ASIS INTERNATIONAL
Advancing Security Worldwide®
SECURITY MANAGEMENT

A Brief Guide to ESRM Implementation

Transparency, good governance, stakeholder partnerships, and a holistic approach are all key for a successful ESRM program. Here's some guidance for those considering implementation.

By David R. Feeney, CPP

"I stated my concerns, but no one listened."
"I knew it was a problem, but I didn't know who to tell."
"We didn't assess that type of risk."
"We were in reactive mode."
"You'd have to ask the asset owner."

These statements are common examples of how security workers reply when they are asked after an incident: "What went wrong?"

But when an organization adopts an enterprise security risk management (ESRM) strategic approach, the concerns driving these statements can be addressed before an incident occurs, thus reducing the chance that an incident will occur in the first place.

ESRM is an approach to security management that focuses on risk-based decisions and partnerships with asset owners, and it requires taking a holistic view of overall security risk. Although increasingly popular, ESRM still remains new to some, depending on one's particular role in the industry. But it is not new to ASIS International.

Back in 2017, ASIS created an ESRM Commission as its first step in formalizing ESRM for the benefit of its members. In 2018 and 2019, the association worked to create both an ESRM Guideline and a Maturity Model. The ESRM Guideline is the result of collaboration of dozens of ESRM experts from around the globe, and the document will be the framework for all additional ESRM content.

After months of hard work by staff and volunteers, the ESRM Guideline was released at the 2019 Global Security Exchange (GSX) in September, and the Maturity Model is now available on the ASIS website. GSX featured a rich array of ESRM programming, with more than a dozen sessions throughout the week.

ESRM places the responsibility for security risk management decision making with the asset owners. In other words, whoever owns the asset owns the risk.

In addition, ASIS conducted a survey that will help users gauge the level of maturity of their ESRM programs. Even security professionals without a full ESRM program will be able to identify which aspects they may already have in place. ASIS will use the data from this survey to identify areas of need and create educational materials to help users advance their program's level of maturity.

What are the specifics of the ESRM approach? How can an organization implement ESRM? What are the benefits of doing so? These are all common questions, which this article is meant to address.

HOW ESRM WORKS

The ASIS International ESRM Guideline defines ESRM as a "strategic approach to security management that ties an organization's security practice to its overall strategy using globally established and accepted risk management principles."

ESRM places the responsibility for security risk management decision making with the asset owners. In other words, whoever owns the asset owns the risk. The security professional (a generic title used here to describe the security representative in the security risk management process) supports and guides asset owners through the security risk management decision-making process. ESRM accounts for any security risk—physical, personnel, cyber, information, and more—in a seamless holistic fashion.

In the ESRM context, a security professional adopts the role of advisor, rather than enforcer. This is also a strategic role because security professionals tie security risk decisions to the organization's overall strategy. Thus, security functions as a business enabler and a tool to help the organization accomplish its mission.

COMPLEMENTARY APPROACHES

It's important to understand that ESRM is an approach to managing security risk, not a framework or methodology. Unlike a framework, ESRM describes how to do things and outlines what should be done. But in describing how to do things, ESRM does not go into the same prescriptive or rigid details of how to complete tasks that a methodology does. Given these differences, ESRM can be adopted alongside a framework or methodology, or in operations where no formal frameworks or methodologies are in place.

> ***ERM is an approach to risk management that accounts for the broader pool of all risk. It includes security risk, but it can also encompass strategic risk, technology risk, credit risk, market risk, and any other type of risk.***

Take, for example, a cybersecurity group of a large biotech company. The group previously adopted the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework, and it also employs a mature methodology for managing security. Along with this framework and methodology, the group decided to adopt ESRM.

By doing so, the security group reinvented its role. It incorporated ESRM concepts of tying security to the mission, partnering with stakeholders, and managing risk holistically—all without disturbing its mature methodology and use of the NIST Framework.

Similarly, ESRM can be used in a complementary fashion with enterprise risk management (ERM). ERM is an approach to risk management that accounts for the broader pool of all risk. It includes security risk, but it can also encompass strategic risk, technology risk, credit risk, market risk, and any other type of risk. ERM is a common business function; corporate banks, for example, often have an ERM department or function.

ESRM, in contrast, focuses on security risk and its various domains—physical security risk, cybersecurity risk, information security risk, personnel security risk, and other security risk disciplines. ESRM can be adopted with or without ERM in place. However, a mature and effective ERM program within an organization may make it much easier for that organization to adopt ESRM. The two approaches share common concepts such as stakeholder partnership and holistic risk management, so an organization with ERM in place may already understand the potential benefits of adopting ESRM.

Convergence primarily addresses organizational structure and how personnel should coexist, interact, and operate.

Finally, ESRM can also be employed alongside security convergence, which involves merging security disciplines (such as cyber and physical security) into a single security function to increase effectiveness and reduce cost. Convergence primarily addresses organizational structure and how personnel should coexist, interact, and operate.

In fact, converged security organizations may have even more reason to use ESRM as their security risk management approach. This is because the scope of risk is greater, and the concept of silo-free security disciplines is already in place.

REASONS FOR ADOPTION

For organizations considering adopting ESRM, there are some potential benefits of the approach for the organization, stakeholders, and security professionals.

Organization. ESRM provides a mechanism to elevate identified security risks to top management, which in turn can improve the organization's security program.

Moreover, by prioritizing assets and risks based on the impact to the organization's mission, security risk may be more effectively and efficiently managed. Increased communication between security professionals and stakeholders also helps in ascertaining risk priorities. And increased engagement with security at all levels of the organization will help the department become more integrated into the culture and fabric of the organization. For example, take a large company that decided to adopt ESRM prior to its recent acquisition of a smaller company. To maximize its value to the organization, the large company's security group interviewed the acquired organization's stakeholders and used an ESRM approach to position itself as a trusted advisor and advocate, as well as to learn about their priorities, concerns, operations, and strategy. This information was ultimately factored into a successful plan for post-acquisition integration.

Consider how the acquired organization would have received a more authoritative message of enforcement, such as "This is how it is, and this is what we need you to do." Such an approach could have poisoned these critical relationships from the onset and significantly undermined the new organization's security as a result.

Stakeholders. ESRM offers increased engagement with security professionals, which allows stakeholders to develop a consistent and more accurate understanding of the security function's role.

Through increased communication with security professionals, stakeholders' priorities are more effectively communicated and understood. By positioning security professionals as trusted advisors instead of authoritarian enforcers, the stakeholders are more inclined to share their insights and priorities.

This often leads to increased inclusion in the security risk management process, such that stakeholders develop a sense of ownership and pride in the security program. In the end, these positive results can improve the security program's overall effectiveness, and stakeholders will be safer and more secure as a result.

Security managers. By taking the time to understand the context of ESRM initially, many security professionals will benefit from a broader and deeper understanding of the organization and its overall strategy.

And by developing a greater number of substantive relationships with stakeholders, security professionals benefit from increased stakeholder input, which will usually result in a broader and deeper understanding of the range of security risks.

Because the ESRM approach positions security professionals as trusted advisors, security managers may move into an elevated and more strategic role within the organization.

IMPLEMENTING ESRM: THE COMPONENTS

The components of ESRM as described in the ASIS

International ESRM Guideline help convey what specific actions should be taken to adopt and embrace ESRM as a security risk management process. The guideline describes the following components—the context of ESRM, the ESRM cycle, and the foundation of ESRM.

Context. Before adopting ESRM, security professionals should understand the context of the security program, which in most cases means the organization and the broader environment in which security operates.

Because the ESRM approach positions security professionals as trusted advisors, security managers may move into an elevated and more strategic role within the organization.

First and foremost, understand the organization's mission and vision. This includes the organization's primary purpose (what it exists to do), its short-term goals and objectives, and its long-term aspirations. The security professional should consider how security can help the organization fulfill these, which in turn will change security from a necessary evil to a business enabler.

Core values are also crucial to understanding context. The security professional should learn what cultural core values permeate the organization (whether or not they are explicitly stated), and then ask: How might these values support or hinder the adoption of ESRM? Are stakeholders steeped in these values inclined to adopt a sense of ownership over the security of their organization?

The operating environment is another major component of context. The security professional should learn the key aspects of the organization's internal and external operating environments and how they might impact security. Consider physical, non-physical, and logical factors such as geographic location, strategic plans, threat intelligence, and digital footprint.

