INFORMATION SECURITY & ISO 27001

AN INTRODUCTION

January 2018

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, regulatory requirements, terrorist activities and escalating cyber threats. Furthermore, organisations seeking contracts with governments or large corporate clients are increasingly finding ISO 27001 is a prerequisite for doing business. Certification is seen as a powerful assurance of your commitment to meet your obligations to customers and business partners.

This situation is all the more pressing with the advent of the EU General Data Protection Regulation (GDPR), which requires businesses to secure the personal data of all EU residents, and hefty fines (up to 4% of global annual turnover or €20 million, whichever is the greater) can result from serious data breaches.

While the GDPR 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 These variations are sometimes renamed or superseded by newer standards, which can cause some confusion.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 ISO 27001 certification and explore the benefits of following the information security rules set by governments.

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 – specifically one 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 organisations of all sizes, in all

A fundamental aspect of IT governance is the protection of the information – and its 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.

sectors, anywhere in the world. More guidance and information is available from our ISO 27001 page.

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 information security management. Of primary interest are ISO 27001 and ISO 27002.

ISO 27001 is a technology-neutral, vendor-neutral information security management standard, but it is not a guide. Of the above standards for 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.

These 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 and ISO 27002.

See the 'IT Governance Solutions' section at the end of this paper for additional resources and materials.

Information security and the regulatory environment

The two key reasons for the growing interest in certification to ISO 27001 are the proliferation of threats to information ('cyber threats') 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. Data is also exposed to many other dangers, such as acts of nature, external attack, and internal corruption and theft.

The last twenty 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 be engaged 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; and
- 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 70 national accreditation bodies.

Market value of certification

In addition to protecting your data and complying with data handling laws like the GDPR, 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 well as complying with the GDPR and other related laws such as those aligned with the Directive on Security of Network and Information Systems (NIS Directive), the ability to prove that your organisation complies with ISO 27001 is likely to open business opportunities across the globe.

It should be noted that many markets have already shown a desire for ISO 27001 certification, with over 33,000 organisations worldwide having received certification.[2]

The argument for deploying a formal ISMS is fully developed in a short book called The Case for ISO27001.

Certification vs conformance

It is possible for an organisation to select controls and follow the guidance from ISO 27002 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 comply 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 a 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 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 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 a number of other management

system standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management) that follow what is called Annex SL – a standardised structure for management system standards. The numbering systems and document management requirements are designed to be compatible, and thus enable organisations to develop management systems that integrate the requirements of each standard an organisation may be using. ISO 27001 is also generally compatible with ISO 31000 and ISO 20000.

Generally speaking, organisations should seek ISO 27001 certification from the certification body they currently use for certifying their ISO 9001 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 that 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 the IT team. An ISMS overtly and specifically recognises that decision-making responsibility should sit with the organisation's 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 continual improvement cycle

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

ISO 27001:2013 offers a structured approach to developing the ISMS. The clauses describe the requirements of the ISMS, and Annex A provides controls that can be used to protect the organisation's information assets. There are no mandated stages to the project, but you need to apply a continual improvement process from the

The PDCA cycle is a continual improvement methodology that 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.

outset; the PDCA cycle (see info box above) is one possible methodology.

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 within the context of and 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 that 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 produce consistent, valid and comparable results, and analyse and assess the risks.

System documentation

The most time-consuming 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 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.

IT Governance Solutions

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 use different elements to build something bigger and better.

ISO 27001 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 management compliance) projects.

ISO27001 bespoke consultancy

IT Governance has helped over 400 companies successfully implement an ISO 27001 ISMS. Drawing on our unique blend of practical information security know-how and proven management system consultancy expertise, our team will help you implement an ISO 27001-compliant ISMS without the hassle, no matter where your business is located.

ISO27001 Gap Analysis

A specialist, in-person review of your current information security posture against the requirements of ISO/IEC 27001:2013. Get the true picture of your ISO 27001 compliance gap, and receive expert advice on how to scope your project and establish your project resource requirements.

ISO27001 DIY packages

Four specially formulated combinations of best-selling tools and trusted resources helps you manage the ISMS implementation project from end to end.

ISO27001 FastTrack™ Consultancy

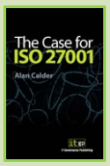
A fixed-price online consultancy package designed to help small organisations reach ISO 27001 certification readiness in just three months.
Receive a 100% guarantee of certification.

ISO 27001 Internal Audit Service

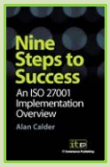
Outsource your internal audit to a qualified auditor with deep experience of ISO 27001 and the audit process, and gain the assurance you need to ensure you meet your clients' and stakeholders' demands. This service consists of two separate audit days spread over one year.

ISO 27001 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. Our publishing team also 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.



The Case for ISO 27001
This book 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 ISO 27001 Implementation Overview (e-book)
A thorough overview of the steps that are critical to success when implementing ISO 27001.

ISO 27001 standards

The ISO/IEC 27000 family of mutually supporting information security standards (also known as the ISO 27000 series) is developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to provide a globally recognised framework for best-practice information security management.

The official ISO/IEC standards
Reading and understanding the official ISO 27000 standards is an essential starting point for an ISO 27001 project.

ISO 27001 policies and procedures

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

ISO 27001 ISMS Documentation Toolkit
ISO 27001 certification requires organisations to prove their compliance with the Standard with appropriate documentation, which can run to thousands of pages for more complex businesses. With this toolkit, you will have all the direction and tools at hand to streamline your project.

ISO 27001 training and qualifications

We offer training courses for all levels, 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.

ISO 27001 Certified ISMS Foundation
Delegates who successfully complete this one-day introductory course will be awarded the ISO27001 Certified ISMS Foundation (CIS F) qualification.

ISO 27001 Certified ISMS Lead Implementer
This three-day course covers all the key steps involved in planning, implementing and maintaining an ISO 27001-compliant information security management system (ISMS). Gain an ISO27001 Certified ISMS Lead Implementer qualification.

ISO 27001 Certified ISMS Lead Auditor

This fully accredited course equips you with the skills to conduct second-party (supplier) and third-party (external and certification) audits. Build your career as a lead auditor, lead a team of auditors and achieve compliance with ISO 27001.

ISO 27005 Certified ISMS Risk Management

Learn the process of conducting an effective information security risk assessment through practical risk management methodologies as promoted by ISO 27005. Presented by an ISO 27001 practitioner offering real-world expertise and insights.

ISO 27001 Certified ISMS Internal Auditor

Developed by the UK's leading ISO 27001 consultancy company, this two-day course provides the knowledge and skills required to perform ISO 27001 internal audits that maintain compliance and drive continual improvement within your organisation's ISMS, in accordance with clause 9.2 of the Standard.

ISO 27001 E-learning

Hassle-free, cost-effective e-learning courses constantly reinforce the importance of compliance and security, develop good habits and put you on course to achieve and maintain your ISO 27001 accreditation.

Information Security & ISO 27001 Staff Awareness E-Learning Course

This e-learning course enables employees to gain a better understanding of information security risks and compliance requirements in line with ISO 27001:2013, thereby reducing the organisation's exposure to security threats.

ISO 27001 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 ISO 27001 compliant.

vsRisk risk assessment tools

vsRisk software empowers the user to comply with the requirements of ISO 27001:2013 and effectively conduct an information security risk assessment, apply controls, and produce audit-ready reports.

Speak to an expert

Please contact us for further information or to speak to an expert.

Contact us

Contact us: **+44 (0)333 800 7000**

www.itgovernance.co.uk servicecentre@itgovernance.co.uk

[1] http://www.european-accreditation.org/benefits.
[2] ISO Survey 2016, https://www.iso.org/the-iso-survey.html.