Introduction and Overview

1

1.1 WHY SRMBOK?

We live in a world of uncertainty; the world is changing at an ever accelerating pace. Life, society, economics, weather patterns, international relations, and risks are becoming more and more complex. The nature of work, travel, recreation, and communication is radically altering. We live in a world where, seemingly with each passing year, the past is less and less a guide to the future.

Security is involved in one way or another in virtually every decision we make and every activity we undertake. The contributions that Security Risk Management (SRM) make to society, personal safety, and national stability are easy to underestimate but hard to overlook. We have been concerned about safety, security, and protection since the dawn of our species and yet will still struggle to consistently define or reliably manage our security risks.

This is to a large extent understandable—although the fundamentals remain consistent, advances in security and related disciplines continue unabated. The global environment has never been more volatile, and societal expectations for security are increasing if anything.

The complexities of globalization, public expectation, regulatory requirements, transnational issues, multijurisdictional risks, crime, terrorism, advances in information technology, cyber attacks, and pandemics have created a security risk environment that has never been more challenging.

Despite the continuing development of security as a discipline, no single framework pulls together all the excellent but disparate work that practitioners and researchers are continually developing. Overall, there is little dispute that risk is a factor that must be considered by decision makers when deciding what, if anything, should be done about a risk that falls within their responsibility. Security is one such area where there has been less than total agreement as to what this means in practical terms.

> *The body of knowledge (BOK) surrounding Security Risk Management continues to evolve, but even the most dynamic of fields needs a point of common agreement, or at least agreed debate. It is unreasonable to expect SRMBOK to be all things to all people, but we the society, and the profession, need a place to collectively discuss and shape our thinking surrounding core concepts in SRM.*

Much of the existing body of knowledge on risk management was developed for issues that do not possess the same degree of complexity, uncertainty, and ambiguity as those associated with modern security-related decision making. For example, managing financial or operational risk can be quantified more easily than some of the abstract concepts that security practitioners must manage. These areas offer us insights into the tools and techniques that have been pioneered in other disciplines. Areas such as safety management systems, financial formulas, project methodologies, engineering science, hazard identification, and human factors analysis, to name just a few, also have much to offer security practitioners.

1.1.1 Key Challenges

The abundance of valuable but disparate material from Security Risk Management and other disciplines presents a significant challenge for developing a common framework to assess and consider risk when making security and related policy decisions. In addition to risk assessment methodological questions, other questions plague organizational risk deliberations. Among them are the following:

- Who is responsible for the risk assessment?
- Who is responsible for managing risk?
- How should alternative courses of action be developed, and how should they be evaluated?
- How does one perform cost/benefit analysis on an abstract problem where potential consequences are astronomical but probability is unknown and may be close to zero?

- How should terrorist and criminal adaptive responses to security measures be taken into account as potential security measures are being considered?

Security professionals everywhere are making some progress in answering these questions, and more significantly, the profession is developing a more mature understanding of the complexities involved. Increasingly, academic and practical research is also refining our understanding of the issues and giving us a basis for more risk-informed decision making.

Much of the past practices in security have revolved around the three Gs (guns, guards, gates), national security, intelligence and defense, firewalls, and cryptography. As important as these are, moving from a focus on threat mitigation to benefit realization is a growing imperative for many security professionals and for most organizations.

1.2 WHERE DO WE GO FROM HERE?

> "The empires of the future are the empires of the mind."
>
> *Sir Winston Churchill*

We are facing an increasingly complex and interdependent future in which information and intangible assets are likely to become increasingly valuable, and tangible assets are likely to diminish in value by comparison.

Risk-management activities in the 21st century are likely to continue to move away from the early focus on compliance and loss minimization toward opportunity realization. Although Security Risk Management will continue to require sound management of threats and minimization of losses, already we are starting to see threat mitigation as just part of standard management practice, rather than a standalone discipline.

The organizations and societies of today are seeking a greater understanding of the true nature of risks. This is not an altruistic or inherent desire for risk management per se, but it is an endeavor to better exploit opportunities and minimize harm.[1] As illustrated in Figure 1.1, organizations typically start out as risk controllers with a focus on compliance and loss minimization. Over time, they realize that quality SRM adds value to operational performance, and if integrated across the enterprise, SRM can become a significant contributor to both organizational resilience and opportunity realization.

It is likely that some organizations will always view security as a cost center rather than as profit center. Those that have sound Security Risk Management systems in place, however, will have competitive advantages in many areas:

- Personnel screening can help to select the best candidates and also increase marketability to clients who may be concerned about protecting their intellectual property or funds.
- Information security management helps to introduce products to market without advance knowledge by competitors.

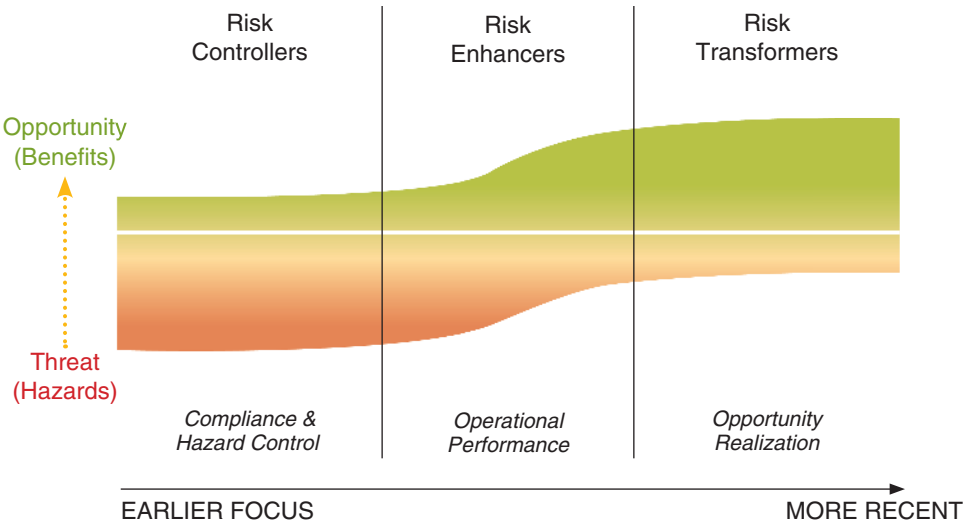


FIGURE 1.1 The security risk management journey

- Appropriate physical security is likely to increase profitability at a venue when customers know they will be safe and their cars will not be vandalized while they are inside.
- Organizations that have prepared by developing a sound Security Risk Management system can quickly and safely deploy to higher risk locations to take advantage of opportunities ahead of their competitors.
- Appropriate security will mean that managers can focus on opportunity realization rather than on filling out incident reports or chasing down missing equipment.

Just as threat mitigation seeks to avoid threats turning into losses, so does opportunity realization seek to manage the conversion of opportunities into benefits. Although most of us realize intuitively that Security Risk Management is integral to opportunity realization, the framework and tools to demonstrate this transition from risk controllers to risk transformers is comparatively in its infancy. The process of moving from being perceived as a cost center to being recognized as a profit center is integral to achieving effective organizational Security Risk Management.

SRMBOK aims to provide a framework that security professionals can use to integrate Security Risk Management along with lessons from other disciplines, such as engineering, occupational health and safety, behavioral psychology, and finance.

1.3 WHAT IS SECURITY RISK MANAGEMENT?

It is appropriate from the outset to define the scope of SRMBOK by defining the term "Security Risk Management." SRMBOK starts with the fundamental

premise that Security Risk Management is an essential part of any individual's, organization's or community's wider risk-management activities.

