Enterprise Security Risk Management

ASIS International

Draft Guideline dated September 2018

Abstract

This guideline describes the fundamentals of Enterprise Security Risk Management (ESRM), a security-program management approach that uses risk principles to link an organization's security practice to its mission and goals. This guideline explains how ESRM creates partnerships between security and those who manage the assets at risk, applies to all aspects of security within the organization, works in any type of organization, and places risks in context, enabling enterprise leadership to prioritize risk mitigation efforts.

CONTRIBUTORS

The following individuals from the ESRM Standards and Guidelines value stream, contributed to the development of this draft document.

ASIS Board Member Sponsors:

- Timothy M McCreight, CPP
- Richard F Lisko, CPP

Program Management Office:

- Michael Gips, CPP, CSyP, CAE
- Rachelle Loyear, CISM, MBCP
- Amy Poole, PMP

ESRM Subject Matter Experts and Volunteers:

- Brian J Allen, CPP, CEF, CISSP, CISM
- David R Feeney, CPP
- Stuart C Hughes, CPP
- J Kelly Stewart
- Mark Schreiber, CPP
- William E Phillips
- Paul E Zikmund

Technical Writer/Editor:

- Peter E Ohlhausen

ASIS Staff Members:

- Susan M Carioti, CStd
- Aivelis Opicka

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Enterprise Security Risk Management (ESRM) is a strategic security-program management approach that ties an organization's security practice to its mission and goals using globally established and accepted risk management principles.

ESRM provides a consistent practice of risk-based security management that benefits organizations and the Security functions that serve them, mainly involving the proper alignment of responsibilities, resources, risks, and mitigation efforts.

ESRM begins with understanding the organization's:

- Function and mission;
- Strategy and operating environment; and
- Stakeholders.

After those preparations, the security professional begins to implement the ESRM cycle, which consists of four processes:

1. Identify and prioritize assets;
2. Identify and prioritize risks;
3. Mitigate prioritized risks; and
4. Improve and advance.

Additional ESRM components:

- Transparency regarding both risks and security processes; and
- Governance, including both organizational governance and ESRM governance (in the form of a security council).

By continually repeating the processes in the ESRM cycle, the security professional can bring ESRM practice to maturity and maintain high performance over time. In sum, the practice of Enterprise Security Risk Management:

- Creates partnerships between the security function and those who manage the assets at risk;
- Is agnostic and applies to all aspects of security within the organization; and
- Places risks in context (qualitatively and quantitatively), enabling enterprise leadership to prioritize risk mitigation resources and efforts.

DRAFT GUIDELINE

Enterprise Security Risk Management

1. SCOPE

Enterprise Security Risk Management (ESRM) is a working philosophy and an application of fundamental risk principles to manage all security-related risks. This guideline describes the concept of ESRM, including its four principal elements or processes, as well as additional steps security professionals can take to strengthen an ESRM effort, bring it to maturity, and maintain it over time. ESRM can be applied in any type of organization.

The Security function exists to support the enterprise. Through ESRM, the security leader becomes intimately familiar with the organization's mission, strategy, and activities, the larger environment in which the organization operates, and the organization's stakeholders. The practice of ESRM creates partnerships between security and those who manage the assets at risk, applies to all aspects of security within the organization, and places risks in context, which enables enterprise leadership to make informed decisions on risk mitigation efforts for the benefit of the organization as a whole.

ESRM's principal processes are these:

1. Identify and prioritize assets;
2. Identify and prioritize risks;
3. Mitigate the prioritized risks; and
4. Improve and advance the security program.

2. NORMATIVE REFERENCES

There are no normative references pertaining to this document.

3. TERMS AND DEFINITIONS

For the purposes of this Guideline the following terms and definitions apply:

	Term	**Definition**
3.1	asset	Anything that has tangible or intangible value to an enterprise.
3.2	assets – intangible	Assets which do not have a physical presence, including information, intellectual property, credibility and reputation, and brand identity.
3.3	assets - tangible	Assets which have a physical presence, including human and environmental assets.

