it governance™

INFORMATION SECURITY & ISO 27001

AN INTRODUCTION

February 2013

Protect • Comply • Thrive

INFORMATION SECURITY & ISO 27001

Introduction

Information security is one of the central concerns of the modern organisation. The volume and value of data used in everyday business increasingly informs how organisations operate and how successful they are. In order to protect this information – and to be seen to be protecting it – more and more companies are becoming ISO 27001 certified.

The main drivers for security are undoubtedly globalisation, government directives, terrorist activities and threats from hackers. Furthermore, organisations seeking opportunities to build markets in the UK are increasingly seeing ISO 27001 as a prerequisite for doing business. Certification is increasingly seen as a powerful assurance of your commitment to meet your obligations to customers and business partners.

In the United Kingdom, the Data Protection Act (DPA) requires businesses to secure their customers' data, and hefty fines (up to £500,000) and sanctions can result from serious data breaches.

While the DPA offers no specific guidance to ensure the protection of data, ISO 27001 offers a set of specifications that describe the features of an effective information security management system (ISMS).

We realise that pursuing the right certification for your organisation can be overwhelming, particularly because there are so many variations. These variations are sometimes renamed or superseded by newer standards, which can cause some confusion. The purpose of this paper is to help you understand ISO27001 certification and explore the benefits of following the information security rules set by the Government.

Overview

- What is ISO 27001? How does this standard help organisations more effectively manage their information security?
- What is the relationship between ISO 27001 and ISO 27002?
- What is the value of ISO 27001 certification?
- How do these standards relate to ISO 9001?
- What does someone need to know to initiate, or take on responsibility for, an organisational information security project and, specifically, one that is intended to lead to ISO 27001 certification?

This paper, written by ISO 27001 expert Alan Calder, answers these basic questions and more. It also points to online resources and tools that are useful to anyone tasked with leading an information security project.

The information in this paper is suitable for all sizes of organisations, and all sectors, anywhere in the world. It reflects the guidance and information available from our ISO 27001 page.

A fundamental aspect of IT governance is the protection of the information – and the confidentiality, integrity and availability (CIA) – on which everything else depends.

In parallel, international standards related to information security have emerged and have become one of the cornerstones of an effective IT governance framework.

IT governance and information security

The last few years have seen corporate governance requirements become increasingly more defined and specific. Information technology has become more pervasive – underpinning and supporting almost every aspect of the organisation; manipulating and storing the information on which the organisation depends for its survival. The role of IT in corporate governance, in that case, has become more clearly defined, and IT governance is increasingly recognised as a specific area for board and corporate attention.

The information security standards

The ISO 27000 family of standards offers a set of specifications, codes of conduct and best practice guidelines for organisations to ensure strong IT service management. Of primary interest to information security are ISO 27001, ISO 27002 and ISO 27005.

ISO 27001 is a technology-neutral, vendor-neutral information management standard, but it is not a guide. Of the three parts to IT security governance, ISO 27001 offers the specification – a prescription of the features of an effective information security management system.

As the specification, ISO 27001 states what is expected of an ISMS. This means that, in order to receive certification or to pass an audit, your ISMS *must* conform to these requirements.

While ISO 27001 offers the specification, ISO 27002 provides the code of conduct – guidance and recommended best practices that can be used to enforce the specification. ISO 27002, then, is the source of guidance for the selection and implementation of an effective ISMS. In effect, ISO 27002 is the second part of ISO 27001.

Just as ISO 27002 provides a set of guidelines for best practice in implementing an ISMS, ISO 27005 provides guidelines for risk management. As part of constructing a suitable and secure information management system, you must assess the risks to your information and be prepared to mitigate these risks.

The information security standards are the essential starting point for any organisation commencing an information security project. Anyone contemplating such a project should purchase and study copies of ISO 27001, ISO 27002 and ISO 27005. Also see 'Useful resources' below for additional resources and materials.

The information security and regulatory environments

The two key reasons for the growing interest in certification to ISO 27001 are the proliferation of threats to information and the growing range of regulatory and statutory requirements that relate to information protection.

Information security threats are global in nature, and indiscriminately target every organisation and individual who owns or uses (primarily) electronic information. These threats are automated and loose on the internet. In addition, data is exposed to many other dangers, such as acts of nature, external attack, and internal corruption and theft.

The last fifteen years have seen the emergence of a growing body of legislation and regulation around information and data security. Some such regulations focus upon the protection of individual data, while others aim at corporate financial, operational and risk management systems.

A formal information security management system that provides guidance for the deployment of best practice is increasingly seen as a necessity in terms of compliance, and certification is increasingly required of organisations (and governments) before they will engage in any significant commercial transactions.

International recognition

In the United Kingdom, accreditation of certifying bodies is handled by the United Kingdom Accreditation Service (UKAS), which maintains a list of all organisations qualified to certify ISO 27001. Through a number of agreements with other international bodies, a certification in the UK is recognised across the globe.

