INFORMATION SECURITY MANAGEMENT PRINCIPLES

Second edition

Andy Taylor (editor), David Alexander, Amanda Finch, David Sutton

bcs
The Chartered Institute for IT

INFORMATION SECURITY MANAGEMENT PRINCIPLES

BCS, THE CHARTERED INSTITUTE FOR IT

BCS, The Chartered Institute for IT champions the global IT profession and the interests of individuals engaged in that profession for the benefit of all. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

Our vision is to be a world-class organisation for IT. Our 70,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised qualifications.

Further Information
BCS, The Chartered Institute for IT,
First Floor, Block D,
North Star House, North Star Avenue,
Swindon, SN2 1FA, United Kingdom.
T +44 (0) 1793 417 424
F +44 (0) 1793 417 444

www.bcs.org/contact

bcs
The
Chartered
Institute
for IT

INFORMATION SECURITY MANAGEMENT PRINCIPLES

Second edition

Andy Taylor (Editor), David Alexander, Amanda Finch and David Sutton

bcs
The Chartered Institute for IT

Published by BCS Learning and Development Ltd, a wholly owned subsidiary of BCS, The Chartered Institute for IT, First Floor, Block D, North Star House, North Star Avenue, Swindon, SN2 1FA, UK.
www.bcs.org

ISBN: 978-1-78017-175-3
PDF ISBN: 978-1-78017-176-0
ePUB ISBN: 978-1-78017-177-7
Kindle ISBN: 978-1-78017-178-4

Paperback
available

British Cataloguing in Publication Data.
A CIP catalogue record for this book is available at the British Library.

Disclaimer:
The views expressed in this book are of the author(s) and do not necessarily reflect the views of the Institute or BCS Learning and Development Ltd except where explicitly stated as such. Although every care has been taken by the authors and BCS Learning and Development Ltd in the preparation of the publication, no warranty is given by the authors or BCS Learning and Development Ltd as publisher as to the accuracy or completeness of the information contained within it and neither the authors nor BCS Learning and Development Ltd shall be responsible or liable for any loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication or by any of the aforementioned.

Typeset by Lapiz Digital Services, Chennai, India.
Printed at CPI Antony Rowe Ltd, Chippenham, UK.

CONTENTS

LIST OF FIGURES AND TABLES

AUTHORS

Andy Taylor, after initially teaching in secondary schools, has been involved with information assurance for over 20 years, starting when he served in the Royal Navy in several posts as security officer. He had responsibility for all classified and cryptographic materials in both warships and shore establishments, at times helping to maintain the effectiveness of the nuclear deterrent. After leaving the Royal Navy he chose a further career in consultancy and was instrumental in achieving one of the first accreditations for a management consultancy against the information security standard ISO17799 (now ISO27001).

As one of the earliest members of the CESG Listed Advisor Scheme (CLAS) approved by Government Communications Headquarters (GCHQ), he has provided information assurance advice to a wide variety of organisations in both the public and private sectors including the Health Service, Home Office, utility regulators, the Prison and Probation Services and web developers. He has developed and delivered a number of specialist security briefings to help educate users in the effective use of information in a secure manner, and has been lecturing to all new staff in the Treasury Solicitors for over 10 years. He has a passionate interest in maintaining the highest standards of information assurance and helping others to gain expertise in it. To that end he is now the lead assessor for one of the three bodies that certify IA professionals against a framework of competences through the government's CESG scheme, which was set up in 2012.

David Alexander is Head of Vulnerability Research at Regency IT Consulting and specialises in information security architectures, the security of industrial control systems, information assurance and governance. He has 15 years' experience as an information security practitioner and consultant. In that time he has worked on a wide range of commercial, central government and defence projects around the world. David started his career as an officer in the RAF, learning the need for information security at the outset of his working life. He has been involved in IT for over 25 years, the first 10 of these as a software engineer, operations manager, project manager and IT consultant, after which he changed sides from 'poacher to gamekeeper' and became an information security practitioner. He has been a CLAS consultant for 10 years and was one of the first 50 people in the world accredited as Lead Auditor for what is now ISO27001. David is a director and full member of the Institute for Information Security Professionals (IISP), he is a Chartered IT Professional, Fellow of BCS and a committee member of their Information Security Special Interest Group.

Amanda Finch has specialised in information security management since 1991 when she helped establish the function within Marks & Spencer. As security manager, she has been at the heart of shaping information security within the company and has developed an extensive understanding of the commercial sector and its particular security needs. Amanda is engaged in all aspects of information security management and takes a pragmatic approach to the application of security controls to meet business objectives. As an active contributor within the industry, Amanda is particularly interested in raising levels of education and in gaining recognition for the discipline as a recognised profession. She is involved with the principal organisations in order to encourage this. Amanda has a Masters' degree in Information Security and holds full membership of the Institute of Information Security Professionals (IISP). In 2007 she was awarded European Chief Information Security Officer of the year by *Secure Computing* magazine.

David Sutton's career spans more than 45 years and includes computing, voice and data networking, radio transmission, information security and critical information infrastructure protection. He joined Cellnet (now Telefónica O2 UK) in 1993, where he was responsible for ensuring the continuity and restoration of the core cellular and broadband networks, and represented O2 in the electronic communications industry's resilience forum. In December 2005, he gave evidence to the Greater London Authority enquiry into the mobile telecoms impact in the London bombings. David has been a member of the BCS Professional Certification Information Security Panel since 2005 and delivers lectures on risk management, business continuity and disaster recovery at the Royal Holloway University of London, from which he holds an MSc in Information Security. Since retiring from O2 in 2010, he has undertaken a number of critical information infrastructure projects for the European Network and Information Security Agency (ENISA), and is currently developing training material for InfoSec Skills.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contributions made by Karen Webb and Stef Venn of BCS for bringing them together, providing good lunches and generally trying to keep them in order to enable the examinations to be developed effectively, which in turn, enabled this book to be written. Thanks are also due to Ed Brown for the cartoons.

For this second edition, the authors would like to thank Jutta Mackwell for her help in getting this second edition into print. We would also like to thank colleagues and clients, families and friends who willingly, or more usually unwittingly, have provided many of the anecdotes, examples and stories with which we have tried to explain some of the principles in this book.

ABBREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BCP	Business Continuity Plan
BCS	BCS, The Chartered Institute for IT
BIA	Business Impact Analysis
BS	British Standard
BYOD	Bring Your Own Device
CA	Certification Authority
CBT	Computer-Based Training
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CCT	CSIA Claims Tested
CCTV	Closed-Circuit Television
CESG	Communications-Electronics Security Group
CIO	Chief Information Officer
CISMP	Certificate in Information Security Management Principles
CISO	Chief Information Security Officer
CLEF	Commercial Licensed Evaluation Facility
CMM	Capability Maturity Model
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPNI	Centre for the Protection of National Infrastructure
CSIA	Central Sponsor for Information Assurance
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DES	Data Encryption Standard
DHS	Department for Homeland Security
DMZ	Demilitarised Zone
DoS	Denial of Service
DPA	Data Protection Act
DR	Disaster Recovery
EAL	Evaluation Assurance Level
EDGE	Enhanced Data Rates for GSM Evolution

EDI	Electronic Data Interchange EDSETSI Documentation Service
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
ETR	Evaluation Technical Report
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS PUBS	Federal Information Processing Standards Publications
FIRST	Forum for Incident Response and Security Teams
FoIA	Freedom of Information Act
FSA	Financial Services Authority
GATT TRIP	General Agreement on Tariffs and Trades, Trade Related Aspects of Intellectual Property Rights
GCHQ	Government Communications Headquarters
GFS	Grandfather–Father–Son
GIPSI	General Information Assurance Products and Services Initiative
GPRS	GSM Packet Radio Service
GSM	Global System for Mobile communications
HIDS	Host Intrusion Detection Systems
HIPAA	Health Insurance Portability and Accountability Act
HRA	Human Rights Act
HSDPA	High-Speed Downlink Packet Access
IA	Information Assurance
IaaS	Infrastructure as a Service
ICSA	Institute of Chartered Secretaries and Administrators
ICT	Information Communications and Technology
ID&A	Identification and Authentication
IDC	Inter-Domain Connector
IDS	Intrusion Detection System
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
IRT	Incident Response Team
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	IT Infrastructure Library

ITPC	Infosec Training Paths and Competencies
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
LAN	Local Area Network
LOB	Line of Business
MIFID	Markets in Financial Instruments Directive
NDA	Non-Disclosure Agreement
NIDS	Network Intrusion Detection Systems
NIST	National Institute for Standards and Technology
OSA	Official Secrets Act
PaaS	Platform as a Service
PACE	Police and Criminal Evidence Act
PAS	Publicly Available Specification
PCI	Payment Card Industry
PDCA	Plan–Do–Check–Act
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFC	Request for Comments
RIPA	Regulation of Investigatory Powers Act
ROI	Return on Investment
SaaS	Software as a Service
SANS	Sysadmin, Audit, Network, Security
SEAP	Security Equipment Assessment Panel
SLA	Service Level Agreement
SOMA	Security Operations Maturity Architecture
SSL	Secure Sockets Layer
TOE	Target of Evaluation
UPS	Uninterruptible Power Supply
VOIP	Voice Over IP
VPN	Virtual Private Network
WA	Wassenaar Arrangement
WAN	Wide Area Network
WAP	Wireless Access Point
WiFi	Wireless Fidelity

PREFACE

Information has been important for a very wide variety of reasons and for as many centuries as man has been able to pass valuable data to another person. The location of the nearest water hole, herd of wild animals or warm cave was a carefully guarded secret that was only passed on to those with a need to know and who could be trusted not to divulge the information to other, possibly hostile, tribes. The method of transfer and the storage of such information were, perhaps, rather more primitive, but the basic principles of information security have not changed too much since those days.

Information assurance is now well founded in three major concepts – those of confidentiality, integrity and availability. Managing these concepts is critical and, as information has increasingly become one of the modern currencies of society, it is the retention of assurance in an appropriate and cost-effective manner that has become of keen interest to businesses in all sectors, of all sizes and in all locations. Specific measures taken to ensure that information is held securely are termed information security – the method of achieving information assurance.

As an example, even within living memory, the quantity of numbers we are given and require to enable us to exist and participate in modern society has risen almost exponentially from virtually zero in the early part of the twentieth century to several hundred (and still growing) now: PIN codes; licence numbers; credit card numbers; number plates; telephone numbers; employee numbers; health, tax and insurance numbers; access codes; customer numbers; train times; and tram or bus numbers, the list is seemingly endless. We now need to know and remember these on a day-to-day basis and that is before we start work proper and have to deal with all those things that allow us to earn our salary, where even more numbers and other elements of information will occur.

The mechanisms we use to manage information are the areas where we have seen very significant change, notably in the last few decades. The advent of computers in particular has altered the way we manage information extensively and has also meant that we have much more information to worry about than ever before. Information has become the key to success in almost any field of adventure and so the assurance of it has gained in significance and, perhaps more importantly, in value to a business or organisation. It may not necessarily be financial value that is the most important factor. Lack of knowledge of some issues, the way things are done, or knowing the currency of specific pieces of information may be more important than any financial evaluation. Nevertheless looking after information properly is still very important.

One other factor that has significantly altered our need for assurance of information is that of mobility. When the only place we had business information (and where we were able to look after it properly) was the office, life was straightforward. To secure information we closed and locked the office door. Today we expect and need to have information in a wide variety of locations, including when we are on the move in cars and trains. With open-plan offices and the increasing mobility of the office environment, we now have a critical need for improved assurance if we are not to allow others to gain access to our information inappropriately.

Threats, vulnerabilities and countermeasures have also changed and grown in complexity in some areas, although it is still essential to consider the easiest and often cheapest countermeasures before getting into large or expensive solutions. The increase in capability of those intent on causing harm to companies, public bodies and other organisations, means that the role of the information assurance manager and professional has increased in complexity to such a degree that it is now quite possible to have a full and very satisfying working life entirely within this field of expertise.

The legislation that is introduced by governments to address the increasing problems of information assurance in all its guises is also an area of concern, and this book covers the most important principles and implementation of such laws. Once again though, it is important that readers understand that this book has been written in the UK and is based on English law. Other countries, even devolved administrations within the UK, may have further or different legislation with which you should become acquainted.

This book accompanies the BCS Certificate in Information Security Management Principles. This qualification is an introduction to the whole area of information assurance management and is the first step towards a full understanding of the issues and the comprehensive management of the assurance of information, wherever it may be. Whilst BCS is clearly concerned with the impact and effective use of computers in the main, it is recognised that it is impossible to divorce the management of information security in computers from the management of information in any other media, or from the security of the tools used to process information. Thus, in this book, the boundaries between different forms of information storage, processing, transmission and use are deliberately blurred or indeed removed entirely. It is not significant whether a particular piece of information exists in electronic form, paper form or, indeed, in someone's head. Its appropriate protection is the main factor and all aspects of its assurance must be considered from all angles.

The technical aspects of information security, including the technical details of information systems (IS), computer networks, communication systems, cryptography and related areas, are not part of the syllabus for this examination despite their importance. They appear in higher qualifications and so (in this book) reference is made to them in passing, but they are not covered in any detail. The syllabus and this book have remained technology-neutral as far as possible.

The examination syllabus was updated to version 7.3 in 2012, and it is the guide for the contents of the second edition of this book. As a result of studying this book, the reader should have a very clear understanding of the various elements of information assurance and should be able to consider taking the professional examination.

A simple scenario has been introduced in order to help develop full understanding and to provide a close-to-life example of the real world. Activities based on the scenario are suggested throughout the book, again to help bring reality into the concepts discussed, and it is hoped that the reader will do these in an appropriate manner – formally or informally as suits them best.

Reference has been made to national and international standards that are applicable to information assurance, but there is no requirement for detailed specific knowledge of any of those standards. They are, naturally, important, but it is recognised that they will change over time and be more applicable in some parts of the world than in others. Readers should ensure they are familiar with the standards relevant to their country, their area of interest, their organisation and their business sector.

After studying this book and the related syllabus, the reader should be able to demonstrate a good knowledge and basic understanding of the wide range of subject areas that make up information assurance management. The examination tests the knowledge of principles rather than the knowledge of specific technologies, products or techniques. This means that where in the book specific technical examples are used to illustrate particular principles, it is the understanding of the principles that is of prime importance when considering the examples and not the examples themselves.

1 INFORMATION SECURITY PRINCIPLES

This chapter covers the basic principles of information assurance. It introduces some specific terminology, together with its meaning and definitions, and considers the use of such terminology across the field of information assurance management. It also discusses the way in which information assurance management relates to its environment.

CONCEPTS AND DEFINITIONS

As in any area of business, information assurance management has its own language although, being very closely related to the business need, it is limited in scope and complexity to enable the wider business population to appreciate the concepts with little difficulty. Each of the terms listed below will be further discussed and expanded upon later in the book in the appropriate section.

In the following sections, the definitions in italics have been taken from the General Information Assurance Products and Services Initiative (GIPSI) Security Glossary and Terminology Definitions where available. GIPSI have taken the definitions from BS ISO/IEC 27001: 2005 where the definition exists, from other ISO standards where there was no 27001 definition, and from SC27 or SD6 where ISO standards provide no definition. Where there is no extant definition, this is provided from other sources (or from the authors with sources where applicable).

Learning outcomes

Following study in this area, the reader should be able to define and explain each of the following terms and to describe their appropriate use as applicable.

Information security

Confidentiality. The property that information is not made available or disclosed to unauthorised individuals, entities or processes (ISO 27001)

Information will often be applicable only to a limited number of individuals because of its nature, its content or because its wider distribution will result in undesired effects including legal or financial penalties, or embarrassment to one party or another. Restricting access to information to those who have a ‘need to know’ is good practice and is based on the principle of confidentiality. Controls to ensure confidentiality form a major part of the wider aspects of information assurance management.

Integrity. The property of safeguarding the accuracy and completeness of assets (ISO 27001)

Information is only useful if it is complete and accurate, and remains so. Maintaining these aspects of information (its integrity) is often critical and ensuring that only certain people have the appropriate authority to alter, update or delete information is another basic principle of information assurance.

Availability. The property of being accessible and usable upon demand by an authorised entity (ISO 27001)

Information that is not available when and as required is not information at all, but irrelevant data. Availability is one area where developments in technology have increased the difficulties for the information assurance professional very significantly. In the past, in an ideal world, all important information could be locked up in a very secure safe of some form and never allowed to be accessed – just about perfect assurance but, naturally, totally impractical. There will, therefore, always have to be a compromise between security in its purest sense and the availability of the information. This compromise has to be acknowledged throughout all aspects of information assurance and has a direct bearing on many of the principles covered in this book.

Assets and asset types

Asset. Anything that has value to the organisation, its business operations and its continuity (ISO 27001)

Assets come in as great an array of types as the mechanisms for using them. In information assurance, three main types of assets are considered although the subcategories that fall within each of these main types can be numerous. The three main types are (1) pure information (in whatever format), (2) physical assets such as buildings and computer systems and (3) software used to process or otherwise manage information. When assets are considered in any aspect of information assurance, the impact on all three of these asset types should be reviewed. The value of an asset is usually calculated by means of a business impact assessment, which estimates the cost or value of its loss or unavailability to the business. There are, however, other aspects to consider including, but not limited to, the value to a competitor, the cost of recovery or reconstruction, the damage to other operations and even the impact on such intangibles as reputation, brand awareness and customer loyalty.

Threat, vulnerability, risk and impact

The understanding of these terms is critical to the whole of information assurance.

Threat. A potential cause of an incident that may result in harm to a system or organisation (ISO 27002)

A threat is something that may happen that may cause some unwanted consequence. As a simple example, if we see clouds in the sky that look large and dark we talk about the threat of rain. Naturally to some, farmers perhaps, this threat is not unwanted at all and so they would not have the same view of the clouds and of the potential for rain, and this is an important point to recognise. Threats to one organisation may well be opportunities to another – it is all very dependent on the viewpoint, the environment and the situation that is being considered.

Vulnerability. A weakness of an asset or group of assets that can be exploited by one or more threats (ISO 27002)

A vulnerability is a weakness, something that, if exploited, could cause some unwanted effect(s). To continue the example above, if someone was to venture out into the cloudy environment without an umbrella, this could be considered a vulnerability. If something else (the threat) happens (it rains) then the consequences could be detrimental.

Risk. The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation (ISO 27002)

Risk is, then, the combination of these two. If there is a threat (of rain) and a vulnerability (of not carrying an umbrella), then there is a risk that the individual concerned might get wet and ruin their expensive clothes. There may well be other risks associated with this same set of circumstances –damaged hairstyle, late attendance for an appointment, and so on. It is also important to recognise that sometimes there may be a combination of circumstances that lead to further, more serious risks as well. The lateness of attendance at an appointment, combined with a number of other similar occurrences, could result in the termination of employment.

