ISO27001 in a Windows® Environment

The best practice implementation handbook for a Microsoft® Windows® environment

Brian Honan

Third edition

itgp™

ISO27001 in a Windows® Environment

The best practice handbook for a Microsoft® Windows® environment

Third edition

BRIAN HONAN

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2009
by IT Governance Publishing.

ISBN 978-1-905356-24-9

Second edition published in 2010.
ISBN 978-1-84928-050-1

Third edition published in 2014.
ISBN 978-1-84928-604-6

FOREWORD

The standard for Information Security Management Systems (ISMS), ISO/IEC 27001, provides a significant implementation challenge for all organisations. ISO27001 is a management standard: it sets out a specification for how management should identify, from a business risk perspective, the controls and safeguards that should be applied to information assets in order to assure their confidentiality, integrity and confidentiality. Management – and also the ISMS implementation project manager – will usually have a general or quality management background.

A significant number of the controls to be applied will, of necessity, be technical and will relate to how IT hardware and software are set up and configured. The technical knowledge to carry out this configuration is usually within the IT or corporate information security team and, because information security is a business responsibility, this team should never have overall accountability for determining the actual controls required by the ISMS.

As a result, there is often a gulf in understanding as to what is required between the ISO27001 ISMS project manager and those responsible for implementing the technical controls. This book does an outstanding job of helping parties on both sides to bridge the gulf. It identifies the recommended technical controls of ISO27001's Annex A and, for a Microsoft environment, provides guidance on how (if, on the basis of a risk assessment, they are considered necessary) to implement them.

This book fills a major hole in the guidance literature for ISO27001 and will make a significant contribution to

helping both project managers and IT and security staff get to grips with what controls are appropriate to mitigate identified risks.

While this book covers implementations in a wide range of Windows® environments, this third edition is completely up to date for Windows® 8 and Server® 2012. This book is so useful that it should be a core part of every information security professional's library.

Alan Calder

June 2014

PREFACE

This book is the culmination of my work with various clients in implementing their ISO27001 information security management systems. Having watched clients struggle to understand and grasp the concepts of ISO27001 and then having to further translate those concepts so that their technical IT personnel could appreciate what was required, I decided to write this book to make that task easier for them.

I also decided that since the Microsoft® Windows® platform and various other Microsoft products are so commonly used in many organisations, I would base the technical details on those Microsoft technologies.

So began a long and interesting journey as I delved further into the workings of Microsoft® Windows® 7, Microsoft® Windows Server® 2008 and various other products. (And, since then, I have updated this book to account for newer products including, crucially, Microsoft® Windows® 8 and Microsoft® Windows Server® 2012.) My goal was to identify how an IT Manager could leverage the Microsoft technology already available to them to support their implementation of the ISO27001 information security management standard.

That journey brought me into contact for the first time with the numerous tools, utilities and products that Microsoft provides, which can be readily applied to most environments and to which I will introduce you in this book.

This book is designed as a step-by-step guide through the journey of implementing ISO27001 in a Microsoft® Windows® environment. You can choose to read the book in a linear fashion from the first to the last page as a companion for your ISO27001 journey, or it can be used as a reference guide to which you can refer when you need to verify a control or associated technical setting.

Approached in the right way, the journey to achieving certification to the ISO27001 information security management standard can be smooth, without too many bumps, twists or turns. Using this book will assist you on that journey, providing you with a roadmap and signposts along the way to get to your destination.

ABOUT THE AUTHOR

Brian Honan is recognised as an industry expert on information security, in particular the ISO27001 information security standard, and has addressed a number of major conferences relating to the management and securing of information technology.

An independent consultant based in Dublin, Ireland, Brian provides consulting services to clients in various industry segments and his work also includes advising various Government security agencies and the European Commission. Brian also established Ireland's first ever Computer Security Incident Response Team.

Brian is also an Adjunct lecturer at University College Dublin lecturing on Information Security Management.