SRMBOK takes the position that there is no such thing as perfect security and that all security involves making trade-offs. For example, most of us willingly accept the risk of being involved in a car accident or assaulted in exchange for the benefits of living in a modern society. If we wanted to avoid completely the risk of being assaulted, we would live on a deserted island. This deserted island choice, however, is likely to increase other personal risks and reduce our longevity as a result of the lack of health-care services. We also accept the additional cost of fitting a lock to our front doors and the inconvenience of having to lock the door on the way out in exchange for reducing the risk of burglary. Similarly, we accept a little inconvenience when undergoing security checks before flying as well as a small additional cost for that security with good grace because it reduces our real or perceived risk.

1.3.1 Security

Security is the condition of being protected against danger or loss. It is achieved through the mitigation of adverse consequences associated with the intentional or unwarranted actions of others.

In general usage, security is a concept similar to safety, but as a technical term, security means that something is not only secure but also that it has been secured. In this context, security refers to the measures used to protect sensitive organizational assets that collectively create, enable, and sustain organizational capability. Such assets will differ depending on the nature of the organization's activities but typically include classified or sensitive information, physical assets of value, people, unique processes, alliances/partnerships, and intellectual capital.

Individuals or actions that encroach on the condition of protection cause a breach of security.

As suggested from the word "unwarranted" in this definition, the intentional actions of others that are legal and acceptable, at least in the eyes of the defender, are excluded from the scope of security. For example, the actions of others in derivatives trading or commercial enterprise may have adverse consequences, but preventing those lawful and normal consequences is the domain of areas such as financial risk management. They would not normally be security issues unless fraud or similar was involved.

The use of the word "intentional" similarly clarifies the distinction between security and areas such as safety. Security involves protection from deliberate acts, whereas safety risk management includes the management of risks from unintended events such as motor vehicle accidents and falls.

There is a strong overlap between safety and security (as there is between security and finance, engineering, psychology, etc.); in fact, many languages have only one word for both concepts. Many activities will involve a wide range of threats from different sources (e.g., a journey to a high-risk country involves risks from crime, foreign currency fluctuations, and road safety, to name but a few).

It can be tempting to include security as a subset of safety, and in some cases, this would be correct. For example, even the protection of national security classified information could be indirectly related to protecting the lives of the nation's citizens or the identity of agents in the field. However, security as a subset of safety is inappropriate when we consider financial and property threats such as fraud, embezzlement, commercial espionage, and website hacking, where the impact on personnel safety is tenuous, if it exists at all.

1.3.2 Perceived versus Actual Risk

Like many other areas of risk management, security involves making trade-offs. Security decisions often include a range of costs as well as compromises to convenience, privacy, and so on, and in many cases, we will have to trade one or more of these elements.

Within this, we will often be called on to make decisions and trade-offs regarding perceived versus actual risks. Sometimes, managing the actual risk will also mitigate the perceived risks and vice versa. Sometimes not.

Often, it might appear that the actual risks are more important than the perceived risk, and in some cases, this is appropriate. There are many reasons, however, why we might choose to focus more on managing perceived risks. Removing nail clippers from airline passengers may have little to do with managing the actual risk of hijack, but it is part of the process that visibly demonstrates that something is being done. In fact, the risk of hijack may well be perceived by the traveling public to be much higher than it actually is. The greater risk associated with airline hijackings is probably not one of hijack but the economic losses to the community and the increased incidence of road fatalities if people lose confidence in aviation safety.[2,a]

Similarly, it will often be appropriate to put in place measures such as tamper-proof packaging on food and drugs, even though it is still entirely possible to contaminate the goods inside. Such measures in practice will only deter the lazy or ignorant would-be poisoner, but they do reassure the consumer to continue purchasing the product.

---

[a]In December 2001, David Myers, who is a Professor of Psychology at Hope College, postulated that if Americans "now fly 20 percent less and instead drive half those unflown miles, we will spend 2 percent more time in motor vehicles. This translates into 800 more people dying as passengers and pedestrians. So, in just the next year the terrorists may indirectly kill three times more people on our highways than died on those four fated planes." As it transpired, domestic air travel in the United States following the terrorist attacks of September 11 dropped more than 30% relative to the same period the previous year, and U.S. motor vehicle fatalities were 1,085 higher in 2002 than in 2001.

