SCRM Working Group Kickoff

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) to begin its SCRM Working Group, July 2024

During the initial Supply Chain Risk Management (SCRM) Working Group, Federal experts from government and industry discussed challenges with SCRM in the Federal government.

Current SCRM Landscape

"One of the biggest challenges with maturing and iterating C-SCRM programs is how to scale and meet the needs of an organization with such a diverse mission set, while taking into account the different risk tolerances and thresholds of those diverse mission entities."

Government participants shared a variety of ongoing initiatives aimed to effectively manage, standardize, and mature SCRM programs within their respective agencies while navigating requirements of different mission areas.

Risk Assessments

Some agencies are working towards standardizing certain aspects of the SCRM process, such as risk assessments. One agency conducts rapid, pre-screen assessments and more thorough assessments, and have found that executive summaries outlining the findings are more useful to key decision makers than comprehensive reports.

Early Policies

Others are developing more expansive and proactive SCRM policies that include cybersecurity and enable agencies to evaluate risk prior to awarding contracts. One agency shared insight into a drafted policy which includes a provision that will allow for risk assessments to occur prior to award, during performance, and during the planning phase of acquisition. During the planning phase, requirements will be screened for specific categories. If requirements are met, they are deemed critical to the mission and earmarked for a risk assessment prior to the award, and the provision will be included in the solicitation. Furthermore, the provision requests certain information from the supplier, and requires the contractor to notify the government if this information should change. The findings of the risk assessments are included in the responsibility determination of the contracting officer. If an award is made to a contract with a risk assessment provision, then the clause from the deviation is included in the contract, allowing the agency to conduct post-award risk assessments.

SCRM Harmonization

“Everyone is looking at [SCRM] a little differently.”

Members agree there is a notable disconnect, or a lack of harmonization, in how SCRM processes are applied and interpreted across government and industry partners. Working group members refer to the concept of harmonization in terms of standardization and alignment within a number of categories.

Based on the discussion, the following is a proposed summary definition: SCRM harmonization is to achieve a level of standardization within SCRM processes across government in order to engender transparency and trust among agencies and suppliers, realize cost savings for agencies and suppliers, support vendor compliance, and ultimately reduce supply chain risk.

Standardization

The working group members discussed standardization within the following categories, topics, and recommendations.

“How do we help [business units] assess, distinguish, and differentiate all the possible risks that can infiltrate IT purchases without engaging them at a 1-on-1 level?”

- **Risk Assessments** - Standardizing risk assessments is challenging because risk changes daily, and the mission requirements of agencies differ too greatly. A member proposed developing a broader framework to guide assessments. Dependent on SCRM program maturity, the framework provides a consistent strategy for agencies to assess criteria within broad categories, such as network, internet, and software. When it comes to assessing more specific services, applications, or mission requirements, agencies would then utilize their own assessment framework. Standardizing assessments can increase transparency across the supply chain by making requirements clear and consistent. When suppliers are aware of and adhere to these standards, agencies can begin to build trust and confidence in their products and services.

“Developing a shared language is vital and important to the SCRM practice. It’s something that will ultimately help us facilitate the communication and collaboration that we’re trying to achieve across public and private sectors.”

- **Shared Language** - A lack of shared language around risk prevents the development of standard policies, standards, requirements, and regulations. Currently, risks are not defined consistently, and agencies and industry partners may refer to the same risks by different names. Additionally, risks may be categorized differently by government and industry. One working group member from industry is developing a list of standard risks defined using measurable, defendable data. Members also acknowledge the importance of defining different categories within SCRM, including C-SCRM and other subsets of SCRM programs.
- **Benchmarking Criteria** - Similarly, members noted the importance of companies to be able to compare their risk maturity to others in the industry, and identify areas of improvement.

- **Information Sharing** - While agencies are theoretically encouraged to share information, working group members note that in reality, sharing information is a risk in and of itself. Information sharing typically occurs between trusted individuals through personal relationships, not through official sharing channels. Working group members discussed a need for information sharing specifically for non-Title 50 entities. Other agencies in the working group are working on building a system portal for agencies and supplies to share information in order to enhance their risk-based decision-making during the acquisition cycle. The hope is for the portal to be a resource similar to the FEDRAMP database for cloud services.
- **Duplicative Requirements** - With numerous SCRM frameworks at play, working group members note significant duplication of requirements.

Challenges

Working group members discussed the following challenges with achieving SCRM harmonization.

Organizational Culture

> **"Harmonization is challenging for most organizations, especially culturally."**

Working group members discussed a needed culture shift within organizations and industry alike. Depending on the agency, SCRM programs may fall under the purview of different divisions or leadership roles. For one member, the C-SCRM program resides under the CISO's purview, but sometimes this can fall to risk management officials who oversee all risk.

Along similar lines, members have witnessed strong collaboration and camaraderie within SCRM working groups quickly dissolve when things go wrong. Ultimately, as one member noted, the success of SCRM programs, policies, and procedures comes down to collaboration between people.

Cost

Members acknowledged the rising costs of tools, and subsequently, the need for a better way to evaluate costs and standardizing pricing. For small agencies, accessing SCRM tools is already an insurmountable challenge.

SCRM Program Evaluation

Members noted the importance of identifying weaknesses in SCRM programs, and the ability for agencies to proactively address the weaknesses to improve overall supply chain resilience.

Contract Inclusion

Some working group members identified challenges with crafting contract provision language. One member acknowledged that larger agencies with mature SCRM programs have the resources to craft provision language for inclusion in contracts, yet smaller operatives may not even be aware of the agency's SCRM policy. Additionally, these smaller entities typically do not have the personnel resources to conduct risk assessments.

Supplier Compliance

There are numerous SCRM frameworks being used across government, making it more challenging for suppliers to maintain compliance with requirements. Some working group members point to a lack of awareness of these requirements among suppliers. One member noted that some major suppliers have never heard of an SBOM, which illuminates the significance of this issue.

Similarly, the overwhelming majority of suppliers are unaware of the CISA attestation letter requirement in Executive Order 1428. Government members consider the letter a first attempt at building better security around software, but acknowledge the downsides of the requirement. The attestation is based on the Secure Software Development Attestation Form (SSDF), but the requirements in the attestation are not identical to those in the SSDF form. Moreover, there are numerous steps involved for a supplier to produce an attestation letter and then for the government to review and verify it. However, the first step is to inform suppliers of this requirement.

Final Thoughts

SCRM is about collective collaboration rather than any single organization trying to optimize SCRM on their own. The primary challenge lies in harmonizing the diverse standards, requirements, and risk levels across government, but the working group is dedicated to working collaboratively to improve SCRM across industry.