	Term	Definition
3.4	enterprise	An organization, institution, agency, business, or company.
3.5	enterprise security risk management	A strategic approach to security program management that ties an organization's security practice to its mission and goals, using globally-established and accepted risk management.
3.6	risk	Effect of uncertainty on the achievement of strategic, tactical, and operational objectives.
3.7	risk assessment	Overall and systematic process for evaluating the effects of uncertainty on achieving an enterprise's objectives. Risk Assessment includes: Risk Identification, Risk Analysis, and Risk Evaluation.
3.8	risk owner	Member of an enterprise responsible for mitigating the impact of a defined risk.
3.9	root cause analysis	A technique used to identify the conditions that initiate the occurrence of an undesired activity or state.

4. GENERAL PRINCIPLES

4.1 What is Enterprise Security Risk Management?

4.1.1 ESRM Defined

Enterprise Security Risk Management (ESRM) is a strategic security-program management approach that ties an organization's security practice to its mission and goals using globally established and accepted risk management principles. It addresses all security risk across an enterprise. In ESRM, security professionals and senior management share security responsibilities, but all final security decisions are the responsibility of the business leaders in charge of managing assets.

ESRM does not refer to the convergence of traditional and information-technology security functions under one leadership structure. ESRM also differs from Enterprise Risk Management (ERM), which addresses all organizational risks, including those that are not related to security.

A mature ESRM program encompasses the whole range of security risk mitigation practices, including such matters as physical security, cyber security, information security, loss prevention, organizational resilience, brand protection, travel safety, business continuity, crisis management, threat management, and prevention of fraud and workplace violence. ESRM is the functional management that connects all the key elements of the security effort with the assets that require protection.

4.1.2 Mission

The mission of ESRM is to identify, evaluate, and mitigate the impact of security risks to the business with prioritized protective activities that enable the business to advance its overall mission. Through ESRM, the security professional furthers that business mission by communicating security risks to senior management and asset owners (personnel who are responsible for particular assets). Asset owners and stakeholders are the owners of security risk decision making. Engagement with the business to establish organizational policies, standards, and procedures to identify and manage enterprise security risks is essential to the success of an organization.

Because it is a holistic, enterprise-wide risk management approach, ESRM works across all aspects of security in the organization. Activities like vetting new staff, ensuring cyber security, conducting investigations, and planning for business continuity can all be prioritized in terms of the risk they may pose to the organization.

ESRM puts security tasks in context and helps leadership set protection priorities and allocate resources.

4.1.3 Importance

ESRM provides many benefits to the organization, such as:

- Asset owners and other stakeholders have a proper understanding of the Security function's role;
- Better alignment of security resources to effectively manage risk;
- Improved effectiveness and efficiency of the security program and process;
- Greater risk mitigation and proper risk prioritization throughout the organization;
- Better support for the organization's legal responsibilities; and
- More direct connection to the protection of higher priority assets.

Security functions also benefit from ESRM, as they:

- Develop a more intimate knowledge of the organization;
- Achieve opportunities to speak with diverse stakeholders (both internal and external) to learn what they consider important;
- Develop a better understanding of the organization's objectives;
- Identify risks more completely; and
- Obtain greater support from asset owners by aligning security efforts with their needs.

4.2 Fundamentals of ESRM

ESRM begins with three preparatory efforts:

- Understanding the organization's function and mission;
- Understanding the organization's strategy and operating environment; and
- Understanding stakeholders.

4.2.1 Understanding the Organization's Function and Mission

To best serve the organization, the security professional should develop detailed knowledge of the organization's mission, strategy, and operating environment. Such knowledge aids in identifying risks that could impede the organization's efforts to achieve its goals and objectives. Topics to study include, but are not limited to, operating structure, key staff and leadership, products and services, regulations and legal requirements, and long-term goals and objectives.

Security professionals should consider consulting the following information sources, among others:

- **Organizational insiders.** Engaging with the people who run the organization day-to-day is a forthright way to learn what is critical to the business. That means speaking with leaders and other employees with deep

knowledge of the organization, including C-suite personnel such as the chief risk officer, chief compliance officer, chief operating officer, and corporate legal counsel, as well as business unit leaders and personnel in charge of purchasing, human resources, information technology, finance, auditing, strategic planning, public relations, and marketing.