Of course, these issues of perceived versus actual risk are largely subjective and will vary depending on individual risk appetite and understanding. The greater driver in this decision-making process is likely to be personal or organizational agendas, which will involve greater or lesser good to various parties.

Although most people as individuals are concerned about the safety of the traveling public, for example, the various stakeholders all have different agendas. The airlines are not as interested in treating the real risk of hijacking as they are in treating the perceived risk. An actual hijack is a dramatic but rare event. The perceived risk of hijack can result in a dramatic impact on every quarterly revenue statement. Airlines, like any business, have an agenda to spend the bare minimum of their own money but recognize the return on investment by managing security perceptions. Meanwhile, politicians are facing the next election cycle—or next coup if not in a democratic society, and have their own agenda to consider. Being seen to be doing something and acting quickly will generally be more important in the first instance than actually understanding and addressing the real security risk.

The key word here of course is "risk." Each stakeholder's agenda is driven by their own perception of risk, and it might not be the same as the actual risks. For example, mobile phone technology has sufficient encryption on most digital systems to allow them to ensure that it can be marketed as encrypted but not enough to ensure that an average personal computer (PC) with some basic equipment cannot break the encryption. The cost of research and the bandwidth implications for significantly enhanced encryption are not commercially rewarded in the current threat environment, so the security is a compromise.

These are just a few of the examples of how various security agendas interact with the perceived and real security threats to make trade-offs that affect us all. This is a theme that is reflected throughout SRMBOK and one to which there is no easy or immediate answer.

1.3.3 Security Risks

A security risk is any event that could result in the compromise of organizational assets. The unauthorized use, loss, damage, disclosure, or modification of organizational assets for the profit, personal interest, or political interests of individuals, groups, or other entities constitutes a compromise of the asset, and it also includes the risk of harm to people. Compromise of organizational assets may adversely affect the enterprise, its business units, and their clients. As such, consideration of security risk is a vital component of risk management.

Several methods can be used to identify security risks. One method of identifying threats with the potential to affect the organization adversely is to group them according to their source, motivation, and method of operation, as shown in Table 1.1.

Table 1.1 Threat groupings by source, motive and method

Source	Motive	Method of Operation
Criminal	Profit	Theft, robbery, assault, fraud, disclosure
Terrorist	Political manipulation	Bombing, hijacking, kidnapping, assassination
Foreign intelligence services	Strategic, military, political, or economic advantage	Espionage, sabotage, subversion, disclosure
Commercial or industrial competitors	Profit, competitive edge	Industrial or economic espionage
Malicious people	Revenge, fame, discredit	Disclosure, destruction, vandalism

Table 1.2 Grouping assets by risk and threat

Organization Assets	Risks	Threats
Buildings, facilities	Destruction, damage, or unavailability of the building or facility	Fire, explosion, hoaxes, power failure, contamination, unauthorized access
Information system	Loss or compromise of security classified material, loss of confidentiality, availability or integrity of information	Unauthorized users, forensic disc examination, careless handling of printout, careless transmission
Management's confidence in the business unit or program	Loss of management or public confidence in the business unit or program, or its processes	Mishandling of sensitive data, inconsistent policy or service delivery, adverse media coverage
Organizational reputation	Loss of organizational reputation	Poor service, mishandling of sensitive data, inconsistent policy or service delivery, adverse media coverage

Another method to identify threat sources that can become security risks is to focus on the assets (functions, resources, and values) that are essential for the organization to perform its role and to group them according to the threat and consequent risk posed, as shown in Table 1.2.

A third method is to examine at the organizational exposures or vulnerabilities and to then use these to review the suitability of existing security controls (Table 1.3).

