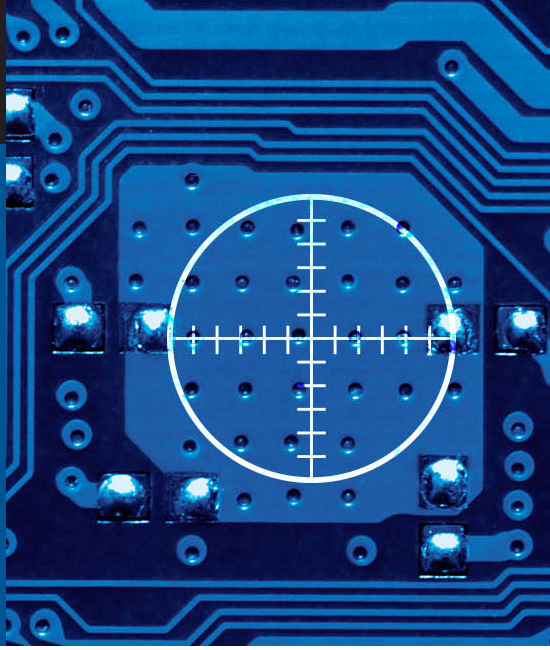
Software Engineering Institute
Carnegie Mellon University

Manage Cybersecurity Risk Across the Lifecycle

The CERT Software Assurance Framework (SAF) Assessment



How do you ensure that you deliver products with low cybersecurity risk? Do you pay attention to cybersecurity only after software products and systems are deployed? You can adopt practices that change how you acquire and engineer systems and greatly improve your ability to manage cybersecurity risk. And we can help.

What We Do

At the SEI we have years of experience working with organizations like yours to improve acquisition and engineering processes. We also have expertise in risk management and cybersecurity.

We regularly apply this expertise in our collaborations with high-level government organizations, including the U.S. Department of Defense, the Department of Homeland Security, and the U.S. Secret Service; federal, state, and local governments; multiple levels of law enforcement, including the FBI; the intelligence community; operators of critical infrastructures; and many industry organizations.

The CERT SAF Assessment

We can help you improve your management of cybersecurity risk across the lifecycle with our new CERT SAF Assessment. We comprehensively examine your lifecycle acquisition and engineering practices to show you where and how to integrate cybersecurity into those practices from the early planning stages through deployment.

Our CERT SAF Assessment puts our experts in your organization to work with you to understand your needs and provide individualized attention. We learn your development and acquisition processes, interview those involved in the processes, and search for evidence to corroborate the facts.

From that information, we analyze how well you're addressing cybersecurity risk in your software products and systems. Finally, we recommend what you can do to improve how you build security into your software products and systems.

Compatibility & Applicability

The SAF is a front-end complement to other improvement technologies; regardless of which technology you're currently using, whether it's Capability Maturity Model (CMM), CERT Resilience Management Model (CERT-RMM), Risk Management Framework (RMF), or Capability Maturity Model Integration (CMMI). The SAF adds cybersecurity practices to your acquisition and engineering approach and ensures that you create products that have lower residual cybersecurity risk.

Benefits of Improvement

By improving your cybersecurity practices, you

- establish confidence your program's ability to acquire reliable, safe, and secure software-reliant systems
- reduce the risk of deploying software-reliant systems that have security vulnerabilities
- increase the integrity of the DoD supply chain and support DoD strategic goals
- fix engineering-related vulnerabilities before systems are deployed, saving time and money

Conversely, failing to integrate cybersecurity practices into your acquisition and engineering practices increases the risk of mission failure in deployed software and systems.

The SAF Is Different

Most cybersecurity improvement technologies focus on operational systems that are already deployed in an enteprise. What differentiates the SAF from other cybersecurity risk management and improvement technologies is that it covers the early phases of the system lifecycle—from initial planning activities through deployment.

The Future of the SAF

The CERT SAF Assessment is a service we tailor to your individual needs. As we work with you, we also gather information about what works and what we could improve in the CERT SAF to generalize it to meet the needs of the broader cybersecurity community.

We envision the CERT SAF as someday being a product. Our work with you and your feedback on the experience will guide our efforts to develop a solution to organizations with similar challenges.

We expect that the CERT SAF of the future will define a set of cybersecurity practices that organizations can integrate with their existing acquisition and engineering practices to better manage cybersecurity risk.

Take the First Step

To be successful, risk and cybersecurity objectives must be translated into practices that managers, acquirers, and developers can apply throughout the system lifecycle.

Leverage our years of experience in cybersecurity, risk management, acquisition, and software engineering to tailor a solution for your program.

Contact us to learn how we can help you.

The SAF Team

Our SAF team is part of the CERT Division of Carnegie Mellon's Software Engineering Institute (SEI), world-recognized leaders in cybersecurity. We study and solve problems with widespread cybersecurity implications, research security vulnerabilities in software products, contribute to long-term changes in networked systems, and develop cutting-edge information and training to help improve cybersecurity. And we are more than a research organization. We help organizations determine how effective their security-related practices are and we're experienced in showing them how to improve their cybersecurity practices.

About

For nearly 30 years, the CERT Division of the SEI at Carnegie Mellon University has been a leader in cybersecurity. Originally focused on incident response, we have expanded into cybersecurity areas such as network situational awareness, malicious code analysis, secure coding, resilience management, insider threats, digital investigations and intelligence, workforce development, DevOps, forensics, software assurance, vulnerability discovery and analysis, and risk management.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu