
BLACKDUCK | carahsoft

Black Duck and NIST RMF: Strengthening Application Security and Compliance

What is NIST RMF?

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a structured process developed by NIST, an agency of the U.S. Department of Commerce, to help identify, prioritize, and manage cybersecurity risks. It provides a comprehensive, repeatable seven-step process that integrates security, privacy, and cyber supply chain risk management into the system development life cycle. By following the RMF, organizations can systematically assess, select, implement, and monitor security controls to ensure appropriate measures are in place based on their specific needs.

The RMF links to a suite of NIST standards and guidelines, such as NIST Special Publication (SP) 800-53 or SP 800-37. This publication provides a catalog of security and privacy controls that help organizations meet compliance requirements and address key risk management elements such as supply chain risk management, systems security engineering, and cyber resiliency. Originally developed for federal agencies, the RMF has been widely adopted across the U.S. government and various industries to implement a risk-based approach for security and privacy and to align with legislation, such as the Federal Information Security Modernization Act (FISMA). The NIST Cybersecurity Framework (CSF) can be used alongside the RMF and implemented using established NIST risk management processes.

The CSF is a voluntary framework that any organization can adopt, and the RMF is mandatory for government agencies. Many organizations use both the NIST RMF and the CSF, leveraging the CSF to identify broader cybersecurity needs, and using the RMF to conduct risk assessments and implement security and privacy controls on systems.

The Importance of NIST RMF

Federal agencies are required to use the NIST RMF for security and privacy risk management. This helps agencies satisfy laws like FISMA, the Privacy Act of 1974, and Federal Information Processing Standards (FIPS). The NIST RMF provides a standardized approach for ensuring uniformity across departments and systems while aligning mission objectives throughout the organization. Additionally, updates to FISMA in 2014 mandate continuous, real-time monitoring of networks to identify and mitigate cyber vulnerabilities, reinforcing the importance of a proactive risk management strategy.

Black Duck & NIST RMF

Black Duck Resource

Thank you for downloading this Black Duck resource! Carahsoft is the Master Government Aggregator and Distributor for Black Duck's open source solutions available via NASA SEWP V, The Quilt, Technology Solutions Products and Services (TIPS) and other contract vehicles.

To learn how to take the next step toward acquiring Black Duck's solutions, please check out the following resources and information:

For additional resources:
carah.io/BlackDuckResources

For upcoming events:
carah.io/BlackDuckEvents

For additional [vendor] solutions:
carah.io/BlackDuckProducts

For additional Open Source solutions:
carah.io/OpenSourceSolutions

To set up a meeting:
BlackDuck@carahsoft.com
(877)-742-8469

To purchase, check out the contract vehicles available for procurement:
carah.io/BlackDuckContracts

BLACKDUCK | carahsoft

Black Duck and NIST RMF: Strengthening Application Security and Compliance

What is NIST RMF?

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a structured process developed by NIST, an agency of the U.S. Department of Commerce, to help identify, prioritize, and manage cybersecurity risks. It provides a comprehensive, repeatable seven-step process that integrates security, privacy, and cyber supply chain risk management into the system development life cycle. By following the RMF, organizations can systematically assess, select, implement, and monitor security controls to ensure appropriate measures are in place based on their specific needs.

The RMF links to a suite of NIST standards and guidelines, such as NIST Special Publication (SP) 800-53 or SP 800-37. This publication provides a catalog of security and privacy controls that help organizations meet compliance requirements and address key risk management elements such as supply chain risk management, systems security engineering, and cyber resiliency. Originally developed for federal agencies, the RMF has been widely adopted across the U.S. government and various industries to implement a risk-based approach for security and privacy and to align with legislation, such as the Federal Information Security Modernization Act (FISMA). The NIST Cybersecurity Framework (CSF) can be used alongside the RMF and implemented using established NIST risk management processes.

The CSF is a voluntary framework that any organization can adopt, and the RMF is mandatory for government agencies. Many organizations use both the NIST RMF and the CSF, leveraging the CSF to identify broader cybersecurity needs, and using the RMF to conduct risk assessments and implement security and privacy controls on systems.

The Importance of NIST RMF

Federal agencies are required to use the NIST RMF for security and privacy risk management. This helps agencies satisfy laws like FISMA, the Privacy Act of 1974, and Federal Information Processing Standards (FIPS). The NIST RMF provides a standardized approach for ensuring uniformity across departments and systems while aligning mission objectives throughout the organization. Additionally, updates to FISMA in 2014 mandate continuous, real-time monitoring of networks to identify and mitigate cyber vulnerabilities, reinforcing the importance of a proactive risk management strategy.

How Black Duck Supports NIST RMF Compliance

Black Duck® provides a comprehensive suite of security tools that align with the NIST RMF, the CSF, and SP 800-53, ensuring organizations can effectively manage risk throughout the software development life cycle (SDLC).

Application Security and Vulnerability Management

Black Duck's portfolio—featuring Coverity® Static Analysis, Black Duck® SCA, Seeker® Interactive Analysis, and Black Duck® Continuous Dynamic—supports vulnerability management through continuous monitoring and scanning, and it aligns with controls specified by NIST to support developmental testing and evaluation. These solutions integrate essential security controls into the SDLC, including secure coding, penetration testing, vulnerability scanning, and code reviews. The Black Duck portfolio also enables testing approaches like manual code review, security architecture review, and static, dynamic, or binary analysis, aligning with industry standards and best practices to enhance application security (AppSec).

Developer Security Training

NIST SP 800-53 emphasizes the importance of security training for developers. Black Duck's tools integrate with Secure Code Warrior to provide training for developers, ensuring the effectiveness of the controls implemented within agency systems. The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems. Training and upskilling development teams is another way to align to these principles.

SSDF Readiness Assessment

As an independent provider of Building Security In Maturity Model (BSIMM) assessments, Black Duck has created a Secure Software Development Framework (SSDF) Readiness Assessment, aligned to the NIST SSDF, to help organizations improve the security and integrity in their software development processes. This assessment allows organizations to identify gaps in their AppSec programs, address inconsistencies, and discover where consistent outcomes will result in secure software products. Most SDLC models do not explicitly incorporate software security, integrating secure development practices, such as those in the SSDF, throughout the process which is essential.