SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Policy and Guidelines >

Faculty Advisor: How to Assess Security Vendors for the Best Outcome

Contracting with a vendor that can't meet your needs is a costly error, and often an avoidable one. SEC Subject Matter Expert in Supply Chain Security Mark Kelly weighs in on what you can do to ensure you get the right solution outcome from your vendor.

The ever-evolving threat landscape presents security leaders with new challenges. With the rise of artificial intelligence, IoT, rapidly advancing technologies, and the convergence of physical and cyber security teams, the process of identifying and vetting suppliers has become more crucial than ever.

Although many organizations engage procurement teams to aid in vendor selection, these teams often lack security subject matter expertise. Instead, their primary focus is cost. Considering cost is necessary, but if it is the only criteria, then you may end up with only a partial solution, which creates additional risk.

Imagine if you bought a logistics security solution for a multi-country transit but it doesn't survive the first cross-border inspection. Or perhaps your new GPS units only support 5G and aren't backward compatible for less advanced markets. Maybe your new investigative contractor isn't licensed in all the countries where you conduct operations. Ultimately, scenarios like these end up costing the company more than if you had bought a more robust solution at the outset.

It's therefore imperative to ensure that security interests are given due consideration during the vendor selection process. In this article, we'll delve into the key steps and best practices for finding the right supplier. This involves more than just comparing prices; it entails a comprehensive evaluation of their capabilities, alignment with your organization, an innovative and flexible mindset, and a commitment to ethical practices.

Defining Internal Objectives

Before embarking on the supplier selection process, it's crucial to clearly define your objectives and ensure alignment with the business. Consider the following factors:

- *Security Problem:* Identify the specific security issue you intend to address. Was it prompted by financial losses, the need for cost reductions, gap analysis results, or an attempt to remediate an audit finding? Are you aiming to reduce frequency or improve processes? Can you articulate the value proposition?
- *Business Value-Adds:* Explore potential additional benefits from the vendor relationship. Collaborating with suppliers offering operational insights can foster goodwill with key stakeholders and lead to a shared vision, potentially increasing ROI and better supporting your business case.
- *Technology Fit:* Identify preferred or incompatible technologies, software, or solutions that align with your needs. Can automation be integrated into your solution? Is your existing technology capable of handling newer tech?
- *In-House vs. Outsourcing:* Evaluate whether outsourcing is more cost-effective than insourcing, or if there's a plan to transition between the two. Can your solution be scaled over time? Selecting a vendor positioned for growth is crucial for long-term strategic plans.
- *Geographical Considerations:* Determine whether a regional, global, or centralized solution is most suitable. Weigh the balance between central project management and potential regional cost savings.

Due Diligence for Vendor Selection

Security vendors, like any others, require thorough due diligence. This involves assessing various aspects:

- *Business Strength:* Evaluate the supplier's financial stability and resilience to economic downturns. Consider their historical performance, funding, and ability to withstand challenges. Economic downturns in your organization can lead to reduced vendor spending, impacting smaller and startup suppliers significantly.
- *Ownership and References:* Investigate the vendor's ownership history and relationships. Contact their references for insights into their reputation and reliability. Can they share similar use cases for the product you are considering? Does the vendor have a history of adversarial nation-state influence, negative incidents, criminal cases, regulatory violations, or relationships with competitors?
- *Contract Terms:* Define contract terms related to billing, payment, value-added tax (VAT), pass-through costs, insurance implications, data ownership and visibility, and other variable costs. Specify service level agreements, quarterly business reviews, key metrics, and penalties for failure to deliver.
- *Certifications:* Check for relevant certifications such as ISO, SOC, NIST, or industry-specific accreditations that demonstrate the vendor's commitment to quality and compliance. Are they respected by government or industry licensing organizations? In heavily regulated industries, the supplier's reputation must be impeccable.
- *Geographical Capability:* Assess whether the vendor's geographical reach aligns with your needs and if they have the necessary presence and resources. If services span multiple geographies, are they compatible and complementary? Does the vendor have the maturity to establish business entities in new markets?

- *Social and Environmental Impact:* Evaluate the supplier's social and environmental practices if they impact people or the environment. Ensure alignment with your organization's values where applicable.

Evaluating Capabilities and Solutions

Understanding vendor capabilities and solutions, from a security perspective, is essential. Evaluate whether the solutions can deliver:

- *Technology Compatibility:* Ensure the vendor's technology aligns with your organization's systems and infrastructure. If they house your data, can you access and import it easily? If there are multiple hand-offs, do you retain visibility?
- *Solution Fit:* Assess whether the vendor's solution effectively addresses your problem. Consider factors like implementation ease, user-friendliness, and adherence to geographical regulations.
- *Innovation and Flexibility:* Seek vendors open to innovative approaches and continuous improvement, avoiding those with vague perpetual roadmaps.

Budget and Creative Financing

Managing costs is central to all vendor selection processes. Discuss creative financing options and performance-based incentives with vendors. Request multiple financial models for comparison. Adjust net billing terms, explore tax/VAT credits based on revenue and location, consider tiered pricing, or explore end-of-year credits.

Piloting and Continuous Improvement

When vendor ratings are comparable, consider their willingness to pilot and compare products against competitors. Encourage real-world scenario piloting for valuable insights into solution effectiveness and the vendor's willingness to collaborate. This approach is also useful when implementing in phases or expanding into new markets.

By investing time in the due diligence process up front, security leaders can avoid the cost and additional risk of incomplete or ill-fitting security solutions and services.

Visit the Security Executive Council web site to view more resources in the Program Best Practices : Policy and Guidelines series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

