

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	9
1.1	Status of this document	9
1.2	Acknowledgements	10
1.3	Sponsors	11
1.4	Notice on intellectual property rights and copyright	12
1.5	Foreword	13
2	ABOUT SRMBOK	15
2.1	What is SRMBOK?	15
2.2	How can SRMBOK help?	16
	2.2.1 Terminology	17
	2.2.2 Framework	17
2.3	What does SRMBOK cover?	17
2.4	What SRMBOK does not include	19
2.5	Working through the chapters	19
	2.5.1 Applications and case studies	20
2.6	Audience for SRMBOK	21
2.7	Understanding the icons	22
2.8	Language	24
2.9	Learning is a continuous process	24
3	INTRODUCTION AND OVERVIEW	25
3.1	Why SRMBOK?	25
	3.1.1 Key Challenges	26
3.2	Where to from here?	27
3.3	What is Security Risk Management?	29
	3.3.1 Security	30
	3.3.2 Perceived versus Actual Risk	31
	3.3.3 Security Risks	32
	3.3.4 Security Risk Management	36
3.4	How does SRM relate to risk management?	37
3.5	Conclusion	39

4	SECURITY RISK MANAGEMENT CONTEXT	41
4.1	The changing security environment	41
4.2	Changing concepts in security risk management	42
4.3	Origins of security and risk management	44
4.4	Trends and future directions	44
4.5	Globalization, opportunity and volatility	45
4.6	Transnational and extra-jurisdictional risks	46
4.7	Law, regulatory framework, and ramifications for management	47
4.8	Diversification or concentration?	48
4.9	Political awareness	49
4.10	Risk versus reward	50
4.11	Summary of key points	51
5	SECURITY GOVERNANCE	53
5.1	Introduction	53
5.2	What is security governance?	54
5.3	Duty of care	54
5.4	Resilience	57
	5.4.1 What is Resilience	57
	5.4.2 Individuals, Organizations, Communities	58
	5.4.3 The Concept of Resilience	60
	5.4.4 Building Resilience	61
5.5	Security culture	64
5.6	Governance frameworks	65
5.7	Incident management and reporting	69
5.8	Summary of key points	70
6	SRMBOK FRAMEWORK	71
6.1	SRMBOK guiding principles	73

7	<b>PRACTICE AREAS</b>	81
7.1	<b>Introduction</b>	82
7.2	<b>Security management</b>	85
	7.2.1 What is Security Management?	85
	7.2.2 Elements	86
	7.2.3 Applying Security Management Practices	87
	7.2.4 Summary of Key Points	87
7.3	<b>Physical security</b>	88
	7.3.1 Physical Security and SRM	88
	7.3.2 Asset Identification in Physical Security Risk Management	89
	7.3.3 Controls and Protective Barriers	89
	7.3.4 Design of Physical Security Measures - Access	90
	7.3.5 Visibility and Sustainability	90
	7.3.6 Protecting Mixed Access Areas	91
	7.3.7 Restricted Access Group (RAG) Modeling	91
7.4	<b>People security</b>	92
	7.4.1 Human Security	94
	7.4.2 Personnel Security	94
	7.4.3 Personal Protective Practices	98
	7.4.4 Identity Security	100
	7.4.5 Identity Management	101
	7.4.6 Human Factors in Security Risk Management	101
	7.4.7 Human Resource Management and Security Procedures	106
	7.4.8 Summary of Key Points	107
7.5	<b>ICT security</b>	107
	7.5.1 ICT Identification	108
	7.5.2 Protecting ICT Systems	108
	7.5.3 ICT and Other Practice Areas	108
	7.5.4 Interdependency of Systems	108
	7.5.5 Physical Elements of ICT Security	108
	7.5.6 Threats to ICT assets	110
	7.5.7 Summary of Key Points	111
7.6	<b>Information security</b>	112
	7.6.1 Principles of Information Security	113
	7.6.2 The Information Security Lifecycle	114
	7.6.3 Vulnerability of Information	116
	7.6.4 Compartmentalization of Information	118
	7.6.5 Classifying Information	118
	7.6.6 Intellectual Property	128
	7.6.7 Summary of Key Points	129

8	STRATEGIC KNOWLEDGE AREAS	131
8.1	Introduction	131
	8.1.1 The Four Pillars of Security Risk Management	132
	8.1.2 The Quadruple Constraints of Security Risk Management	134
8.2	Exposure	140
	8.2.1 Assessing Exposure	142
	8.2.2 What is Threat?	144
	8.2.3 Vulnerability Assessment	153
	8.2.4 Criticality Assessment	157
	8.2.5 The External Environment	158
	8.2.6 Internal Environment	167
	8.2.7 Temporal Qualities	167
	8.2.8 Frequency of Activities	168
	8.2.9 Summary of Key Points	168
8.3	Risk	169
	8.3.1 History of Security Risk Management	169
	8.3.2 Key Challenges	170
	8.3.3 Current Issues in Risk Management	171
	8.3.4 Security Risk Management	172
	8.3.5 Methodologies	175
	8.3.6 Risk Management Process	176
	8.3.7 Risk Appetite	198
	8.3.8 Swiss-Cheese Model	200
	8.3.9 The Risk Bow-Tie	201
8.4	Resources	210
	8.4.1 Security Barriers	210
	8.4.2 Types of Resources	210
	8.4.3 Resource Attributes	211
	8.4.4 Resource Allocation and Prioritization	211
	8.4.5 Hierarchy of Controls	213
8.5	Quality	216
	8.5.1 Defining Needs and Expectations	217
	8.5.2 As Low As Reasonably Practicable (ALARP)	220
	8.5.3 Appropriate and Cost Effective	222
	8.5.4 Leadership	228
	8.5.5 Staff and Stakeholder involvement	228
	8.5.6 Continuous Improvement	229
	8.5.7 Capability Maturity Models	230
	8.5.8 The SRMBOK Capability Maturity Model	232
	8.5.9 Summary of Key Points	239