In 2013, Brian was appointed as a special advisor on Internet Security to Europol's Cybercrime Centre

He has also had a number of technical papers published and has been technical editor and reviewer of a number of industry-recognised publications. Brian is also the European editor for the SANS Institute's weekly SANS NewsBites, a semi-weekly electronic newsletter.

He is a member of the Irish Information Security Forum, Information Systems Audit and Control Association, and a member of the Irish Computer Society, and is president of the Irish Chapter of the Cloud Security Alliance.

ACKNOWLEDGEMENTS

This book would not have been possible without the support of many people. They provided encouragement and guidance from the concept of this book to its final publication. For fear of forgetting to mention anyone I shall not list them here.

There is one person, though, without whose help and support I would not have been able to complete this book, my wife, Veronica. She provided me with encouragement when I needed it, scolding when I deserved it and time and space when required. For all that, and much more, she will always have my undying love and appreciation.

CONTENTS

INTRODUCTION

Information security, once viewed as being solely within the domain of the IT department, is now a key issue for many businesses and organisations. Industry regulations, legal requirements, media coverage of information security incidents and a growing demand from clients that companies better manage and secure the information within their care have forced information security out of the IT department and into the boardroom.

Companies are now faced with the dilemma of ensuring their information is secure enough to satisfy their business needs and is also compliant with various legal and regulatory requirements, such as the Data Protection Act, Basel II and III, or the US Sarbanes-Oxley Act.

Information security is not solely about compliance, demonstrating best practices or implementing the latest technical solutions. It is about managing the risks posed to the business by the accidental or deliberate misuse of confidential information. It is important to note that no matter what the industry, whether in the private or public sector, every organisation has confidential information it needs to protect. This information could be customer details, payroll information, credit-card numbers, business plans, financial information or intellectual property, to name but a few examples.

The problem many companies face is that there are no recommended benchmarks or minimum grades clearly stated in most of the compliance regulations they need to meet and the business is often not clear about what it requires. Those faced with the responsibility of securing a

company's information are confronted with the onerous task of trying to determine how best to implement effective security controls for their systems and information, without any clear guidance on what constitutes legal compliance.[1]

The ISO27001 information security standard offers companies a way to address this problem. Originally known as BS7799 part 2, ISO27001 is a vendor and technology-neutral internationally recognised standard that provides companies with a risk-based approach to securing their information assets.

ISO27001 certification provides organisations with independent third-party verification that their information security management system (ISMS) meets an internationally recognised standard. This provides a company, and its employees, customers and partners, with the confidence that it is managing its security in accordance with recognised and audited best practices.

By adopting the risk- and standards-based approach to implementing an ISMS in accordance with ISO27001, you can reap many advantages, not least of being better able to demonstrate compliance with legal and industry regulatory requirements.

It is important to note that the ISO27001 information security standard can simply be used as a framework against which a company can implement and measure its ISMS, without necessarily having to be accredited. This is particularly useful for companies wishing to ensure they are

[1] Read *Information Security Law: The Emerging Standard for Corporate Compliance*, Smedinghoff T, ITGP (2008) for guidance on this issue.

implementing an effective ISMS but without necessarily wanting full certification to the standard.

However, implementing ISO27001 can be a challenge for many organisations. While the standard is prescriptive in terms of the management system, it is not prescriptive about the controls that must be implemented; nor does it provide a checklist of items that an organisation can tick off to be secure against all relevant risks.

So, after the business has decided that the ISO27001 information security standard will enable it to meet its information security requirements, very often the task of implementing the standard falls to the IT Manager. This can be a major challenge for them as they must first become familiar with ISO27001 and interpret it in accordance with their organisation's unique business requirements and risk profile, while ensuring that any controls that are identified are properly implemented.

This book is designed to assist the IT Manager along the road to successfully implementing the ISO27001 information security standard by introducing them to the concept of what an ISMS is and how to use ISO27001 to ensure its quality.

