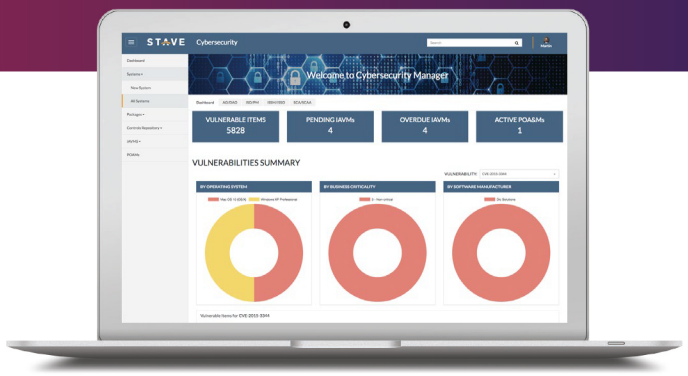
STAVE
BUSINESS APPS THAT SIMPLIFY WORK

CYBERSECURITY MANAGER

staveapps.com/cybersecurity



Cybersecurity Manager provides guided, step-by-step process to managing the NIST Risk Management Framework (RMF) process, track authorization and compliance, manage system security plans, automate assessment and authorization, and operationalize end-to-end continuous monitoring.

KEY BENEFITS

- Complete the RMF and Assessment & Authorization (A&A) process in days, not months
- Centrally track RMF activities, processes, and tasks for a single system or an entire portfolio of systems, applications, and networks
- Guided process to create and manage system profiles, RMF packages, and achieve Authority to Operate (ATO)
- Easily download or export 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 Federal and Enterprise
- Maintain full situational awareness with graphical charts, reports, and dashboards that are fully responsive from mobile devices to workstations and command center screens

FEATURES

CYBER PORTFOLIO MANAGEMENT AND AUTHORIZATION TRACKING // Monitor and track the RMF process and ongoing authorization of your system or portfolio of systems. Also track your cyber workforce and assignments in the same tool.

GUIDED COMPLETION OF RMF PROCESS // Managed completion and task/milestone reporting of the RMF process allows you to ensure the categorization, selection, implementation, assessment, and authorization steps are completed on time using automation, inheritance, and re-use.

SYSTEM DOCUMENTATION // Create a complete system security plan (SSP), fully exportable or downloadable, that thoroughly documents your systems, environment, architecture to enable risk management reporting and organizational approval process.

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

COMPLIANCE TASK MANAGEMENT // Security Technical Implementation Guides (STIGs) act as a cybersecurity methodology for standardizing security implementation and compliance in your environment. Ensure STIG compliance with tasks, 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 ensure the resolution of information security vulnerabilities. POA&Ms can be tailored to include detailed lists of the resources, task milestones, and scheduled completion dates.

CONTINUOUS MONITORING ENABLEMENT // Integrate continuous monitoring system with ServiceNow Security Operations and Configuration Management activities to ensure fully operationalization of your continuous monitoring plans and activities.

servicenow Silver Technology Partner

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