Impact. The result of an information security incident, caused by a threat, which affects assets (ISO 27005)

The impact of the risk actually occurring is perhaps the most important concept of all to grasp. It is the potential impact that has to be considered and managed in information assurance. If the impact is small and insignificant – a wet coat in the example above – then it may be entirely appropriate to accept the risk and to take no further action other than to monitor it. On the other hand, if the potential impact could be dismissal from a well-paid job, then more appropriate countermeasures need to be considered – the purchase of an umbrella, hiring a taxi or similar. As far as businesses are concerned, the impact on the organisation and its daily activities is usually the crucial consideration and will often warrant further measures being taken.

Information security policy concepts

Any organisation should have a policy for its management of information assurance. This would normally be a short, punchy statement from the chief executive stating that they acknowledge the risks to the business resulting from poor information assurance and will take appropriate measures to deal with them. It should include statements that make it clear that the organisation regards risk as a serious issue, which should be discussed at all appropriate meetings. Moreover, those with the correct authority and responsibility should take an active interest in risk prevention. It is common for organisations to form an information assurance working group to lead the activities necessary to ensure appropriate levels of assurance within the organisation.

The purpose of controls

Controls, in the information assurance sense, are those activities that are taken to manage the risks identified. There are four main types of control, although the actual implementation of each of these types can be very varied.

Eliminate. Risk avoidance – Decision not to be involved in, or action to withdraw from, a risk situation (ISO Guide 73)

This means taking a course of action(s) that removes the threat of a certain risk occurring at all. This could entail removing a particular item that is unsafe, choosing to do things a completely different way or any number of other options. This action is sometimes referred to as 'prevent', 'avoid' or 'terminate'.

Reduce. Risk reduction – Action taken to lessen the probability, negative consequences, or both, associated with risk (ISO Guide 73)

This means to take one or more actions that will reduce the impact or the likelihood of a risk occurring. It is often necessary to use several of these measures in partnership to have the desired overall effect. This could include having contingency measures in place that mitigate the effect if the risk does occur – a backup plan or 'plan B'. This action is sometimes referred to as 'treat'.

Transfer. Risk transfer – Sharing with another party the burden of loss, or benefit of gain, for a risk (ISO Guide 73)

This means to take steps to move the accountability for a risk to another organisation who will take on the responsibility for the future management of the risk. In practice, this might mean taking out some form of indemnity or insurance against the risk occurring or perhaps writing contracts in such a way that the financial impact of a risk occurring is borne by a third party – liquidated damages. This action is sometimes referred to as 'share'.

Accept. Risk acceptance – Decision to accept a risk (ISO Guide 73)

This means senior management accepting that it is not considered practical or sensible to take any further action other than to monitor the risk. This could be for a number of reasons including, but not limited to: the likely impact of a risk is too small; the likelihood of a risk occurring is too small; the cost of appropriate measures is too high in comparison with the financial impact of the risk occurring; the risk is outside the organisation's direct control. The decision would also be related to the organisation's risk appetite, which determines the level of risk the organisation is prepared to accept. This is sometimes referred to as 'tolerate'.

Identity, authentication and authorisation

Identity. The properties of an individual or resource that can be used to identify uniquely one individual or resource (Authors)

Frequently there is a need to establish who is accessing information and the identity of individuals may well be required. This may enable, for example, audit trails to be produced to see who changed a specific item of data and hence to assign an appropriate level of confidence to the change. This concept is equally applicable to assets such as specific pieces of information that need to be identified uniquely.

Authentication. Ensuring that the identity of a subject or resource is the one claimed (Authors derived from Authenticity in ISO 13335)

This process ensures that the individual is who they say they are and confirms their identity to a level of confidence that is appropriate for the task in hand. This could be simply asking them for their date of birth, or it could mean completing a complex identity check using, for example, tokens, biometrics and detailed biographical-data checks.

Authorisation. The process of checking the authentication of an individual or resource to establish and confirm their authorised use of, or access to, information or other assets (Authors)

In order for anyone to use a system of information retrieval, management, and so on, it is good practice to have a method of authorisation that makes clear the assets to which someone should have access and the type of access they should have. This authorisation will vary depending on the business requirement, the individual, the type of asset and a range of other aspects. Who has the authority to detail and approve such authorisations will vary according to the type of usage required.

Accountability, audit and compliance

Accountability. The responsibility for actions and processes (Authors)

When any action is carried out on an information system, or as part of the information assurance management system, an individual needs to be accountable for that action. The person who has the accountability may delegate the actual work to someone else, but they would still retain the accountability.

Audit. Formal or informal review of actions, processes, policies and procedures (Authors)

This is the checking (formal or informal) of the records of a system to ensure that the activities that were anticipated to have taken place have actually happened. The purposes of an audit could include identifying gaps in the system's functionality, noting trends over time to help with problem resolution or identification, or a number of other requirements. It can also help to identify misuse of information or the inappropriate use of an authorisation, for example, and thus identify unauthorised activity.

Compliance. Working in accordance with the actions, processes, policies and procedures laid down without necessarily having independent reviews (Authors)

Ensuring that a system or process complies with the defined or expected operating procedures is compliance. This could cover a major operation, such as a whole organisation being compliant with a recognised national standard for information assurance, or it could be much more limited with just certain aspects of the operation, or individual users of a specific system, being compliant. In general, compliance should be independently audited to achieve certification against a standard, legal or regulatory framework, for example.

Information security professionalism and ethics

The general awareness of the work done by information assurance professionals (as distinct from IT security professionals) is gradually growing as organisations become increasingly complex with more and more information being managed and processed. The adage that the staff are the most important asset of an organisation could now be seen to be outmoded since it is often the case that it is the information an organisation holds and uses effectively that has become its most important asset. Therefore looking after it has also gained in importance and the whole profession has grown to meet the need. New professional bodies, such as the Institute of Information Security Professionals (IISP), which was set up in 2006 in the UK, have helped to raise the profile very significantly, as have the various qualifications ranging from this introductory level to master's degrees and beyond.

The IISP has developed a competency framework for the information assurance professional. This, in turn, has been adopted and adapted by CESG into a certification scheme where individuals can demonstrate their competence and experience to independent assessors from one of three certification bodies, which will recommend the award of a certificate at various levels for a number of roles.

