

Achieving Best Practice in Public Sector Information Security

ANDREA C SIMMONS



Achieving Best Practice in Public Sector Information Security

is published by Ark Group



UK/EUROPE OFFICE

Ark Group Ltd
266/276 Upper Richmond Road
London SW15 6TQ
United Kingdom
Tel +44 (0)20 8785 2700
Fax +44 (0)20 8785 9373
info@ark-group.com

NORTH AMERICA OFFICE

Ark Group USA
4408 N. Rockwood
Suite 150
Peoria IL 61615
Tel +1 773 529 5750
Fax +1 773 529 5760
info@ark-groupusa.com

ASIA/PACIFIC OFFICE

Ark Group Australia Pty Ltd
Main Level, 83 Walker Street
North Sydney NSW
Australia 2060
Tel +61 1300 550 662
Fax +61 1300 550 663
aga@arkgroupasia.com

Head of editorial

Kate Clifton
kclifton@ark-group.com

Publishing director

Lucy Brazier
lbrazier@ark-group.com

Head of production

Danielle Filardi
dfilardi@ark-group.com

UK/Europe marketing enquiries

Adam Scrimshire
ascrimshire@ark-group.com

US marketing enquiries

Daniel Smallwood
dsmallwood@ark-group.com

Asia/Pacific marketing enquiries

Laura Scully
lscully@arkgroupasia.com

ISBN: 978-1-906355-39-5

Copyright

The copyright of all material appearing within this publication is reserved by Ark Conferences 2008. It may not be reproduced, duplicated or copied by any means without the prior written consent of the publisher.

Achieving Best Practice in Public Sector Information Security

ANDREA C SIMMONS



Contents

Executive summary	VII
About the author	XI
Chapter 1: Introduction	3
Why is information security important?	3
Regulatory and moral drivers for improving data security	7
Chapter summary	8
Chapter 2: Once more into the breach	11
Roll call.....	11
Handling	11
The summer of reporting	15
Security policy framework	19
The influence of the ICO.....	20
Chapter summary	26
Chapter 3: It's all about the data	31
In defence of the DPA	31
Principle 7 internally.....	32
Principle 7 externally	34
Adequacy.....	35
Principle 7 – Defence in depth	35
Principle 7 – Key steps to compliance	36
Chapter summary	37
Chapter 4: Information governance	39
Introduction	39
The five initiatives.....	40
Supporting evidence.....	40
Chapter summary	40
Chapter 5: ISO27001 explained	43
Introduction	43
What is an information security management system (ISMS)?	43
PDCA – Plan, do, check, act	45

Understanding ISO27001 – Part 1	46
What are the benefits of ISO27001?	48
Certification.....	48
Chapter summary	50
Chapter 6: Putting it all together	53
Risk assessment	53
Information security policy	55
Organisation of information security.....	57
Ownership and asset management	62
Human resources for information security	66
Information security awareness.....	70
Physical security	71
Communications and operations management	73
Access control	76
Information systems acquisition, development and maintenance	77
Security incident management.....	80
Business continuity management (BCM).....	83
Compliance	87
Chapter summary	89
Chapter 7: Payment Card Industry Data Security Standard (PCI DSS)	97
Introduction	97
What is required?	97
Protecting sensitive data	98
Chapter summary	99
Chapter 8: Government Code of Connection (CoCo).....	101
CoCo overview.....	101
Chapter summary	101
Chapter 9: The environmental angle	103
Introduction	103
Energy consumption.....	103
Reduce, reuse, recycle.....	103
Where security fits in	104
Questions to ask your (actual or potential) service provider	105
Best practice.....	105
Applicable standards.....	105
Chapter summary	106
Chapter 10: Ethics and professionalism	109
The ethical dimension	109
The IA community	109

