**Implementing the Risk Management Framework**

Jake Espinosa

The University of Arizona

CYBV 498 – Senior Capstone

Professor Jordan VanHoy

April 10, 2022

**Abstract**

Developed by the National Institute of Standard and Technology (NIST), the RMF is an extensive process that amalgamates supply chain risk management, privacy, and security objectives into the development and deployment processes of a system, application, or capability (SAC) by gathering necessary information, gaining situational awareness, choosing security controls, implementing the selected controls, bringing their SAC online, and continuously monitoring the SAC. The RMF covers the SAC’s entire operational life cycle from authorization to decommissioning. It ensures that the system is cyber survivable and secure. While United States Government systems must undergo each step in the RMF to obtain Authority to Operate (ATO), many companies choose not to reinvent the wheel and often model their policies around the RMF to secure their systems and networks. This essay maps the seven steps within the RMF and will expand upon each step.

*Keywords:* SAC, PMO, AO, cybersecurity, control, document

**Table of Contents**

**Implementing the Risk Management Framework** 3

[**Literature Review** 5](#_Toc99140439)

[**Benefits of Using RMF** 8](#_Toc99140440)

[**Prepare** 8](#_Toc99140441)

[**Risk Management Roles (Organizational)** 9](#_Toc99140442)

[**Risk Management Strategy (Organizational)** 9](#_Toc99140443)

[**Risk Assessment (Organizational)** 9](#_Toc99140444)

[**Tailored Control Baselines (Organizational, Optional)** 10](#_Toc99140445)

[**Common Control Identification (Organizational)** 10](#_Toc99140446)

[**Impact-Level Prioritization (Organizational, Optional)** 11](#_Toc99140447)

[**Continuous Monitoring Strategy (Organizational)** 11](#_Toc99140448)

[**Mission or Business Focus (System)** 12](#_Toc99140449)

[**System Stakeholders (System)** 12](#_Toc99140450)

[**Asset Identification (System)** 12](#_Toc99140451)

[**Authorization Boundary (System)** 13](#_Toc99140452)

[**Information Types (System)** 13](#_Toc99140453)

[**Information Life Cycle (System)** 14](#_Toc99140454)

[**Risk Assessment (System)** 14](#_Toc99140455)

[**Requirements Definition (System)** 15](#_Toc99140456)

[**Enterprise Architecture (System)** 16](#_Toc99140457)

[**Requirements Allocation (System)** 16](#_Toc99140458)

[**System Registration (System)** 16](#_Toc99140459)

[**Categorize** 17](#_Toc99140460)

[**System Description** 17](#_Toc99140461)

[**Security Categorization** 18](#_Toc99140462)

[**Security Categorization Review and Approval** 18](#_Toc99140463)

[**Select** 19](#_Toc99140464)

[**Control Selection** 19](#_Toc99140465)

[**Control Tailoring** 20](#_Toc99140466)

[**Control Allocation** 20](#_Toc99140467)

[**Documentation of Planned Control Implementations** 21](#_Toc99140468)

[**Continuous Monitoring Strategy – System** 21](#_Toc99140469)

[**Plan Review and Approval** 22](#_Toc99140470)

[**Implement** 22](#_Toc99140471)

[**Control Implementation** 23](#_Toc99140472)

[**Update Control Implementation Information** 23](#_Toc99140473)

[**Assess** 23](#_Toc99140474)

[**Assessor Selection** 24](#_Toc99140475)

[**Assessment Plan** 24](#_Toc99140476)

[**Control Assessments** 24](#_Toc99140477)

[**Assessment Reports** 25](#_Toc99140478)

[**Remediation Actions** 25](#_Toc99140479)

[**Plan of Action and Milestones** 25](#_Toc99140480)

[**Authorize** 26](#_Toc99140481)

[**Authorization Package** 26](#_Toc99140482)

[**Risk Analysis and Determination** 26](#_Toc99140483)

[**Risk Response** 27](#_Toc99140484)

[**Authorization Decision** 27](#_Toc99140485)

[**Authorization Reporting** 28](#_Toc99140486)

[**Monitor** 28](#_Toc99140487)