An information assurance professional will, inevitably, become party to some of the most important information an organisation might hold. This could be sensitive for a number of reasons but, in all cases, it is critical that the professional deals with it in the appropriate manner. Releasing information to a third party or other organisation, albeit with the best of intentions but without the approval of the owner, is probably one of the easiest ways to be dismissed. Non-disclosure agreements (NDAs) are now commonplace even in seemingly innocuous areas such as publishing and the retail marketplace as well as the more usual research and development, product innovation and financial areas.

The bottom line of all assurance is trust. Without it, it is impossible to operate in the world as it is today. The degree of trust is where there is room for manoeuvre and it is often the degree to which staff, customers, suppliers, shareholders and the like can be trusted that will determine the measures that have to be put in place. It is crucial, however, that the trust placed in information assurance professionals is not misplaced in any way. They must be above reproach and never be seen to compromise in this critical area.

Information security management system (ISMS) concepts

Information security management system (ISMS). That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (ISO 27001)

The main principle behind the ISMS is that there should be a 'one-stop shop' for all information pertinent to the assurance of information within an organisation. As soon as there is a need to go looking for documentation, policies, practices or anything else to do with assurance, the chances are that someone will not bother and will do their own thing instead.

Whilst there may well be good reason for them not to do this in terms of rules, regulations, punishments and the like, human nature being what it is, they will find a reasonable excuse for going down a different route if only because 'I thought it was OK and couldn't be bothered to check if it was the right way to do it'. The result of this approach will inevitably be a reduction in the overall level of assurance. In addition, any system that is too complex or difficult to use will result in users finding ways to get around the security measures put in place, perhaps again resulting in weakened assurance.

It is therefore critical that organisations make their information as freely and easily available as is possible, practical and necessary and this equally applies to the security rules controlling it. Naturally, there will be elements of policy that have to be more secure and that are available only to those with a strict 'need to know' but, in general, everyone should be able to access easily and quickly the appropriate information and the security measures pertinent to it.

The national and international security standards

Information assurance is the subject of several international and national standards and these should be considered when studying for the examination. The questions set in the examination will never be specific to any one standard, but will be generic to all best practice where applicable. The knowledge of the appropriate standards required for the examination is therefore limited to a general understanding of the principles involved as they reflect on best practice. In the UK, awareness of, for example, the ISO/IEC 27000 series and related British Standards would be helpful but not critical to the passing of the examinations. It is the broad principles that should be used as a basis for study as reflected in the examination syllabus.

There is though another aspect of this. When an information assurance professional is working in an organisation to deliver a secure and effective information management system, the relevant standards should always be viewed as the achievable goal for that system. Whether it is necessary to gain simple compliance or go the extra step to achieve certification is an arbitrary decision often based on other factors. Nevertheless, it is considered good practice to base an effective information assurance management system on the principles of the relevant standards. The use of an internationally accepted standard such as the ISO/IEC 27000 series makes sense in the global nature of operations today.

THE GROUP FOR THE APPRECIATION OF THE NATTERJACK TOAD (GANT) SCENARIO

The Group for the Appreciation of the Natterjack Toad (GANT) is a conservation group that is keen to promote and preserve the well-being of the Natterjack toad. It has a significant number of members in a number of different countries around the world, all of whom are keen to promote the work of the group, which is a charity registered in the UK. All the Group's information is either on a web-based application form, available to members on the internet, or on old-fashioned, paper-based documents held by Dr Jane Peabody, the honorary secretary/treasurer.

The Natterjack toad is an endangered species that is gradually being destroyed by the development of areas where it prospers and also by pollution, which affects the brackish water and sand dunes in which it lives.

The membership of the organisation is growing, and the system for managing the records of members is one area where there are some concerns about information assurance. Details of the Group's activities, meeting places, website and other aspects of its work have been compromised in the recent past owing to the server containing them having no significant security in place. The chairperson (Ms Rachel Jackson) believes it is the right time to take information assurance more seriously. She has heard a bit about information assurance, but needs to be clear what it really means and, most importantly, what the benefits and costs would be to the organisation.

The GANT scenario is a fictitious scenario that will be used throughout the book to provide examples and to be the basis of some questions to aid your understanding of the theory. The main objective of the scenario is to implement an effective information assurance system, but we will take you through various steps along the way to help with your understanding.

ACTIVITY 1.1

Assume that you have been invited to a committee meeting of GANT by the chairperson, who wants you to 'start the ball rolling' by explaining why it would be a good idea for GANT to think about information assurance.

To make your points most forcefully, she has asked you to define three threats to the organisation, three vulnerabilities and consequently three risks that any information assurance system would need to manage.

Solution pointers for the activities can be found at the end of the relevant chapters.

We have started above with developing an initial idea of the reasons for considering information assurance based on three possible problems. We will take that on to a more formal approach in due course – this is simply to get you thinking about some of the terms we have introduced in the first section of the book.

THE NEED FOR, AND BENEFITS OF, INFORMATION SECURITY

Any business will have information that is critical to its continued effective operation. Looking after this information in an appropriate way does not come free but has a price tag attached that can be, in some circumstances, very considerable. It is therefore essential that information assurance professionals are able to justify their recommendations for appropriate security measures in a sensible yet pragmatic manner, which must take into account the specific environment in which the business is based.

Learning outcomes

Following study in this area, the reader should be able to explain and justify each of the following concepts and to describe their appropriate use as applicable.

The importance of information security as part of a business model

Information security – Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (ISO 27001)

Neither information nor assurance operate in a vacuum. Both need to take into account the environment in which they are operating and to address the issues this environment brings with it. It is therefore critical that any information assurance system must be grounded firmly in the business world. This means that information assurance is not an issue for the IT manager or the security officer alone, but for the whole organisation. As soon as only one part of the organisation is given the task of running assurance, the rest of the organisation will bother less about it. All staff members of any organisation, regardless of its nature, its business, its location or any other factor, should be concerned about information assurance. It might be from a purely personal viewpoint (what happens to my personal data in this place?) or from a wider view of the effective continued operation of the organisation, but in either case all should be concerned and involved.

Information assurance (IA) – The confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users (UK Cabinet Office)

Physical, technical and administrative controls are needed to accomplish these tasks. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analogue or physical form. These protections apply to data in transit, both physical and electronic forms, as well as data at rest in various types of physical and electronic storage facilities. Information systems include any means of storing, processing or disseminating information including IT systems, media and paper-based systems.

