FORTRA®

WHITE PAPER (TRIPWIRE)

Adjusting to the Reality of RMF

For many reasons, aligning IT security, compliance and IT Operations has been an ongoing challenge in the federal ecosystem. There are plenty of stories about waste and misalignment of IT security for federal systems, such as systems that are compliant but not secure, and investments on tools that didn't make anything more secure or were difficult to run. IT Operations people will point to issues effecting security and compliance like very complex systems, special equipment and differing missions. And compliance and security professionals understand that the challenge to compliance reporting is measuring the right thing, not a prescribed checklist of baseline measures.

How can we address the security risks brought about by technical complexity, internet hacking, insider threats and legal requirements with consistency, accuracy and management awareness? How can we ensure that the measurement of security (i.e. compliance) is aligned and calibrated correctly? Gone are the days when you could protect systems by simply installing a firewall or configuring a DMZ. Similarly, it's a myth that compliance can be achieved simply by categorizing the data sensitivity level of a system and applying prescribed controls. There's no doubt that the answers include working diligently towards improved skills, communications and tools.

The Department of Defense, along with their civilian and Intelligence Community (IC) agency colleagues, has introduced a common method to address these issues — the Risk Management Framework (RMF). This effort comes from recognizing that all federal, public and private organizations are addressing similar problems. Common issues include explosive technical change and complexity, unplanned-for demands for communications and service protocols, and wide variation in the level of skill and experience of stakeholders and operators. Because the issues are threats to stability, reliability and security, what's needed is a risk management approach that allows organizations to customize, prioritize and work around what have been "one size" security approaches in the past. Also, as many organizations have learned over time, security and technology are dynamic elements — just because you are secure today does not guarantee security tomorrow. There's a need to assess the risk to systems in an ongoing manner to reflect changes to technology, infrastructure and organization needs. Ongoing measurement and reporting on security posture is critical to this approach.

What Is the RMF?

The Risk Management Framework is not easy to describe quickly. It could be said RMF describes an approach to systems security management that adjusts security controls based on risk factors. Or that RMF provides the process outline for the security accreditation process of any government system. Both are true, but following the RMF blindly does not ensure security or Authority to Operate (ATO). The focus must be on applying consistent and incremental improvement in the risk management practice. The practice involves a continuous cycle of identification of new threats, choosing effective controls, measuring their effectiveness and improving system security in a timely fashion. It includes using the best tools to support the process. Ideally, it means the bar is raised for many participants, including IT operations, security, compliance, and overall management of federal IT.

Initially documented in NIST Special Publication 800-37, RMF has been part of the core FISMA-related NIST guidance since 2004. Those who have supported FISMA certification will recognize the essential reference to RMF in relation to accreditation and control selection (such as in NIST SP 800-53 and other core guidance). RMF describes an approach to using risk management practices as key part of systems security, and helps FISMA practitioners understand which NIST guidance to examine. It's worked well for the federal civilian agencies, demonstrated by steadily improved security compliance scoring over the past decade. And there are now many public and private industries being encouraged to leverage NIST for their cybersecurity efforts. For example, the Federal Communications Commission (FCC) is now urging the telecom and cable industry to move to the NIST framework, and the Federal Drug Administration (FDA) is recommending medical device manufacturers apply the framework in their product lifecycles.

In 2008 a decision was made to take the NIST model for security management to the broader range of federal government organizations, including DoD and IC. The ICD 503 update to reflect RMF was published in 2008. Updates in 2010 and 2014 were made to address the Joint Task Force Transformation Initiative, and DoD determined they would develop unique new guidance to help meet the objectives of RMF. The result has been DoDI 8510.01, which instructs DoD elements on the common RMF approach. Updates in