[**System and Environment Changes** 28](#_Toc99140488)

[**Ongoing Assessments** 29](#_Toc99140489)

[**Ongoing Risk Response** 29](#_Toc99140490)

[**Authorization Package Updates** 29](#_Toc99140491)

[**Security and Privacy Reporting** 30](#_Toc99140492)

[**Ongoing Authorization** 30](#_Toc99140493)

[**System Disposal** 30](#_Toc99140494)

[**Conclusion** 31](#_Toc99140495)

[**References** 32](#_Toc99140496)

**Implementing the Risk Management Framework**

The year is 2050, and the rise of self-programming artificial intelligence has led to new software constantly emerging around the globe. Developers and Information Technology (IT) personnel freeze in their seats from the sheer amount of new applications being created. No organization can keep up, and profits fall through the floor while downtime skyrockets. The United States Government faces the decision to succumb to the overwhelming tidal wave of software appearing daily or implement a process to understand what they already have and deploy new capabilities in an orderly and defined manner. Unfortunately, self-programming artificial intelligence is already here, but the Risk Management Framework (RMF) exists to manage new software deployment.

# **Literature Review**

Disorganization and disarray are counterproductive to efficient task execution. Structure leads to better results, especially when deploying SACs. This applies to both the private sector and the public sector alike. RMF provides a framework to work within, and when the framework is applied holistically it is significantly correlated with cybersecurity effectiveness. Due to this, selecting controls is the most time-consuming but important part of the framework.

## **NIST SP 800-37**

Tried and tested frameworks are critical to reducing cybersecurity, supply chain, and privacy risks while still providing the flexibility to accommodate unique SACs. According to NIST’s (2018) Special Publication 800-37 Risk Management Framework for Information Systems and Organizations (800-37 for brevity), the RMF’s seven steps of Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor will minimize administrative and technical overhead. RMF will also reduce cybersecurity, supply chain, and privacy risks.

The RMF process aims to decrease risk by ensuring that the organization and Program Management Office (PMO) responsible for a SAC have all the ducks in a row regarding paperwork and documentation. Next, SACs must be categorized based upon their impact on organizational operations and the type of data they process. Next, proper physical, administrative, and technical controls must be selected to fit the SAC's categorization. Then, the previously selected controls must be implemented at the SAC and potentially organizational level. After, the SAC's controls must be assessed for effectiveness by either the organization or an independent third-party assessor. Next, the SAC must be approved for deployment by an Authorizing Official (AO) responsible for the SAC. Lastly, the organization or program office must monitor the SAC and change its controls to adapt to the ever-evolving cybersecurity threat landscape. All seven of these steps comprise a holistic approach to risk management that ensures product ownership and responsibility, understanding of the SAC and its necessary controls, and continuous evaluation and improvement of the SAC’s security posture. 800-37 provides a robust framework for cybersecurity throughout a SAC’s life cycle, but it falls short on delivering prescriptive instructions.

## **RMF in the Private Sector**

NIST’s RMF is a public sector policy that must be implemented within the federal government, but it also has merit in the private sector. Hess (2021), in his doctoral thesis, backs up NIST’s claim that the RMF, when evaluating the framework, correlates statistically significantly with cybersecurity effectiveness in the private sector. However, when organizations apply the seven RMF steps in a vacuum, they hold no statistical significance. Thus organizations greatly benefit from a holistic approach as offered by RMF. A significant gap in measuring the effectiveness of the RMF in both public and private SACs is the degree of confidentiality that the program managers wish to maintain. While this is understandable, it reduces the claim’s reliability by not revealing the specific controls leading to successful outcomes. The NIST Cybersecurity Framework is similar to the RMF, a voluntary framework that aims to reduce cybersecurity risk in the private sector. Not much academic research exists on the effectiveness of the Cybersecurity Framework or the RMF, and academic research on how the two stack up against each other is similarly lacking.