Finally, the security professional should learn who the key stakeholders are and what is important to them, and then ask: How can stakeholder priorities be incorporated into security risk management to encourage stakeholder engagement? How can security provide value to its stakeholders?

In contrast, the global firm's mission is focused on maintaining its established brand and marketplace presence, gaining market share, and managing risks

To illustrate these contextual factors, consider the comparative example of two companies—a small IT start-up and an established global manufacturing company, both of which are interested in implementing ESRM.

The start-up's vision includes a focus on attaining aggressive growth, establishing a brand, and earning a position in the marketplace. It does not have formal or clearly defined core values; its culture is naturally fast-paced and sales focused, and there is not much focus on deliberate efforts to build a culture.

The start-up's operating environment is dominated (mainly by default) by the focus on sales and revenue. However, like a small boat on a turbulent sea, the start-up is more vulnerable to changes in the external environment. Stakeholders prefer less involvement. Surrounding communities are content to be disengaged.

In contrast, the global firm's mission is focused on maintaining its established brand and marketplace presence, gaining market share, and managing risks. With significant HR resources, core values are clearly stated in the employee manual, and HR and management take deliberate measures to maintain a positive workplace culture.

Similarly, the global firm's internal operating environment is clearly understood and proactively managed. Given this proactive management, the effect of changes in the external operating environment can be mitigated before they disrupt the internal environment. Stakeholders may perceive larger firms as presenting larger risks. As such, the number and engagement of stakeholders may be greater.

Prioritization is based on how the risks might impact the organization's ability to execute its mission. The result of this phase is a prioritized list of risks.

Cycle. Once the context and environment are understood, it is time to begin managing security risk to the organization. ESRM prescribes a four-step process for managing security risk.

The first step is to identify and prioritize assets. ESRM starts with understanding the organization's assets—what they are, where they are, and why they are important to the organization. Asset prioritization is based on the impact each asset has on the organization's ability to execute its mission. The result of this phase is a prioritized list of assets.

The second step is to identify and prioritize risks. Once assets are understood, security professionals can look towards risks—what are the probable areas of concern and how they might impact the organization's assets. Prioritization is based on how the risks might impact the organization's ability to execute its mission. The result of this phase is a prioritized list of risks.

The third step is to mitigate those prioritized risks. In this phase, security professionals identify mitigation strategies for the prioritized risks that potentially impact the prioritized assets. Combining the asset and risk lists from the previous phases into a matrix may add clarity.

The fourth step is ongoing continuous improvement. ESRM incorporates a mechanism for continuous improvement of the organization's security program. Various operational tasks, such as incident response and investigations, offer the ancillary benefit of fueling continuous improvement of the security program. ESRM encourages security professionals to leverage this benefit.

Foundation. For an organization utilizing ESRM, the entire scope of the security risk management operation should be based on a foundation with the following four pillars.

The first is holistic risk management. ESRM should consider all types of security risk.

The second is a partnership with stakeholders. ESRM positions security professionals as trusted partners who advise asset owners, not as authoritarians who unilaterally define and enforce security policy. This is a cultural shift for many organizations, and it can happen in parallel with ESRM adoption.

The third pillar is transparency. Security professionals must be transparent with stakeholders about the nature of identified risks and the ESRM-prescribed process used to identify, prioritize, and mitigate them.

The fourth is governance. The organization should create a governing body or committee to lead the risk tolerance discussion and make top-level decisions. ESRM governance should align with overall organizational governance.

Again, consider the differences between a small IT start-up and an established global manufacturing company when it comes to the foundational pillars of ESRM.

The typical fast pace of a small start-up may pose challenges to holistic risk management, undermining the efforts to manage risk holistically or strategically because different components are often put in motion by operational changes.

Some stakeholders at a start-up may consider themselves too busy or focused on other things to dedicate time to engage with security. ESRM teaches us that the secret to success for security managers is to identify our stakeholders' priorities and explain how security risk management will help stakeholders successfully achieve their goals. This is how security garners support from stakeholders.