- **Current and recent communications published by the organization.** The details contained in written materials add specificity to this research. Items to review include internal reports released to the public, short- and long-term plans, contracts, annual reports, government filings, strategic or operational plans, press releases, board minutes, vision and mission statements, organization charts, budgets, projections, and policies and procedures.
- **Outsiders and the media.** Security professionals can gain a different view and further insights from sources outside the organization. These include trade and professional organizations and publications, risk surveys and white papers, open/government sources, auditors, purchased intelligence, mainstream news sources, financial media, consumer publications and websites that feature relevant product and service reviews, competitors' advertising, and social media.

In addition, the security professional should study the organization's underlying, unwritten culture. That culture may include answers to questions such as:

- What motivates the organization?
- Does the culture support or hinder security?
- How does the enterprise handle change?
- How much risk will the organization accept regarding various vulnerabilities?
- Are some business units more amenable to working with the security organization than others?
- Who among senior management are the unofficial security champions, those who electively promote the importance of security?

One may best be able to understand the organization's culture by speaking with long-term, widely connected employees—those who understand the spirit of the organization.

4.2.2 Understanding the Organization's Operating Environment

To gauge risk, it is essential to understand the environment in which the organization operates. Like the organization's structure and mission, its environment also affects its risks, which ESRM attempts to address. The environment consists of two main categories:

- Physical**:** Factors such as the organization's type of building or campus, its surroundings, the amount of pedestrian or vehicular traffic, the amount of nonemployee access needed for the business to operate, and the sensitivity and criticality of on-site business processes and assets.
- Nonphysical: Factors such as rapid growth, intense competition, industry pressures, legal requirements, organizational growth mode, and speed of decision making

The information sources in Section 4.2.1 apply here as well. In addition, security professionals should consult peers in other, similar organizations.

4.2.3 Understanding Stakeholders

Stakeholders—those with a significant interest in the organization's effectiveness—are both clients of and resources for the security function. They include organizational owners of tangible and intangible assets, that is, people responsible for an asset of the organization. Stakeholders may also include:

- Persons with some form of ownership in the organization's mission;
- Persons who can contribute knowledge or support to the organization;
- Persons who may be affected by the organization;
- Persons who may be affected by the security professional's risk management knowledge and skills; and
- Persons who may not always be considered, such as the organization's board of directors.

The assets under consideration may consist of money, data, property, equipment, intellectual property, and brand reputation. One asset may be controlled by or affect multiple stakeholders.

Understanding stakeholders does not necessarily mean harmonizing their interests, which sometimes conflict. Instead it means understanding their needs and their risk insights to better carry out the ESRM cycle.

4.2.4 Applying the ESRM Cycle

After the preparatory efforts (understanding the organization's function and mission, operating environment, and stakeholders), it is time to implement the ESRM cycle. As Figure 1 shows, the cycle employs the following processes:

- Identifying and prioritizing assets;
- Identifying and prioritizing risks;
- Mitigating prioritized risks; and
- Improving and advancing the security effort through root-cause analysis, ongoing risk assessment, and incident response.

Figure 1: Enterprise Security Risk Management Cycle
As appears in Enterprise Security Risk Management: Concepts and Applications, Brian J. Allen & Rachelle Loyear, copyright©2018, Rothstein Publishing. Used with permission

At the beginning of an ESRM implementation, it is preferable to start with Process 1, identifying and prioritizing assets, instead of assuming that the assets are known. However, in reality one might not always start with Process 1. It may be that the organization's assets have already been identified, or an un identified serious risk could be discovered (Process 2), requiring immediate evaluation and mitigation (Process 3). The security professional should start with whichever process is most appropriate at the time and should frequently repeat the ESRM cycle. In ESRM, security professionals manage security risks proactively and, as required, reactively.

