ASIS Foundation

Request for Proposals (RFP)

From Data to Intelligence to Actions: Governance and Decision Support in Corporate Security

August 2026

The ASIS Foundation seeks proposals from qualified researchers to conduct a study on an important topic related to the security profession and industry to provide an engaging, informative, and actionable report. The audience for this study consists of (1) practitioners in the corporate, organizational, and private security fields and (2) stakeholders who are interested in security, such as suppliers, investors, academics, corporate executives, and government policy makers, among others.

RFP DETAILS AT A GLANCE	
Maximum Budget	US$40,000
Proposal Deadline	August 27, 2026 (midnight, US PT) as SINGLE PDF to RFP Contact
Intent to Submit (optional)	By August 17, 2026
Inquiries/Questions	By August 21, 2026
Awardee Announced	September 25, 2026
RFP Contact	Submit proposal, intent, questions to the Project Manager: Polly Karpowicz polly@karpstrategy.com

ASIS International is a global community of 34,000 security professionals representing all aspects of security, including security risk management, physical security, cybersecurity, and business continuity. ASIS members represent virtually every industry in the public and private sectors, and organizations of all sizes—serving as chief security officers, security directors, security managers, and entry-level managers, as well as chief executive officers, consultants, product or service suppliers, law enforcement, and military personnel.

The ASIS Foundation, a not-for-profit ASIS affiliate, advances the profession through education and research designed to build knowledge among security professionals and executives as well as stakeholders, including suppliers, investors, academics, corporate executives, and policy makers, among others. The Foundation partners with third-party professional researchers to conduct independent rigorous research and deliver evidence-based research which is made freely available to ASIS members and as paid content to non-ASIS members. More information: asisonline.org/about-asis/asis-foundation.

1. Overview

1.1. Summary

The ASIS Foundation invites proposals from qualified researchers to conduct a scholarly study on intelligence governance and decision support in corporate security. The selected researcher will provide an engaging report of their research findings and actionable recommendations relevant and applicable to the ASIS global community of security management practitioners and stakeholders spanning across all sectors, industries, and security domains.

1.2. Background

The objective of this research is to gather insight into existing research, literature, frameworks, and current practices and to identify and address notable gaps and critical unresolved questions that are relevant and applicable to the ASIS global community of security practitioners, executives, and stakeholders across industries and domains of security management.

A cursory review of literature revealed notable gaps and need for this study, providing initial understanding of what we currently know about this topic, what critical gaps and questions exist, why this research matters, and why now. For instance, a 2017 ASIS white paper recommended rethinking the intelligence cycle for corporate security contexts, arguing the cycle must adapt to private sector realities including new consumers, new requirements, and limited resources.[1] However, no subsequent empirical research has built on that call to produce a validated governance framework for how corporate security functions should manage the intelligence process in practice. For additional insight into the issue, read the Harvard Business Review article entitled "How Corporate Intelligence Teams Help Businesses Manage Risk" written by Paul R. Kolbe and Maria Robson Morrow and published on January 4, 2022.[2]

Security functions are increasingly expected to contribute to high-stakes organizational decisions, but they often lack the governance structures, analytical capabilities, and decision-support processes needed to do so effectively. Yet, no comprehensive, evidence-based framework exists for how corporate security functions should govern the transition from data to intelligence to decisive action—nor for how the quality of that governance process determines the speed, confidence, effectiveness of security-related decisions under pressure, and security support for business decisions.

This study will be conducted at a fitting moment for security practitioners and stakeholders around the world. ASIS began the process of developing an Intelligence Standard for the security profession in early 2026. This research project outlined in this RFP is separate and apart from the standard development process, however, working to develop a standard signals that the profession is actively grappling with how intelligence should be defined, governed, and applied in corporate security contexts. Research that produces validated, practitioner-grounded frameworks in this space contributes to a broader professional conversation at exactly the right moment.

---

[1] Davydoff, D. (2017). *Rethinking the intelligence cycle for the private sector* [White paper]. ASIS International. https://www.asisonline.org/globalassets/security-management/current-issues/2018/01/white-paper_intelligence-cycle_11-29-17.pdf

[2] Kolbe, P. R., & Morrow, M. R. (2022, January 4). *How corporate intelligence teams help businesses manage risk*. Harvard Business Review. https://hbr.org/2022/01/how-corporate-intelligence-teams-help-businesses-manage-risk

2. Research Requirements (Scope of Work)

2.1. Research Focus

The ASIS Foundation study will investigate the intelligence governance process, studying how organizations can effectively collect, disseminate, and ultimately use intelligence to make decisions that improve business outcomes, mitigate risks, and protect assets. The central research question (below) outlines the primary focus envisioned for this study.