Table 1.3 Asset group and organizational exposures

Asset Group	Possible Exposures or Vulnerabilities Identified
People Assets	Abduction Assassination Attack, assault, or harassment Bombing Civil disorder Co-location with high risk tenants Conferences/exhibitions Crime Cultural or religious differences Discrimination/prejudice Disgruntled employee Domestic violence Drive by shooting Family influence Financial stress or gain/influence Impersonation of staff member Inadequate procedures Inadequate training Inadequate vetting Isolation Kidnap Language Loyalty/coercion/corruption/collusion Mail handling and receipt Mismanagement Organizational structure and responsibilities Physical assault Poisoning Reluctance to adopt security policy Robbery Sexual assault Sexual preference or discrimination Stress related behavioral issues Travel Verbal assault or harassment Workplace violence Public perception Staff attraction Staff retention

Asset Group	Possible Exposures or Vulnerabilities Identified
Information Assets	Destruction or corruption Disruption of service Commercial espionage Fire/arson Fraud Inadvertent disclosure Leakage Loss of data or sensitive trade material Manipulation of data/information Sabotage Staff loyalty
Physical Assets/Information and Communications Technology (ICT)	Break-in Co-location with high-risk tenants Commercial espionage—electronic surveillance/listening Device Fire/arson Inadequate emergency management procedures Inadequate threat details Failure of equipment (e.g., maintenance and reliability) Hacking Funding Mail handling Maintenance Procurement methodology Unauthorized or forced access Vandalism Vehicle bombing Sabotage Theft

Identified threats will represent sources of security risks (i.e., how and why a particular security risk event might happen). Information obtained from a formal threat assessment will then assist in determining the likelihood of particular risks occurring.

1.3.4 Security Risk Management

The focus of SRMBOK is toward the direct and unwarranted actions of people. The term "security" can of course be a much broader term. For example, if we consider security as a "state of being protected from hazards, danger, harm, loss or injury," it also includes elements of protection from natural disasters and concepts of organizational resilience. SRMBOK accordingly, although focused

on intentional acts, takes an all-hazards approach that considers the broader interplay of environment and other factors that can impact an organization or individual. In terms of natural hazards, for example, organizational resilience takes into account both the direct impact of natural disasters (e.g., power outages and infrastructure) and the indirect impacts, such as fire, looting, civil unrest, and so on.

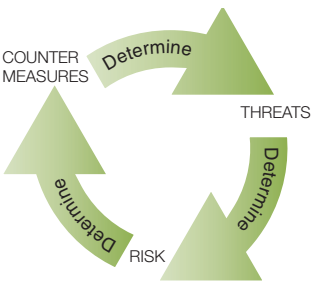
> *Security Risk Management is the culture, processes, and structures that are directed toward maximizing benefits and minimizing adverse effects associated with the intentional and unwarranted actions of others against organizational assets.*[3]

The definition used above complements and supports an all-hazards approach to organizational resilience that, in practice, is achieved by supporting the preparedness, protection, and preservation of people, property, information, and organizational capability.[4]

Although some terminology used in Security Risk Management is common to other forms of risk management, most threat assessment processes and risk treatments used are unique to the Security Risk Management profession and play a definitive role in the progression of an organization's objectives.

Like most security professionals, SRMBOK considers threat and risk as different concepts. Threat is a hazard or source of risk (criminals, terrorists, etc.)—usually measured in terms of intent and capability. Meanwhile, risk considers the likelihood of an attack with the most credible impact(s) or consequence on assets. Security Risk Management, therefore, involves understanding the threat as part of the objective of determining and applying countermeasures to manage (treat) the risks.

> *Threat determines risk, which in turn determines countermeasures.*
>
> *In practice, this is a cycle where each countermeasure changes the context and either introduces new risks or at the very least will modify the threat actors' methods of attack. This in turn modifies the risk and so on.*



1.4 HOW DOES SRM RELATE TO RISK MANAGEMENT?

Security Risk Management is a subset and essential part of a broader risk management system. As illustrated in Figure 1.2, SRM is simply another management discipline fitting predominantly within the sphere of risk management.

