Book Review: Information Governance and Assurance: reducing risk, promoting policy

Alan MacLennan
London, 2014
ISBN: 978-1-85604-940-5

Reviewed by Professor Charles Oppenheim, Consultant, c.oppenheim@btinternet.com

This book's blurb describes it as a "comprehensive textbook". Textbook it clearly is, appearing as it does to be primarily aimed at students of the subject and to busy information managers who need to get a quick overview of the topic. But it does not go into enough detail to justify the word "comprehensive". This 196 page paperback has chapters entitled: Introduction; The Laws and Regulations; Data Quality Management; Dealing with threats; Security, Risk management and business continuity; and Frameworks, policies, ethics and how it all fits together. This is complemented by a list of acronyms and definitions of some technical terms, answers to some exercises and discussion points, and a reasonably good index. The book provides an introduction to the subject from a UK point of view, though most of the principles enunciated would apply in other countries.

The book is written in a clear, concise and readable style. The text includes appropriate and interesting case study examples in places, and the exercises and discussion points would make it useful for a small group to work together. Towards the end of the book, suggested points that should have arisen in these discussions are provided. There is a selective, but useful list of references to further reading after each chapter. So there is no question that the book provides a user-friendly and helpful introduction to information governance and assurance. I was particularly pleased to see the author urging extreme caution before using the cloud to store sensitive information, and was also pleased to see a decent discussion of CILIP's ethical principles for library and information staff included.

It is a strange book review by Charles Oppenheim that does not include some caveats, and this book review is no exception. Whilst I recognise that the decision on the price of the book is the publisher's alone, this is an expensive paperback for the (I presume) primary market, i.e., students on information management courses. I have also have some criticisms of the content. In the list of acronyms, the explanation for the name "Jisc" is badly out of date, and some acronyms to be found in the body of the book are not noted in the listing. In the glossary of terms, the definition of "data" is not one that is widely accepted. On page 14, The National Archives are mis-named. The statement on page 15 that the European Community issues Directives overlooks the fact that it also uses so-called Regulations, and the text fails to distinguish EC Regulations from UK Parliamentary Regulations properly. It also fails to distinguish legislation that emanates from the UK alone, such as Freedom of Information, from legislation that is driven by the EC, such as data protection, and from legislation that is a mixture of the two, such as copyright. The author states wrongly that a Freedom of Information requestor must give their real name; they don’t have to, but failure to provide one means their ability to appeal against a refusal is reduced. He also fails to discuss the copyright limitations on what a requestor can do with requested information. In the discussion on data protection on page 21, the important word “school” is missing before “educational”, and when discussing the data protection principles, the author fails to stress that all UK organisations are obliged to follow them. It is also surprising that the further reading for the chapter on the law fails to offer references to basic textbooks on those laws. I found the chapter on threats somewhat paranoid in places, but others may well find it reassuringly robust. However, the claim that the way to deal with the disgruntled employees is “not to have disgruntled employees” is naïve, to say the least. I would have liked to have seen more on how to assess risk and to identify the greatest risk factors, so that prioritisation of risk reducing efforts can be carried out. Finally, the discussion of the COSO Enterprise Risk Management Framework should have been accompanied by a reference to the source.

To sum up: despite my numerous minor criticisms, this is a user-friendly text that is not only aimed at students in the field, but is also of value to practitioners in all types of organisation needing a quick overview of the issues.