C4ISRNET
www.C4ISRNET.com
EDITORIAL WHITEPAPER

DoD faces risk

Challenges on the road to the Risk Management Framework

Challenges on the road to the Risk Management Framework

BY ADAM STONE

In March 2014 the Defense Department's then-CIO Teri Takai changed the face of IT security across the military when she called for the transition from the DoD Information Assurance Certification and Accreditation Process, or DIACAP, to the National Institute of Standards and Technology (NIST) Risk Management Framework, or RMF.

The transition to RMF, now underway and slated for completion by mid-2018, marks a sweeping cultural shift in the department's approach to IT security. DIACAP established a standard set of activities to certify and accredit DoD information systems, and looked to refresh every three years. RMF, on the other hand, takes a dynamic approach, focusing on risk management as its primary approach and emphasizing a need for ongoing continuous monitoring.

Some in defense are rising to the challenge. The Army's Medical Communications for Combat Casualty Care (MC4) organization, for example, declared it had reached full implementation of RMF in 2015. Others have been slower to adopt the new standards, according to a recent survey by Splunk, a provider of a data-analytics platform for security and other IT-driven business needs.

Splunk found that among defense IT leaders…

- One-third report that less than half of their information systems have baseline security controls, based on the security categorization.
- Nearly half say that less than 50 percent of their security controls have been implemented with the deployment approach documented.
- Almost 40 percent say they fall well short of the RMF's prescription for frequent and ongoing reviews.

It is perhaps not surprising that so many defense and intelligence community technology leaders find themselves struggling to adopt the RMF. The Rand Corporation sums up the situation in a research paper titled Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles.

The paper, while aimed at Air Force systems, could apply equally across all DoD components. "The stakeholders for cybersecurity in the Air Force are confronted with a welter of laws and policies that are voluminous, complicated, and changing faster than the life cycle of a military system," the authors write. That rapid pace of change certainly impacts RMF adoption, but it's not the only cause for delays.

Drawing from the Splunk findings, this paper will explore the most common hurdles encountered by military IT professionals as they strive to align their systems with the RMF security vision. We'll look at the likely sticking points, explore best practices and finally lay out a vision for what steps IT can take to accelerate the move toward an RMF environment.

SIX STEPS TO RMF IMPLEMENTATION

In order to explore the challenges impeding RMF adoption, it's helpful to first take a high-level view of the actual requirement. The RMF asks IT planners to consider security as a function of risk: How likely a negative event is to happen; how severe might the consequences be if it did. With this in mind, the RMF then directs a six-step approach to mitigating risk.

- Categorize the information that is processed, stored and transmitted on the system.
- Select an initial set of controls for the information system, culled from a NIST menu of over 360 possible controls.
- Implement the controls, documenting what actions you are taking and why they make sense.
- Assess the controls. Review the implementation to ensure it is meeting the mission.
- Authorize the IT operation, now secure.
- Monitor the performance of the security controls continuously.

The RMF does not specify the mechanics of security for defense or intelligence community systems. NIST offers a hundreds-long menu of possible controls, but it is up to the system owner to determine what will best meet the need. Rather than give a prescription for security, “RMF is meant to give people hope, and a process to rally around,” said NIST Fellow Ron Ross.

That process hasn’t always been easy to implement. Consider the following challenges.

DODGING RISK

Splunk asked IT leaders: Within your office or agency, what percentage of information systems have set baseline security controls based on the security categorization? Nearly a third of respondents said than less than half of their systems met this mark. Yet categorizing risk is a crucial first step in RMF compliance.

“Before you can set controls, you have to categorize systems,” said Splunk Security Strategist John Stoner. “There are ways to talk about the criticality of a system, ways to talk about the confidentiality of the data, to talk about system availability and the integrity of the data. These are basic initial categorizations that you need in order to select controls.”

> “You can wish you didn’t live in a risk-based world, but anybody who’s driven on a highway . . . understands there is risk in everything we do.”
>
> **NIST Fellow Ron Ross**

Sometimes people may be reluctant to set even the most elemental levels of risk categorization: High, medium and low. Technology managers in DoD and the IC may shy away from taking this step because it is a de facto admission that risk exists. There is “an unwillingness to articulate in writing their risk tolerance,” according to MITRE, in the RMF research report Beyond Compliance. In the report, MITRE authors note that such an approach is counterproductive “due to continually evolving adversary capabilities and intentions. Some risks will always materialize, and they need to be managed.”

Security experts shy away from such an admission, but the failure to admit risk is generally an unrealistic stance.

“This is a world where you have threats and bad actors, and where you have systems with inherent vulnerability,” Ross said. “You can wish you didn’t live in a risk-based world but anyone who’s driven on the highway or ridden on an airplane understands that there is risk in everything we do. You can’t ignore that and hope it will go away. There will always be vulnerabilities.”

DEARTH OF DOCUMENTS

Paperwork is another common stumbling block in adopting the RMF. The survey asked: Within your office or agency, what percentage of security controls have been implemented with deployment approach documented? Forty-six percent admitted than less than half their security control implementations have been properly documented.

It’s true that the RMF does ask IT leaders to document their security choices, but while some may find this onerous, NIST’s Ross says the requirement is not nearly so heavy-handed as some might think. “This is something that is constantly raised as a negative aspect of the RMF, but there is nothing in the process that demands an excessive degree of documentation,” he said.

In fact, documentation serves a vital role in IT security, especially in an organization like the DoD, where turnover may run high as civilians swap out to the private sector and uniformed staff move through their rotations. “You have a constant churn of personnel and if things are not well documented someone is going to spend a lot of time trying to figure out what the last guy did, and so operational effectiveness suffers,” Stoner said.