The European Cooperation for Accreditation (EA) is comprised of 35 national accreditation bodies across Europe (including several associate members further afield). The EA multilateral agreement affirms:

- the equivalence of the operation of the accreditation systems administered by EA Members;
- that the certificates and reports issued by organisations accredited by EA Members are equally reliable.[1]

This means that certification approved by one member of the EA is accepted across all other member states.

ISO 27001 is not only recognised throughout the EU, but also has a broader appeal in other key markets via the International Accreditation Forum (IAF). The IAF ensures that ISO 27001 certification is recognised across the world through a 'mutual recognition arrangement', agreed by more than 60 national accreditation bodies.

Market value of certification

In addition to the protection of your data and compliance with data handling laws like the DPA, it is simple to argue that there is a distinct market value to ISO 27001 certification. It is financially prudent to protect your organisation's data and to meet the legal requirements of nations in which you seek to do business.

Achieving certification is a valuable and visible proof of your organisation's willingness to meet internationally-accepted data security standards. Achieving this international standard is not simply marketing: as nations implement their own regulations regarding data protection comparable to the DPA, the ability to prove that your organisation complies with ISO 27001 is likely to open business opportunities across the globe.

It should be noted many markets have already shown a desire for ISO 27001 certification, with 100+ US organisations, 220+ German and 4100+ Japanese organisations having received certification.[2]

The argument for deployment of a formal ISMS is fully developed in a short book called The Case for ISO 27001.

Certification vs conformance

It is possible for an organisation to develop its ISMS in line with ISO 27002 only, because the good practice identified is universally applicable. Because it was not designed to be the basis of a certification scheme, however, it does not specify the system requirements with which an ISMS must be compliant in order to qualify for certification.

Those specifications are contained in ISO 27001. In technical terms, this means that an organisation that is using ISO 27002 on its own can conform to the guidance of the code of practice, but it cannot get an outside body to verify that it is complying with the Standard. An organisation that is using ISO 27001 and ISO 27002 in conjunction with one another can design an ISMS that is in line with the specification and which follows the guidance of the code of practice and is, therefore, capable of achieving external certification.

In order to achieve internationally recognised certification, your ISMS must be audited by an organisation approved by the appropriate body associated with the EA and IAF (in the UK, this is the United Kingdom Accreditation Service – UKAS). Furthermore, the auditing organisation cannot be your consultant – their whole involvement in your ISMS must be limited to their audit.

Certification and other management standards

ISO 27001 is designed to be compatible with other management standards, such as ISO 9001 and ISO 14001. It is also compatible with ISO/IEC 20000:2005. The numbering systems and document management requirements are designed to be inter-compatible, and thus enable organisations to develop management systems that integrate the requirements of each standard an organisation may be using.

Generally speaking, organisations should seek ISO 27001 certification from the certification body they currently use for certifying their ISO 9000 or other management system. The experience of the organisation's quality manager in this process will be invaluable to the ISMS project.

There is no reason, however, why organisations shouldn't tackle ISO 27001 without having first implemented another form of management system. In that case, they will choose a certification body on a commercial basis from among those available and operating in their country.

Most countries have their own accreditation services and these will maintain lists of the organisations that are accredited for ISMS certifications.

Information security and technology

Most people think of information security as a technology issue. They think that anything to do with securing data or protecting computers from threats is something that only technological specialists – and specifically computer security professionals – can deal with.

This could not be further from the truth.

It is the computer user who should decide which threats are to be protected from, and what trade-offs between security and flexibility he or she is prepared to accept. Yes, once these decisions have been made, the computer security expert should design and implement a technological solution that delivers these results – but they should operate according to the user's risk assessment.

In an organisational environment, those decisions should be made by the management team, not by the IT team. An ISMS overtly and specifically recognises that decision-making responsibility should sit with the organisation's board and management, and that the ISMS should reflect their choices and provide evidence as to how effective the implementation has been.

As a result, it is not necessary for an ISMS project to be led by a technology expert. In fact, there are many circumstances in which that could be counter-productive. These projects are often led by quality managers, general managers, or other executives who are in a position to develop something that has an organisation-wide influence and importance.

Preparing for an ISMS project and the PDCA (Plan-Do-Check-Act) cycle

An ISMS project can be a complex one. It is likely to encompass the entire organisation, and should involve everyone from the management down to the post room operatives. It may well take many months or, in some cases, years.

ISO 27001 certification is still relatively new and, as a result, hard experience of successful implementations is in short supply. This means that the handful of

The PDCA cycle was conceived in the 1950s by W. Edwards Deming and says that business processes should be treated as though they are in a continuous feedback loop, so that managers can identify and change those parts of the process that need improvement.

publications that describe, from a practical and pragmatic point of view, how to go about achieving certification should be studied at an early stage in the project planning process.

ISO 27001 sets out how an organisation should approach its ISMS project and specifies the components that are essential. Our free demo provides an overview of the ISMS project, the timeline and the various ways you might tackle it. As you will see, there are specified stages to the project and it is essential to follow the PDCA cycle (see info box above).

