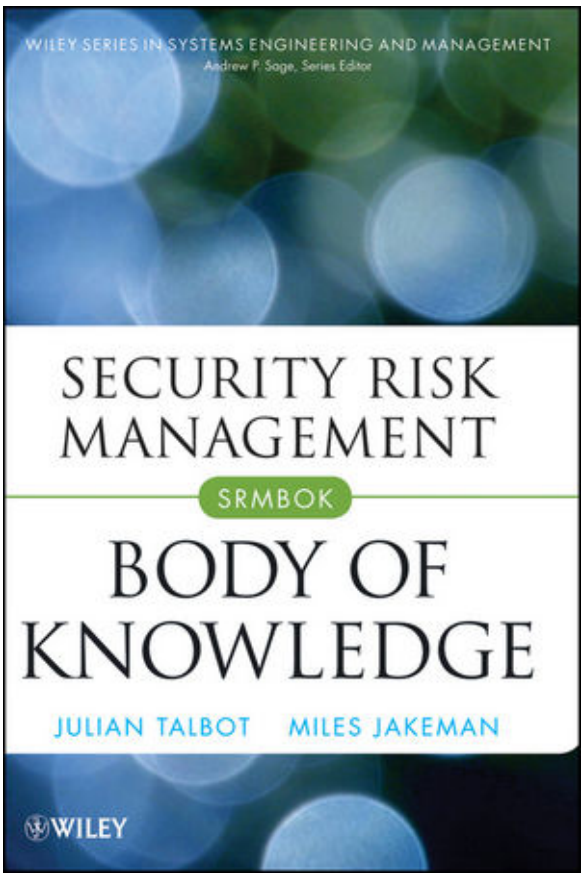
WILEY SERIES IN SYSTEMS ENGINEERING AND MANAGEMENT
Andrew P. Sage, Series Editor
SECURITY RISK MANAGEMENT
SRMBOK
BODY OF KNOWLEDGE
JULIAN TALBOT
MILES JAKEMAN
WILEY

Contents

1

Preface

The Security Risk Management Body of Knowledge (SRMBOK) was developed as an initiative of the Risk Management Institution of Australasia Limited (RMIA) to contribute to the identification and documentation of agreed better practice in Security Risk Management.

It is designed to provide the reader with a framework for formalizing risk management thinking in today's complex environment and details the security risk management process in a format that can be applied by executive managers and security risk management practitioners.

SRMBOK provides both a graphical and written framework for bringing better practice to bear when addressing and treating security risks. The objective of SRMBOK is to support Security Risk Management practitioners with both technical and business guidance.

1.1 Status of this document

This document is the second release of SRMBOK. It endeavors to remain consistent with the overall body of better practice guidance in the discipline of security risk management while also introducing new material from other disciplines, such as occupational health and safety, financial risk management, engineering and business continuity.

In particular, SRMBOK has been developed to align with the ISO 31000 Risk Management Standard and the Australian and New Zealand Standard for Risk Management (AS/NZS 4360:2004).

The intention of SRMBOK is that it should be a living document. Thus, this document will be updated, replaced, or made obsolete by other documents over time. Interested parties and subject matter experts are invited to contribute to the ongoing development and refinement of this body of knowledge.

It is hoped that there will be feedback and suggestions for improvement from subject matter experts about this relatively young document. Comments on SRMBOK should be submitted via the online discussion forum at www.srmbok.com or sent to srmbok@rmia.org.au. Subject matter experts who are interested in contributing to subsequent editions in a closed 'wiki' environment should in the first instance contact the administrator at www.srmbok.com or www.rmia.org.au. Alternatively, please feel free to contact the Lead Authors at julian.talbot@jakeman.com.au and miles@jakeman.com.au.

1.2 Acknowledgements

RMIA gratefully acknowledges the assistance provided by members of the SRMBOK Working Group who contributed to, wrote components of, edited or peer reviewed this material before publication. Unlike other books and standards, SRMBOK was developed by practitioners who donated their time and knowledge for the advancement of the profession, rather than their own personal gain. A very special thanks must go to Jakeman Business Solutions Pty Ltd (JBS), which not only provided the lead authors and project managers to compile the numerous articles and comments received, but also financially underwrote SRMBOK.