Assurance should not be viewed as an ‘add-on’ to be included only if there is the time and the money to do it. To be truly effective, it has to be built into business processes at all stages. Whilst it might be possible in some areas to add in security measures at the last moment (an extra lock on a door or an additional staff security check) these will usually cost more and be less effective than if they had been added at the appropriate time earlier in the design process.

Different business models and their impact on security

In the last 30 years, the world of business has changed dramatically – perhaps more than in the previous 50 or 100 years. One of the principal reasons for this is the increased use of technology that has enabled business to be transacted remotely rather than in person. One of the consequences of this is that more people are able to make business transactions themselves rather than expecting others to act as intermediaries. No longer do we need to use travel agents to book our flights, local garages to obtain our cars or financial advisers to obtain investment packages for us. All these and many more transactions can be carried out directly with the supplier (often via the internet) or with a trader in another part of the country or the world who can offer a better deal. Whilst the access to such facilities is a huge advantage and can provide very significant financial savings, amongst other benefits, it has brought with it major issues of security both for the individual and for the organisation wishing to trade in this way.

The other very significant change in business has been the shift in the UK away from manufacturing and related primary industries to service and financial industries where the use of technology has an even bigger impact.

It is clear that the use of technology in manufacturing has changed those industries too but, it might be argued, in a more controlled and manageable manner. In the service industry, the availability of information has increased many times over and has liberated the industry based on information in a manner that is similar to the impact of the introduction of the steam engine or electricity in their day. This in turn has increased the importance and difficulty of keeping information securely.

Many organisations are now based and/or operate in more than one country. With global organisations now moving very sensitive information or other assets around the world at a moment's notice, the need to ensure that this is done securely and with proof of receipt, integrity and authority has grown too. Proving that the authorised person sent the correct document at the appropriate time only to the intended recipients, not to mention ensuring that it arrives in the same state as when it left the originator, are all issues that the information assurance manager now has to deal with to the satisfaction of their management and any ambitious litigant. In addition, organisations that operate within different countries need to understand the differing restrictions that local legislation may place on how their information can/must be handled.

There are many further risks from this change in the business model. With an increasing amount of trade being conducted across the internet, organisations must be aware of the dangers of virus infection, Denial of Service (DoS) attacks, unauthorised changes to their information in the public domain (for example internet websites) and the impact of any such issues on their reputation, financial status and other related areas. In addition, organisations have to deal with people about whom they know very little, but with whom they still need to establish an appropriate level of trust. The ability of disillusioned employees, ex-employees or groups of activists to damage an organisation by taking, deleting, altering or otherwise misappropriating critical business information from the employer and either passing it on to a competitor, or simply using it for their own ill-gotten gains, is now a very real issue. Whilst companies who have been the victims of such events are not inclined to increase the damage caused by making such acts public knowledge, there are so many apocryphal tales of the theft of client databases, deletion or alteration of critical financial data and other similar acts that it suggests that some at least are true.

There are also cautionary tales of laptop PCs containing highly sensitive or confidential information being lost or stolen from parked cars, to the embarrassment of the company or organisation.

The use of the internet for transactions, be it shopping for cars, food or financial services, as well as the storage of client, stock, financial and related information in a secure manner, has further increased the problems to be managed. The ability of the consumer to deal directly with the manufacturer has increased the risks for industry as well as for the consumer where the problems of unreliable services or products still abound. With the rise of business-to-business transactions, just-in-time operations and other similar services that rely heavily on the timely and accurate movement, storage and retrieval of critical information, the loss of a computer system for a comparatively short while can and has created serious financial losses for the businesses concerned. In 2010, Detica (an independent research organisation working on behalf of the UK Cabinet Office) estimated that £27 billion was lost by businesses in the UK through the business impact of malicious software (malware – viruses and the like) on their systems alone.

The effect of the rapidly changing business environment

'It is change, continuing change, inevitable change, that is the dominant factor in society today.' This quotation is from Isaac Asimov and it is now well understood that for a business to survive in the current climate of change, it must adapt and be able to adapt rapidly. This means that what was acceptable as a business practice last week may no longer be acceptable this week. Therefore any assurance system put in place must reflect this changing climate and be flexible enough to cope with it. However, this does not mean that the assurance can be relaxed or reduced in any way. Indeed if anything, the flexibility should produce a higher level of security and assurance that risks are being managed effectively.

Balancing cost and impact of security with the reduction in risk

Life can never be risk-free. Indeed, it is often considered that life is all about risk and its effective management. The measures taken in an organisation to reduce risk to an acceptable level can, at times, become excessively expensive. A careful balance must be struck between the cost or business impact of a risk if it occurs and the cost of the measures taken to reduce its likelihood or impact.

A typical example is insurance. An insurance policy may help to offset the cost of a risk occurring by providing the necessary financial backing to be used to deal with the occurrence of a risk. However, if the cost of the insurance policy is too high, it may simply be cheaper to accept that the risk might occur and pay the smaller amount out to deal with its consequences. It must also be remembered that whilst it may be possible to transfer to a third party some of the impact of a risk occurring – that is, the financial impact for example – it is frequently very difficult to transfer the other consequences of a risk, notably the impact on reputation, public opinion or other related results.

It is not uncommon for organisations to put in place extravagant measures to reduce the impact or likelihood of risk occurring when in reality the consequences of the risk occurring are limited, or the actual chance of it happening is so small that the expense is a waste of both money and effort in managing the risk unnecessarily.

A second problem is that of maintaining the currency of risk countermeasures. Once defined and planned, it is critical that they are not simply put on the shelf to await the risk arising. The world around us changes and so the countermeasures may not be valid or may change in their effectiveness or cost as time moves on. Thus risk management, and the maintenance of the consequential actions taken, is a continual and iterative process that must not be allowed to wither through lack of action or misplaced belief that the situation will not change.

Information security as part of company policy

Assurance is not an add-on. It is not possible to deal adequately with assurance by considering it as an additional expense to be avoided if at all possible. The most effective way to deal with it is to include it from the beginning, in all areas of the organisation. To this end, the inclusion of assurance as part of the operational policy of the organisation is the only cost-effective way of covering the issues adequately.