ESRM transitions the security professional from a **delegate** role (someone to whom an asset owner assigns tasks without requesting input) to a **partner** role (someone who helps the asset owner understand and manage the risks that could affect the asset). In task management (a delegate role), the security professional executes specific steps to implement security services as directed by the asset owner. By contrast, in ESRM (a partner role), the security professional takes a more holistic viewpoint, providing information to help asset owners and stakeholders prioritize

assets, assess risks, weigh their tolerance for those risks, choose mitigation strategies, and improve security processes. ESRM's Process 4, improving and advancing, acknowledges that risk management is never complete.

5. ESRM CYCLE

The ESRM cycle is presented as an ongoing undertaking, logically flowing from Process 1 to Process 4. However, that order of operations might not always be optimal in an unpredictable world. As noted in Section 4.2.4, an organization's circumstances may require starting with an ESRM process other than Process 1. The cycle can run successfully from any starting point.

5.1 Process 1: Identify and Prioritize Assets

The ESRM cycle begins by focusing on the identification of assets. According to the ANSI/ASIS/RIMS *Risk Assessment Standard (2015)*, an asset is "anything that has tangible or intangible value to the organization." The standard states that tangible assets include "human, physical, and environmental assets," while intangible assets include "information, intellectual property, brand, and reputation."

In ESRM, it is understood that organizations rely on many assets to operate and that each asset should be linked directly to an asset owner.

5.1.1 Asset Owner

The asset owner is the person with the greatest responsibility for the asset. The asset owner was not necessarily responsible for procuring the asset but is responsible for operating and maintaining it. The asset is crucial to the asset owner's operations; therefore, the asset owner is likely to be concerned enough to have developed valuable insights regarding risks to the asset.

5.1.2 Stakeholder

The term *stakeholder* was addressed earlier (Section 4.2.3). In brief, stakeholders are people with a significant interest in the organization's effectiveness. In ESRM, one interprets the term broadly to collect the greatest amount of information. Like asset owners, stakeholders are likely to possess useful insights regarding risks.

5.1.3 Value and Prioritization

Assets should be identified, valued, and prioritized in relation to the enterprise's missions and goals. The valuation and prioritization of all worthwhile assets depends on the organization's resources, but over time the task can mature and become a stable and integral process for all departments.

Asset value can be established in several ways. One can measure the cost of purchasing the asset, the impact of operating without it, the effect of harm to the asset, the reputational damage following from loss of the asset, the length of time required to replace it, and many other factors. Asset valuation may be quantitative (numerical measurements), qualitative (interviews, surveys, and industry publications), or a mixture of both. Valuing assets is complex, as the cost of replacing an asset may be minor while the losses that follow harm to the asset, such as disruption of operations and supply chains, may be great. In other words, an asset's direct monetary value may be small while its overall value to the organization is great.

A business impact analysis (BIA) is a widely known process used to value assets and can be performed in many ways. In some organizations, personnel involved in disaster recovery, business continuity, or financial risk management may possess information that is useful when conducting the BIA.

5.2 Process 2: Identify and Prioritize Risks

Using common risk management principles, the ESRM approach helps the security professional take an organization-wide approach to security risk management. ESRM focuses on a broad array of security risks (including physical, personnel, and cybersecurity risks) but generally does not address non-security risks (such as market risk, technology risk, or credit risk) that are often addressed by ERM programs.

Risk identification requires expansive thinking, as risks may arise from many quarters, both within and without the organization. Risks may even originate thousands of miles away, as in the case of supply-chain vulnerabilities that could severely disrupt the organization's operations.

5.2.1 Asset and Risk Association

Assets are identified in Process 1, identifying and prioritizing assets, and risks are identified in Process 2, identifying and prioritizing risks. A key feature of Process 2 is the linking of risks to assets and their owners (described in Section 5.1.1). As the person with the greatest responsibility for a particular asset, the asset owner is ultimately responsible for mitigating risk to that asset.

5.2.2 Risk Assessment

After being identified, risks must also be assessed. The security professional can choose from several security risk assessment methods. One way to develop criteria for risk tolerance is to prepare a matrix that weighs an event's likelihood against its consequences. Topics to examine include risk controls and their effectiveness, criticality, general and specific threats, vulnerabilities, consequences, likelihood, severity, and velocity. Security risk assessments should ultimately address risks to all assets.

5.2.3 Risk Prioritization

The key value of a security risk assessment is to inform risk prioritization. In ESRM, the security professional identifies risks to the right level of executive within the organization, provides those managers with an objective perspective on the risk, and then lets the executives decide what path to take regarding the risk. In ESRM, the security professional's role is not to determine which risks to address but to guide the business through a security risk decision making process with data and subject matter expertise. ESRM communicates with business leaders in a language they understand—the language of risk.

One tool of risk prioritization is the business impact analysis, as discussed earlier in Section 5.1.3. The BIA can be useful in both Process 1, identifying and prioritizing assets, and Process 2, identifying and prioritizing risks.

5.2.4 Risk Tolerance

In ESRM the security professional works with senior management to define parameters for how to respond to various levels of risk—in other words, how to decide which risks to accept, transfer, mitigate, or avoid. The parameters will vary by organization. For example, one organization might tolerate high-likelihood, low-impact risks and choose to aggressively mitigate certain low-likelihood, high-impact risks, while another organization might take the opposite approach.

If management accepts or tolerates a particular risk, that is their decision to make. However, if the security professional feels a serious risk is being ignored, he or she should make a special effort to ensure that management clearly understands and accepts the risk. The final decision should be documented.

5.3 Process 3: Mitigate Prioritized Risks

Once the security professional and stakeholders have identified and prioritized assets and risks, it is time to develop and put into practice a suite of risk mitigation measures, otherwise known as security policies, practices, and equipment.

5.3.1 Mitigation Development

Risks may be accepted, transferred, mitigated, or avoided. Acceptance may make sense when a risk is small and the consequences are minor; transference typically refers to insurance; and avoidance may be possible by changing or ceasing certain operations. The other response to risk is mitigation—the effort to reduce the likelihood or impact of an undesired event. Mitigation efforts, also known as countermeasures, include the full range of security devices and practices, such as crisis planning, security officer operations, access control, video surveillance, perimeter protection, cyber security, investigations, and employee background screening. At this stage of the ESRM cycle, the security professional proposes a means of mitigating the risks identified as a priority in Process 2.

5.3.2 Mitigation Implementation

Once a mitigation strategy has been approved, the security professional must oversee normal project management concerns to see the mitigation measures through to implementation. Earlier processes in ESRM focused on asset owners; in this stage, the focus is on security implementation, a responsibility owned by the security professional.

Even though ESRM orients security efforts toward risks prioritized by senior management, mitigation implementation may encounter conflicts. For example, budget owners may reduce funding for security efforts, stakeholders might differ on how best to address risks, or security measures might hinder asset owners in their work for the organization. Professional application of planning, engineering, and design will support the implementation process and mitigate organizational friction.

5.4 Process 4: Improve and Advance

ESRM's fourth process propels the security program toward constant improvement. The ESRM cycle continues without end so that Process 4 may continually strengthen the other three processes. No enterprise security risk management strategy can remain fixed, as processes always need improvement, new risks arise, and incidents take place. Process 4 responds to security shifts and collects data to right-size security measures (which may need to be increased or decreased, as appropriate). Throughout this process, security professionals should compare their current security efforts to those that are best in class as well as to stated goals and objectives.

Security professionals can employ many ways of improving and advancing the ESRM effort. Three, in particular, are incident response, investigation, and information sharing.

5.4.1 Incident Response

The security professional can improve and advance the ESRM effort by developing incident reporting systems and response plans through strategic partnerships with asset owners and stakeholders. Incident reporting systems provide data for ongoing improvement. Incident response plans address security events small and large. Some security incidents might require dispatching a security officer, while others might call for a multipart procedure consisting of preparation, identification, containment, eradication, recovery, and lessons learned.

5.4.2 Root Cause Analysis and Investigation

The security professional improves and advances the ESRM program by conducting ongoing investigations of both risks and incidents.

