

Key Findings from THE STATE OF SECURITY MANAGEMENT

A Baseline Phenomenological and Empirical Study

Funded by



MODULE 6: Leverage ESRM

Enterprise security risk management (ESRM) is the wave of the future for many if not most security management executives. The study confirmed that the philosophy is indeed becoming accepted globally and that good progress has been made in defining the principles, making security professionals aware of the concept, and developing educational and informative materials on the practice of ESRM.

This study confirms that ESRM is alive and well. Despite the early perception by some that ESRM was simply a buzzword, its development, application, and advancement since its inception have proven its value.

ESRM began to enter the lexicon, generally as an amalgam of the concepts of security risk management and enterprise risk management (ERM), almost two decades ago. Since then, candid discussion, critical thinking, pilot application and strong advocacy have led to a widely accepted, practical, and maturing approach. Many individuals and groups participated in initiatives to define and develop ESRM. Publication of the Risk Assessment Standard, a collaborative effort in 2014-2015 between ASIS International and the Risk and Insurance Management Society (RIMS), served to advance the thinking in this area as well.

A bibliometric study published in *Security Journal* (Marquez-Tejon et al., 2021) analyzed 463 articles and concluded, "Security Risk Management is a subject area on its own and is closely linked to ERM." It went on to partially define and discuss the progression of ESRM:

ASIS International has played an important role in the past few decades in improving a new security paradigm in the context of risk management... The first major initiative was the joint creation by ASIS-ISACA in 2005 of the Alliance for Enterprise Security Risk Management (AESRM), which proposed that ESRM requires multifunctional collaboration in the ERM context across various management areas, including but not limited to physical and logical security,

occupational risk prevention, legal, risk management, and crisis management and business continuity planning.

Additionally, a paper produced by the ASIS International CSO Roundtable in 2015 emphasized the holistic nature of ESRM. Later work by Petruzzi and Loyear (2016) discussed the life cycle of ESRM and highlighted that “this philosophy encourages all company sectors to proactively recognize and deal with risk from a security perspective.”

ESRM has become a valid and fitting approach that can be effectively leveraged, especially considering the growing complexities and interdependencies of security management evident from survey findings, interviews, literature search, and observation. Overall, almost 72 percent of our respondents stated that applying the principles of ESRM is either “very important” or “absolutely critical” in performing their duties. Moreover:

- 61 percent of respondents stated that ESRM is adequately defined.
- 49 percent of respondents stated that adequate information and educational materials about ESRM are available.

SECURITY THOUGHT LEADER PERSPECTIVE:

Relevance of ESRM

“As an industry, we need to partner with other functions and other professions that own other aspects of operational risks in the business.”

-Whit Chaiyabhat, CPP, MBCI, CBCP, CEM

In 2019, ASIS International published the *ESRM Guideline*, which memorialized the concept and provided a unifying baseline. According to the guideline, ESRM is a strategic approach to security management that aligns an organization’s security practices to its overall strategy using globally established and accepted risk management principles. Further, it states that security executives must understand the context of the organization in terms of its “mission and vision, core values, operating environment, and stakeholders.... [ESMR] addresses all domains of security risk in a holistic manner and without silos.”

The sixth in a series of nine modules, this paper explores the findings of an ASIS Foundation study conducted by Kevin E. Peterson, CPP, CIPM II and Joe Roberts, Ph.D. in 2020 and 2021. To download the full *State of Security Management* report, visit [asisfoundation.org](https://www.asisfoundation.org).

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters, and organizations. Online at www.asisfoundation.org.