Key Findings from

THE INFLUENCE OF SECURITY RISK MANAGEMENT

Understanding Security's Corporate Sphere of Risk Influence

Funded by

ASIS FOUNDATION™

FINDING SIX:

ORGANIZATIONAL CONTEXT HAS A SIGNIFICANT IMPACT ON SECURITY'S RISK INFLUENCE

Influence is impacted by organizational context, notably when security resourcing and implementation is mandated within a compliance-directed, regulatory environment. For instance, personnel security vetting is accepted and standard practice because it is legislated and audited—there is a mandated and collective agreement on the importance, and therefore security influence. Focus group participants acknowledged that often security risk management does not form part of a regulatory framework, therefore the implementation of security programs within a self-directed environment result in security risks being prioritized behind compliance driven concerns, resulting in reduced influence.

The study found that the key to success and ultimately influence in security risk management lay in the assessor's ability to effectively establish the context and communicate the security message within that context. This point was well supported by the senior-level participants who were more acquainted with models and had worked in the development of standards, frameworks, and processes.

Consequently, it was found that the accuracy in establishing the risk context was of more importance for achieving security risk influence rather than any specific model or format. As one participant stated:

> *Every business has context; every business needs to be protected. Really, if we don't understand that bit, the rest of the process is a waste of time. And this is where the whole thing lies… security needs to understand its context. It's not about being the corporate policeman anymore, it's about protecting the ability of the organization to continue… and we find out what that looks like by establishing the context.*

However, this study also uncovered significant nuances in understanding the difference between organizational context and organizational risk context. All participants supported the view that establishing the context was often poorly done, with security rarely fully understanding their full organizational context, including their organizational risk context.

One corporate executive (nonsecurity) provided examples of an organizational risk taxonomy, illustrating that within the broader organizational risk hierarchy, security risk featured in only three out of 36 business unit risk concerns. This discussion highlighted the appearance that security risk was less important than other risks in the wider risk framework, and importantly, a distinct lack of widespread use of these tools such as a formalized risk taxonomy document or an enterprise risk management framework. When further questioned on the existence of an ESRM/ERM program, or an organizational risk taxonomy, the significant majority of participants from noncritical infrastructure organizations stated that either a framework did not exist or, if one did exist, it was not communicated widely nor understood by security and other operational business units.

One security manager highlighted that he was aware of an enterprise-level risk taxonomy, but saying “that’s way above my level,” highlighting again the hierarchy and relegation of security risk to the lower echelons, and indeed being omitted from the broader organizational risk conversation. This supported the premise that notwithstanding best intentions to understand the organizational context, one of the biggest limitations to attaining influence by security professionals is in understanding the broader organizational risk context and being able to leverage that information successfully. As one security manager stated:

> *We get this instruction to “establish the context” – blah blah, and we go and do our facility characterization and we ask about their risk appetite because that’s what we think risk context is, but the fact is, we have absolutely no idea about the risk context of our business. I know that money ... for new CCTV is going on SOCs and networking and whatever, but I don’t see anything else because I’m not part of those conversations and unless I’ve been through the ranks, I don’t know what I’m asking. You talk about a taxonomy? I bet most security managers have no idea what that is.*

The study found that this results in failure to understand the business needs, a lack of understanding of where security fits in to the organizational risk framework, and a communication disconnect in terms of treatment.

This finding highlights the implied understanding, yet lack of explicit direction towards a risk context. As one participant commented, “If anyone is out there who says they can give you a risk template, they’re lying to you...they can share concepts and ideas, but... no one can share a template because they all see and interact with risk differently.”

The study found that aligning their risk management work directly to the broader organizational risk hierarchical framework through engagement with an enterprise-level risk taxonomy is required in order for security professionals to clearly, concisely, and accurately inform decision makers about their risk message. This would ensure this message is aligned to the precise business risk context and communicate their findings in exacting and comparable business terms, using business metrics. This approach will enable business leaders to fully comprehend and align all business unit assessments for comparable decision making.

Funded by ASIS FOUNDATION™

This is part of a series of nine short synopses, this paper explores the findings of an ASIS Foundation study conducted by Dr. Michael Coole, Nicola Lockhart and Jennifer Medbury of Edith Cowan University in Australia in 2022.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achiever 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.