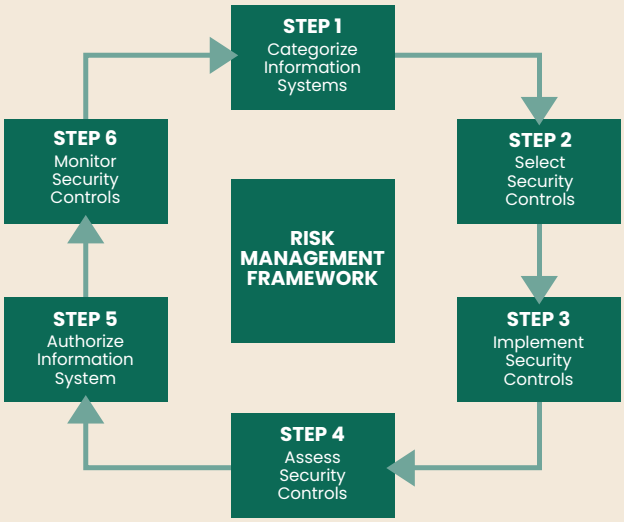
2016 underscore the seriousness of the approach and the expected compliance goals. The promise of more universally followed RMF includes improved communications between government programs, improved resource utilization and, most importantly, a risk-based approach to systems security and IT management.

How to Begin an RMF Program

Start by reading the original source material in NIST SP 800-37, then, depending which part of the government you support, read DoDI 8510.01 or ICD 503 for further organizational instructions. The RMF initiative might seem daunting, but this initiative is an evolutionary step and it relies on well-understood concepts such as ATO, applying baseline security controls, and tailoring practices.

HOW FORTRA'S TRIPWIRE FITS INTO EACH STEP OF THE FEDERAL RMF MODEL

RMF
References: NIST SP 800-37, DoDI 8501.01, ICD 503



Step 1: Categorize Information Systems
Categorize the system (e.g., by following CNSSI1253) to analyze, then register accordingly. References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-59, 800-60; CNSS Instruction 1253.

Step 2: Select Security Controls
Identify core component types, and gather the associated Tripwire® Enterprise Compliance Policies to understand the initial set of controls associated with each. Use Fortra's vulnerability management for monitoring of enterprise-wired devices and systems that require agentless monitoring. As systems are hardened and tested, tailor policies to reflect the actual controls in place. References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253.

Step 3: Implement Security Controls
Implement Tripwire Enterprise policies tailored to each device to provide alignment with security documentation. Apply Tripwire File Integrity Monitoring rules to specific configuration files to ensure control and visibility to change in the system architecture. Apply Tripwire LogCenter® as part of security architecture to simplify log aggregation, and apply typical security assessment rules to log events. References: FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253; Web: SCAP.NIST.GOV.

Step 4: Assess Security Controls
Use Tripwire Enterprise to provide continual monitoring of controls, configurations and settings and to report on the status of security controls. Reports and alerting from Tripwire can inform and automate some of the remediation actions by either automatically returning configuration to known good settings, or alerting appropriate security and administrative personnel. References: NIST Special Publication 800-53A, 800-30, 800-70.

Step 5: Authorize Information System
Tripwire reporting is designed to work with POA&M (Plan of Action & Milestones) reporting, providing the tracking and status information for any failed controls. Tripwire Enterprise console also provides a means to grant waivers to failed controls, assign responsibility and action dates, and monitor accordingly. This automation provides the Authorization Official (AO) and responsible security officers better assurance that security management practices are being followed. References: OMB Memorandum 02-01; NIST Special Publications 800-30, 800-39, 800-53A.

Step 6: Monitor Security Controls
Use Tripwire products to provide ongoing security management and monitoring for the system. Tripwire reports on configuration drift and potential security incidents associated with unexpected change to core components and configurations, and provides AO standard reporting. References: NIST Special Publications 800-30, 800-39, 800-53A, 800-53, 800-137; CNSS Instruction 1253.

All steps may include specific agency/organizational instructions or guidance not included here.

Not all references are used for all authorized systems. Organizations must look to specific agency instructions to clarify references based on variables such as classification of system data or size and complexity of system.

RMF Issues and Solutions

Issue	Solution
Security Configuration Management: Security Engineers and IT Operations personnel will already recognize the challenge of getting systems setup and configurations "hardened" for operations. Based on the risk assessment of a unique system, you may have to deviate from standard hardening of operating systems, devices or applications. Based on operations requirements, and as part of risk assessment, security engineers may have to customize or increase the level of protection of a control setting to ensure security. It is challenging to easily customize settings from a known baseline and then perform security monitoring for that custom configuration.	Tripwire provides simple implementation and customization of security baseline configuration by way of compliance assessment "policies" which come with the product and are pre-configured to match NIST 800-53/CNSS 1253/DISA Gold baseline controls. Your organization can modify these policies to match your configuration setting requirements, and then use the customized policy to monitor compliance to the prescribed settings.
Change Management: As IT security configurations are changed, there are several ongoing risks to operations if those controls are not well documented or understood by operations personnel. The challenge by many AO to the operations teams are to ensure that configurations will not change, ensure that personnel have a common source for approved remediation steps, and assurance that compliance reporting will be accurate.	Based on specific risk assessment of controls, features of the Tripwire tool can a) return settings automatically if changed, b) alert to operations with specific custom instructions to remediate, and/or c) change custom weighting of specific controls so that alerting can be escalated to the appropriate level. Reports from Tripwire Compliance Assessment policies can serve as part of the documentation of controls and included in system security documentation for a system. Change management requires knowing what the state of your systems are at all times. That means tools to ensure configuration and monitoring logs for events that cause change to systems. Tripwire Enterprise and Fortra's vulnerability management products are considered best of breed solutions for Security Configuration Management (SCM). Additionally, Tripwire LogCenter is an integrated log aggregation tool.
Continuous Monitoring: Monitoring of systems for configuration change is a risk to operations management, security and compliance. The requirement is to improve controls monitoring to make near real time assessment possible.	Tripwire's File Integrity Monitoring (FIM) feature can provide strong assurance of near real time monitoring of system files, data files or other configurations that control security settings. This solution can be paired with Tripwire LogCenter for an integrated control that both monitors and triggers appropriate alerting. Reporting from Tripwire can provide assurance to compliance personnel and AO that primary and backup control measures are maintained, and not tampered.
Risk Assessment: Risk assessment practices are a significant change in the standard operating procedures for many security, compliance and engineering programs. The challenge is to start assessment activities early in the system lifecycle to make security control selection and control compliance easier. This requires security requirements are better understood by systems designers, engineers and acquisitions personnel.	Tripwire's control assessment policies are a template for most basic control information. Using the policies as templates will help staff address common security settings earlier in the accreditation process, and can make the assessment process more structured. Tripwire Enterprise offers organizations the ability to integrate risk acceptance into the risk management process through waivers.
Reporting: Risk Management processes such as managing Plan of Action and Milestone reporting is a challenge as control failures involve tracking multiple systems, control specifics, mitigation plans and assignees.	Tripwire's configuration assessment feature provides control assessment with both waivers and scoring capability. A failed compliance test in Tripwire affects overall scoring, but with the waivers feature, the organization can manage controls sent to the Plan of Action and Milestone (POA&M) reporting. Failed tests can be associated with specific persons, and waived tests can be aged for any period approved. Reports can treat waived controls on scoring.
Compliance Management: Compliance involves continued support of security and configuration documentation to provide trust of the controls and in the actual operations of a federal system. Because each system is unique, the security and related compliance assessment program must also be customized to the features, risks, and environment of that system.	Making Tripwire a part of the Assessment Authorization (A&A) tasks makes the documentation and Security Plan creation easier for the key stakeholders. Control test content in compliance policies can be "tuned" to include or exclude tests and weigh tests to match the risk assessment. Risk Assessment and categorization information can be reflected in policy and documented by reporting on Tripwire policy configuration – providing additional assurance to the AO that risks identified are monitored with automation. Tripwire reports then become part of the well documented risk assessment.

Key Takeaways

- If you're involved in security compliance, you'll quickly note two important features of the RMF program: 1) sometimes shorter assessment cycles (depending on organization) with continuous monitoring, and 2) the risk assessment component to each phase of the program. The goal is clearly to assess risk more often, and then tie that assessment to the management of the system and the associated ATO. The expectation is that security compliance must align to assessment activity, include faster response to the assessment cadence, and ensure non-compliance findings are addressed in alignment with agreed controls.
- If you're a system owner or manager of systems, note that the governance model is designed to take into consideration both strategic and tactical risks to "blend" risk information to correctly manage security of any specific system. This will mean recognizing risks at different levels and using this information to help select the most appropriate controls. Key to this model is improving communications between groups responsible for the system, and improving the culture of security.
- If you're involved in IT Operations or IT Administration you'll be expected to be part of the assessment process. This means being aware of threat types and the types of security controls applicable. There is expectation for efficiency between IT and Security teams, and for improved communications flows between operations and management levels.