## **NIST SP 800-53**

The most time-consuming and crucial step in the RMF process is step 3, selecting security controls. To aid this endeavor, in 2020, NIST authored NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (800-53 for brevity), which is over two and a half times the size of the RMF document itself. Over 1,000 physical, administrative, and technical controls are identified and discussed as potential controls for a SAC. While 800-53 is not all-encompassing, control selectors enjoy a complete and comprehensive set of controls to sufficiently secure a SAC and satisfy the RMF requirements. Proper control selection makes the difference between a SAC earning Authority to Operate status or not and affects the real-world cybersecurity and cyber survivability of a SAC against a realistic threat. Adversaries range from script kiddies to organized crime syndicates to advanced nation-state-sponsored threats. It is essential to ensure that controls protect a SAC instead of just fluffing up an RMF package to be approved by any means necessary. 800-53 details a more than sufficient amount of controls for PMOs to work with, but it is recommended that 800-53 provide examples and further discuss how controls interplay.

# **Benefits of Using RMF**

Organizational cybersecurity underlies everything the organization does, from commerce to patient data storage. Loss of data confidentiality, integrity, or service availability spells disastrous results. Fines, legal sanctions, and denial of payment processing are just a few of the possible consequences of poor security. Thankfully, creating and following a cybersecurity framework takes some difficulty away from securing an organization, and the RMF is no exception. Hess (2021), in his dissertation, analyzed the relationship between a private sector organization’s RMF implementation and its cybersecurity effectiveness. Hess found that organizations that implemented the entire RMF had statistically higher cybersecurity effectiveness than those that implemented only part or none of the RMF (Hess, 2021). Therefore, holistically applying the RMF to a private sector organization positively correlates with higher cybersecurity effectiveness and better cybersecurity outcomes.

**Prepare**

In 2018, NIST added the Prepare step in the second revision of the RMF to increase the effectiveness and efficiency of the process while simultaneously reducing the cost and labor burden. This may shock those who have not been involved with (or updated to, if in the private sector) the latest framework revision. Prepare’s purpose, as stated by NIST in 800-37, is “to carry out essential activities at the organization, mission, and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks” (2018). This step creates a foundation for the remainder of the RMF process steps, and thus many Prepare tasks may be satisfied due to previous policies. Seven organizational-level tasks and six system-level tasks comprise this step. NIST (2021) states in their NIST RMF Quick Start Guide: Prepare Step Frequently Asked Questions (FAQs) that tasks are split between organizational and system levels to make roles and responsibilities easier to understand and assign.

## ***Risk Management Roles (Organizational)***

The first task towards accomplishing something is assigning responsibility to those tasked to carry out the objective. Individuals or groups may be assigned roles and responsibilities within the RMF process, and some individuals or groups may be assigned multiple. It is encouraged to assign individuals or groups based on their subject matter expertise. However, multiple assigned roles and responsibilities mustn't cause a conflict of interest. For example, AOs cannot also be assigned the role of control assessor for the same SAC.

## ***Risk Management Strategy (Organizational)***

The second task is to create an organizational risk management strategy. An integral part of the overall risk management strategy is determining the level of risk tolerance or the amount of acceptable risk the organization is willing to take on (NIST, 2018). Once this is decided, the organization uses the level of risk tolerance to draft one or more documents containing policy regarding supply chain, cybersecurity, privacy, and other risk and how it is managed. Operational constraints, trade-offs, assumptions, and priorities guided by the predetermined risk tolerance are also documented. The risk management strategy and policies outlined in the document or documents will be followed throughout the entire life cycle of the SAC.

## ***Risk Assessment (Organizational)***

The third task is to evaluate the risk faced by the entire organization and keep the risk assessment relevant and up to date. An organization may deploy systems that process payment card information (PCI) or personal health information (PHI), among other things, and thus must be aware of threats, trends, and groups targeting those datasets. Data gathered from individual SAC risk assessments, recorded security incidents, and internal or commercial threat reports form the basis of the organizational risk assessment (NIST, 2018). As the cybersecurity landscape evolves, so must the organization’s risk assessment documentation.

## ***Tailored Control Baselines (Organizational, Optional)***

The fourth task is entirely optional but highly recommended. It will make the later RMF steps easier to execute and more relevant to the organizational and industry-specific risks. A control baseline tailored to the organization's specific situation reduces risk by personalizing the controls in place and limits unnecessary overhead and the overall attack surface by removing irrelevant or ineffective controls. Additionally, organizations can create control baselines to account for SACs that may operate outside the usual deployment environment, such as in a foreign country, warzone, or regulated industry. Control baselines will also speed up the later steps because sufficient controls can be implemented within a system and tailored further to match the SAC.

Outside organizations have also developed control baselines, which can be used as a starting point for organizationally tailored control baselines. SACs processing certain types of data, such as PCI or PHI, are required by law, regulations, or policies to have specific controls. The overseeing bodies provide baselines of their own or at the minimum guidance, and some mandate that specific controls or control families be used. Organizations should keep the type of data processed by SACs in mind when selecting or creating control baselines.

## ***Common Control Identification (Organizational)***

The fifth task is to establish, record, and disseminate common controls associated with the organization (NIST, 2018). Common controls associated with the organization may include physical security controls inherited from data centers, administrative controls required by the organization, or technical controls inherited from the network boundary. Common controls may vary due to hosting location, the type of data processed, or the impact level of the SAC.

Identifying already existing controls eases the technical and documentation burdens of the RMF process and encourages standardization and consistency. There may be cases where the common controls do not satisfy internal or external policies and must be supplemented with SAC-specific controls. While this is highly likely, the overall volume of controls required to bring the SAC into compliance is significantly reduced with inherited common controls.

## ***Impact-Level Prioritization (Organizational, Optional)***

The sixth task relies on categorized organizational systems, so this step can only be done if previous RMF activities have been performed. Organizational SACs are categorized by impact into low impact, moderate impact, and high impact (NIST, 2018). These impact levels can be further categorized into low-low impact, low-moderate impact, and low-high impact. Subdividing the impact levels into more granular groups allows the systems within a given impact level to be prioritized when making risk management and risk assessment decisions. Additionally, limited human capital and other resources can be allocated accordingly.

## ***Continuous Monitoring Strategy (Organizational)***

The seventh Prepare task is to evaluate the overall organizational risk and determine the effectiveness of existing controls. Operational risk factors such as supply chain, cybersecurity, and privacy risks must be assessed alongside the controls to mitigate them (NIST, 2018). This ensures that the organizational risk and security posture is relevant to and defensible against the organization's threats. Frequency, depth, and type of monitoring should be determined and consistently enforced across the organization. Automation is essential to make this step realistic, repeatable, reliable, and cost-effective to execute.

## ***Mission or Business Focus (System)***

The eighth task is to understand the function of the SAC. Providing rugged and reliable communications, helping the warfighter seek medical care, or providing highly available payment processing are all mission or business focuses. Once the function of the SAC is understood, better-informed decisions can be made about risk management, human capital investment, prioritization, and much more (NIST, 2018). Meeting with users and stakeholders is the prime method of gathering a thorough understanding of the SAC’s mission or business focus. Meetings can also be held to ensure that users and stakeholders are satisfied with the SAC’s performance.

## ***System Stakeholders (System)***

The ninth task goes hand in hand with the previous one. Identify those who have a stake in the SAC’s operations, such as the PMO, AOs, developers, suppliers, and many more (NIST, 2018). Remembering that stakeholders may not be located where the SAC is hosted is vital to constructing a complete picture of the stakeholder community. Creating a chart to document the community is recommended. Gathering information beyond just the stakeholder names, such as contact information, role, location, impact on the SAC, etc. allows for ease of communication and collaboration.

## ***Asset Identification (System)***

The 10th task is to identify what assets are within the scope of protection with the SAC. Assets may be tangible, such as hardware, human capital, and buildings, or intangible, such as classified information, intellectual property, or trade secrets. Both types of assets are necessary for the successful operation and security of a SAC. Assets should be inventoried, categorized, and accounted for in risk management decisions. Meeting with stakeholders is recommended to understand what assets fall within the protection scope and what assets are not the responsibility of the PMO.

## ***Authorization Boundary (System)***

The 11th task is to identify the authorization boundary of the SAC in question. A SAC’s authorization boundary defines what is within the organization’s scope of protection, management, and responsibility (NIST, 2018). The organization only controls assets within the authorization boundary. Assets within the boundary may include the software or hardware that the organization is hosting, the physical location where the SAC is hosted, or the human capital running the SAC. Assets outside the boundary may include the Internet Service Provider, the underlying cloud-based hardware hosting the SAC, or other systems interfacing with the SAC.