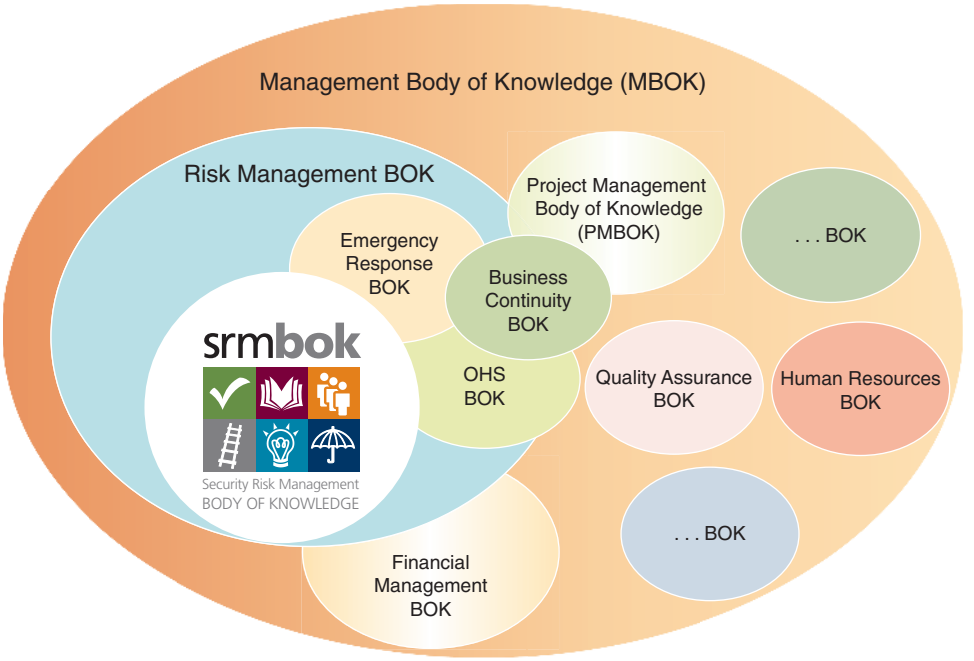


FIGURE 1.2 Relationship of SRMBOK within the Risk Management Body of Knowledge

Risk management is "the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects."[3]

This definition implies that risk management is a coordinated activity to direct and control an organization with regard to risk.[5]

In a fully integrated risk-management system, Security Risk Management is interlinked at each stage with all other risk-management activities being undertaken (e.g., financial, safety, marketing, reputation, regulatory, etc.). Although the application of Security Risk Management requires discipline-specific knowledge, the overall risk-management process remains the same.

As noted in ISO 31000 Risk Management, the elements of a framework for managing risks are shown in Figure 1.3.

SRMBOK addresses this in more detail in section 5 on Governance Frameworks (page 65), and section 13 on Implementing an Integrated ERM Program (page 331).

A typical risk-management process as described in both ISO 31000 Risk Management and the AS/NZS4360:2004 Risk Management Standard is illustrated in Figure 1.4.

FIGURE 1.3 Risk-Management Framework (ISO 31000:2008)

FIGURE 1.4 Risk-Management Process (AS/NZS4360:2004)

SRMBOK generally adopts the ISO 31000 Risk Management Standard or the AS/NZS4360:2004 model of risk management, and it is consistent with the HB167 Security Risk Management Handbook (companion guide to AS/NZS4360:2004) and AS/NZS ISO/IEC 27001:2006 Information Security Standard. Of course, many more international standards are of relevance, and SRMBOK is inclusive of the broader body of knowledge rather than of any single methodology or system.

1.5 CONCLUSION

SRMBOK has been prepared as a framework in which our current and evolving understanding of the answers to many issues discussed in this chapter can be integrated. The focus is not on a specific assessment methodology but rather on a flexible and customizable overview of the organizational and managerial aspects of risk management, including:

- The integration of security into enterprise risk management
- The focus on opportunity realization
- Efforts to increase standardization and comparability across various methodologies
- The futility of searching for a one-size-fits-all risk-assessment methodology
- The necessity of retaining more narrowly focused risk assessments.