The Case for ISO27001:2013

Alan Calder

Second edition

itgp™

The Case for ISO27001:2013

Second edition

ALAN CALDER

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 2005
by IT Governance Publishing.

Second edition published in 2013.

ISBN 978-1-84928-531-5

ABOUT THE AUTHOR

Alan Calder is the founder and Executive Chairman of IT Governance Ltd (*www.itgovernance.co.uk*), an information, advice and consultancy firm that helps company boards tackle governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors.

The company distributes a range of books, tools and other publications on governance, risk management, compliance and information security through its website.

ACKNOWLEDGEMENT

Some of the material in this book has appeared elsewhere in books and articles by Alan Calder; this is the first time that all the material germane to the Case for ISO27001:2013 has been gathered together in one place, re-purposed and expanded.

CONTENTS

INTRODUCTION

The replacement, in late 2005, of BS 7799-2:2002 by the international Information Security Management System Standard ISO/IEC 27001:2005 marked the beginning of the age of information security management. The update to ISO/IEC 27001 in 2013 was released to an ever-expanding information economy.

In the first eight years that BS 7799 existed as a Standard against which organisations could gain an external certification, about 1,000 were successful, worldwide. This number doubled in the subsequent 12 months. Under ISO/IEC 27001, that number has grown geometrically. This book looks at why organisations are increasingly turning to this information security management Standard.

By far the most common drivers for organisations that were successful in achieving BS 7799 'were commercial: to increase the confidence of customers, or possibly to encourage suppliers, when dealing with the organisation.'[1] By 2011, 87 percent of respondents to a BSI survey reported that implementing ISO/IEC 27001 had a positive or very positive outcome.[2]

Technology – specifically information technology – is transforming the economic and social worlds in which we work, play and live. Whether or not this is a good thing is irrelevant. The fact is that, for most people, information was stored, 20 years ago, on pieces of paper. Small numbers of

[1] Information Security BS 7799 Survey 2005 – Information Security Ltd.

[2] Benefits of ISO/IEC 27001 Information Security Research Report, 2011.

large mainframe computers batch-processed mundane transactions and a credit card application could take several weeks. Corporations wrote their own computer programs and avoiding GIGO (garbage in, garbage out) was the Head of IT's prime objective. Fax machines were transforming a business communication infrastructure that still depended on expensive fixed telephone lines. Information, when it existed, was hard to lay your hands on and even harder to use, manipulate or transform.

Today, 'information overload' is a commonplace complaint. Computers are ubiquitous, data is mobile, communication can be globally instantaneous and someone else can get a credit card in your name in a matter of minutes.

As we've shifted from a manufacturing to an information economy, the structure of organisational value has changed dramatically. The intangible assets (mostly intellectual capital) of most OECD organisations are now worth substantially more than their tangible assets and this trend is unlikely to reverse.

Information is the life blood of the modern business. All organisations possess and use critical or sensitive information. Roughly nine-tenths of all businesses now send e-mail across the Internet, browse the web and have a website; and 87 percent of them now identify themselves as 'highly dependent' on electronic information and the systems that process it. Information and information systems are at the heart of any organisation trying to operate in the high-speed wired world of the 21st Century.

Business rewards come from taking risks; managed, controlled risk-taking, but risk-taking nonetheless. The

business environment has always been full of threats, from employees and competitors, through criminals and corporate spies, to governments and the external environment. The change in the structure of business value has led to a transformation of the business threat environment.

The proliferation of increasingly complex, sophisticated and global threats to this information and its systems, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is forcing organisations to take a more joined-up view of information security. Hardware-, software- and vendor-driven solutions to individual information security challenges no longer cut the mustard. On their own, in fact, they are dangerously inadequate.

News headlines about hackers, viruses and online fraud are just the public tip of the data-insecurity iceberg. Business losses through computer failure, or major interruption to their data and operating systems, or the theft or loss of intellectual property or key business data, are more significant and more expensive.

Organisations face criminal damages, reputation loss and business failure if they fail to adequately secure their information. Directors face loss of personal reputation and time in prison if they fail in their duty to protect the information their organisations are holding.

But computer security technology, on its own, simply does not protect information. On its own, it just wastes money, gives a false sense of security and decreases business efficiency. What organisations need is a structured method for identifying the real information risks they face, the

financial impact of those threats and appropriate methods of mitigating those specific, identified risks. Securing information is not rocket science, whatever the technology vendors might say. Information is at risk as much through human behaviour (and inattention) as it is through anything else. Securing information therefore requires an approach that is as much about process and individual behaviour as it is about technological defences.

And no organisation has either the time or the resources to try and work out, on its own and from first principles, how to do this effectively. Apart from anything else, the time and error profile is likely to be unattractive.

