



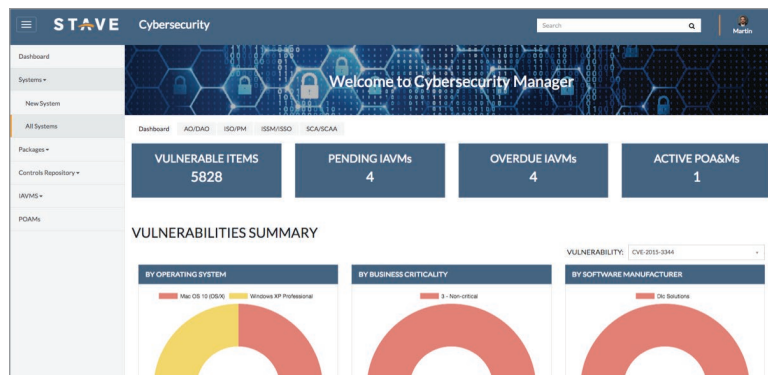
CYBERSECURITY MANAGER

AUTOMATE THE ASSESSMENT & AUTHORIZATION (A&A) AND CONTINUOUS MONITORING REQUIREMENTS OF THE RISK MANAGEMENT FRAMEWORK.

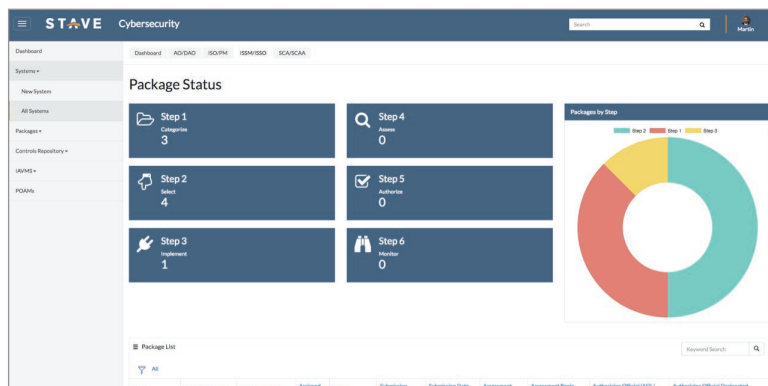
KEY BENEFITS

- Complete the entire Assessment & Authorization (A&A) process requirements in hours, not months
- Easily follow a guided process to record and document your complete System Security Package (SSP)
- Download a completed System Security Package (SSP) directly for review, auditing, and submission
- Continuously monitor your information systems and stay up-to-date on vulnerabilities with real-time IAVA and IAVB reports from U.S. Cyber Command
- Maintain full situational awareness with graphical charts, reports, and dashboards, available on mobile devices, workstations, and command center screens

Cybersecurity Manager delivers a modern web-based capability to automate the NIST SP 800-37 RMF process and accelerate compliance, define remediation workflows, and provide real-time tracking, insight and reporting. Organizations follow a guided, step-by-step process to complete and download a comprehensive security plan and System Security Package (SSP).



Role-based dashboards for continuous and real-time security posture monitoring



System Security Package review and approval dashboard

| Number | Availability | Confidentiality | Control Number | Control Text | Control Title | Family | Integrity | Supplemental Guidance |
|-----------------|--------------|-----------------|----------------|--|--|--------|-----------|---|
| BMFCTSEPO000369 | Medium | Medium | SC 2 | The information system separates user functionality (including user interface) from information system management functionality. | APPLICATION PARTITIONING | SC | Medium | Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, applications, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different users or operating units, different instances of operating systems, different network addresses, virtualization techniques, or container-based or other methods, as appropriate. This guard separation includes, for example, web administration interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include hosting administrative interfaces on different domains and with additional access controls. Related controls: SA 4, SA 6, SA 7. |
| BMFCTSEPO003672 | Medium | Medium | SA 55 (B) | The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analysis from vendor systems, components, or services to inform the current development process. | DEVELOPMENT PROCESS STANDARDS AND TOOLS (INCLUDE OF VULNERABILITY INFORMATION) | SA | Medium | Supplemental Guidance: Analysis of vulnerabilities found in vendor software applications can inform potential design or implementation issues for information systems under development. Similar information systems or system components may pose similar design or implementation vulnerabilities. Information is available from a variety of public and private sector sources including, for example, the National Vulnerability Database. |
| BMFCTSEPO003680 | Medium | Medium | SA 57 (B) | The organization requires the developer of the information system, system component, or information system service to (a) produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of operations, messages, and effects; (b) show via proof of concept demonstration or modeling that the formal top-level specification is consistent with the formal policy model; (c) show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and | DEVELOPER SECURITY ARCHITECTURE AND DESIGN CORRESPONDENCE | SA | Medium | Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model and that any addition of code or implementation details present have no impact on the behaviors or policies being modeled. Formal methods can be used to prove that the top-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a above-tolerance hardware level, for example hardware description. Consistency between the formal top-level specification and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formalized methods may be needed to ensure such consistency. Consistency between the formal top-level specification and the implementation may require the use of an informal demonstration that includes the specific methods used to prove that the specification accurately reflects the implementation. Hardware, software, and firmware models are strictly internal to security-relevant hardware, software, and firmware include, for example, mapping registers and direct memory instructions. Related control: SA 7. |

Complete steps 1-6 of the RMF process



KEY OUTCOMES

- Complete Assessment & Authorization (A&A) requirements in hours, not months
- Compliance tracking up to 95% faster
- Compliance remediation up to 70% faster
- Reduce time to assess IT configurations by up to 70%
- Automate the generation of package documentation, test plans, and plan of action and milestones (POA&Ms)
- Incorporate applicable guidance from NIST SP 800 series, CNSSI 1253, FIPS 199, and others into your organization's comprehensive cybersecurity and risk management plans

CONTACT US

learn@staveapps.com
855-248-5780

FEATURES

GUIDED WALKTHROUGH OF THE SYSTEM SECURITY PACKAGE (SSP) PROCESS // Create a complete SSP in downloadable format that thoroughly documents your organization's information systems, environment and architecture, risk management report and organizational approval process.

VULNERABILITY COMPLIANCE & REMEDIATION TRACKING // Manage and track compliance with information assurance vulnerability alerts and bulletins (IAVA and IAVB) automatically and map mitigation activities against the systems and equipment deployed in your organization.

COMPLIANCE TASK MANAGEMENT // Security Technical Implementation Guides (STIG) act as a cybersecurity methodology for standardizing security protocols within networks, servers, computers and logical designs. Implement all STIGs with automatically-generated compliance tasks, complete with assignment rules and deadlines to enhance security for software, hardware, physical and logical architectures to reduce vulnerabilities.

PLAN OF ACTION & MILESTONES AUTOMATION // Automatically create and assign Plan of Action and Milestones (POA&M) to plan the resolution of information security vulnerabilities. POA&Ms can including detailed lists of the resources, task milestones, and scheduled completion dates.

6 STEP PROCESS

