Vendor Risk Assessment Matrix

Effective Risk Management for Supply Chain Security

TYPE	CONFIDENCE	RISK RANK	COST	SCALABILITY	PARTICIPATION
Self-Attestation	Low	Low	Low	Moderate	Likely
Third Party	High	Medium	High	Low	Likely
OSINT/Scoring	Very Low	Low	Low	Very High	Not Needed
Technical	High	High	Medium	Low	Unlikely
Validated	Medium	Medium	Medium	Moderate	Likely
Onsite	High	High	Very High	Very Low	Unlikely

Risk Triaging

Understanding the procurement's risk level is crucial. We use a short risk triaging process to categorize vendors into low, medium, and high risk, informing the assessment process and frequency. Here are five yes/no questions commonly used:

- *Does the vendor have my data?*
- *Does the vendor have logical access?*
- *Does the vendor have physical access?*
- *Is the vendor offshore?*
- *Is the vendor in the cloud?*

After triaging, you'll have three discrete risk groups. Ideally, the number of high-risk vendors should match your assessment resources. High-risk assessments are resource-intensive, so choose wisely.

Data Confidence

Understanding our risk targets helps determine the level of data confidence needed for our assessments. Initially, even low-confidence results can provide a general overview. However, you shouldn't take severe action based on these. For high assurance, use assessment types that produce reliable results, such as third-party assessments, validated technical assessments, and on-site evaluations.

Assessment Constraints

We face key constraints in performing high assurance assessments, notably high costs and low scalability. Another critical factor is vendor participation. If a vendor is uncooperative, it complicates the assessment process. Each interaction incurs costs for the vendor, especially for validated assessments requiring extensive coordination or on-site visits, making them less likely to participate willingly.

Assessment Types

Self-Attestation: This involves asking the vendor to answer questions or provide a statement that they meet your security requirements, through methods like vendor questionnaires and the CISA RSAA portal. These responses are not validated and are trusted upon receipt. Self-attestations are low-effort and low-confidence, suitable for low-risk vendors or when vendor participation is poor. However, they require some effort and trusting these answers without verification can impact your risk management decisions.

Third-Party Assessment: These are conducted by trusted assessment firms or tools, such as CyberGRX or Fortress. They can be more cost-effective than traditional assessments but may lack specific context due to their generic nature. While more rigorous than self-attestation, third-party assessments can be expensive and shift trust decisions to the third party. It's advisable to use these assessments for findings only and make your own risk determinations.

OSINT/Scoring: This method is popular due to its low cost and high scalability. However, data confidence is extremely low, and findings are unvalidated signals rather than high-confidence results. It's useful for new programs with zero visibility or as a continuous activity between assessments. This approach can help target areas for more rigorous assessments and requires no vendor participation, significantly reducing effort while providing broad visibility.

Technical: These assessments involve technical details like architecture diagrams, system logs, and other artifacts. Combined with validated assessments, they offer very high confidence but are also very expensive. A technical SME is required, and convincing vendors to share sensitive details is challenging. From the vendor's perspective, providing such information is risky. Typically, this level of detail is needed for high-profile or risky procurements. Be prepared for pushback.

Validated: Adding a validated attribute to assessments involves reviewing evidence to ensure it supports the provided answers, conducted by you or a trusted third party, not the vendor. This increases costs and time, often requiring multiple rounds of follow-up due to additional questions. Despite the added complexity and delays, validation is essential for high assurance, akin to zero trust in the supply chain.

Onsite: Onsite assessments involve physical access to verify claimed processes or evaluate physical security controls, such as wireless or RF site assessments. They are used for specific needs, like ensuring proper handling of source code in manufacturing facilities. These assessments require significant coordination, travel expenses, and labor. It's beneficial to interact with individuals not typically involved in the assessment process, such as shadowing workers who could wnegatively influence the processes.

This supports content and knowledge from SEC547: Defending Product Supply Chains and was created by SEC547 author Tony Turner.