The competent professional	112
Chapter summary	113
Chapter 11: Summary of best practice	115
Technical recommendations	115
Chapter summary	115
Chapter 12: Legislative and regulatory drivers.....	121
Data Protection Act (DPA) 1998	121
Freedom of Information Act (FOIA) 2000	121
Code of practice on records management.....	122
Environmental Information Regulations 2004	122
Regulations on the Reuse of Public Sector Information (RPSI) 2005	123
Protective marking.....	124
Human Rights Act (HRA) 1998 and the European Convention on Human Rights.....	125
Children Act 2004	125
Disability Discrimination Act 1995.....	125
Common law duty of confidence.....	127
Public Records Act 1958, etc.	127
Local Government Acts	128
Town and Country Planning (Electronic Communications) Order 2003	128
Civil Contingencies Act 2004	128
Regulation of Investigatory Powers Act (RIPA) 2000	129
Computer Misuse Act 1990.....	130
Privacy and Electronic Communications Regulations (PECR) 2003	130
Retention of Communications Directive.....	131
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	132
Convention on Cybercrime.....	132
Electronic Communications Act 2000.....	133
Intellectual property.....	133
Official Secrets Act 1911.....	133
Private Security Industry Act 2001	134
Public Interest Disclosure Act 1998.....	134
Chapter summary	134
Chapter 13: Further Reading.....	137
Index	139

Executive summary

SO, WHY bother about information security? Recent high-profile data security breaches in the UK have brought data and information security into sharp focus. A vast amount of information is held by public sector organisations and much of it is of a sensitive nature, including banking details, income, personal addresses, telephone numbers and health records. As technology evolves, personal data becomes more readily available to those who would (and do) exploit it, so public sector organisations need to be sure they are taking the inherent security issues seriously to ensure that citizens' personal data is in safe hands.

It is important that senior management demonstrate commitment and leadership and ensure everyone understands that information security is not just an IT issue, but a critical organisational issue which affects the long-term success (and indeed the survival) of the organisation. Information systems are vital to the majority of public sector activities, therefore it is appropriate that responsibility starts at the most senior level of management; but to be effective, it must be delegated to all staff.

No organisation can ever be described as either 100 per cent compliant with best practice nor 100 per cent risk free – information assurance is a journey, not a destination, for the want of a hackneyed cliché – from IT security, through information security (IS), through information assurance (IA) and maturing to information governance (IG) over time.

This report considers the importance of information security in the public sector and reviews a number of cross-cutting themes. The author has worked extensively with local government and other public sector bodies and so is well-versed in the transformational agenda and the plethora of competing priorities that face many of the readers of this report. The following statement best encapsulates the intentions of this report:

...to pull together the themes, issues, strands, tools, resources available and provide a view on them in order to be able to signpost the reader towards clarity in understanding what is required, with the starting blocks of a route map to stronger, more embedded information security.

With this in mind, the relevant available controls in ISO/IEC 27001:2005 (ISO27001) are referenced throughout this report, where it is appropriate to highlight their applicability. This is particularly relevant since this is becoming the most oft-quoted standard for services and supply, and forms the basis of the requirements for the government secure exchange system (see Chapter 8). Relevant and apposite cases of information security incident as identified or reported in the press are notated in boxouts throughout the report, with a cross reference to the security issue (i.e. confidentiality, integrity or availability) and the ISO27001 control that would have reduced the risk and/or the impact of the incident.

“No authority can ever say it will never lose information but by ensuring the standards in your authority are equivalent to, or exceed, the best practice identified ... the public will be reassured that all reasonable steps were taken to preserve and protect their information.”

LGA Data Handling Guidance, October 2008.

