ISO27001 / ISO27002

A Pocket Guide

Second edition

Alan Calder

itgp™

ISO27001 / ISO27002

A Pocket Guide

Second edition

ISO27001 / ISO27002

A Pocket Guide

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 2008 by
IT Governance Publishing.

Second edition published in 2013.

ISBN 978-1-84928-523-0

FOREWORD

ISO/IEC 27001:2013 is the international Standard for Information Security Management Systems (ISMSs). Closely allied to ISO/IEC 27002:2013, this Standard (sometimes called the ISMS Standard) can help organisations meet all their information-related regulatory compliance objectives and can help them prepare and position themselves for new and emerging regulations.

Information is the lifeblood of today's organisation and, therefore, ensuring that information is simultaneously protected and available to those who need it is essential to modern business operations. Information systems are not usually designed from the outset to be secure. Technical security measures and checklists are limited in their ability to protect a complete information system. Management systems and procedural controls are essential components of any really secure information system and, to be effective, need careful planning and attention to detail.

ISO/IEC 27001 provides the specification for an ISMS and, in the related Code of Practice, ISO/IEC 27002**,** it draws on the knowledge of a group of experienced information security practitioners in a wide range of significant organisations across more than 40 countries to set out best practice in information security. An ISO27001-compliant system will provide a systematic approach to ensuring the availability, confidentiality and integrity of corporate information. The controls of ISO27001 are based on identifying and combating the entire range of

potential risks to the organisation's information assets. This helpful, handy ISO27001/ISO27002 pocket guide gives a useful overview of these two important information security standards.

ABOUT THE AUTHOR

Alan Calder is a leading author on IT governance and information security issues. He is Chief Executive of IT Governance Limited, the one-stop-shop for books, tools, training and consultancy on IT governance, risk management and compliance.

Alan is an international authority on information security management and on ISO27001 (formerly BS7799), the international security standard. With colleague Steve Watkins he wrote the definitive compliance guide, *IT Governance: An International Guide to Data Security and ISO27001 / ISO27002*, the 5th edition of which was published in 2012. This work is based on his experience of leading the world's first successful implementation of BS7799 (the forerunner of ISO27001) and is the basis for the UK Open University's postgraduate course on information security.

Other books written by Alan include *The Case for ISO27001* and *Nine Steps to Success: An ISO27001:2013 Implementation Overview*, as well as books on corporate governance and IT governance, and several pocket guides in this series.

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets.