

Contents

- 1 PREFACE**
 - 1.1 Status of This Document**
 - 1.2 Acknowledgements**
 - 1.3 Sponsors**
 - 1.4 Notice on Intellectual Property Rights and Copyright**
 - 1.5 Foreword**

- 2 ABOUT SRMBOK**
 - 2.1 What is SRMBOK?**
 - 2.2 How can SRMBOK help?**
 - 2.2.1 Terminology
 - 2.2.2 Framework
 - 2.3 What does SRMBOK cover?**
 - 2.4 What SRMBOK does not include**
 - 2.5 Working through the chapters**
 - 2.5.1 Applications and Case Studies
 - 2.6 Audience for SRMBOK**
 - 2.7 Understanding the Icons**
 - 2.8 Language**
 - 2.9 Learning is a continuous process**

- 3 INTRODUCTION AND OVERVIEW**
 - 3.1 Why SRMBOK?**
 - 3.1.1 Key Challenges
 - 3.2 Where to from here?**
 - 3.3 What is Security Risk Management?**
 - 3.3.1 Security
 - 3.3.2 Perceived versus Actual Risk
 - 3.3.3 Security Risks
 - 3.3.4 Security Risk Management
 - 3.4 How does SRM relate to Risk Management?**Error! Bookmark not defined.
 - 3.5 Conclusion**

- 4 SECURITY RISK MANAGEMENT CONTEXT**
 - 4.1 The changing security environment**
 - 4.2 Changing concepts in security risk management**
 - 4.3 Origins of security and risk management**
 - 4.4 Trends and future directions**
 - 4.5 Globalisation, opportunity and volatility**
 - 4.6 Transnational and extra-jurisdictional risks**
 - 4.7 Law, regulatory framework, and ramifications for management**
 - 4.8 Diversification or concentration?**
 - 4.9 Political awareness**
 - 4.10 Risk versus reward**

4.11 Summary of Key Points

5 SECURITY GOVERNANCE

5.1 Introduction

5.2 What is security governance?

5.3 Duty of care

5.4 Resilience

- 5.4.1 What is Resilience
- 5.4.2 Achieving Resilience
- 5.4.3 Assets, Functions and Capability
- 5.4.4 Resilience and Culture

5.5 Security Culture

5.6 Governance Frameworks

5.7 Incident management and reporting

5.8 Summary of key points

6 SRMBOK FRAMEWORK

6.1 SRMBOK Guiding Principles

7 PRACTICE AREAS

7.1 Introduction

7.2 Security Management

- 7.2.1 What is security management?
- 7.2.2 Elements
- 7.2.3 Applying security management practices
- 7.2.4 Summary of Key Points

7.3 Physical Security

- 7.3.1 Physical Security and SRM
- 7.3.2 Asset identification in physical security risk management
- 7.3.3 Controls and Protective Barriers
- 7.3.4 Design of physical security measures - Access
- 7.3.5 Visibility and sustainability
- 7.3.6 Protecting Mixed Access Areas
- 7.3.7 Restricted Access Group (RAG) Modelling

7.4 People Security

- 7.4.1 Human Security
- 7.4.2 Personnel Security
- 7.4.3 Personal Protective Practices
- 7.4.4 Identity Security
- 7.4.5 Identity Management
- 7.4.6 Human Factors in Security Risk Management
- 7.4.7 Human Resource Management and Security Procedures
- 7.4.8 Summary of Key Points

7.5 ICT Security

- 7.5.1 ICT identification
- 7.5.2 Protecting ICT Systems
- 7.5.3 ICT and Other Practice Areas
- 7.5.4 Interdependency of Systems
- 7.5.5 Physical Elements of ICT Security
- 7.5.6 Threats to ICT assets
- 7.5.7 Summary of Key Points

7.6 Information Security

- 7.6.1 Principles of information security
- 7.6.2 The Information Security Lifecycle
- 7.6.3 Vulnerability of information
- 7.6.4 Compartmentalisation of information
- 7.6.5 Classifying information
- 7.6.6 Intellectual Property
- 7.6.7 Summary of Key Points

8 STRATEGIC KNOWLEDGE AREAS

8.1 Introduction

- 8.1.1 The Four Pillars of Security Risk Management
- 8.1.2 The Quadruple Constraints of Security Risk Management

8.2 Exposure

- 8.2.1 Assessing Exposure
- 8.2.2 What is Threat?
- 8.2.3 Vulnerability Assessment
- 8.2.4 Criticality Assessment
- 8.2.5 The External Environment
- 8.2.6 Internal Environment
- 8.2.7 Temporal Qualities
- 8.2.8 Frequency of Activities
- 8.2.9 Summary of Key Points

8.3 Risk

- 8.3.1 History of Security Risk Management
- 8.3.2 Key Challenges
- 8.3.3 Current Issues in Risk Management
- 8.3.4 Security Risk Management
- 8.3.5 Methodologies
- 8.3.6 Risk Management Process
- 8.3.7 Risk Appetite
- 8.3.8 Swiss-Cheese Model
- 8.3.9 The Risk Bow-Tie

8.4 Resources

- 8.4.1 Security 'Barriers'
- 8.4.2 Types of Resources
- 8.4.3 Resource Attributes
- 8.4.4 Resource Allocation and Prioritisation
- 8.4.5 Hierarchy of Controls

8.5 Quality

- 8.5.1 Defining 'Needs' and Expectations
- 8.5.2 As Low As Reasonably Practicable (ALARP)
- 8.5.3 Appropriate and Cost Effective
- 8.5.4 Leadership
- 8.5.5 Staff and Stakeholder involvement
- 8.5.6 Continuous improvement
- 8.5.7 Capability Maturity Models
- 8.5.8 The SRMBOK Capability Maturity Model
- 8.5.9 Summary of Key Points

9 OPERATIONAL COMPETENCY AREAS

9.1 Business Integration

- 9.1.1 Introduction
- 9.1.2 Business Cases for Security
- 9.1.3 General management practice
- 9.1.4 Understanding and leading the security risk management process
- 9.1.5 Organisational requirements
- 9.1.6 Sustainability and maintenance, future proofing
- 9.1.7 Safety management
- 9.1.8 Quality management systems
- 9.1.9 Financial management
- 9.1.10 Summary – Business Integration

9.2 Functional Design

- 9.2.1 Introduction
- 9.2.2 Functional design of security treatments

9.3 Implementation Management

- 9.3.1 Introduction
- 9.3.2 Organisational Structure and Culture
- 9.3.3 Training
- 9.3.4 Quality Management Systems (QMS)
- 9.3.5 Project management
- 9.3.6 Change Management in SRM
- 9.3.7 Summary

9.4 Assurance and Audit

- 9.4.1 Introduction
- 9.4.2 Assurance
- 9.4.3 Audit
- 9.4.4 Grading Performance

10 ACTIVITY AREAS

10.1 Introduction

- 10.1.1 Comprehensive Approach
- 10.1.2 Alignment with other systems

10.2 Intelligence

- 10.2.1 Intelligence Process
- 10.2.2 The Intelligence Cycle
- 10.2.3 The OODA Loop
- 10.2.4 Who Is Involved?

10.3 Protective Security

10.4 Response

- 10.4.2 The 'comprehensive approach'
- 10.4.3 Emergency Response Management and SRM
- 10.4.4 Effecting emergency management planning
- 10.4.5 Tips and Tricks with Emergency Plans

10.5 Recovery and Continuity

- 10.5.1 The Benefits of Business Continuity Management
- 10.5.2 A General Approach to BCM
- 10.5.3 Standards

10.6 Summary of Key Points

11 SECURITY RISK MANAGEMENT ENABLERS

11.1 Introduction

- 11.1.1 Regulation and Policy
- 11.1.2 Training and Implementation
- 11.1.3 Operations and Application
- 11.1.4 Governance and Accountability
- 11.1.5 Sustainability and Resilience

11.2 Summary of Key Points

12 ASSET AREAS

12.1 What is an asset?

- 12.1.1 A traditional view
- 12.1.2 An emerging view

12.2 Key Asset Groups

- 12.2.1 Physical Property
- 12.2.2 People
- 12.2.3 Information
- 12.2.4 Information and Communications Technologies (ICT)
- 12.2.5 Summary of Key Points

13 SRM INTEGRATION

13.1 SRM Integration with Enterprise Risk Management

13.2 ERM Frameworks

- 13.2.1 RIMS Risk Maturity Model for Enterprise Risk Management
- 13.2.2 COSO ERM Framework

13.3 Implementing an Integrated ERM Program

- 13.3.1 Structuring for Success
- 13.3.2 Five Steps to implementing ERM
- 13.3.3 Common challenges in ERM implementation
- 13.3.4 ERM key success factors

13.4 Summary of Key Points

14 SRM LEXICON

14.1 Introduction

14.2 Illustrations

14.3 Notes to Readers

14.4 Definitions

15 SAMPLE TEMPLATES

15.1 Security Risk Register Form (Example 1)

15.2 Security Risk Register Form (Example 2)

15.3 Risk Treatment Schedule (Example 1)

15.4 Risk Treatment Schedule (Example 2)

15.5 Outline Security Plan

15.6 Day-to-Day Operational Governance Registers

15.7 Property Selection and Security Planning Checklist

15.8 Evaluation Criteria for Business Continuity and Organisational Resilience

15.9 Sample Commitment Statement to Security and Risk Management

15.10 Sample Bomb Threat Checklist

15.11 Sample Bomb Threat Room Search Checklist

16 ABOUT THE LEAD AUTHORS

16.1 Mr Julian Talbot, CPP

16.2 Dr Miles Jakeman

17 INDEX

18 BIBLIOGRAPHY AND OTHER REFERENCES