Once the IT Manager understands the requirements of an ISMS, the book will then describe the various inbuilt features within Microsoft's current family of server and desktop operating systems and some additional products, which can be employed to support the ISMS. This book focuses primarily on Microsoft technologies as they are so predominant in many business environments. By employing the native features of the Windows® operating systems, and some additional complementary Microsoft products, this book will demonstrate how certification

against ISO27001 can be achieved. As most of the technologies are already built into the Microsoft platform, it should be possible for an organisation to achieve certification without having to purchase additional third-party software products.

Finally, this book will also provide technical details on what IT technicians should be considering to ensure that the controls identified as necessary are in place and are effective.

CHAPTER 1: INFORMATION AND INFORMATION SECURITY

Before we begin our ISO27001 journey, it is important that we understand what it is that we are trying to achieve. When most people hear the phrase information security, they automatically think that it is applicable only to IT and the securing of computers and networks.

But information can take many forms and is not only bits and bytes on computers or networks. Information can be printed or written on to paper; it can be verbal, whether spoken face to face, in a crowded room or over a telephone; or it can indeed be stored or transmitted electronically by computers, networks or fax machines.

Information is considered to be one of the most valuable assets a company can have. Customer databases, business plans and intellectual property are just some examples of how information becomes the lifeblood of many organisations. Without the correct information, senior management may make the wrong strategic decisions; information in the hands of a competitor could undermine a company's competitiveness; or information lost from a laptop or a briefcase, or accessed by unauthorised people, could expose sensitive customer data, leaving the organisation facing negative publicity and, in some cases, serious fines.

Therefore it is important that we take steps to protect information when it is being transmitted, exchanged or stored, whatever format it is in.

This is where information security comes into play. When we speak about information security, what we are actually talking about is how we prevent security incidents and minimise their impact on the business. To do this we need to understand the various information security concepts.

Information security concepts

To better understand information security, there are a number of concepts that you should keep in mind when considering what controls to put in place to secure information. In the context of the ISO27001 information security standard, there are three core concepts that we need to consider when designing our controls or measures to protect our information. Widely referred to as the CIA of information security, these are specifically:

- Confidentiality
- Integrity
- Availability.

Confidentiality is where we ensure that information is only available to the appropriate individuals.

Integrity is ensuring that the information has not been altered in any way, either deliberately or accidentally.

Availability is how we ensure that the information can be accessed by those (and only by those) with the appropriate permissions.

Other information security concepts

While the CIA concepts are widely viewed as the three pillars upon which to build your information security, there

are a number of other concepts that we should also keep in mind:

- **Identification:** This involves the mechanisms we would put in place to identify a user to a system; for example, their photo on an ID card or their unique user ID to log on to a network.
- **Authentication:** This is the means of proving that an individual is who they claim to be. This could be a security guard checking the picture on an ID card is that of the person holding the card, or a secret password to match the person's unique user ID.
- **Authorisation:** Once a person has been identified and authenticated, we then need to ensure they have the appropriate authorisation to do what they need to do. We could restrict an individual to access only certain folders on the network by using network permissions on the files, or restrict physical access by only allowing their swipe card to open certain doors in the building.
- **Accountability:** It is important that we can identify what an individual has done once they have access to a system or an environment. Computer security logs and audit trails can record what a person does when authenticated to a system or a closed-circuit TV system could be used to record who accesses certain parts of the premises.
- **Privacy:** This concept relates both to the fundamentals of the confidentiality of the company's data and to the protection of the privacy of those who use the systems.
- **Non-repudiation:** Non-repudiation is where we can prove that a particular action or transaction was completed by a specific individual; for example, a signature on a cheque or someone signing a contract, making it impossible to repudiate that contract.

- **Reliability:** Any action or behaviour should be consistent, so a consistent action should produce consistent results. For instance, the processes involved in providing authorisation should always give the same user the same authority.

