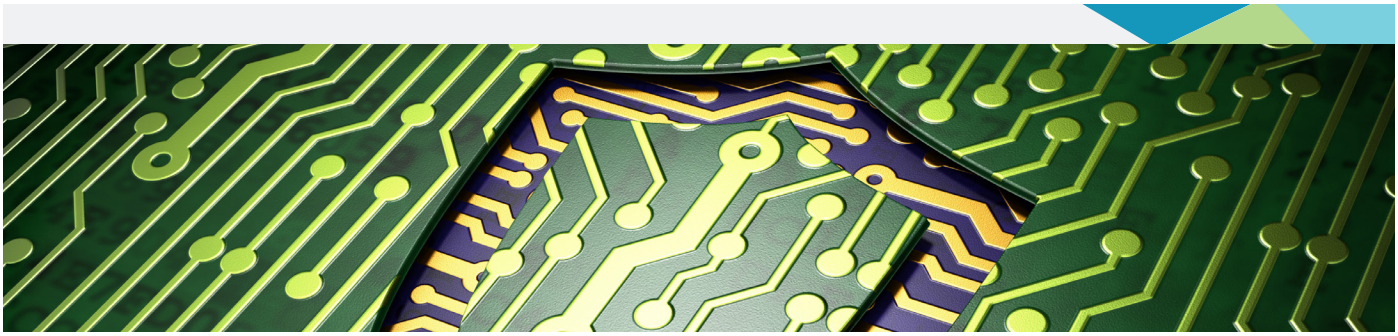

SmartRMF™

Cybersecurity: Managing the Risk Management Framework process for your organization

SmartRMF™ guides you through the Risk Management Framework (RMF) process while saving time and centralizing management of your critical RMF data and documents. Our SmartRMF tool puts your organization in control of its RMF process, reduces time required for documentation, offers continuous monitoring, and helps maintain your security posture with minimal effort.

Key Benefits

- Adaptable SmartRMF modules are available for DoD, DFARS, and federal and state agencies
- Save time and centralize local management of your critical RMF data and documents
- Quickly view up-to-date continuous monitoring status and security posture for your organization
- Manage risk, vulnerabilities and pending expiration dates using dashboards and alerts
- Provide role-based access for your entire team, without specialized training
- Step-by-step guidance through the RMF process

RMF is required for cybersecurity. Are you ready?

The RMF structure has been mandated by the Office of Management and Budget (OMB) for all Department of Defense (DoD) and federal information systems. It is also required by Defense Federal Acquisition Regulation Supplement (DFARS) Part 252.204-7000 to protect Controlled Unclassified Information (CUI). In parallel, Cybersecurity Workforce (CSWF) regulations are in effect for all DoD systems.

The RMF cybersecurity framework is significantly more complex, comprehensive, and time-consuming than the previous DoD framework, DoD Information Assurance Certification and Accreditation Process (DIACAP). The RMF process now involves your entire organization on a daily basis, not just cybersecurity professionals. This requires up-to-date security information and documents for your all personnel. SmartRMF will guide your organization through the RMF process providing all required standards at each step as well as managing your critical RMF data and documents.

Is SmartRMF right for you? Ask yourself these questions:

1. Will your organization be RMF compliant before your deadlines?
2. Do you know where to begin with the RMF process?
3. Are you overwhelmed by RMF regulations or frustrated by the Enterprise Mission Assurance Support Service, eMASS?
4. Is your organization prepared to make the transition from the DIACAP to RMF?
5. If you have achieved RMF authorization, how well are you managing the process, documents, reports, daily scans, and risk posture?

The SmartRMF Difference

In today's environment, cybersecurity plays a critical role for everyone within your organization. Access to relevant information is paramount for making smart decisions. SmartRMF provides role-based management for cybersecurity information, status, and documents. With SmartRMF, dashboards allow for personnel to quickly assess system risk, Plan of Action and Milestones (POA&M) status, CSWF requirements, as well as expiration dates for software and hardware maintenance, Memorandum of Agreement, or Service Level Agreement support.

SmartRMF sends alerts for vulnerabilities, POA&M tasks, Information Assurance Vulnerability Alerts (IAVAs), and upcoming expirations. The tool also provides a convenient, local, configuration-managed repository for all RMF artifacts including security plans, scans, System Assessment Report (SAR) results, authorization packages, POA&M, and process and procedure documents. For DoD organizations, updated RMF artifacts are published periodically to eMASS, but typically, only cybersecurity specialists have eMASS access and training. SmartRMF provides an easy and convenient way to centralize, understand, and maintain this information.

Technical Features

- Augments eMASS functionality for DoD RMF and manages data and documents uploaded to eMASS
- Easy data entry for later upload to eMASS
- Preserves security design decisions not captured in eMASS
- Supports use of inheritable and common controls for organizations and enclaves, enabling support for Navy Defense-in-Depth Functional Implementation Architecture (DFIA)
- Includes all standards, arranged by RMF process steps for quick reference
- Imports scan results to assess control compliance and/or update risk status and POA&M
- Configurable for stand-alone laptop, web server, or cloud

SmartRMF Functionality Step-by-Step

Step 1 Categorize: Use an electronic worksheet similar to the Navy System Categorization Form or NIST SP 800-60v1 to document and preserve the adjusted impact values and rationale for each information type. SmartRMF computes the system categorization and the security categorization.

Step 2 Select: SmartRMF quickly and efficiently gathers Security Plan (SP) information collaboratively with your team at your site. The tool enables personnel to upload to eMASS later as required. Next, establish control baselines (CNSSI 1253 and NIST SP 800-53v4) either from eMASS or generated for non-DoD users. Then, document your implementation strategy as you select inherited controls and common controls. SmartRMF allows for automatically linking process and procedure artifacts to control families.

Step 3 Implement: SmartRMF verifies control compliance after importing test scans. Next, it allows for refinement of control specifications, update process and procedure artifacts, document implementation, and upload to eMASS.

Step 4 Assess: The tool supports development of Security Assessment Plans (SAP). After the assessment, SmartRMF imports the SAR from eMASS.

Step 5 Authorize: A dashboard displays the Risk Assessment Report (RAR) metrics. This allows your organization to manage the POA&M and upload to eMASS.

Step 6 Monitor: SmartRMF automatically imports daily scans, identifies new vulnerabilities, and allows the user to update POA&M as necessary. Next, the current risk posture and upcoming expirations are displayed in a dashboard. SmartRMF tracks cybersecurity workforce, CSWF certifications, software and hardware maintenance, and MOA/SLA. Last, the system publishes the latest documents to eMASS.

Implementation

In SmartRMF, standards and regulations are always available for immediate access and are organized by RMF step and topic areas for ease of use. The information available also includes links to major standards websites.

SmartRMF can be implemented as a stand-alone tool, on a web server, or in the cloud. As a testament to its functionality and reliability, Hexagon uses SmartRMF internally for cybersecurity as well as for cybersecurity service engagements.

Contact Us

Email: info@hexagonusfederal.com
Tel: +1 800 747 2232
hexagonusfederal.com

About Hexagon US Federal

Hexagon US Federal is an independent subsidiary for Hexagon's U.S. federal business. Hexagon US Federal provides mission-critical and business-critical solutions to governments and service providers. A global leader, proven innovator, and trusted partner, our software and industry expertise help improve the lives of millions of people through safer communities, better public services, and more reliable infrastructure. Visit hexagonusfederal.com.

Hexagon US Federal is part of **Hexagon** (Nasdaq Stockholm: HEXAB; hexagon.com), a leading global provider of information technologies that drive productivity and quality across geospatial and industrial enterprise applications.