tel: +44 (0)1494 452450
Email: servicedesk@apmg-uk.com

## THE AMERICAS

### US OFFICE

Tel: +1 (0)781 275 8604
Email: info-us@apmg-us.com

## CENTRAL ASIA

### INDIA OFFICE

Tel: +91 (0)80 6583 6280
Email: info@apmg-india.com

## SOUTH-EAST ASIA

### MALAYSIA OFFICE

Tel: +6.03.6211 0281
Email: exams@apmg-malaysia.com

## CHINA & HONG KONG

### CHINA OFFICE

Tel: +86 (0)532 85 78 95 91
Email: admin@apmg-china.com

## AUSTRALASIA

AUSTRALIA OFFICE
Tel: +61 (0)2 6249 6008
Email: admin@apmg-australasia.com

## KEEPING IN TOUCH

- www.facebook.com/APMGInternational
- @APMG _Inter
- blog.apmg-international.com
- www.linkedin.com/company/apmg-international
- www.apmg-international.com