Like other strategic changes, you're likely to be most successful if you start with a single project from which you can practice and learn essential lessons before rolling it out to wider program efforts. There are some advantages to working with an existing certified system, since it will allow you to focus on the gap to meet new security and compliance practices described in SP800-37 and DoDI 8510.01. Expect to measure issues around schedule, scope and costs of a pilot projects to help plan for full compliance efforts across the department/enterprise. Start the pilot project by using the most qualified and senior staff you can afford. The advantage of using senior staff is that they'll be the leaders and early adopters the organization is already likely to respect. Involve engineers, security and compliance people in the project from the beginning; by getting multiple specialties involved in brainstorming on the outcome there will be natural buy-in on measures or indicators for future success.

The RMF model consists of six major steps that address numerous tasks. Tasks naturally blend from one step to the next as inputs or outputs in a continuous loop of activity. As you implement the process, choose tools that support the program model and help you meet risk, security and compliance needs.

Expected Lessons, Tools to Help

Many organizations will recognize the issues during implementation of RMF (see table). Proven automation tools can facilitate management of security information and enable the organization to better manage tasks prescribed by the RMF model.

Conclusion

To understand the new RMF model and the best approach to take, it's important to recognize that the RMF tries to provide a common federal approach to IT security and compliance. The instruction to use the RMF approach is a change for government organizations, but an evolutionary one. The RMF is less of a map, and more of a compass — providing guidance regardless of the terrain. The new methodology prescribes risk assessment tasks that promise to improve security profiles for systems; it requires that personnel look at risk assessment and security in a new way. In implementing this process, it's also important to select tools that support multiple areas of the RMF and address both implementation the security controls and monitoring for ongoing compliance and risk assessment. These should include mature, robust tools such as Tripwire Enterprise, which includes FIM and policy compliance features that support the RMF guidance.

References

Committee on National Security Systems (CNSS) Instruction 1253, "*Security Categorization and Control Selection for National Security Systems*", March 2014.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.

Office of Management and Budget Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 2001.

National Institute of Standards and Technology Federal Information Processing Standards Publication (FIPS) 199, "*Standards for Security Categorization of Federal Information and Information Systems*", February 2004.

National Institute of Standards and Technology Federal Information Processing Standards Publication (FIPS) 200, "*Minimum Security Requirements for Federal Information and Information Systems*", March 2006.

National Institute of Standards and Technology Special Publication 800-30, "*Risk Management Guide for Information Technology Systems*", July 2002.

National Institute of Standards and Technology Special Publication 800-37, "*Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach, Revision 1*", July 2014

National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), "*Managing Risk from Information Systems: An Organizational Perspective*", April 2008.

National Institute of Standards and Technology Special Publication 800-53, Revision 4, "*Recommended Security Controls for Federal Information Systems and Organizations*"

National Institute of Standards and Technology Special Publication 800-53A, "*Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*", July 2008.

National Institute of Standards and Technology Special Publication 800-59, "*Guideline for Identifying an Information System as a National Security System*", August 2003.

National Institute of Standards and Technology Special Publication 800-60, Revision 1, "*Guide for Mapping Types of Information and Information Systems to Security Categories*", August 2008.

National Institute of Standards and Technology Special Publication NIST SP 800-64, Revision 2, "*Security Considerations in the System Development Life Cycle*"

National Institute of Standards and Technology Special Publication NIST SP 800-70, Revision 2, "*National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*"

National Institute of Standards and Technology Special Publication NIST SP 800-137, "*Information Security Continuous Monitoring for Federal Information Systems and Organizations*"

Intelligence Community Directive (ICD) 503 "*Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation*", September 15, 2008

Department of Defense Instruction (DoDI) 8510.01, Change 1 "*Risk Management Framework (RMF) for DoD Information Technology (IT)*", May, 2016

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 (fta-tw-gd-1124-r2-hm)