There are clear similarities between information assurance and health and safety issues. As soon as health and safety is seen as one person's problem (that of the health and safety officer) the battle for a safe working environment has been lost. Similarly, assurance is not the concern solely of the information security manager, but of the whole organisation. It is essential also that this involvement is from the top of the organisation to the bottom. Just implementing information assurance at middle management or on the shop floor is meaningless and will inevitably lead to further assurance issues. Senior management have a critical role to play to ensure they engender a working environment where information assurance is the norm and is accepted by all.

Policy, standards, guidelines and procedures documentation

Just having an information assurance policy on its own is meaningless. It must be fully supported by a range of other documentation covering the standards expected, the guidelines of how to do things correctly and procedures for what must be done to preserve the assurance of the information in question. This documentation must be comprehensive in its coverage, must be written in a style that is understandable to the intended audience, which may well be the ordinary staff member with very limited experience or knowledge of assurance matters, and must be readily available in an appropriate format.

It is good practice to ensure that any procedures to be followed are detailed in an easily digestible format, perhaps as desk cards or prompts for users, or as checklists for operators or support technicians. It must be remembered, however, that this is not only about computers. For example, procedures are also required for

the management of physical assets such as filing cabinets including how they should be cleared before their disposal to avoid the inadvertent inclusion of a confidential file for the second-hand filing cabinet marketplace. Where information critical to the organisation's continued operation is held solely in the heads of its staff, it is almost inevitable that, one day, this will result in one of the key staff members being ill, having an accident or being otherwise indisposed when a crucial decision or operation is required. Considering the management of the information in staff members' heads is just as important as the effective management of technical systems – some might say more so.

Corporate governance and related areas of risk management

In recent years the advent of some very high-profile commercial criminal investigations has resulted in much more stringent and invasive legislation regarding risk taking in companies. Sarbanes–Oxley in the USA, the effects on corporate governance of the Turnbull Report, the Companies Act in the UK and related issues have all had the effect of bringing risk management to the top of the agenda in many a boardroom. It is no longer effective or acceptable (even if it ever was) to delegate the responsibility for risk management down to the manager of the IT section.

The proper implementation of effective information assurance should lie at the heart of all organisations regardless of their sector, size or business. Properly implemented, the secure management of information can provide assurance that risk is being managed effectively in that area at least and can form the firm foundation for further risk management in related areas. If all information is covered by the measures implemented, then the financial, operational, Intellectual Property Rights and a whole range of other risk areas can be managed through the establishment of a single framework.

Security as an enabler

In the information economy in which we all now live, the cost of the loss, corruption, non-availability or unauthorised release of information can be very high. The effective implementation of information assurance measures can have a very beneficial effect on the potential costs of such events. Thus it is easy to develop a convincing and compelling business case for the effective management of information through the use of an approved standard and related processes. Whilst it may not be possible to remove the risk entirely, it should be possible to ensure at least that the probability of the risk occurring is significantly reduced, or that the effects of the risk materialising are significantly reduced in terms of the business impact.

The use of appropriate countermeasures and contingency plans can also have the very beneficial effect of making the work done by an organisation much more orderly by being based on best working practices. Piles of paper and computer disks left lying around on desks, floors and shelves can be the security disaster waiting to happen. With an information assurance standard in place such things should be a thing of the past and the need to spend many hours finding a specific piece of information should be long gone.

With the advent of photocopiers in almost every workplace, the ease with which a sheet of information could be reproduced became very much greater. This in turn meant that where previously there might be only the original and perhaps one handwritten copy to look after, there was now the possibility of many copies to worry about and to try and control. Many a leak from organisations, including governments, has been caused by the proliferation of photocopies, mislaid CDs or inappropriate, perhaps covert, use of USB memory sticks. With improved working practices, instigated through effective information assurance, the need to reproduce information declines since those who need to see a piece of information can do so easily and in a controlled way through the appropriate use of technology, and perhaps without recourse to the production of ever more copies.

The role of information security in countering hi-tech and other crime

Crime is always advancing and developing, often a little quicker than the enforcement agencies that are established to combat it. The hi-tech industry (covering computers, the internet, digitisation, communications and related areas) over the last 30 years or so has provided criminals with ever-increasing opportunities for more advanced and profitable crime in a wide range of activities. Some crimes are the old ones that had effectively been removed from the criminals' handbook. One example is that of fraud, which had been dealt a severe blow by the introduction of sophisticated security devices in banknotes, passports and the like. However, with the ever-increasing use of the internet, it has now returned with much more 'effectiveness'. Emails with 'too good to be true' headings, such as lottery win notifications, have been estimated to have taken up to £110,000 from a single individual with the overall loss being well into millions of pounds in the UK alone. All these are no more than old-fashioned fraud dressed up in new clothes. In addition, the ability to obtain personal information through phishing, key-loggers, screen-scraping or similar tactics has increased the opportunities for criminals to achieve their nefarious purposes. Information assurance can help to address all these issues, at least in the workplace. Good practices at work can also lead to better practices at home, where the proliferation of computers in particular has led to increasing instances of criminal activity targeting the home user. The social duty of companies to help reduce the overall crime is well established and setting good work practices with the care of information is an excellent opportunity that should not be missed.

The growth of such crime has increased the importance of forensic investigation and notably the requirement to preserve evidence based on IT systems. Later in this book this subject will be discussed in more detail but in recent years it has been ever more evident that the skill of the IT practitioner in the preparation of evidence for trials has needed to develop very considerably from the early days of computing when IT evidence was rarely used except in the most complex of cases. Now, with internet crime on the increase and the use of IT becoming the norm for many areas of criminality, the use of investigative techniques based on IT systems has increased enormously. With effectively managed information assurance high on the priority list for all organisations, these techniques are now vital piece of the jigsaw of helping to reduce criminality. The information assurance professional is now a crucial element in the fight against crime, both internal and external to the organisation itself.

Ms Jackson, the chairperson, has asked you to help to develop a sound business case for the implementation of an information security management system (ISMS). She needs to be able to convince her fellow committee members to authorise the expenditure and so needs to be clear why this would be a good idea. The key aspect is the balance between the costs of implementing an ISMS against the costs of suffering a serious attack on GANT's information.

Property developers are keen to know where the Natterjack toad can currently be found so they can either avoid buying the land or, if they already have ownership of it, possibly 'remove' the toad in advance of planning applications being submitted to 'avoid' any problems with the approvals required. This information is on the website, which has no firewall protecting it.