Chapter 1 provides an introduction to the concept of information security as it is widely accepted now – particularly through the information security standards available to us all. There follows, in Chapter 2, a review of the scale of breaches experienced during the past 18 months and their impact on how we operate in the light of various government reports and the influence of the information commissioner. suffice to say that no doubt this list will already be out of date once this report is printed, given the almost daily round of breaches being referenced in the media. As a result of the issues elucidated in Chapter 2, Chapter 3 expands on the specifics of data within the context of the scale of direction provided within Principle 7 (the ‘security principle’) of the Data Protection Act 1998. To position this within a context of operational tools, Chapter 4 explains the concept of information governance in relation to the Information Governance toolkit. An overview of ISO27001, the information security management standard, is provided in Chapter 5. The various approaches and techniques that can and should be used to evaluate and embed information security are explored in Chapter 6, which provides a full assessment of a range of options for embedding information security management, ranging from roles and responsibilities through to incident management and business continuity. The subject of the Payment Card Industry Data Security Standard (PCI DSS) is covered in Chapter 7, which is supported by similar handling of the

Government Code of Connection (CoCo) in Chapter 8. The environmental angle and related issues are covered in Chapter 9, and Chapter 10 discusses the impact and importance of ethics and professionalism within the information security arena. Chapter 11 provides a summary of best practice in information security.

We all need to be able to give a consistent message and add value to our organisations by virtue of our security posture and actions. This report is written in a more personal style than many of you may have read during 2008. Clearly all the words and all the edicts over time have not really sunk in – even though we all know what best practice actually is. So perhaps it is time for a change of direction. A dialogue is required, one that shakes the current firmly-held views to see if enough leaves fall from the autumnal trees to actually enable new growth in the Spring of 2009.

Thanks are due to the many colleagues and peers in the industry, nationally and internationally, who have made so many resources available online and in circulation over a number of years. There is no shortage of information available on this subject, although it is appreciated that it takes a certain type of mentality to be able to digest it all and then process it appropriately for whatever organisation you are working for at the time. It is hoped that this report pulls a lot of the latest thinking together (as well as some age-old adages that have not changed in a number of

decades – there are some basics that must be done) and constructs the nearest thing to a roadmap towards information security best practice as possible. The nuggets of gold are all in here. Any errors or omissions are my own and I apologise for any glaring unintentional oversight. Equally, this report will be, in some places, out of date as soon as it is produced as so many changes are ongoing. It should also be noted that the contents, in the main, are as applicable to the public sector as they are to the private sector – it's just the legislative landscape that tends to differ slightly. So the contents should be useful in dealing with third-party service providers, too.

Rest assured I am well aware of an extremely active community of information governance specialists working across local government and beyond. In other words, there are those who have been constantly seeking to address these issues and protect their organisations for many a long year. Perhaps now they can come out of whatever shadows they have been forced to hide behind, and can be listened to in all seriousness and with greater understanding as a result of the past couple of years' worth of experience in relation to information security breaches and the resultant requirements to change. This can only be a good thing going forward. The 'truth' has long been out there.

About the author

Andrea Simmons, M.Inst.ISP, CISSP, CISM, MBCS CITP, BA, independent information governance consultant, founder and director, Simmons Professional Services

www.simmonsprofessionalservices.co.uk

ANDREA SIMMONS is an experienced information compliance evangelist/business consultant and project manager with expertise in several disciplines: information security management (ISO27001 – ISMS, strategy and planning, policies and procedures development and implementation, and so on); information rights legislation/regulation and standards (including data protection and freedom of information) and information and records management.

She has over 12 years' experience in the IT industry within both the public and private sector, implementing compliance programmes and information security management systems (ISMS). Andrea is currently running her own consultancy business (Simmons Professional Services Limited) and works associatively with several professional services organisations in the public and private sector.

Andrea undertakes consultancy, speaking and writing assignments and enjoys a varied portfolio of activities across the information governance space.

Andrea has also held the role of consultant security forum manager for the British Computer Society (www.bcs.org/security) and has been a member of the Management Committee of IAAC (www.iaac.org.uk) for several years. She is also a full, chartered member of the BCS and its relevant specialist groups – security, audit, law – and is on the BCS Register of Security Experts. Andrea is also a member of ISACA, ISSA, ISC2 and the Cyber Security KTN, and a founding member of the Institute of Information Security Professionals, to name but a few! Andrea achieved Chartered IT Professional Status in February 2007 and M.Inst.ISP in 2008.