Transparency is especially crucial for start-ups. A lack of transparency may slow down the entire process of managing risk. This in turn could derail it completely in a fast-paced organization, if risk management cannot keep up with the speed of operations. And as with stakeholder partnerships, participation in security program governance can be more difficult to establish at smaller firms, where many are focused on sales and revenue.

In contrast, the typically deliberate and slower operational pace of an established global company may provide a better environment, with more support for holistic risk management. Stakeholder engagement is likely to already be greater compared with small companies because larger firms are often perceived to present larger, more diverse risks. Those engagements can be expanded to include security (if they do not already include it), and often the stakeholders will take a broader focus compared with small company stakeholders.

Stakeholders at a global firm may also be more likely to demand transparency in any process in which they participate, so the foundation for security transparency may already be set there. Similarly, the tendency of global firm stakeholders to adopt broad considerations and an emphasis on the holistic organization may also serve as motivation to participate in security governance.

MOVING FORWARD

If ESRM sounds like it might be a good fit for your organization, here are a few starting steps that can help lay the groundwork for a smooth adoption process.

Improve your knowledge of your organization's overall strategy. That may include your firm's mission and vision, its core values, and its operating environment.

Identify stakeholders in your organization's security effort and build or enhance partnership-oriented relationships with as many as possible.

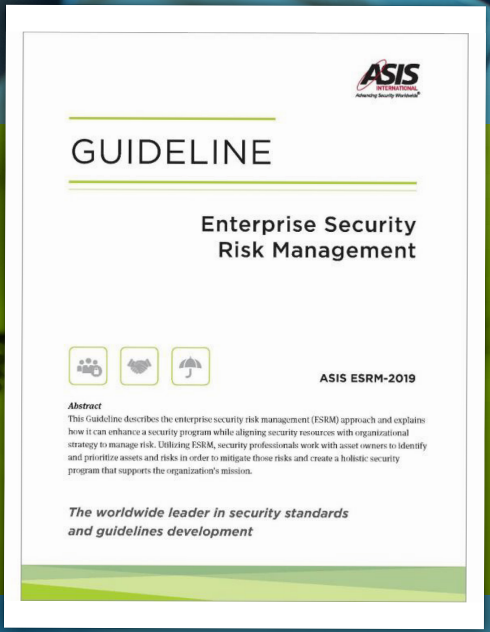
Finally, consider how to most effectively define the role of security within the organization. This may mean incorporating a more strategic advisory capacity for both asset owners and top management.

In the end, a successful ESRM implementation could lead to benefits for the organization, stakeholders, and security professionals alike—a win–win–win scenario. ▨

DAVID R. FEENEY, CPP, IS ADVISORY MANAGER, CYBER AND PHYSICAL SECURITY RISK SERVICES, AT DELOITTE. HE CHAIRS THE ASIS ESRM GUIDELINE TECHNICAL COMMITTEE AND SERVED AS 2018 CHAIR OF THE PHYSICAL SECURITY COUNCIL. HE HAS ALSO BEEN A MEMBER OF THE ASIS IT SECURITY AND SECURITY SERVICES COUNCILS.

ASIS INTERNATIONAL

STAY INFORMED WITH THE LATEST INDUSTRY STANDARDS AND GUIDELINES



ASIS INTERNATIONAL
Advancing Security Worldwide

GUIDELINE

Enterprise Security
Risk Management

ASIS ESRM-2019

Abstract
This Guideline describes the enterprise security risk management (ESRM) approach and explains how it can enhance a security program while aligning security resources with organizational strategy to manage risk. Utilizing ESRM, security professionals work with asset owners to identify and prioritize assets and risks in order to mitigate those risks and create a holistic security program that supports the organization's mission.

The worldwide leader in security standards and guidelines development

The Enterprise Security Risk Management (ESRM) Guideline outlines how to enhance the security function with an approach that embeds it in the organization’s overall strategy. Working with asset owners to identify and prioritize risks, security professionals can use ESRM to create a holistic security program that mitigates vulnerabilities and supports the organization’s mission.

Discover the latest ASIS standards and guidelines at
asisonline.org/standards

ASIS
INTERNATIONAL
Advancing Security Worldwide®

SECURITY
MANAGEMENT

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals. *Security Management* is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

To join ASIS International and become a subscriber to *Security Management*, visit *asisonline.org/membership/join*.