The key to success here is to systematize. “You need to make it part of operations,” said Matt Coose, CEO and founder of cybersecurity consultancy Qmulos. “For example, you get new user account requests all the time. As part of that process the group can automatically review all users and see if there is anyone who needs to be taken out. Then it is not a separate exercise. The [creation] of that documentation is just a byproduct of doing your normal operations.”

COMPLIANCE MENTALITY

Close observers of the military IT environment say the effort to comply with the RMF may, in itself, be a hurdle to compliance. Why? Because for many, “compliance” exists as the end goal. They evaluate and remediate simply in order to check the box labeled “RMF compliant.” But that approach can be counterproductive.

Take the fundamental activities of account management as an example. IT needs to know who logs in and out, where they go in the system and what they do there. “People will collect that and show that as part of the compliance requirement. They will buy tons of software to parse that data into a specific relational database just for the sake of showing and proving compliance. Then they will build a completely separate system for security [operations], where you can see that data in real time, where the data is dynamic,” Coose said.

This compliance-centric approach is a common pitfall in a regulated IT environment. “This is not just a DoD thing,” Ross said. “If you look at the power plants for instance, or look at HIPAA, people are trying to follow the law and they are working in a compliance mentality.” By thinking only in terms of compliance, people fail to leverage the full potential of the RMF and ultimately fall short of its actual aim, which is to create safer systems.

In its RMF guiding document, the DoD Defense Security Service (DSS) spells out this need to look beyond the mere letter of the RMF instruction. “More than simply achieving compliance, implementing RMF will assure leadership that security personnel have used critical thinking to ascertain the threat picture, assess risks, and have instituted sufficient security controls to protect assets from theft and organization information systems from intrusion,” according to DSS.

FIX-AND-FORGET

One of the main tenets of the RMF is the call for ongoing review and revision. It’s a place where many fall short, the Splunk study found. Asked how often security controls are assessed to determine status of implementation, functionality and effectiveness, 37 percent said they do it annually, biannually or never. Asked what percentage of authorized information systems are assessed and monitored on an ongoing basis, 39 percent say less than half.

Yet ongoing review is a basic principle of the RMF, and with good reason. As RAND researchers note, cyber risk to the military “changes over time as systems are upgraded or new attacks are enabled by newly discovered vulnerabilities; therefore risk assessments need to be conducted with sufficient regularity to keep up with the pace of change.”

When this doesn’t happen, the fault is usually cultural. “In the past, folks have said: ‘I will certify the system and until something substantial changes, I am good.’ Now under the RMF process, that is changing,” Stoner said. “The expectation now is that you will be constantly monitoring, that your security controls will change as your system changes. The mission may evolve, the software may change, and you will be pulling out security controls, updating them, getting rid of those that are no longer necessary. RMF intends for that to be a constant loop.”

THE AUTOMATION FIX

Clearly IT planners face a number of potential pitfalls on the road to RMF compliance. They may be reluctant to categorize risk. They may resist the call to document their actions, they may think too narrowly in terms of compliance or they may fail to implement the critical process of ongoing review.

THE BIG PICTURE

Where is the Risk Management Framework taking military IT? The National Institute of Standards and Technology (NIST) offers these as the essential characteristics of RMF:

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions
- Integrates information security into the enterprise architecture and system development life cycle
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems
- Links risk management processes at the information system level and organization level
- Establishes responsibility and accountability for security controls

Given these myriad challenges, many will find that a technological implementation rooted in big data can help to ensure a smooth RMF implementation. Along these lines, automation holds particular promise, said one DoD official.

“It takes a lot of time and effort for someone to do all these scans and analyze them and publish those results,” said Kevin Dulany, chief of the Risk Management Framework Division in the Office of the Secretary of Defense. “If we leverage automation, I can get a more complete risk picture and I can do it more often. I can get more of an up-to-date picture and I can be more efficient in finding my major problems and allocating my resources.”

The number of possible controls and their relative merits “is too much for any human being” to manage, MITRE reports. In such circumstance, automated tools “are necessary to aid security practitioners in making informed decisions regarding the effectiveness, cost and relevance of the various controls in different environments and different threat settings.”

IT in general has been slow to adopt the tools of automation. In a survey of IT security professionals, the Ponemon Institute found that when it comes to keeping up with security changes, only 15 percent are using automated risk impact assessments and just 13 percent say they are using continuous compliance monitoring. Yet there is much to be gained from an automated approach.

Take, for example, security information and event management, or SIEM, the real-time analysis of security alerts generated by network hardware and applications. Analytic-driven security solutions can leverage network and application security logs to correlate and detect threats on risky behavior, tracking not just where a user goes inside the system but what files and processes they might tap into, what documents they may download or what materials they may try to exfiltrate from the system.

“You need to understand what your system can do and what the acceptable behaviors for that system look like. Then you can put up guardrails. Then you start to get alerts when behavior seems out of step with those limits,” Stoner said. Given the complexity and fast-changing nature of today’s threats, defense IT needs this kind of big-data type approach if it is to achieve the continuous security and compliance monitoring, rapid detection and fast incident response capabilities it needs.

There is much that automation can help to achieve when it comes to RMF implementation, creating a valuable context for security data and thus enabling deeper insights. At the same time, technology alone won’t take IT planners across the finish line. At the end of the day RMF represents a fundamental cultural shift, a very different way of understanding and approaching IT security.

It’s no longer sufficient to check the box: There’s no one right way to implement security in the RMF world. Rather, compliance comes through ongoing engagement and a persistent, thoughtful exploration of both external threats and internal vulnerabilities. Understanding and embracing the notion of risk thus becomes the critical first step on the road to RMF implementation. ■

Thank you to our underwriter

splunk>®