A STRATEGIC APPROACH TO ACQUISITIONS IN CYBER SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

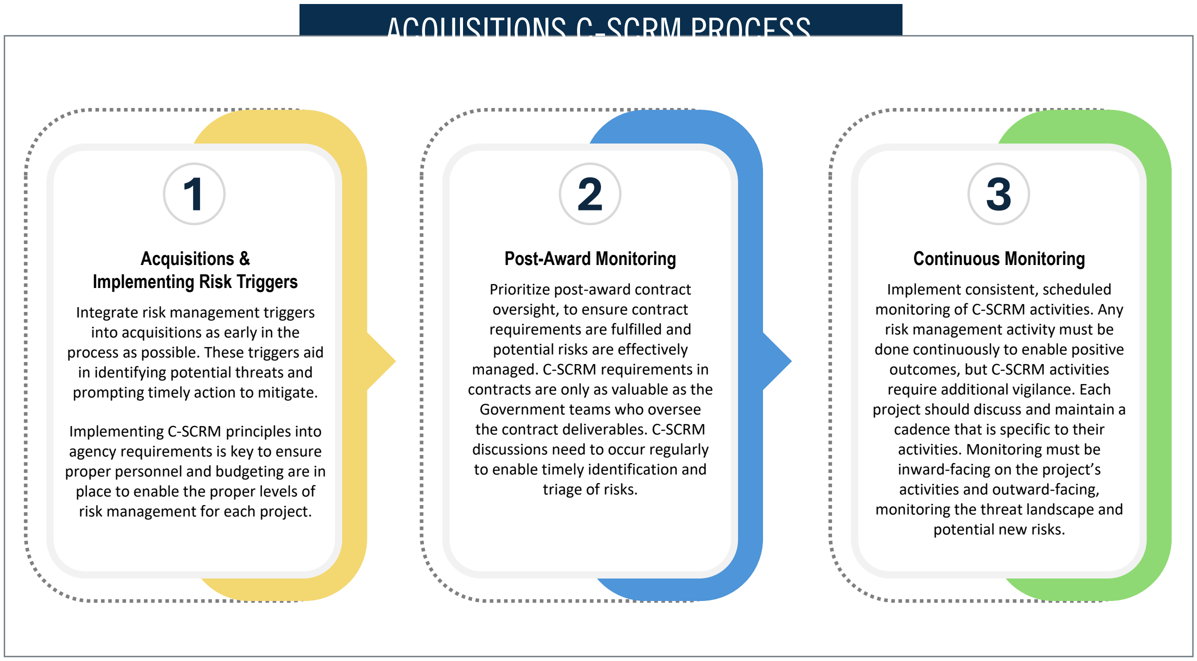
Government agencies are responsible for managing and protecting critical infrastructure and sensitive data that are essential to the nation's security and economy. If a government agency fails to properly vet a software supplier or manage the associated risks, it is introducing vulnerabilities into its systems that can have critical implications for national security. Malicious actors are scanning and testing government systems and networks 24/7 looking for opportunities to infiltrate and undermine U.S. interests.

At MITRE, we have the tools and networks to help sponsors apply rigorous cyber supply chain risk management (C-SCRM) both during the acquisition process, and throughout day-to-day operations. Some of our activities include vetting suppliers, contractors, and subcontractors, such as those who provide components with data egress and those who outsource and leverage third party software code; as well as crafting acquisitions and technical documentation, such as program protection plans and software bill of materials, for C-SCRM that matches projects' complexity and unique parameters.

In addition to supporting projects as they implement C-SCRM today, we also work on improving the regulatory and policy side of C-SCRM, to enable future outcomes. To this end, we work with sponsors to ensure they are implementing processes and procedures that will institutionalize C-SCRM best practices, and help drive impacts at an enterprise level.

To learn more, contact us at

supplychainsecurity@mitre.org



ACQUISITIONS C-SCRM PROCESS

1

Acquisitions & Implementing Risk Triggers

Integrate risk management triggers into acquisitions as early in the process as possible. These triggers aid in identifying potential threats and prompting timely action to mitigate.

Implementing C-SCRM principles into agency requirements is key to ensure proper personnel and budgeting are in place to enable the proper levels of risk management for each project.

2

Post-Award Monitoring

Prioritize post-award contract oversight, to ensure contract requirements are fulfilled and potential risks are effectively managed. C-SCRM requirements in contracts are only as valuable as the Government teams who oversee the contract deliverables. C-SCRM discussions need to occur regularly to enable timely identification and triage of risks.

3

Continuous Monitoring

Implement consistent, scheduled monitoring of C-SCRM activities. Any risk management activity must be done continuously to enable positive outcomes, but C-SCRM activities require additional vigilance. Each project should discuss and maintain a cadence that is specific to their activities. Monitoring must be inward-facing on the project's activities and outward-facing, monitoring the threat landscape and potential new risks.

AI IN ACQUISITIONS: With an eye toward the future, MITRE is looking to expand its focus to the impact of new technologies like AI on C-SCRM. This involves understanding how AI can be used to improve the acquisition process, with a focus on serving as a force multiplier for the workforce, more so in post-award monitoring and continuous identification of potential risks. This will greatly enhance vulnerability assessments, especially where software and components are continuously updated.