Central Research Question

How do corporate security functions currently manage the transition from data to intelligence to decisive action—what governance, structural, and capability factors explain why that process succeeds or fails—and how does the quality of that process determine the speed, confidence, and effectiveness of security-related decisions and business strategy under pressure?

The research should study related best practices with scholarly rigor and prepare a comprehensive report containing evidence-based findings and actionable recommendations in a clear, articulate, and accessible way to ASIS's global community of security professionals and stakeholders. As such, the ASIS Foundation welcomes proposals from researchers from within the security profession and from a wide spectrum of disciplines, fields, and sectors and from research teams formed from multiple organizations.

The selected researcher(s) will investigate how security practitioners can better understand, measure, apply, and enhance intelligence governance within their organization, directed by evidence-based research. The research should also explore and define gaps in knowledge about intelligence governance. The research and resulting report should be relevant to security professionals in all sectors and to a worldwide audience.

The specific topic and methodology may be suggested by the research applicant, but proposed research should consider:

- Current intelligence governance practices, theories, models, frameworks, metrics/KPIs, regulations, standards, guides, or application to relevant global security professionals and to all organizational executives and other general staff who have a role and/or stake in enhancing intelligence governance within their organizations.
- Contemporary definition, language, terminology, understanding, influence, maturity, etc., of intelligence governance, including elements that constitute "intelligence governance."
- Current understanding and knowledge of intelligence governance as a concept and of best practices and resources related to developing and sustaining intelligence governance.
- Robust methodological approaches, data collection, and analysis methods in ways that result in and can demonstrate validity and reliability of findings.

- Actionable guidance and recommendations to security professionals and the organizational executives on why and how effective intelligence governance improve business outcomes, mitigate risks, and protect assets.
- Relevance and application to all security functions, and should not focus only on a single security function such as security management, enterprise security risk management (ESRM), business continuity management (BCM), cybersecurity, or governance and culture.

2.2. Guiding Questions

Researchers should use the following questions to guide their proposed research approach, in addition the central research question:

- How is "intelligence" defined and distinguished from "data" or "information" in corporate security contexts, and what does that distinction mean for how it is governed?
- What governance structures, roles, and processes enable security functions to effectively collect, analyze, and disseminate intelligence to support organizational decisions?
- What are the most common failure modes in the data-to-decisive action process in corporate security, and what organizational conditions cause them? Conversely, what do success factors look like?
- How do corporate security functions currently evaluate whether their intelligence process is working, and what metrics or feedback mechanisms would enable meaningful, repeatable self-assessment across different organizational contexts?

2.3. Exclusions (Areas Out of Scope)

The following areas are considered beyond the scope of this research (i.e. explicit exclusions).

- Cyber threat intelligence or information security intelligence should not be the primary research focus. Findings from cyber contexts may be drawn on comparatively, but the research must address the broader corporate security intelligence function.
- National security or law enforcement intelligence functions are only in scope as far as they inform or provide context for other settings, such as corporate security or security in NGOs, schools, government agencies outside defense and law enforcement, and other organizations.
- Technology solutions, platforms, or specific tools for intelligence collection or analysis should only be examined in the context of their role in the governance process.
- The research must produce usable tools or frameworks. Any purely theoretical or conceptual outputs with no practitioner application should only be considered as in scope in limited ways, such as articulating the need for future research in particular areas.
- Study of a single aspect of the intelligence governance structure to the exclusion of other aspects is not desired.

2.4. Value Proposition

To the extent possible, proposed research should align with the study value proposition below:

- Advances security management's understanding, relevance, and practice of intelligence governance.
- Presents practical, specific, and actionable guidance to global security practitioners.

- Supports security leaders in building the internal credibility and influence needed to drive intelligence-informed decisions at the executive level and throughout the organization. Articulates security as a core corporate value rather than a compliance function or expense.
- Facilitates better intelligence practices and decision-making based on sound intelligence governance.
- Provides a validated framework and practical tools that security functions can adopt and adapt regardless of sector, size, or maturity.

2.5. Research Report

The research team will prepare a final research report of the study findings and recommendations (maximum 30 pages, not counting appendices). The report should be engaging, informative, evidence based, professionally presented, academically sound (with citations), relevant and actionable to the target audience of security practitioners. The report should include, at minimum, the following sections:

1. Executive Summary
2. Background
3. Literature Review
4. Methodology
5. Analysis
6. Findings and Interpretations
7. Recommendations, including further research

2.6. Dissemination Activities

The Foundation anticipates that the researcher will present research findings to the industry through the following means:

- At least two ASIS-hosted or sponsored global or regional conferences.
- Live webinar presentation on report findings facilitated by ASIS International media.
- Interview with representative of ASIS media outlet for article or blog post.
- Recorded podcast interview on the report, facilitated by ASIS International media.
- PowerPoint deck (8-10 slides) of key findings and data visualizations for ASIS use its discretion.
- Other activities and/or means, mutually agreed upon by the ASIS Foundation and the researcher.