9	<b>OPERATIONAL COMPETENCY AREAS</b>	241
9.1	<b>Business integration</b>	241
9.1.1	Introduction	242
9.1.2	Business Cases for Security	243
9.1.3	General Management Practice	244
9.1.4	Understanding and Leading the Security Risk Management process	245
9.1.5	Organizational Requirements	246
9.1.6	Sustainability and Maintenance, Future Proofing	246
9.1.7	Safety Management	246
9.1.8	Quality Management systems	246
9.1.9	Financial Management	247
9.1.10	Summary – Business Integration	248
9.2	<b>Functional design</b>	249
9.2.1	Introduction	249
9.2.2	Functional Design of Security Treatments	249
9.3	<b>Implementation management</b>	251
9.3.1	Introduction	251
9.3.2	Organizational Structure and Culture	252
9.3.3	Training	253
9.3.4	Quality Management Systems (QMS)	254
9.3.5	Project management	255
9.3.6	Change Management in SRM	258
9.3.7	Summary	258
9.4	<b>Assurance and audit</b>	259
9.4.1	Introduction	259
9.4.2	Assurance	260
9.4.3	Audit	261
9.4.4	Grading Performance	264

10	<b>ACTIVITY AREAS</b>	267
10.1	<b>Introduction</b>	267
	10.1.1 Comprehensive Approach	269
	10.1.2 Alignment with Other Systems	270
10.2	<b>Intelligence</b>	273
	10.2.1 Intelligence Process	273
	10.2.2 The Intelligence Cycle	274
	10.2.3 The OODA Loop	276
	10.2.4 Who is Involved?	278
10.3	<b>Protective security</b>	280
10.4	<b>Response</b>	280
	10.4.1 Emergencies	281
	10.4.2 The Comprehensive Approach	283
	10.4.3 Emergency Response Management and SRM	284
	10.4.4 Effecting Emergency Management Planning	285
	10.4.5 Tips and Tricks with Emergency Plans	290
10.5	<b>Recovery and continuity</b>	294
	10.5.1 The Benefits of Business Continuity Management	296
	10.5.2 A General Approach to BCM	296
	10.5.3 Standards	305
10.6	<b>Summary of key points</b>	306
11	<b>SECURITY RISK MANAGEMENT ENABLERS</b>	307
11.1	<b>Introduction</b>	307
	11.1.1 Regulation and Policy	308
	11.1.2 Training and Implementation	309
	11.1.3 Operations and Application	309
	11.1.4 Governance and Accountability	309
	11.1.5 Sustainability and Resilience	310
11.2	<b>Summary of key points</b>	311
12	<b>ASSET AREAS</b>	313
12.1	<b>What is an asset?</b>	313
	12.1.1 A Traditional View	314
	12.1.2 An Emerging View	314
12.2	<b>Key asset groups</b>	316
	12.2.1 Physical Property	317
	12.2.2 People	318
	12.2.3 Information	318
	12.2.4 Information and Communications Technologies (ICT)	319
	12.2.5 Summary of Key Points	321

13	SRM INTEGRATION	323
13.1	SRM integration with Enterprise Risk Management	328
13.2	ERM frameworks	328
	13.2.1 RIMS Risk Maturity Model for Enterprise Risk Management	329
	13.2.2 COSO ERM Framework	330
13.3	Implementing an integrated ERM program	331
	13.3.1 Structuring for Success	331
	13.3.2 Five Steps to Implementing ERM	332
	13.3.3 Common Challenges in ERM Implementation	335
	13.3.4 ERM Key Success Factors	336
13.4	Summary of key points	337
14	SRM LEXICON	339
14.1	Introduction	339
14.2	Illustrations	340
14.3	Notes to readers	344
14.4	Definitions	344
15	SAMPLE TEMPLATES	391
15.1	Security risk register form (example 1)	392
15.2	Security risk register form (example 2)	392
15.3	Risk treatment schedule (example 1)	393
15.4	Risk treatment schedule (example 2)	393
15.5	Outline security plan	394
15.6	Day-to-day operational governance registers	395
15.7	Property selection and security planning checklist	401
15.8	Sample commitment statement to Security Risk Management	413
15.9	Sample bomb threat checklist	414
15.10	Sample bomb threat room search checklist	416
15.11	Evaluation criteria for business continuity and organizational resilience	417
16	ABOUT THE LEAD AUTHORS	469
16.1	Julian Talbot, CPP	469
16.2	Dr Miles Jakeman	470
17	INDEX	471
18	BIBLIOGRAPHY AND OTHER REFERENCES	475



## 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](http://www.srmbok.com) or sent to [srmbok@rmia.org.au](mailto: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](http://www.srmbok.com) or [www.rmia.org.au](http://www.rmia.org.au). Alternatively, please feel free to contact the Lead Authors at [julian.talbot@jakeman.com.au](mailto:julian.talbot@jakeman.com.au) and [miles@jakeman.com.au](mailto: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](http://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.

Copyright © RMIA  
September 2008  
All Rights Reserved

## 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