NIST Ushers In a New Era of IT Risk Management

By Stephen Berk – ISSA member, Minnesota Chapter

The 2019 NIST Risk Management Framework update incorporates a critical paradigm shift requiring greater C-suite involvement and oversight, bringing a formal preparation step to the process that permeates every level of the organization and requires that management drives assessment and authorization efforts going forward.

Abstract

The NIST Risk Management Framework (RMF) guides enterprise defense contractors through the assessment and authorization (A&A) process to prove their government-connected or -supporting systems are secure and that they have adequate processes to address and mitigate cybersecurity risk.

The National Institute of Standards and Technology (NIST) finalized the update to Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" this year [7]. A joint task force made up of members of the intelligence community, NIST, the US Department of Defense (DoD), the MITRE Corp., Homeland Security, and others wrote the second revision to the Risk Management Framework (RMF) to address the concerns of the Defense Science Board's Task Force report, "Resilient Military Systems and the Advanced Cyber Threat" [10]. The board is a seasoned group of former military, government, and industry leaders who advise the DoD on scientific and technical issues. In the 2013 report, the board notes:

> "…that the cyber threat to US critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable US adversaries. It is clear that a more proactive and systematic approach to US cyber deterrence is urgently needed…"

NIST's goals for the RMF update

NIST responded to this report and other government directives [2][9] by updating the RMF with seven key goals:

1. Tighten communication and planning between C-suite governance and operations staff
2. Formally include *preparation* as step 1 of the RMF
3. Highlight how NIST Cybersecurity Framework (CSF) aligns to RMF
4. Incorporate privacy risk management as a distinct set of controls
5. Secure software and systems via alignment with SP 800-160, "System Development Life Cycle (SDLC)"
6. Bake supply chain risk management (SCRM) deeper into the RMF
7. Give organizations more flexibility to tailor security controls

Goals 1 and 2 of the RMF rewrite are closely related. They lay the foundation for all other goals and will ultimately determine the success or failure of your effort to roll RMF into your enterprise security architecture. Unless your company is strictly a DoD contractor, chances are good that your IT security governance doesn't have NIST frameworks and controls guiding your policies. Your policies are likely a homegrown set of documents that loosely follow the standards in the ISO 27000 family or possibly the NIST CSF. Yet the business unit in your organization that handles federal contracts—and I mean this with no disrespect to C-suite folks in your or my company—are the red-headed stepchildren of the IT department. The C-suite doesn't want to talk to you about RMF because every briefing you've provided to them highlights the depth and complexity of building an information system to achieve ATO (authority to operate). They look at these contractual requirements as ancillary to the existing security policies, and when the costs are ballparked, many make the decision to not bid or to abandon their contracts and facility clearances.

The National Industrial Security Program Policy Advisory Committee (NISPPAC), a group that advises the US Information Security Oversight Office on matters affecting cleared defense companies, raised concerns [4] that the increased complexity of RMF (albeit needed given the Defense Science Board's grim outlook) will have a chilling effect on smaller companies. These companies don't have the money or expertise to implement RMF, and parallel efforts to reduce or eliminate security consultants qualified to advise companies on these frameworks will force smaller cleared defense contractors out of the supply chain [11]. This creates two problems:

1. Larger defense contractors rely on smaller ones to make up their supply chain. If companies start leaving gaps in the supply chain, there's a risk that projects will be delayed, canceled, or swell in cost to accommodate new suppliers getting cleared, which is an arduous and expensive task.
2. There is a national security risk (foreign entities purchasing former defense contractors to obtain their intellectual property) that falls outside the scope of this article, but I include that fact here to underscore the challenges that a robust framework like RMF present to security practitioners and their companies today.

The NIST task force rightly recognized that these challenges must be discussed during the RFP stage and are not easily solved once a contract is awarded. For systems that already have an ATO on a previous framework that will eventually need to get their renewal ATO based on the RMF, NIST has given security practitioners the fodder and impetus to initiate these discussions well ahead of time. Both revision 1 and revision 2 of the RMF talk about the need for risk management to be an enterprise-wide task (see chapter 2 of the publication), but revision 2 bolsters the language behind the need to integrate it at every level of the organization and gives ample suggestions on how to prepare your organization (at a high level) to implement RMF.