A few people also rendered assistance far beyond the call of duty and we owe a special debt to Bob Ross, Jason Brown, Konrad Buczynski, Spanky Kirsch, Lee Hutchison, and Don Williams for their countless comments, suggestions and honest feedback. We would also like to acknowledge the generous assistance and contributions of the following persons:

- Adam Fitzpatrick
- Allan Halsey
- Allen Fleckner
- Anthony Moorehouse
- Anthony Northover
- Athol Yates
- Bernard Peorschke
- Bob Ross
- Brendan Rasmussen
- Brian Kelly
- Brian Roylett
- Broughton Steele
- Charles Bishop
- Clive Williams
- Dai Hockaday
- Damien Hunt
- David Schofield
- David Van Lambaart
- Deborah Watkins
- Don McLean
- Don Williams
- Donna O'Brien
- Frazer Holmes
- Garry Young
- Geoff Harris
- Gerold Knight
- Glen Gardiner
- Glen Morgan
- Grant Whitehorn
- Ian Gordon
- Jason Brown
- Jeff Corkill
- Jim Allen
- John-Martin Collett
- John Greaves
- John Green
- Julian Claxton
- Julian Gaillard
- Katherine Krilov
- Konrad Buczynski
- Leigh Dixon
- Keith Mills
- Le-Anne Jakeman
- Lee Hutchison
- Lennon Hopkins
- Lloyd Masters
- Mark Edmonds
- Mark Dinnison
- Mark Golsby
- Mark Jarratt
- Mark Patch
- Mark Wylie
- Michael MacLean
- Michael Roach
- Mike Rothery
- Neil Connell
- Neil Porter
- Noel Mungovan
- Pam McGilvray
- Paul Curwell
- Paul Longley
- Phil Taleulei
- Phillip Carr
- Rex Stevenson, AO
- Richard Turner
- Rob Krauss
- Rob Smart
- Robert Sadleir
- Roger Fitzgerald
- Ross Babbage
- Ry Crozier
- Scott Petrie
- Shane Cassidy
- Spanky Kirsch
- Steven Hancock
- Steve Rohan-Jones
- Stewart Hayes
- Susan Trappett
- Tonya Graham
- Tim Green
- Tony Pierce
- Tony Solomon
- Wayne Olsen

As RMIA is a not-for-profit organization, proceeds from the sales of SRMBOK will go towards further professionalizing the Security Risk Management community and in funding the ongoing maintenance and development of future editions.

1.3 Sponsors

Finally, RMIA and the members of the SRMBOK working group would sincerely like to thank the sponsors who supported the initial development of SRMBOK through the provision of considerable financial resources. Key sponsors included JBS, ATMAAC International and the Australian Government Department of the Prime Minister and Cabinet. Other sponsors included ADI Thales and Siemens Australia.

Grant Whitehorn, National President, RMIA
September 2008

1.4 Notice on intellectual property rights and copyright

RMIA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights.

Information on SRMBOK procedures with respect to rights in RMIA specifications can be found at www.srmbok.com. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification, can be obtained from the RMIA President.

RMIA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights, which may cover technology that may be required to implement this specification. Please address the information to the RMIA President.

This document and translations of it may not be copied and furnished to others without the express written permission of RMIA. This document itself may not be modified in any way, such as by removing the copyright notice or references to copyright holders, except as needed for the purpose of research as permitted under copyright legislation.

This document and the information contained herein is provided on an 'as is' basis. RMIA disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

1.5 Foreword

We originally set out to write a short reference manual on enterprise security risk management as part of our contribution to increasing the professionalization of the industry, and improving the body of knowledge in this area. It quickly became evident that the field of security, despite an ancient pedigree and growing knowledge amongst practitioners, did not have an agreed body of knowledge to reference.

This, of course, will come as no surprise to our fellow practitioners. They are well aware of the limitations in our profession and that we still struggle to achieve consistency on even such basics as definitions for threat, risk and vulnerability, much less across security practices, approaches or training requirements. It is not for lack of trying – many texts, standards and guidelines exist in the field. What is missing, however, is a unified framework that links elements of physical, information and personnel security with each other and indeed with the latest research in areas such as management, financial theory, behavioral psychology and technology.

After we had repeated numerous times "someone should really write something along these lines", we eventually decided that it may as well be us who started the process. In conjunction with RMIA, we then approached the broader network of security professionals to seek their contributions, peer review, and frank and honest feedback on how to proceed.

The enormity of the subject is daunting as security touches on the most profound elements of society and the human psyche. The literature is also overwhelming and each day new material is published. Consequently, we have had to be selective. We have done our best, however, to ensure that omissions are the result of a decision rather than an oversight.

For this project, we have been dependent on the generosity and contributions of others. Old friends and new from a wide variety of disciplines have provided invaluable assistance, criticism and encouragement. To these people who have volunteered their time, effort and intellectual property with no reward other than our gratitude, we are forever indebted. To this group goes much of the credit; the errors and omissions are ours.

For our part, we have poured the best of our intellectual capital into this document in the interests that it may add to the profession and prove useful to you, the reader. We also encourage you to join us in contributing to future editions so that SRMBOK can continue to reflect the growing body of knowledge for this field.

One day we will finish that short reference manual on security. In the meantime, we hope this contribution proves to be a valuable start point.

Julian Talbot and Miles Jakeman
September 2008