Researchers are responsible for conference proposal submissions; and for related expenses (e.g. travel, hotel) which may be included in the proposal budget. Note: a complimentary 1-day registration is available for up to two researchers for the GSX conference.

2.7. Terms & Conditions

The report will be a work for hire, meaning copyright will belong to the ASIS Foundation. The Foundation plans to publish the executive summary of the report for free online. The full report will be available online for free to ASIS members as a member benefit and for a fee to nonmembers and the public. The research organization will be given permission to post and disseminate the executive summary only, but may use the report's methodology, analysis, and findings to publish in academic peer-reviewed journals.

The researchers must warrant that all the content in the report is (1) an entirely original work including images, charts, or other graphics, or (2) that they have obtained and will supply written permission for the ASIS Foundation to use any copyrighted material, including images, charts, or graphics.

2.8. Anticipated Study Timeline

The projected timeline for the study, subject to change, is as follows:

Anticipated Study Timeline (subject to change)	
Project Launch	Early October 2026
Kickoff Meeting (virtual)	Early October 2026
Progress Meeting (virtual)	Early January 2027
Draft Report Due	February 17, 2027
Final Report Due	April 27, 2027
PowerPoint Due	Early June
ASIS Publishes Report	Mid July
Dissemination Activities	July 2027-TBD (e.g conferences, podcast, etc)

3. Proposal Submission

3.1. Proposal Content Requirements

Proposals must include following information and materials as indicated, as structured, and as ordered below. The main proposal (sections 1-4) should not exceed 15 pages. *Shorter is encouraged.*

All proposal material should be combined into a SINGLE PDF before submission.

1) COVER PAGE

- Proposed study title, submission date, and amount of funding requested (US$40,000 max).
- Researcher information: name, organization, mailing address, email, and telephone number.
- Study abstract summarizing proposed research, plan, and objectives (100 words max):
  (a) Core research question(s)
  (b) Design (e.g. qualitative, quantitative, mixed-methods, etc.)
  (c) Methods (e.g. literature review, survey, focus groups, etc.)
  (d) Relevance to security practitioners

2) RESEARCH DESCRIPTION

- Summary of intelligence governance (as concept) and core components and factors.
- Overview of proposed research plan, objectives, and outcomes.
- Core research question(s) and focus of study (what study will examine).
- Scope of proposed research, and any limitations.
- What is new, original, and useful about the proposed research to the security industry.

3) RESEARCH DESIGN

- Detailed description, rationale, and justification of proposed research; including of the:
  (a) Research design
  (b) Methodology
  (c) Data collection
  (d) Analysis
  (e) Reporting

- Any theories or conceptual frameworks that will guide the research.
- Research sample/participant strategy, if applicable, (e.g. participants recruitment, sample size, sampling technique, etc.).
- Anticipated incentives offered to research participants.
- Applicability, relevance, and timeliness to ASIS global audience.

4) BUDGET

Note: Requested budget should be appropriate to research scope, not exceed US$40,000, and itemize and justify (explain) each expense, including:

- Personnel, specifying anticipated hours and rates (e.g. researchers, assistants, analysts, etc.)
- Travel
- Overhead when required by the researcher's institution
- Conference attendance (e.g. registration, accommodation, and travel)
- Other expenses (e.g. response incentives, data collection costs, etc.).

5) RESEARCHER QUALIFICATIONS, CAPACITY, AND REFERENCES

- Resumes or vitas of all researchers
- Statement about capacity of researcher(s) or organization(s) to perform the project (experience, staffing, access to necessary expertise, resources, etc.)
- A few examples of prior work (in the form of pdf files or URLs)
- References (names and contact information of people who can discuss the researcher's past work)

3.2. Submission Instructions

Submit proposal and requested materials as a single PDF file to the RFP Contact via email and by the deadline listed below.

Prospective applicants may provide "intent to submit" notices (optional) and questions to the RFP Contact.

RFP PROPOSAL - SUBMISSION PROCESS & DEADLINES	
Maximum Budget	US$40,000
Proposal Submission	By August 27, 2026 (midnight, US PT), email as **single PDF** to RFP Contact
Intent to Submit (optional)	By August 17, 2026
Inquiries/Questions	By August 21, 2026
Awardee Announced	September 25, 2026
RFP Contact	Submit proposal, intent, questions to the Project Manager: Polly Karpowicz polly@karpstrategy.com