The importance of information security

As stated earlier, information is probably one of the most valuable assets a company can hold; however, as information is intangible, the value of it can often be overlooked. Unlike stock, factory machinery or company premises, information is not very visible to an organisation even though it sits on every desk, in every computer and in every filing cabinet. This can make it difficult for organisations to fully appreciate its value and implement the appropriate protections.

Information security should therefore be driven by the business needs of the organisation as it must at all times take these into account. Rather than being a technical issue, information security is clearly a management and governance issue and one that must be driven by senior management.

As economies become more and more global, companies are relying more and more on information for the success, and indeed the survival, of their business. New business channels are being facilitated by the Internet and related technologies, allowing many businesses to communicate more directly and effectively with customers, staff, partners and suppliers.

Companies can now expand into global markets using online websites, customer service is better facilitated by the

use of email and instant messaging, and Voice over IP provides cost-effective voice communications. Co-operation with partners and providers is better facilitated by the same technologies and online banking allows for payments to be sent and received faster and far more efficiently than before.

All of the above technologies provide us with ways and means for transmitting, storing and processing information more efficiently. While all of the above provide many advantages to businesses, they also bring with them a greater dependency on the underlying technologies. Any interruptions, be they accidental or deliberate, can have a major impact on a business. Prolonged outages whereby information is not available or issues that result in the information becoming corrupted can have a significant impact on the bottom line of any business.

In addition to the above, most of the technologies that we use to process our information with third parties, customers or remote staff are based on the Internet. The Internet is a collection of networks that are interconnected and the Internet is not policed nor managed by any one entity. This can lead to variances in the quality and security of service that can be experienced as information travels from one point to another.

Against this backdrop, the IT Manager is also challenged with minimising the amount of system down time while at the same time maintaining the competitive advantage these technologies provide to the business.

All of the information processing facilities, be they technical or human based, need to comply with various regulatory and legal requirements. For some industries, e.g. financial and health care, certain types of information need

to be stored and archived in particular formats for predefined periods of time. At all times the legal framework within which an organisation operates has to be complied with, e.g. the EU Data Protection Directive. These issues become more and more of a challenge as an organisation grows its operations globally and operates or deals with customers in different countries, resulting in having to comply with various local laws and regulations.

The IT Manager is often tasked with ensuring the above business security requirements are met while at the same time having to manage everything within an ever-dwindling IT budget.

CHAPTER 2: USING AN ISMS TO COUNTER THE THREATS

According to the International Organization for Standardization (ISO), the developers of ISO27001, an information security management system 'is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process'. Simply put, an ISMS is a framework which management employs to ensure a structured approach is taken to identify the business risks posed against key information assets and how best to manage, eliminate or mitigate those risks.

An effective ISMS will be an integrated part of the overall management system within a company. This is to ensure that senior management is involved and is committed to the ISMS. As with all major initiatives, senior management commitment is critical to ensuring the success of your ISMS. Without such commitment, you will be left fighting to justify the controls you wish to implement; having senior management commitment makes this task a lot easier.

An effective ISMS is based on taking a business-risk approach to establishing, implementing, operating and monitoring the ISMS. It is important to maintain focus on the business requirements at all times. A successful ISMS should not be seen as a barrier to conducting business but rather as a tool to enable the business to meet its goals in a secure manner.

Information security management systems are often likened to the brakes on a car. While brakes are often viewed as a means to stop a car, they are in effect key safety features on

the car that allow the driver to get to their destination safely. Without brakes on a car, the car would crash or the journey would take much longer as the driver would have to drive very slowly to ensure they encountered no accidents. Whereas with brakes on the car, the driver can negotiate twists and turns in the road much more effectively and get to their destination much more quickly and safely. Similarly, an effective ISMS should not prevent a business achieving certain goals but ensure the business can achieve those goals in as safe and secure manner as possible, without any misfortunes happening along that journey.

System security versus information security

It is important that we remind ourselves at all times what the difference between information security and system security is.