Interconnection to systems outside the authorization boundary should be managed by written agreements such as service level agreements. These documents allow all parties involved to understand what is expected of them regarding privacy, security, and operations when disparate authorization boundaries begin to mingle (NIST, 2018). Service level agreements also allow for accountability and recompense if minimum service levels are not met.

## ***Information Types (System)***

The 12th task is to determine the category of information that the system will be creating, processing, transmitting, or storing (NIST, 2018). Information categories may include regular data, PCI, PHI, personally identifiable information (PII), financial data, and sensitive or classified data. Laws or regulations for each category of information require different controls and policies to be in place for effective management and data protection. Violations of these laws or regulations can lead to fines, sanctions, or legal trouble, including imprisonment.

Each SAC’s unique mission or business focus will determine the information category or categories it will be responsible for. The SAC’s documentation should specify the types of data it uses and the reason for using the data. Reducing the categories of information required will lead to less complexity and better privacy and security protections overall.

## ***Information Life Cycle (System)***

The 13th task involves understanding how categories of information must be managed from the cradle to the grave. According to NIST’s (2018) 800-37, “the information life cycle described the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.” Various categories of information have differing requirements at each stage of the information life cycle. Organizations must recognize how each category needs to be treated and create documentation and policies accordingly. If the SAC interfaces with other systems outside of its authorization boundary, the PMO must consider this risk.

## ***Risk Assessment (System)***

The 14th task is to evaluate the SAC’s security and privacy risk and continuously update the results. The first step in conducting a security risk assessment is to identify assets, vulnerabilities, threats, and the likelihood that threats may exploit the assets’ vulnerabilities (NIST, 2018). Next, the organization should assess the tangible and intangible effects of a partial or total loss of assets. Tangible effects may include loss of revenue, loss of hardware, or loss of life. Intangible effects may include loss of reputation or loss of intellectual property. The risk assessment results should be documented in a way that makes sense for the organization. Most organizations use a low-moderate-high scale for likelihood of impact and magnitude of impact. The combined likelihood and magnitude of impact results in an overall low-moderate-high risk level. Overall risk level allows the PMO to prioritize risks and balance risk with operational necessity.

Similar to security risk assessments, privacy impact assessments begin with identifying the privacy information that the SAC handles, the impact of losing control over the privacy information, and the likelihood of occurrence. Unlike security risks, the intangible consequences of privacy breaches are astronomical. Identity theft, threats or kinetic acts of violence, and extreme degradation of user trust are a few debilitating intangible impacts. Tangible impacts include fines or legal sanctions up to and including imprisonment. Like with security risks, privacy impacts should be assessed as low, moderate, or high and prioritized based on operational needs and laws or regulations governing privacy data protection.

The risk posed by interfacing with external systems or service providers should also be factored into the security risk assessment. While this is often forgotten, it is paramount that external systems or service providers are evaluated to prevent short and long-term losses. Short-term losses could entail equipment or software damage and theft. Long-term losses may include intellectual property theft, sabotage, or data theft.

## ***Requirements Definition (System)***

The 15th task comprises laying out security and privacy requirements adequate for the SAC’s impact level. Relevant laws and regulations should be consulted to ensure that data protections meet the required standards. Stakeholders should also communicate their desires and requirements for the SAC to be functional and secure in its intended operational environment (NIST, 2018). All software development life cycle phases should be accounted for, and all approved requirements should be formally documented.

## ***Enterprise Architecture (System)***

The 16th task calls for analyzing the enterprise architecture and then deciding where the SAC fits. The enterprise architecture details how the organization’s tangible and intangible assets are structured and allocated to ensure mission success (NIST, 2018). A clear and complete understanding of the structure of the hardware and software environment allows for greater accountability, visibility, and defensibility. These attributes lead to improved efficiency and reduced risk to the organization and the SAC itself. SACs may be segregated on a hardware or software level, and each SAC should inhabit a dedicated virtual network segment. Segregation and segmentation prevent a successful cyber-attack from exploiting other SACs or the entire network.

