STAVE
BUSINESS APPS THAT SIMPLIFY WORK

staveapps.com/cybersecurity

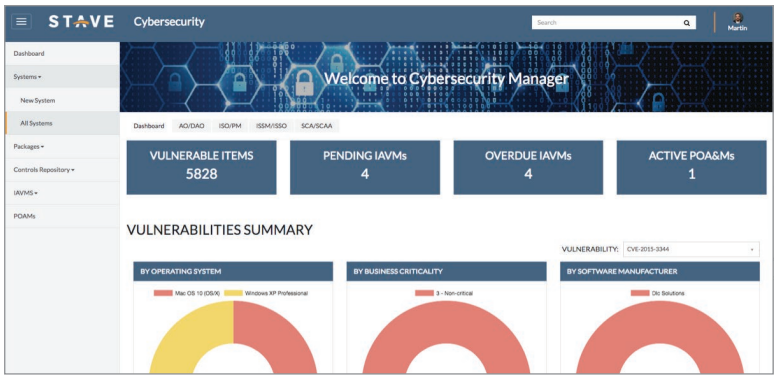
CYBERSECURITY MANAGER

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

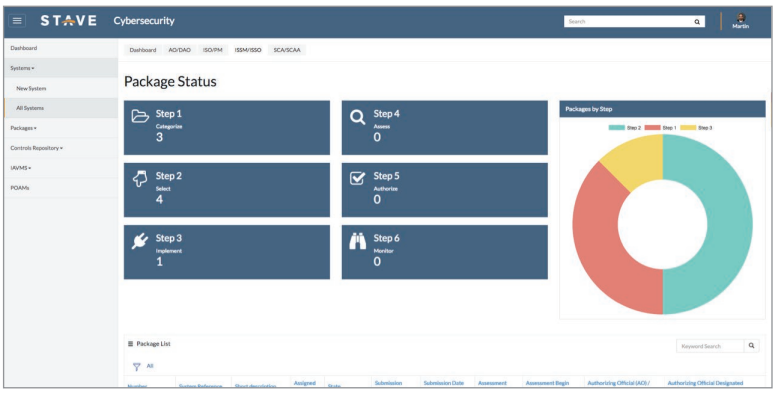
KEY BENEFITS

- 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

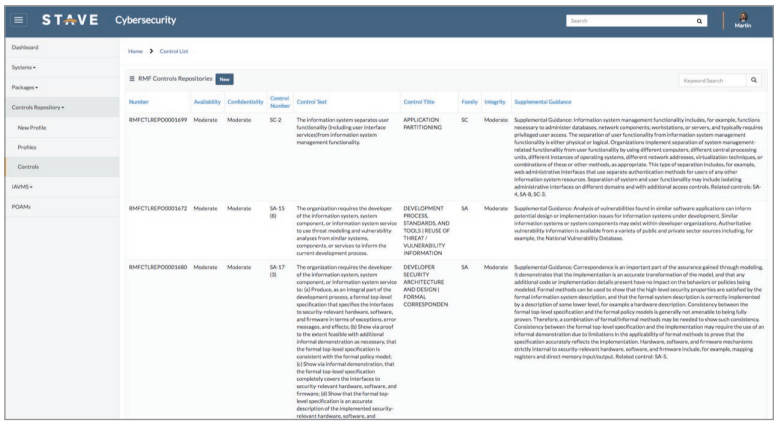
Cybersecurity Manager delivers a modern web-based capability to automate the NIST SP 800-37 RMF process and accelerate compliance, define remediation workflows, and provide real-time tracking, insight and reporting. Organizations follow a guided, step-by-step process to complete and download a comprehensive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



Complete steps 1-6 of the RMF process

STAVE
BUSINESS APPS THAT SIMPLIFY WORK

staveapps.com/cybersecurity

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

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

1 Information System Categorization

- Automatically populate, describe, and assign a security categorization to the system.
- Map categorization to your organization's enterprise architecture in order to protect organizational processes.
- Align categorization to your organization's risk management strategy.
- Register and record the information system and store all modifications for audit purposes.

2 Select Security Controls

- Allocate system-specific, hybrid, or common security controls to each system.
- Assign authorizing officials and define contextual role-based access for all users.
- Document all controls inherited from external providers.
- Tailor security controls for minimum assurance requirements and supplemented common controls.

3 Implement Security Controls

- Allocate security controls as system-specific, hybrid, or common to each system and enterprise architecture.
- Document sound information system and security engineering methodologies.
- Record and audit minimum assurance requirements and all common controls.

4 Assess Security Controls

- Develop a comprehensive plan to assess all security controls.
- Store all assessment-related materials, assessment results, organizational approvals and capture in a unified report.
- Review the organization's comprehensive plan to assess all security controls for the system.

5 Authorize Information System

- Generate a Plan of Action and Milestones (PO&AM) automatically.
- Published an appropriate authorization package and generate digitally.
- Capture and store your organization's risk determination, risk acceptance, and authorization decision.

6 Monitor Security Controls

- Automate the continuous monitoring and reporting of your information systems and its environment of operation.
- Review real-time security status alerts and view graphical dashboard reports.
- Conduct ongoing assessments of security controls and risk management documents.

CONTACT US
learn@staveapps.com
855-248-5780