

srmbook

SECURITY RISK MANAGEMENT BODY OF KNOWLEDGE

A world first publication that integrates knowledge, competency, methodologies and applications across the discipline.



Realising opportunity. Building resilience.

How can I build organisational resilience?

How do I integrate security into enterprise risk management?

How do I develop an integrated security strategy?

How do I build a business case to ensure resourcing?

Lead Authors & Editors
Dr. Miles Jakeman & Julian Talbot



Principal Sponsor



Sponsors



SIEMENS

Supporter



REALISING OPPORTUNITY

srmbook



Security Risk Management BODY OF KNOWLEDGE

Why SRMBOK? Human civilisation is experiencing a transition like no other in history where technology is facilitating the globalisation of markets, culture, organisations and strategic threats. Security risk management has become an essential business tool in the management of risk to meet the challenges that have manifest themselves through this transition. Designing into organisations resilience and continuity demands a more sophisticated and strategic approach to security risk management.

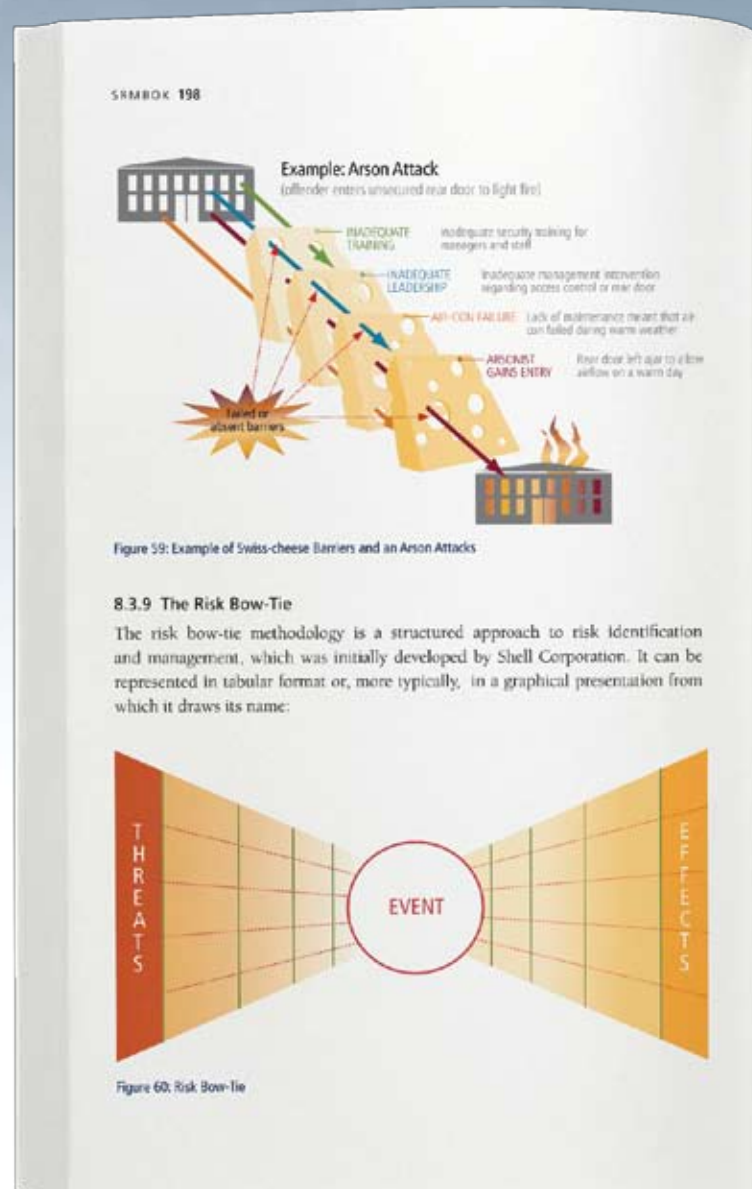
Governments, rating agencies and market regulators are placing an increased emphasis on corporate governance, including effective processes for the management of risk.

Boards now want to be assured that their key business assets of people, information and physical infrastructure are not only being protected but that security risk management contributes to their competitive advantage.

The effective management of risk now requires all organisations to have cohesive and integrated strategies, operations and tactics to optimise their security risk management. Those organisations that effectively manage their security can design resilience and continuity into their competitive advantage through effective protection of people, physical infrastructure and information.

What is SRMBOK?

SRMBOK has been developed by industry and subject matter experts to integrate security practice areas and methodologies in a single source toolkit and reference guide for consultants, managers and practitioners. SRMBOK was developed through strategically focused



R&D to integrate existing better practice from a range of management disciplines and provide new insights into a framework containing:

- Standard descriptions for security risk management processes
- A framework of relationships among the standard processes
- Standard metrics to measure process performance
- Management practices that produce best-in-class performance
- Standard alignment to features and functionality

SRMBOK achieves the convergence, synergy, synthesis and integration of generally accepted better practice from a range of management disciplines including AS4360:2004 Risk Management Standard, unclassified elements of Government SRM Frameworks, Carver Methodology for Target Analysis and Vulnerability Assessment, FEMA426 (Mitigation of Potential Terrorist Attacks Against Buildings), HB167 (4360 SRM Handbook), Capability Maturity Model, Supply-Chain Operations Reference model (SCOR), Hazard Analysis and Critical Control Point (HACCP), Six Sigma, ISO9001, PRINCE2, Balanced Scorecard, Procurement Frameworks, ISO17799 and AS/NZS 4801 (OHS Management Systems).

At the centre of the bow-tie diagram is the top-event which we don't want to happen, i.e. the attack. To the left is what might cause the event to occur (the threat) and between the two are the preventive controls. The right hand side contains details of the potential consequences and the mitigating barriers, illustrated as vertical green lines.

Illustrating this in more detail highlights the nature of the inter-relations between various elements of the equation. This is shown in Figure 61: Risk Bow-Tie Expanded.



Figure 61: Risk Bow-Tie Expanded

8.3.9.1 Comprehensive and Structured Approach

Security risk assessments can have a tendency to follow a linear process and/or to concentrate on the level of risk only, rather than tackling how risks are actually managed. The structured approach of using the risk bow-tie forces an appraisal of how well all exposure causes are being controlled and how well prepared the organisation is to recover in the event of an attack.

It is not a replacement of other techniques but rather a supplemental tool. It provides a structured and repeatable approach which often identifies gaps and issues that can be missed when using other techniques.

Initial bow-tie studies are often conducted during conceptual design stage of new projects or activities, with the objective being to identify and evaluate fundamental security risks as well as control philosophy and criteria.

Who needs SRMBOK?

- Security Risk Managers
- Enterprise Risk Managers
- Risk Managers
- Facilities Managers
- First Responders
- Audit and Assurance professionals
- Directors, Boards and CEO's
- Academics and Researchers
- Students

What can SRMBOK do for you?

Organisations that effectively incorporate security risk management and related governance into their enterprise risk management by applying the methodologies of SRMBOK should be able to answer these key questions:

- How can I build organisational resilience?
- How do I integrate security into enterprise risk management?
- How do I develop an integrated security strategy?
- How do I build a business case to ensure effective resourcing?

Organisations applying SRMBOK to their security risk management plan should be able to document security risk management systems, practices and treatments that can be:

- Implemented purposefully to achieve competitive advantage
- Described unambiguously and communicated
- Measured, managed and controlled
- Tuned and re-tuned to a specific purpose

What is in SRMBOK?

See the back panel of this brochure for the full list of contents.

SRMBOK Application Guides

During 2008 and beyond a range of guides will be produced that will enable professionals to apply the principles of SRMBOK to specific areas of practice. SRMBOK Application Guides will be released on the following areas:

Access Management	Maritime Security and Piracy
Business Continuity and Resilience	Mass Transport Security
Command, Control and Communications	Organisational Structure
Consequence Management and Business Continuity Management	Pandemic
Counter-Terrorism	Personal Protective Practices
Crime Prevention through Environmental Design	Psychology of Security
Crisis Management	Red Teaming and Scenario Modelling
Environmental Security	Resilience and Critical Infrastructure Protection
Events and Mass Gatherings	Security Risk Assessment – Asset, Function or Project Based
Executive Protection	Security Risk Assessment – Enterprise based (ESRA)
Explosives and Bomb Threats	Security Specifications and Postures
Home-Based Work	Security Training
Human Rights and Security	SRM Management Systems (SRM-MS)
Implementing Security Risk Management	Supply Chain Security
Intellectual Property Protection	The Security Manager
Intelligence Approach to SRM	Transnational Security
Investigations and Root Cause Analysis	Travel Security

Practice outcomes that would result from consistent and widespread application include:

- A common platform to establish agreed security risk management frameworks for government, NGO and private sector organisations
- A vulnerability analysis and security risk management framework for protecting critical infrastructure consistent with Australian Government security guidance yet sufficiently original that it can be promulgated in the public domain while still protecting classified doctrine
- Consistent framework, methodology and terminology that supports systematic vulnerability analysis in a repeatable fashion
- Detailed guidance for customising and implementing organisational security standards consistent with better practice across industries
- Support development of consistent vocational training and higher education
- Specific tangible advice and case studies to assist implementation

Product Order and Registration Form

Simply complete and return this form to:
 Risk Management Institution of Australasia Limited
 PO Box 97, Carlton South Vic 3053
 Telephone: +61 3 8341 1000
 Facsimile: +61 3 9347 5575
 Email: eventadmin@rmia.org.au
 ABN 82 106 528 509 ACN 106 528 509

PRIMARY CONTACT DETAILS

Title (Mr/Ms etc) First Name Last Name

Position Organisation

Postal Address

State Postcode Country

Telephone Facsimile Email

RMIA Member No ASIS Member No AIPIO Member No

PRODUCT COST & REGISTRATION FEES (includes 10% GST and is applicable to Australian orders only)

Item	Price (inc GST)	Quantity	AUD\$ Total
SRMBOK	Member	\$187	
	Non Member	\$385	
Postage & handling	Per item	\$22	
Launch	Member	\$55	
	Non Member	\$82.50	
Workshop	Member	\$187	
	Non member	\$242	
Save\$\$ Package price includes launch, workshop and SRMBOK	Member	\$386.10	
	Non member	\$638.55	
Order Total: AUD\$			

LAUNCH/WORKSHOP PARTICIPANT DETAILS and PREFERRED LOCATION (please print)

Please select: Sydney 26 Feb Melbourne 27 Feb Canberra 28 Feb
 Brisbane 29 Feb Perth 4 Mar Adelaide 5 Mar

1. Full name Organisation E-mail

2. Full name Organisation E-mail

3. Full name Organisation E-mail

4. Full name Organisation E-mail

PAYMENT OPTIONS

Product orders & registration fee(s) will be paid in Australian dollars by:

Cheque Forward your cheque with a copy of this registration form to RMIA, PO Box 97, CARLTON STH VIC 3053
 Cheques to be made payable to the Risk Management Institution of Australasia Limited.

EFT A remittance advice quoting our Reference No.SRMBOK-08 and primary contact name must be sent to RMIA either
 by Fax +61 3 9347 5575 or Email finance@rmia.org.au when paying by EFT.
 Account Name: Risk Management Institution of Australasia Limited
 BSB: 033-059 Account No.: 32-4262 Bank: Westpac Branch: Glenferrie Rd, Malvern Vic 3144

Credit Card Debit my - Amex Visa MasterCard Diners
 Card Number: Expiry Date: / Amount: \$ (GST incl)
 Cardholder name Signature

Enquiries on purchasing bulk copies of SRMBOK should be directed to the RMIA Corporate Office on 03 8341 1000 or email srmbook@rmia.org.au.
 A tax invoice will be issued on receipt of this order form. All orders will be confirmed via email within 3 days of receipt.

Terms & Conditions

Registrants may cancel their launch/workshop registration & receive a full refund if notice is received in writing a minimum of 5 working days before the event.
 If a registrant is unable to attend, RMIA will allow a replacement delegate to attend, providing full payment is made.
 While every effort has been made to ensure the accuracy of all details listed herein, RMIA reserves the right to alter or make amendments as necessary.

SRMBOK Costs, Launch & Workshops

SRMBOK (per copy)

Member (ex GST)	Non Member (ex GST)
\$170	\$350

To claim the member rate you must be a financial member of RMIA, ASIS or AIPIO.

A postage and handling charge of \$22.00 applies

SRMBOK Launch & Workshops

Launch Overview:

The lead authors and editors will provide an overview of how the consistent application of SRMBOK can assist you to build resilience into your organisation. They will explain how SRMBOK fits in with the current body of work and standards in the field including alignment with AS/NZS 4360:2004.

Workshop Overview:

- How to use SRMBOK
- Enterprise SRM – how it differs from regular SRM
- SRMBOK framework for organisational resilience
- Integrating SRM and ERM using the SRMBOK framework
- Developing SRM Standards

At the workshops you will learn how to:

- Integrate security into the ERM framework
- Build a business case consistency of SRM spend
- Build organisational resilience into recovery processes
- Understanding the governance implications of security

Dates , venues and timing

Tue 26 February '08	Sydney	The Menzies Sydney	Launch: 07:00 – 09:00 Workshop: 09:30 – 12:30
Wed 27 February '08	Melbourne	Park Hyatt Melbourne	Launch: 07:00 – 09:00 Workshop: 09:30 – 12:30
Thu 28 February '08	Canberra	Rydges Lakeside Canberra	Launch: 07:00 – 09:00 Workshop: 09:30 – 12:30
Fri 29 February '08	Brisbane	Hilton Brisbane	Launch: 07:45 – 09:30 Workshop: 10:00 – 1:30
Tue 4 March '08	Perth	Travelodge Perth	Launch: 07:00 – 09:00 Workshop: 09:30 – 12:30
Wed 5 March '08	Adelaide	Hyatt Regency Adelaide	Launch: 07:00 – 09:00 Workshop: 09:30 – 12:30

Prices: (all prices are in Australian dollars)

	RMIA Member (ex GST)	Non Member (ex GST)
Launch Breakfast	\$50	\$75
SRMBOK ½ day Workshop	\$170	\$220

Workshop program

The launch and workshops will be conducted by the lead authors and editors of SRMBOK.

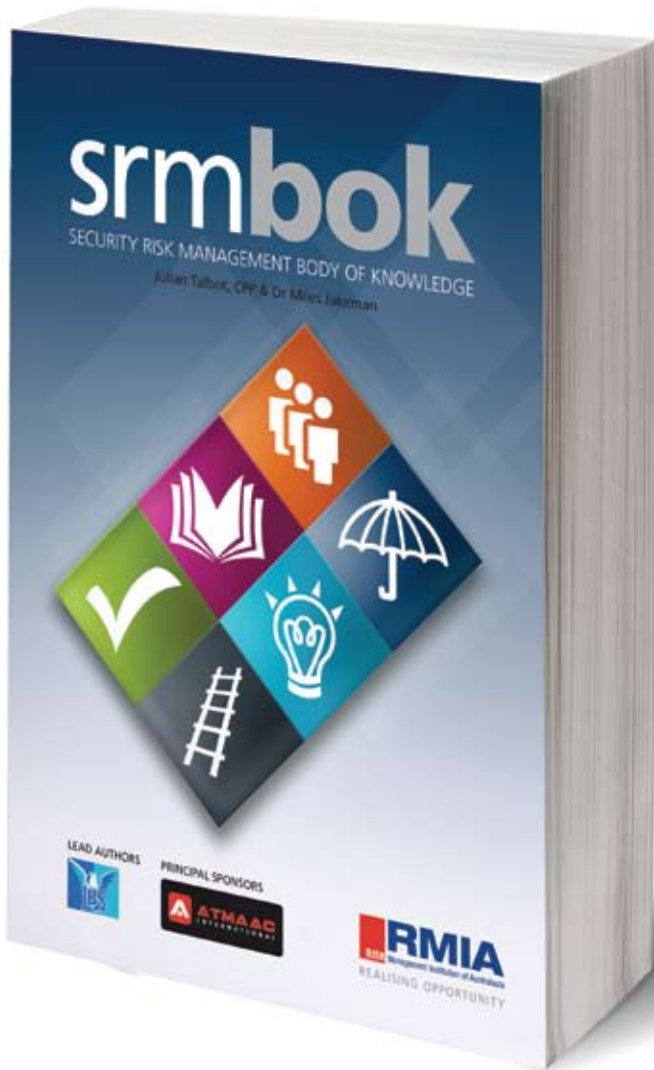
Dr Miles Jakeman:

Miles has an extensive career in security risk management that has seen him at the forefront of the response to key security threats for nations in our region (Australia, Thailand, Indonesia and the Philippines) and major multinational companies. He has top secret security clearance, established the Sydney Olympics Security Intelligence Centre and was intimately involved in the Australian Government's response to the September 11, 2001 attacks, including implementing the inaugural "sky marshal" program. Miles is the principal of Jakeman Business Solutions which continues to provide the region with security risk management solutions.

Julian Talbot:

With more than 20 years' experience in the practice of security risk management, Julian is one of those rare individuals who have worked for neither the defence nor intelligence services. Before joining Jakeman Business Solutions, Julian was responsible for the Australian Trade Commission security across more than 60 countries. Julian has experience of major resource projects in Australia and internationally. He was responsible for establishing RMIA's Security Special Interest Group.

What's in SRMBOK?

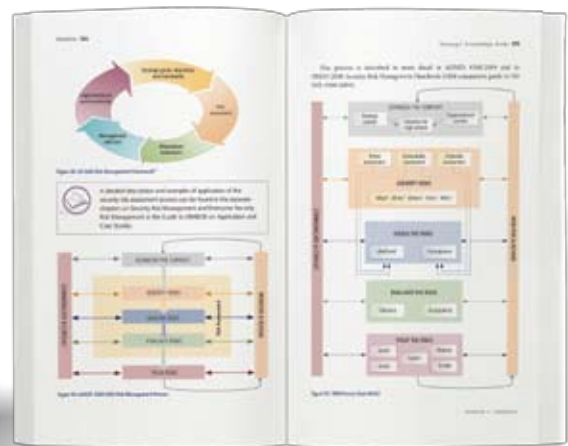


Acknowledgements

SRMBOK is the result of a strategic partnership between RMIA, JBS and government. SRMBOK will make a significant contribution to improving professionalism and enhancing community and organisational resilience. The partners have invested hundreds of thousands of dollars, intellectual property and passion without expectation of commercial return to make this contribution to our community.

RMIA acknowledges the financial and professional contributions of our principal supporter ATMAAC International and supporters Thales Australia, Siemens Australia and ASIS. RMIA also wishes to acknowledge the many practitioners who have contributed their intellectual capital, time and effort as authors, reviewers and quality assurers.

RMIA acknowledges the support from the Australian Government Department of the Prime Minister and Cabinet, which contributed funding to the development of SRMBOK, but has not endorsed the contents or conclusions.



PREFACE

ABOUT SRMBOK

INTRODUCTION AND OVERVIEW

SECURITY RISK MANAGEMENT CONTEXT

SECURITY GOVERNANCE

SRMBOK FRAMEWORK

PRACTICE AREAS

STRATEGIC KNOWLEDGE AREAS

OPERATIONAL COMPETENCY AREAS

ACTIVITY AREAS

SECURITY RISK MANAGEMENT ENABLERS

ASSET AREAS

SRM INTEGRATION

SRM LEXICON

SAMPLE TEMPLATES