Through risk investigations, one identifies new risks and obtains information on the current state of already-known risks. Findings help in updating risk mitigation plans.

Through incident investigations, one gains data that informs security responses, employee disciplinary actions, and other preventive measures. Root cause analysis is particularly useful for preparing security action plans and measuring countermeasure effectiveness.

Identifying and tracking whether those mitigating countermeasures for identified root causes are put in place and measuring the effectiveness of those actions is part of the ongoing cycle of improvement.

5.4.3 Ongoing Risk Assessment and Information Sharing

Incident response, investigations, and root cause analysis feed into a continuous assessment of the organization's view of risk. Information sharing by security professionals strengthens bonds with asset owners, increases stakeholders' awareness of risk, and informs senior management of the fluctuations in risk levels. Risk may be conveyed through graphs, risk heat maps, or various other means. By monitoring stakeholders' awareness of risk, security professionals can better prepare security training and awareness tools.

6. ADDITIONAL ESRM REQUIREMENTS

6.1 Transparency

Because ESRM depends on collaboration with stakeholders, the security professional should be clear and open about security risks and processes. Transparency will strengthen stakeholders' trust in ESRM.

6.1.1 Risk Transparency

Process 2 of ESRM, identifying and prioritizing risks, requires the security professional to present risk information to senior managers so they can set mitigation priorities. Asset owners and stakeholders also need to know about risks if they are to participate fully in ESRM. To enable relevant parties to make informed decisions about risk and mitigations, the security professional must share risk information openly and without exaggeration or minimization—in other words, transparently.

If stakeholders opt not to implement recommended security measures, the risk transparency process provides a record that the organization is educated on the risks and possible mitigation measures. If the organization has a recurrence of impact from a risk, the organization will have the information needed to potentially adjust risk tolerance levels.

6.1.2 Process Transparency

Especially in Process 3, mitigating prioritized risks, ESRM requires an open process so all participants can feel they are being treated fairly. The security professional should keep them informed about current and planned security measures, the reasons for those measures, which stakeholders decided on those measures, other mitigation options that may be considered, and stakeholders' final decisions on risk mitigations.

Maintaining a transparent security process protects the Security function by clarifying the connection between risk ownership and selected mitigation measures—that is, making the decision maker accountable. Transparency shows how well the Security function is serving the organization and encourages cooperation from stakeholders.

6.2 Governance

Governance, which exists at both organizational and security levels, consists of the policies, processes, and practices used to ensure that the organization acts fairly toward its many stakeholders. In general, governance design tends to focus on transparency, accountability, fairness, and responsibility.

6.2.1 Organizational Governance

Organizational governance, the system by which an organization is directed and controlled, typically addresses the role of top executives and the board of directors, the need for audit and oversight, the rights and responsibilities of stakeholders, procedures for decision-making, the need for management transparency, and similar concerns.

6.2.2 ESRM Governance

ESRM governance, a subset of corporate governance, is modeled after organizational governance. ESRM governance is the process for setting enterprise security risk policy and direction, allocating resources, and ensuring compliance. ESRM governance is carried out by the organization's security governance body.

The security governance body leads the security risk tolerance discussion, makes top-level security decisions, and arbitrates stakeholder conflicts. Members include executives and key asset owners and stakeholders. Carrying out ESRM's three preparatory efforts (understanding the organization's function and mission, operating environment, and stakeholders) will help the security professional discover whom to invite onto the governing body. The governing body should clearly understand its role (directing risk management) and the role of the Security function (researching risk and carrying out risk management efforts).

It is a recommended practice in ESRM to have a security governance body that can help assess risk, determine mitigation priorities, and increase security awareness across the enterprise.

Annex A

(informative)

A. BIBLIOGRAPHY

Allen, B. J., & Loyear, R. (2018) *Enterprise Security Risk Management: Concepts and Applications*. Connecticut: Rothstein Publishing.

ANSI/ASIS/RIMS RA.1-2015, *Risk Assessment Standard*

ISO 31000:2018, *Risk management – Guideline*