System, or IT, security focuses primarily on the technologies, such as networks, computers and applications that are used to create, modify or transfer our information assets. Therefore the focus of system security is very much at the technical end of the spectrum and includes solutions, such as intrusion detection systems, anti-virus software, cryptography and firewalls amongst others.

Information security, on the other hand, focuses on how information is protected and concentrates mainly on managerial and business solutions. System security has a place in information security but is simply another part of the information security management solution together with items, such as policies, procedures, people, legal issues, and the security culture of the organisation, the policies and the organisation's approach to risk.

Information security is therefore a much more holistic approach than system security in protecting the information assets of an organisation and ensures that risks to the organisation's information assets are identified, quantified and managed.

The structure of an ISMS

An ISMS is a management system that is put in place to ensure that all safeguards implemented to protect an organisation's information assets are appropriate, operating as expected and providing feedback on ways to continuously improve the ISMS.

A successful ISMS will provide a risk-based framework that contains a number of core elements which will ensure a systematic approach to managing an organisation's sensitive information so that it remains secure. The ISMS is dependent on people understanding their roles within the system and being aware of their responsibilities. It cannot be stressed strongly enough that the ISMS will only succeed if it has the commitment of senior management within the organisation. Without this commitment, the training and awareness required to be given to staff may not be forthcoming, resulting in an ineffective ISMS.

Information security policy

The cornerstone to any successful ISMS is the information security policy. This document drives the whole system and sets the framework for decisions on what controls, be they human, technical or procedural, need to be put in place.

An effective information security policy will align itself with the business needs of the organisation, but at the same time it must take into account the culture and security needs of the organisation in question. An information security policy for a branch of the security services may be much more security focused than, say, a policy for a small business.

It is important that the information security policy balances the levels of security controls with levels of productivity. If the security controls become too intrusive into how people do their jobs, they will invariably ignore or bypass the controls, making the policy ineffective.

To ensure buy-in to the information security policy, a number of people should be consulted regarding its structure and content. Senior management should give their input to the policy and ensure that it is aligned with the requirements of the business. Representatives of the end-users should also be consulted to ensure that the policy will be accepted by staff. Company lawyers and auditors should also be involved with the design of the policy to ensure that it complies with any legal, regulatory or contractual requirements, and that the auditors are familiar with the policy in order to facilitate future audits.

It is also prudent to involve representatives from IT in the policy design process. While the policy should not be a technically focused document, it is important that IT are aware of the implications of what is being proposed by the policy so as to ensure that technical controls can be implemented where required and monitoring solutions implemented to assist in the management and enforcement of the policy.

When developing the information security policy, you should ensure it remains concise and easy to understand. The most successful policies are those that are written in plain language, avoiding legal jargon. It is also important that you include within the information security policy the reasons why it is needed and what exactly is covered by the policy, explain how violations will be dealt with and detail the main roles and responsibilities for information security.

The information security policy should be designed with the size of the organisation in mind. Some organisations may have one policy to cover all information security issues whereas other organisations may have multiple policies to cover specific areas of information security.

The decision to have either a single comprehensive information security policy or a number of smaller policies can be influenced by issues, such as the number of sites within your organisation, the types of business units, the different types of workforce that you may have or indeed the structure of your organisation.

Whether you decide to use one single policy or multiple policies, it is important that they meet the requirements of ISO27001. They should also refer to the following, secondary policies.

Acceptable usage policy

This policy discusses the appropriate usage of the organisation's computing resources. It is essential that all users read and accept this policy before they are allowed to access any of the organisation's computer systems. Ideally this policy should not be technology specific; otherwise you

may end up constantly having to update the policy or it will be superseded by newer technologies.

Remote access policy

In order to ensure that all connections to your internal network are managed in the most appropriate manner, a remote access policy should outline and define the acceptable methods for remote users, such as road warriors, homeworkers and third parties, to connect to the network. Again the policy should be technology neutral and highlight who has the authority, and under what conditions, to grant remote access to people or other organisations.