It would cost GANT many thousands of pounds and several years of effort to re-introduce the toad to a habitat once it has been removed either by natural or man-made effects.

The funding for GANT is through members' fees, grants from other nature conservancy organisations and commercial companies who make donations.

ACTIVITY 1.2

Consider three main areas where the chairperson should gather more detailed information to allow the committee to make reasonable judgments on whether or not it is sensible to carry out the ISMS implementation.

SAMPLE QUESTIONS

Question 1

If the accuracy of information is a major concern, which of the following would be used to ensure this is covered effectively?

a. Confidentiality.
b. Integrity.
c. Availability.
d. None of these.

Question 2

When a user logs onto a computer system and is asked for their mother's maiden name, which of the following aspects is the system ensuring?

a. Accountability.
b. Authorisation.
c. Authentication.
d. Applicability.

Question 3

ISO 27001 is an international standard for information security. Which organisation is responsible for its maintenance?

a. The British Standards Institute.
b. The government of the country in which it has been implemented.
c. The European Union Standards Committee.
d. The International Organisation for Standardisation.

Question 4.

How should the implementation of an information assurance system be seen within an organisation?

a. As a problem for the IS department only to sort out.
b. As a problem on which the senior managers should make a decision, but then leave to others to deal with.
c. As a whole organisation issue.
d. As an issue where outside expertise is the best solution.

Question 5

How should the use of an international standard for information security be viewed by senior managers within an organisation?

a. As a good idea if there was the right business environment in which to implement it.
b. As implementing best practice.
c. As overkill, unless there are very serious problems with assurance.
d. As the pet idea of the IT director, who thinks it will look good to shareholders in the next annual report of the organisation.

POINTERS FOR ACTIVITIES IN THIS CHAPTER

ACTIVITY 1.1

There are a significant number of threats, vulnerabilities and risks to this organisation. You may have come up with others, but here are three of the most serious ones. It is most important that you fully appreciate the differences between the three categories as well as being able to make some specific suggestions.

Three threats

These are areas where there is potential for some adverse consequences if this threat should arise. In this scenario three threats might be as follows.

1. Information about members might be accessed by unauthorised people.
2. Information about the habitats of the Natterjack toad might be used by those who are not inclined to support its ongoing existence.
3. The website might be compromised and unofficial messages added to it.

Three vulnerabilities

These are weaknesses in the system that might allow a threat to materialise. In this scenario and building on the threats given above, the vulnerabilities might be as follows.

1. The records of the members are maintained in a variety of ways including paper and unreliable computer systems.
2. The information about the toad's habitats is maintained on an old internet-based server with very limited assurance in place.
3. There is no firewall between the website server and the internet.

Three risks

There are a large number of risks resulting from the threats and vulnerabilities listed above. Three of them might be as follows.

1. There is a risk that unscrupulous property developers might gain access to the personal details of members of GANT and take positive action against them or their property.
2. There is a risk that a habitat of the Natterjack toad might be destroyed by someone who is not interested in its existenced.
3. There is a risk that someone might gain access to the code of the GANT website and change the messages to information that is offensive to those interested in nature conservancy.

ACTIVITY 1.2

The cost-effectiveness, or cost–benefit analysis, for such an implementation would include a very large number of areas. Three of the most significant following on from the suggestions given above for Activity 1.1 might be the following.

1. Members of GANT could be injured or their families and property adversely affected in some way. The cost of protecting the members and their families would be excessive and could not be found through the membership of GANT alone.
2. The cost of re-introducing the Natterjack toads into the wild after its habitat has been destroyed would be very considerable. This could be the consequence (impact) of allowing unauthorised access to the details of the toad's habitats.

3. GANT relies very heavily on the goodwill of other nature conservancy groups and donations from interested commercial companies. If they were embarrassed by the content of the website, they might reduce or withdraw their support for an organisation they saw as unprofessional and poorly organised. This could be devastating for the existence of GANT.

ANSWERS TO SAMPLE QUESTIONS

1. The correct answer is b.
2. The correct answer is c.
3. The correct answer is d.
4. The correct answer is c.
5. The correct answer is b.

INDEX

INFORMATION SECURITY MANAGEMENT PRINCIPLES

Second edition

Andy Taylor (editor), David Alexander, Amanda Finch and David Sutton

Information is one of the currencies of today's society. As demand for access to fast, reliable data at work and home becomes increasingly digitised and mobile, new risks emerge which threaten the very information that helps businesses and society to function. Globally there are 1.5 million victims of cybercrime every day with 18 adults affected every second (Norton Cybercrime Report).

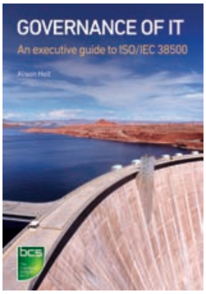
By focusing on the three main areas of information assurance – confidentiality, integrity and availability – this book gives business and IT managers the skills to identify threats and protect against them.

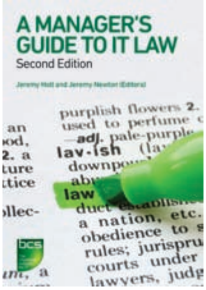
- **Better understand information threats, vulnerabilities and countermeasures**
- **Manage emerging risks caused by 'hyper-connectivity'**
- **Learn best practice from experienced authors**
- **Includes security of cloud-based resources**
- **Supports BCS Certification in IS Management Principles**

ABOUT THE AUTHORS

The authors are at the forefront of information security and are instrumental in shaping policy and implementing best practice. They have gained considerable experience across a wide range of public and private sector bodies, including the Home Office, GCHQ, MoD, RAF, Royal Navy, British Airways, Marks & Spencer and O2.

You might also be interested in:





BUSINESS CONTINUITY MANAGEMENT SYSTEMS
Implementation and certification to ISO 22301
Hilary Estall
bcs

An excellent introduction to information security. Highly recommended.

John Hughes, InfoSec Skills

The security of personal information must keep pace with technology in order to provide a safe and secure environment. This book provides a timely update to ensure that BCS remains an important leader in the education of information security principles.

David Smith, Deputy Commissioner and Director of Data Protection, Information Commissioner's Office

Management;
Information Technology

Cover photo: Thinkstock, Hemera Collection

bcs
The Chartered Institute for IT

Paperback available

ISBN 978-1-78017-175-3
9 781780 171753