No organisation needs to. ISO27001 already exists. This Standard, which contains current information security international best practice that has already been successfully implemented in more than 20,000 organisations around the world, gives organisations a reliable and effective framework for deploying an information security management system that will preserve its assets, protect its directors and improve its competitiveness.

This book explains how.

CHAPTER 1: INFORMATION ECONOMY, INTELLECTUAL CAPITAL

Executive summary

In the information economy, businesses depend on information and a substantial proportion of their value is made of intangible and information assets. The Board has a fiduciary duty to protect and preserve these assets.

The information economy

The information, or knowledge, economy is (as we all know) fundamentally different from the old manufacturing one. Information interchange has sped up the globalisation of markets, products and resourcing. This has led to increasingly similar shopping streets selling increasingly similar products throughout the developed world. All organisations now have an online presence; for many of them, the Internet is their primary or only method of business development and communication. More than 70 percent of workers in developed economies are now knowledge, rather than manual, workers – including those factory and farm workers whose work depends on understanding and using information technology. Information networking and telecommunications connectivity make this 'global village' possible – and bring a number of specific business threats and challenges at the same time.

The key characteristics of the global information economy, in contrast to those of the older manufacturing one, are:

- Information and knowledge are not depleting resources to be protected; on the contrary, sharing knowledge drives innovation.
- Effects of location and time are diminished – virtual organisations now operate round the clock in virtual marketplaces, and organisations based on East Coast America manufacture in China, handle customer support from India and sell globally through a single website.
- Laws and taxes are difficult to apply effectively on a national basis as knowledge quickly shifts to low tax, low regulation environments.
- Knowledge-enhanced products command price premiums.
- Captured knowledge has a greater intrinsic value than 'knowledge on the hoof'.

'What's new? Simply this: Because knowledge has become the single most important factor of production, managing intellectual assets has become the single most important task of business.'[1]

Intellectual capital

Most people are aware that, for most organisations, the value of their tangible assets – land and buildings, plant and machinery, cash and so on – is different from the value of their intangible assets – the ones not carried on their books. The value of the intangible assets is usually taken, in simple terms, as being equal to the difference between the net book

[1] Intellectual Capital: the New Wealth of Organizations, Thomas A Stewart, 1997.

value of the business and its current market capitalisation.

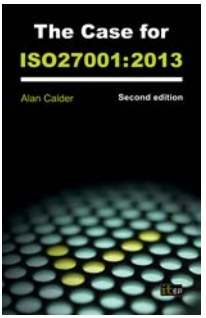
In the last 20 years the apparent value of these intangible assets has grown and now, in many cases, their value exceeds that of their tangible assets – sometimes considerably. In the information age, an organisation's key asset is its intellectual capital: its human resources, retained knowledge and intangible assets. Every organisation with a long-term desire to survive and succeed in its chosen market has to focus on preserving, protecting, developing, and applying its knowledge assets – its 'intellectual capital' – for the benefit of its shareholders.

Because an organisation's intellectual capital is valuable, someone else wants it: you could argue (although most accountants might prefer not to) that the definition of an asset is that it is something valued by more than one person – after all, if no one else wants it, it's not much of an asset. If other people want what you've got, you've got to ensure they don't get it – other than on your terms. You've also got to be sure that assets which you use in your business (even if no one else knows about or wants them – yet) are protected from destruction or corruption – otherwise your business' operating capability will be hampered.

Managing this risk – preserving and protecting these assets – is a key board responsibility. Intellectual capital and information assets need to be protected so that the organisation can continue to exploit them in pursuit of its competitive strategy. Information assets depend, for their productive existence, on information and communication technology. Information security, therefore, is also (but not primarily) about computer security and system security.

ISO27001

ISO27001 is the International Standard for Information Security Management Systems and it provides organisations with best practice guidance for identifying, assessing and controlling information risks in strategic business plans and everyday operational environments. It's ***the*** essential Standard for the information-age organisation.



- Understand ISO27001 and learn how it can help your organisation fight cybercrime, combat cyber-terror and improve your corporate governance
- Updated for ISO27001:2013
- *A concise, readable overview of things to consider when putting together a convincing proposal for an ISMS* (Mike Smith, Consultant)

Buy your copy today!

www.itgovernance.co.uk/shop/product/the-case-for-iso-27001-2013-second-edition

www.itgovernance.eu/shop/product/the-case-for-iso-27001-2013-second-edition

www.itgovernanceusa.com/shop/product/the-case-for-iso-27001-2013-second-edition

www.itgovernancesa.co.za/p-796-the-case-for-iso-27001-2013-second-edition.aspx

www.itgovernance.asia/shop/product/the-case-for-iso-27001-2013-second-edition