Goal 3 of the RMF update is showing how NIST CSF aligns to RMF. If you work for a federal agency and are subject to Executive Order 13800 [9] mandating compliance with CSF, you'll like this update. Each step of the RMF process now includes a summary table that lists the tasks and outcomes of the step. NIST has done an excellent job cross-referencing outcomes to the applicable subcategories of the CSF, as seen in table 1 of SP 800-37r2 [7] (table 1, next page).

Goal 4 relates to privacy and feels like it's a few years late to the party. Ironically, it's a circular from the OMB [2] (yes, that

Tasks	Outcomes
TASK P-1 RISK MANAGEMENT ROLES	• Individuals are identified and assigned key roles for executing the Risk Management Framework. [*Cybersecurity Framework*: ID.AM-6; ID.GV-2]
TASK P-2 RISK MANAGEMENT STRATEGY	• A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: ID.RM; ID.SC]
TASK P-3 RISK ASSESSMENT—ORGANIZATION	• An organization-wide risk assessment is completed or an existing risk assessment is updated

Table 1 – Prepare tasks and outcomes—organizational level

OMB who lost 21 million personnel files of federal employees, contractors, and civilians who applied for federal jobs or national security clearances) that drove the renewed emphasis on securing personally identifiable information (PII).

Goals 5 and 6—SDLC and SCRM—are also intertwined because of how we integrate third-party systems into our information system architecture. You didn't manufacture the common access card reader needed for 2FA, but you need it to authenticate to your system. The question is, do you know where it was made? OK, China is a safe bet, I'll give you that. But can your preferred vendor assure you that the reader hardware and software built into your laptop, keyboard, or external USB device fulfills the DoD "Deliver Uncompromised" [5] philosophy? That's where the emphasis on managing risk throughout the life cycle of your systems and across all the vendors in your supply chain comes into play. It's not that these concepts weren't implicitly or explicitly stated before; it's that the tactics of the adversary have shone a spotlight on the weakness of the supply chain and the vulnerability of contractors.

The *Washington Post* broke a story [3] about how Chinese hackers obtained over 600 GB of data consisting of Navy submarine signals and sensor data, crypto systems, and other sensitive tactical and project data. They didn't hack the Navy—they hacked a contractor. The government has a vested interest in ensuring its supply chain is secure and is asking you to do the same so we don't continually hand over IP to adversarial nation states.

The final goal of RMF rev. 2 is to offer organizations more flexibility in tailoring controls to meet their unique needs. For those of us who are used to having security control overlays prescribed to us, don't rejoice just yet. In practice, if you try to tailor out baseline controls, you will have a battle on your hand; this shift makes it easier to tailor IN additional controls and let you build an appropriately robust information assurance (IA) program.

Be prepared

Building that robust IA program begins with step 1 of the RMF: Prepare. This was referred to as "step 0" [6] prior to NIST bringing this critical aspect of RMF to the forefront. It begs the question of why this wasn't part of the original incarnation of RMF. If you look at revision 1 [1] of the document, you'll see that the focus was squarely on controls: select controls, implement controls, assess controls, monitor controls. These are still the basic steps of the RMF process, but the addition of a formal "prepare" step feels like the focus has (rightly) changed from auditing for authority to operate (ATO) to institutionalized IT risk management. It's declaring that the C-suite cannot shoehorn or bolt-on an industrial security program to the enterprise security architecture and that the information security engineers or IA staff can't operate in a vacuum by withholding vital risk management information from the executive team. The temptation to not fully incorporate RMF into an organization's security policies and architecture is overwhelming when you consider that an RMF ATO can take years and may result in a denial ATO despite the considerable costs. The expense involved and the time frames allocated often are unrealistic, and this leads to a mutual, unspoken understanding in an enterprise that we just need to "get 'er done" and we'll adjust and update our policies as we go. From experience I can tell you that if you jump into RMF at step 2, you will eventually come back and have the discussions from step 1. But this time it will be because of a denial ATO or because your project time line has slipped beyond all reasonable measure because you don't have the buy-in and information that should have been obtained earlier. You must lay the proper foundation now.

Building the foundation

So, what does a proper foundation look like? NIST prescribes five mandatory and two optional tasks that will, if considered carefully and thoroughly, inform the remaining steps of the RMF process.

Task P1: Risk management roles

There is a laundry list of roles involved in RMF, and it is the responsibility of the senior agency or enterprise security to assign those roles to individuals or groups of people. There is a danger in thinking that the CISO or her equivalent need only sign off on an RMF project, but I hope that by listing the roles with a brief description of what their function is you'll see why RMF is so robust and complex and permeates every level of the organization. The RMF roles are:

Government (employee, contractor, or civilian):

- Authorizing Official—this is a senior official who will assume responsibility for the risk of your system. You don't appoint this role; it is identified in your contract.
- Authorizing Official Designated Representative—like the AO, this role is appointed by the government if needed.
- Chief Acquisition Officer—they ensure that RMF issues are addressed throughout the system acquisition process.

- Control Assessor—this is your auditor, be it the agency you are contracting with or another auditing agency like Defense Counterintelligence and Security Agency (DCSA, formerly Defense Security Service).
- Enterprise Architect—the top technical resource on how to implement technology solutions—with consideration for security and privacy—into the mission or business, and they serve as part of the risk executive function.
- Head of Agency—provides the organizational commitment to the security and privacy for a system and its data.
- Information Owner—you don't own the information on your system: the government does. They will work with you (the system owner) to ensure you secure the system appropriately so their data stays safeguarded.
- Mission or Business Owner—high-level official who has input into the SDLC and may serve as the authorizing official.
- Risk Executive (function)—this role is reserved for government employees only and is ultimately responsible for all the risk of a mission or business.
- Senior Accountable Official for Risk Management—they lead the risk executive function.
- Senior Agency Information Security Officer—the top security person for the agency, must be a government employee, and can be a control assessor.
- Senior Agency Official for Privacy—like the previous roles, a government-only employee responsible for privacy issues.

Corporate:

- Chief Information Officer—ultimate responsibility for the system and process from the contractor side.
- Common Control Provider—I'll cover this more in task P5, but basically this person or group identifies what enterprise policies apply to the system needing ATO.
- Security or Privacy Architect—high-level role that advises on risk mitigation strategy and control allocation.
- System Administrator—lower-level configuration of systems.
- System Owner—typically a manager who oversees the SDLC and is responsible for submitting the system for adjudication (think ownership, not data entry—the system security officer will do that).
- System Security or Privacy Officer—these are your corporate IA staff who audit and report.
- System User—self-explanatory.
- Systems Security or Privacy Engineer—higher-level role than the system administrator, they are responsible for integrating security and privacy requirements into the whole information system.

In practice, multiple roles are performed by the same person or team, and as a defense contractor you may only interact with a control assessor and mission owner throughout the RMF process. The reason for listing all the roles is to highlight how complex and involved an RMF ATO can become and how quickly a small staff will burnout because of the extent of their responsibilities. Good planning may help alleviate this.

Task P2: Risk management strategy

You likely already have a risk management strategy, but you should conduct a sanity check on it to ensure it can accommodate the needs of an unclassified or classified system with national security interests. An important distinction should be noted here: the government assumes risk for your system if they provide an ATO after evaluating your security posture. So, while the government agency is the driver of the risk management strategy, they will want to know that you have a risk management strategy in place that will align to theirs. This is something that must be developed at the C-suite, not with your operations or IA staff.

Task P3: Risk assessment – organization

Again, the government is assuming the risk, but you will need to show that you understand and are mitigating against any number of natural disasters, cyber espionage, or insider threats. Spend time here. Reread that last sentence. When you get to step 2 of RMF—select controls—your risk assessment completed here will inform the controls you ascribe to your system.

Task P4: Organizationally tailored control baselines and CSF profiles (optional)

If you perform task P3 well, you will know what tailoring, if any, you need to do. As stated previously, you will be tailoring controls in for the most part—not out.