Information management policy

Your information management policy should provide guidance to users on how they should handle and manage information with regards to its classification. For example, information that is sensitive should be dealt with differently to information that would be available to the public. The main goal of the information management policy should be to ensure that information is appropriately protected from modification and/or disclosure.

Computer malware prevention and protection policy

This policy should detail what the requirements are for protecting your systems from infection from computer malware, such as computer viruses, Trojans, spyware and keyloggers. While most of the controls in place will be technical, it is important that you keep this policy technology and/or product neutral so that the goals of the

policy can adapt to new threats as they arise. The policy should detail what protections need to be installed on the end-user workstations, servers, the network and your network ingress and egress points. Other mechanisms that can be used to transport malicious software into your organisation should also be included, such as Internet downloads, USB keys, CDs, DVDs and floppy disks. The policy should detail how often the software should be deployed, maintained and updated. Guidelines on how to report and contain suspected virus outbreaks should also be included. Ideally you should also integrate this policy with your incident response and business continuity policies.

Password policy

Your password policy should detail the minimum requirements your organisation requires for all passwords, be they user, system or vendor passwords. It should include the rules relating to creating passwords, such as their length, how often they expire, whether the passwords are complex and their uniqueness. The password policy should clearly state how individuals should protect their passwords from disclosure and what to do in the event that this should happen.

Your policies will form the cornerstone of the rest of your ISMS. The key to successful policies is keeping them simple and easily understood. The best policies tend to be short, to the point, relevant and easy to read. Remember that your policies are the main drivers for identifying what processes, procedures, and personal and technical controls you may need to implement to support the policy.

Therefore it is important to remember that policies should very rarely change and should be written in a language that is technology agnostic and should refer to titles and roles rather than individuals.

Your processes and procedures can be more detailed and technically specific as these can be changed as required.

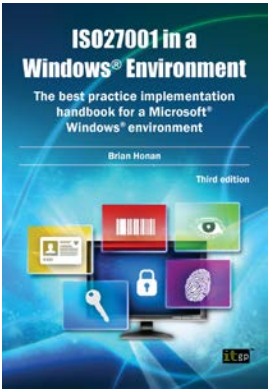
It may help to think of your policies as being the equivalent of a country's constitution while the processes and procedures are the laws to support the constitution. Constitutions rarely get changed as they define the goals while laws are implemented and amended as required.

Managing exceptions to the policy

You should also remember that with all your policies there will no doubt be some exceptions. There will be new technologies or new business requirements that may not comply with the policy. You and your senior management will need to be able to manage such exceptions by conducting a risk assessment to see whether the exception requires the policy to be amended to accommodate it or whether to accept and manage the risk posed by the exception to the policy. For example, the business may require a new application to be installed on the network to enable it to branch into a new market. However, that application's inbuilt password management system may not comply with your own password policy. You may recall from earlier in this chapter that information security should facilitate business and not be seen as a barrier to it. As a result, you should approach senior management and highlight the risks posed by this new application being introduced into the organisation and the controls you

propose to manage the risk. Senior management can then make a business decision based on the risk assessment provided, and either authorise the exception, require that policies are amended to support it, or reject the application as it may pose too great a risk to the organisation.

<<< End of extract >>>



- Bridges the knowledge gap between ISO27001 managers and Windows® security specialists
- Up to date with ISO/IEC 27001:2013
- Details the various controls required under ISO 27001, together with the relevant Microsoft® products that can be used to implement them.

Essential guidance for everyone involved in a Windows®-based ISO 27001 project – buy your copy today!

www.itgovernance.co.uk/shop/product/iso27001-in-a-windows-environment-third-edition

www.itgovernanceusa.com/shop/product/iso27001-in-a-windows-environment-third-edition

www.itgovernance.eu/shop/product/iso27001-in-a-windows-environment-third-edition

www.itgovernance.asia/shop/product/iso27001-in-a-windows-environment-third-edition

www.itgovernancesa.co.za/p-343-iso27001-in-a-windows-environment-third-edition.aspx