The process, or an improvement to the process, should first be planned, then implemented and its performance measured. By comparing these measurements against the planned specification, you will be able to identify any deviations or potential improvements. These can then be reported to management for a decision regarding the correct action to take.

Risk assessment and risk treatment plans

An ISMS must be designed to meet the individual requirements of each organisation. Not only does every organisation have its own specific business model, objectives, unique selling features and culture, it also has its different appetites for risk. In other words, something that one organisation sees as a threat which it must deflect, another might see as an opportunity that it should grasp.

Similarly, one organisation may be less prepared to invest in defences against an identified risk than another. For this and other reasons, every organisation that implements an ISMS must do so against the results of a risk assessment whose methodology, findings and recommendations have been approved by the board of directors.

ISO 27001, in fact, requires a risk assessment to be carried out and, while it does not specify a methodology, it is very clear that this risk assessment must be based on identifying threats and vulnerabilities at an individual asset level and, from there, analysing and assessing risks.

While ISO 27001 offers no specific methodology for identifying risks, ISO 27005 is designed to assist the satisfactory implementation of information security based on a risk management approach. It supports the general concepts specified in ISO 27001 and offers a structured and rigorous process for analysing risks and creating the risk treatment plan.

System documentation

The most time-consuming – and most critical – part of the entire project is the development of the documentation that sets out how the ISMS works.

There are a number of different approaches to this, from using external consultants to tackling it yourself. The major argument in favour of doing it yourself (apart from avoiding, or reducing, consultancy costs) is that you will develop, within your organisation, a much greater depth and awareness of 'how to do security'. By developing such expertise and experience within the organisation, any further such projects can be dealt with more quickly and with a greater degree of confidence.

Without previous experience, development of all the documentation required can be a daunting task. The templates contained in the ISO/IEC 27001 Complete ISMS Toolkit will save you hours of drafting and will help you to avoid trial and error dead ends.

About the author

Alan Calder is an acknowledged international cybersecurity guru and a leading author on information security and IT governance issues. He is also chief executive of IT Governance Limited, the single-source provider for products and services in the IT governance, risk management and compliance sector.

Alan wrote the definitive compliance guide, IT Governance: An International Guide to Data Security and ISO27001/ISO27002 5th edition (co-written with Steve Watkins), which is the basis for the UK Open University's postgraduate course on information security. This work is draws on his experience of leading the world's first successful implementation of BS7799 (now ISO27001).

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets.

Alan was previously CEO of Wide Learning, and of Business Link London City Partners. He was a member of the Information Age Competitiveness Working Group of the UK Government's Department for Trade & Industry, and a member of the DNV Certification Committee, which certifies compliance with international standards including ISO/IEC 27001.

[1] http://www.european-accreditation.org/content/mla/benefits.htm

[2] International Register of ISMS Certificates, http://www.iso27001certificates.com/

Useful Resources

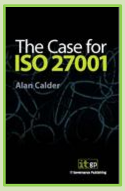
IT Governance offers a unique range of products and services, including books, standards, pocket guides, training courses, staff awareness solutions and professional consultancy services.

Information Security Resources

- **ISO/IEC 27001 Complete ISMS Toolkit**

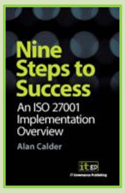
Provides a useful resource which will accelerate your ISO 27001 project and develop an ISO 27001-compliant Information Security Management System (ISMS).

- **The Case for ISO27001**



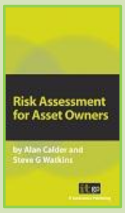
This eBook is designed to provide a project manager with the arguments that may be necessary to get the organisation's board to make the appropriate commitment to the project.

- **Nine Steps to Success: An ISO27001 Implementation Overview (eBook)**



A short but thorough, overview of the steps that are critical to success when implementing ISO 27001.

- **Risk Assessment for Asset Owners**



A pocket guide to the ISO 27001 risk assessment, and designed to assist asset owners and others who are working within an ISO 27001/ISO 27002 framework to deliver a qualitative risk assessment.

- **Information Security Risk Management for ISO27001/ISO27002**

A comprehensive guidance on ISO 27001 risk management. Order this book for advice on information security management that can really benefit your bottom line.

- **vsRisk – ISO 27001:2005 Compliant Information Security Risk Assessment Tool**

This software has been designed with the user in mind and for the first time empowers the user to comply with the requirements of ISO 27001:2005 and effectively assess and align their total assets with their objectives.

IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today's organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial.aspx to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors. Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training.aspx for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting.aspx for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software.aspx for more information.

Contact us:	+ 44 (0) 845 070 1750
www.itgovernance.co.uk	servicecentre@itgovernance.co.uk

[1] http://www.european-accreditation.org/content/mla/benefits.htm

[2] International Register of ISMS Certificates, http://www.iso27001certificates.com/