Task P5: Common control identification

This is the "don't reinvent the wheel" task. You already have security policies and procedures in place; now you need to see if and how they can apply to your system needing ATO. The place where things get sticky is when you are trying to inherit common controls from an external entity. Let's say that you are connecting to a classified network and have been provided a black box encryptor from a three-letter agency. The process to change the encryption keys is an inheritable control. You may perform the key change on behalf of the government, but the process is provided to you…except when it isn't provided to you. If the process is classified, you can't receive it until you've been authorized to receive classified material. And even then, your control assessor may not be able to receive classified materials (I'm looking at you, DCSA[1] unclassified eMASS[2] instance) into their documentation repository. Regardless, nail down as many inheritable controls as you can so you don't have to do more work than necessary. RMF subjects you to the controls listed in NIST SP 800-53 [8]: you have nearly 20 control families consisting of 450+ controls and control enhancements for a standard DCSA baseline. Help yourself and your IA staff out wherever possible by using your existing documentation.

Task P6: Impact-level prioritization (optional)

This is a work flow consideration more than anything else. The gist of it is to prioritize your higher impact systems (needing more robust security) since these will require greater effort to incorporate into your security policies and architecture. Once you have these addressed, the lower impact systems should naturally fit into your architecture.

Task P7: Continuous monitoring strategy – organization

If audit fatigue hasn't bit every person on your staff by now, continuous monitoring will. This is where we deter the adversary and stay off the front page of the *Washington Post*. Yes, you will talk about how often you'll update your policies and the frequency of checking for privilege escalation, but equally important is the strategy—the how—part of this task. You must leverage automation. Period. Hard stop. On small systems you may be able to get away with Powershell or *nix shell scripts to look for interesting security events, but you really need to think about how you will maintain and audit the audit scripts long term. You should plan to look at vendor solutions and start with a conversation on how they secure the supply chain before you ever talk price.

And this is just step 1 of the seven-step RMF process. As I said, though, and as NIST has concurred by elevating it to its place of prominence at the beginning of the process, it must be done before you continue further into RMF. If you don't, you'll play out the adage of not having the money and time to do it right the first time, but you will spend the money and time to do it over. Don't let that happen in your organization.

1 Defense Counterintelligence and Security Agency.
2 Enterprise Mission Assurance Support Service.

Invest the necessary resources early and it will pay dividends in the form of a smother ATO in the end.

Conclusion

NIST's revision to the Risk Management Framework reveals the importance of preparing an organization to undertake an RMF ATO effort. In this iteration of the framework, NIST has inserted a preparation step that lists seven critical considerations for organizations embarking on a new system ATO or renewing an existing system ATO. By investing the necessary resources on this initial step of the RMF, organizations will be better suited to achieve authority to operate efficiently and cost-effectively, which will ultimately result in a more secure system that meets the needs of your company and the government.

References

1. "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." National Institute for Standards and Technology, June 2014. https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.
2. "Managing Information as a Strategic Resource." Office of Management and Budget, July 2016. https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.
3. Nakashima, Ellen, and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." The Washington Post, June 8, 2018. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.
4. "National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting Minutes." Information Security Oversight Office, November 15, 2018. https://www.archives.gov/files/isoo/oversight-groups/nisppac/nisppac-november-15-2018-final.pdf.
5. Nissen, Christopher A., John E. Gronager, Robert S. Metzger, and Harvey Rishikof. "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." The MITRE Corporation, May 20, 2019. https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.
6. Price, Gianna. "The Irony of RMF Step 0." TelosVision, February 13, 2019. https://multimedia.telos.com/blog/the-irony-of-rmf-step-0/.
7. "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." National Institute for Standards and Technology, December 2018. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.
8. "Security and Privacy Controls for Federal Information Systems and Organizations." National Institute for Standards and Technology, January 2015. https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.
9. "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Executive Office of the President, May 2017. https://www.federalregister.gov/executive-order/13800.
10. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat." Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, 2013. https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf.
11. "The Role of Security Service Providers and Security Consultants in the NISP." Issue brief. The Role of Security Service Providers and Security Consultants in the NISP. National Industrial Security Program Policy Advisory Committee (NISPPAC), n.d. https://classmgmt.com/nisppac/security_consultants_in_the_NISP.pdf.

About the Author

Stephen Berk, CISSP, is an Information Systems Security Manager (ISSM) with CenturyLink's public sector business unit. He has over 15 years' experience in network engineering and information assurance with state government, energy industry, and global technology organizations. Stephen is a member of ISSA Minnesota chapter and NCMS Northern Lights chapter. He can be reached at tango636@pm.me.