How to use this book

ANALOGUE AND DIGITAL

This book was designed, and is intended to be used, as both a **digital** and an **analogue** (that is, dual online and hardcopy) resource. The speed of evolution in computing and of the **internet** means that any book on **information security** starts going out of date fairly quickly. On top of that, there is a six- to eight-month gap between completing the text for and the publication of a hard-covered book. This inevitably means that many technologies that were new, new-ish but inadequately tested, or still only dreams at the point I completed the text could not be included in the analogue version of this book. The reader should therefore assume, from the outset, that the KnowledgeBank at www.itgovernance.co.uk is essential and should use it on a regular basis in order to access the most current information on the issues covered in this book.

The updated information is available only to people who have purchased a hardcopy of the book and can be accessed by going to the **subscriber intranet** at www.itgovernance.co.uk and typing the unique user number that is supplied on the back of this book into the logon box. This will enable the reader to access a free six-month subscription to the KnowledgeBank **update services**, of the website, with a low cost option to renew thereafter.

The reader is also able to assess a number of additional services, including information, alert services and mentoring services that are designed to help readers of the book tackle information security issues. A full set of templates, that are compatible with the advice to businesses in this book and also capable of being deployed in an **ISO 17799** or **BS 7799 ISMS**

are also accessible through the website. Full information is available on www.itgovernance.co.uk.

WHAT, AND WHY, NOT HOW?

This book tells you *what* you need to do – or ensure you have done – to secure your information systems and **assets**. It also tells you *why* you need to tackle each of the recommended actions, so that you can clearly understand the consequences of both action and inaction. The book doesn't tell you, screen by screen, *how* to implement any of the recommended **controls**; there are plenty of big, fat books out there that already do this, **operating system** by operating system (for example, Windows 95, 98, 2000, NT 4.0, Windows XP, Server 2003) and version by version. Because you only run one system, you only need a small bit of the information in each book. You don't need to be able to implement controls in a wide range of **systems**, as long as you can implement them in the one you actually run. This book gives you, in one set of covers, everything you need to know about the *what* and the *why*: enough for you to ensure that a trained IT person actually does what you need done.

STRUCTURE

All readers should read Chapters 1 (Threats and compliance) and Chapter 2 (Simply essential) and all business readers should also take in Chapter 9 (Legal and regulatory essentials); thereafter, readers should focus on the chapter (between 3 and 6) that most closely reflects their digital organizational set-up. Essentials for **wireless** networking (Chapter 7) and Essentials for **e-commerce** (Chapter 8) are both areas that might interest organizations of all sizes and the security issues are fairly common.

The alphabetic glossary section of the book is designed to underpin the content of the preceding chapters and can also be used as a direct reference tool. All those terms that appear in bold throughout the book are explained in the glossary. The glossary also highlights key controls (KC) and significant risks (SR) in order to make it easy to identify areas of concern.

This book does not provide guidance on the design and implementation of an **Information Security Management System** that might meet the specification of BS 7799/ISO 17799; an entirely adequate book (*IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799*) already exists to do this. Readers are, therefore, referred to that book for detailed guidance on meeting the requirements of the standard. Readers, particularly from larger organizations, who are interested in the broader **IT governance** agenda are referred to *IT Governance: Guidelines for Directors.*

Acknowledgements

Some of the material in Chapter 1, and several of the definitions or explanations in the glossary, originally appeared in the 3rd edition of *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799*. I considered it important to maintain consistency between the two books and readers of both books will, hopefully, experience a sense of familiarity with this material.

Much of the content of Chapter 9 also originally appeared in *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799* and I would like to repeat here my thanks to Mark Turner, a partner in the IP/IT department of the London office of the international law firm, Herbert Smith, for his insightful comments on this material and for bringing to it the benefit of his many years experience advising companies in the IT and e-commerce sectors.