Privacy should be built into the overall enterprise architecture and should not be bolted on as an afterthought. Network and environment templates can be created for SACs that process similar information to speed up deployment and reduce management overhead.

## ***Requirements Allocation (System)***

The 17th task entails efficiently allocating security and privacy requirements to SACs or the organization to eliminate redundant controls (NIST, 2018). If one control can satisfy multiple security or privacy requirements, that control should be selected instead of multiple controls that only satisfy one requirement. Control efficiency reduces management overhead and allows faster and more consistent SAC deployments. Cost savings in human capital and capital expenditure may result from selecting efficient controls as well.

## ***System Registration (System)***

The 18th and final task in the Prepare step is to document and register the SAC with the organization (NIST, 2018). Registering the SAC makes key leadership aware of its existence, mission or business focus and how it fits into the enterprise architecture. Impact level and other characteristics are added after completing the Categorize step. Inventoried SACs are able to report and disclose information as required by laws or regulations governing their operations.

# **Categorize**

After preparing for the RMF, the PMO works together to categorize the SAC, which is described by NIST (2018) in 800-37, as:

To inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems. (pp. 64).

Categorize used to be the first step in the RMF, but NIST determined that preparation must be done before the Categorize tasks can be successfully executed. This step’s outputs are submitted for approval by the AO before moving onto the Select step.

## ***System Description***

The first task in the Categorize step is to document the aspects and characteristics of the SAC. The system description can be in one document or multiple, but the goal is to avoid redundant information and streamline the documentation process (NIST, 2018). Organizations take the SAC’s security and privacy risk assessment and the impact level into account when mandating the level of detail necessary in descriptive documents. System description documents are living and thus should be updated as the latest information becomes available.

As previously mentioned, the required detail in descriptive documents is determined by the organization. Examples of what may be included in these documents are: the SAC’s internal inventory number, software development model such as Agile or Waterfall, SAC hosting location, interconnections with external systems, vendors, maintenance plans and agreements, and much more. Organizations may find it easier to create documents that cover specific information, but there is no prescribed documentation method. If multiple documents are created, best practice dictates that particular care be taken to prevent redundant information from permeating the documents.

## ***Security Categorization***

The second task in the Categorize step is to determine the SAC’s impact level. Organizations follow certain guidelines to determine the SAC’s impact level depending on the mission or business focus of the SAC and what type of data the SAC processes (NIST, 2018). Federal non-national security SACs use the high water mark concept outlined by NIST (2006) in Federal Information Processing Standard (FIPS) 200 Minimum Security Requirements for Federal Information and Information Systems, where the overall SAC impact level is the highest impact level of confidentiality, integrity, or availability. Other federal systems use different guidelines, and private organizations may use different guidelines as well. System owners and information owners meet with senior leaders within the organization to determine the impact level. The security and privacy risk assessment results are considered alongside the mission or business focus when making the decision. As mentioned in the Prepare step, further categorizing SACs within an impact level as low-low, low-moderate, or low-high, for example, allows risk prioritization.

## ***Security Categorization Review and Approval***

The third and final task in the Categorize step is review and approval by the AO and Senior Privacy Officer if applicable (NIST, 2018). If a SAC processes PHI or PII, then the Senior Privacy Officer must review and approve the security categorization results before the AO. The AO reviews and approves the SAC’s security categorization as well. If either the Senior Privacy Officer or the AO do not approve the proposed security categorization, then the system owner repeats the previous two Categorize tasks and resubmits for approval. The Senior Privacy Official and AO are encouraged to provide feedback if they do not approve a system.

# **Select**

The third step of the RMF is Select, and its purpose, as stated by NIST (2018) in 800-37, is “to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation”. This step is the most critical and time-consuming step for the PMO as the choices made here will impact all of the following steps. Like the previous steps, the documents produced in this step will be submitted for approval by the AO before moving on to the Implement step.

## ***Control Selection***

The first task in the Select step is determining whether to apply a control baseline or direct the organization to select SAC-specific controls. The work done in the Prepare step should streamline applying a control baseline if the SAC is not highly specialized and can fit within a general group. If the SAC is highly specialized, then the organization will find it easier to select SAC-specific controls instead of applying a baseline and then trimming the fat. Organizations must take applicable laws, regulations, and mission or business focuses into account when selecting controls. Both approaches necessitate refining the control selection to minimize security and privacy risk efficiently.

Organizations may also opt for both approaches. NIST employees Ross, Pillitteri, & Lefkovitz (2020), in their web article, Selecting Security and Privacy Controls: Choosing the Right Approach, write that organizations “…can choose the appropriate approach as circumstances dictate. This flexibility is needed to manage security and privacy risks effectively…”. A baseline may cover most of the necessary controls, but additional controls are likely necessary.

Twenty control families with over 1,000 controls total are cataloged in NIST’s (2020) 800-53. 800-53 lists all of the base controls and enhancements to said controls that increase functionality or specificity (NIST, 2020). Organizations should consider employing control enhancements to SACs that require more protection than the base control can offer. This may reduce the number of individual controls applied to a SAC and thus simplify management and documentation.

## ***Control Tailoring***

The second task in the Select step is to modify the applied controls to fully comply with the SAC’s risk assessment and impact level. Security and privacy risk assessment results and mission or business focus lead the modification process (NIST, 2018). Niche or high-impact systems require more granular controls and specific tailoring than general use or low-impact systems. Weak points left by the controls selected in the previous task must be mitigated by applying new or compensating controls. After everything is covered by a control, the organization eliminates redundant or unnecessary controls.

## ***Control Allocation***

The third task in the Select step is to assign control responsibility to either the SAC itself or its operating environment. Controls are designated as common, system-specific, or hybrid (NIST, 2018). Common controls are generalized controls that apply to a broad range of SACs and are inherited from the organization’s security architecture. System-specific controls are niche controls that cover system requirements not satisfied by the common controls. Hybrid controls are a mix of the two. Once designated, controls are assigned to the SAC or the operating environment in a manner agreeable to the enterprise, risk, and security architecture, and with the previously allocated security and privacy requirements.

## ***Documentation of Planned Control Implementations***

The fourth task in the Select step is to capture the common and system-specific controls and how to implement them within security and privacy plan documents. Each planning document should layout the security and privacy requirements and the controls that satisfy each requirement (NIST, 2018). The documents should have enough detail pertaining to system-specific controls to implement them and ensure the effectiveness of the controls. Common controls inherited from the organization must be documented, but enough detail to implement them is not necessary. Hybrid controls must be documented with the level of detail of system-specific controls for the portion that is not provided by the organization.

Organizations may separate or combine the security and privacy plans into one document. Information duplication should be avoided when possible, and already-existing documentation from vendors, system integrators, or other SACs should be integrated to save on labor. As always, documentation should be readable and relevant.

## ***Continuous Monitoring Strategy – System***

The fifth task in the Select step is to establish a system-specific continuous monitoring plan that complements the organizational continuous monitoring strategy. When the organizational strategy is not sufficient for the SAC, the PMO must develop a system-specific strategy to fill in the gaps (NIST, 2018). Each SAC’s individual risk assessment, impact level, and priority in the organization will determine how often controls are monitored. The system-specific strategy should be documented within the security and privacy plans. Changes to both the SAC and the operating environment must be addressed, and any legal or regulatory requirements must be as well.

## ***Plan Review and Approval***

The sixth and final task in the Select step is to have the security and privacy plans approved by senior leadership. The organization’s AO, Chief Information Officer, Chief Information Security Officer, Senior Privacy Officer, and others will collaboratively decide if the security and privacy plans are sufficient for approval (NIST, 2018). The controls outlined in the plans will be evaluated to determine if the security and privacy requirements are met, and if so, the AO will approve the plans. If not, then the PMO will make the necessary changes to be approved by the AO. By approving the plans, the AO agrees to the specified controls and with the overall risk management assessment thus far in the RMF process.

# **Implement**

After selecting controls and creating a plan to implement them, the PMO is responsible for coordinating the execution of the control plans. This step’s purpose, as stated by NIST (2018) in 800-37, is “to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation”. This step does not entail approval by the AO as the guiding documents were approved in the Select step.

## ***Control Implementation***

The first task in the Implement step is to implement the chosen controls. System-specific controls must be implemented in a manner consistent with the security and privacy plans (NIST, 2018). The PMO should ensure that inherited controls are correctly applied. However, no plan survives first contact, so it is inevitable that the implementation will slightly differ from the documented methods. Best practices should be followed throughout the entire implementation process.

## ***Update Control Implementation Information***

The second and final task in the Implement step is to capture any deviation in control implementation and document it (NIST, 2018). The security and privacy plans layout how controls will be implemented, but this is not always feasible. In cases where the actual implementation differs from the planned implementation, the security and privacy plans are updated accordingly. It is imperative that the documents reflect the current implementation state for later assessments, changes, and authorization.

# **Assess**

Once the planned controls are implemented, the PMO must coordinate an assessment to determine the implementation’s effectiveness. NIST (2018) goes into more detail in 800-37 and describes this step as “to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization”. The PMO reports the results from this step to the AO in order to determine the way ahead for the risk management strategy.

## ***Assessor Selection***

The first task in the Assess step is to appoint an individual or group of assessors. The assessment team must be competent with the technology at hand, understand security and privacy risk management, and be proficient with assessment methodologies (NIST, 2018). Team members should synergize and balance out weaknesses for a comprehensive assessment. Independent third-party teams or internal teams may be used, but teams must be impartial and free of conflict of interest.

## ***Assessment Plan***

The second task in the Assess step is to create and approve an assessment plan or plans. The assessment plans for security and privacy are created by the selected control assessors based on the program documentation (NIST, n.d.). Plans should outline the goal of the assessment, whether it is auditing, developmental testing, or control authorization (NIST, 2018). After creation, assessment plans are submitted to the AO for approval.

## ***Control Assessments***

The third task in the Assess step is to execute the assessment plan, so the details of this step are unique to each SAC. The SAC is assessed to ensure that the controls are properly implemented and functioning as intended (NIST, 2018). These assessments should occur as early as possible in the SAC’s development and thus are often referred to as developmental test and evaluation. Automation should be used as much as possible to reduce testing overhead and minimize human error. There is little room for subjectivity as the findings should detail whether the controls are correctly implemented.

## ***Assessment Reports***

The fourth task in the Assess step is to report the findings of the assessment. Observations, risks, and findings, along with recommendations for remediation, should be included in the report (NIST, 2018). Security and privacy assessment reports may be separate or combined into one overall SAC assessment report. Report formatting is usually prescribed by the organization conducting the test, so the final product may vary. Nevertheless, control implementation statuses, vulnerabilities, and recommended remediations will make up the bulk of the report. Reports are typically sensitive documents and must be protected in accordance with organizational policy.

## ***Remediation Actions***

The fifth task in the Assess step is to correct significant findings discovered from the assessment. When findings are so drastic that they pose an unacceptable risk to the SAC or organization, the AO may decide to order immediate corrective action (NIST, 2018). The offending controls are reassessed after correction, and the assessment report is updated to include the results. However, the initial results are not changed. Findings may necessitate updating the SAC or organizational risk assessment.

## ***Plan of Action and Milestones***

The sixth and final task in the Assess step is to plan and schedule remediation actions for the remaining findings. The Plan of Actions and Milestones (PO&AM) describes the details, resources, necessary stakeholders, and timeline for correction and is intended to be included in the authorization package (NIST, 2018). Remediations may be scheduled for completion before or after the SAC achieves an ATO. The AO may accept some findings as residual risk, and these are not required to be included in the PO&AM. Organizations should develop and use a consistent methodology for developing PO&AMs that applies across all SACs under their control.

# **Authorize**

The sixth step of the RMF is Authorize, and its purpose, as stated by NIST (2018) in 800-37, is:

To provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable. (pp. 88)

The PMO submits the authorization package to the AO, who then collaborates with other senior officials to determine whether to grant the SAC an ATO.

## ***Authorization Package***

The first task in the Authorize step is to compile and submit the SAC authorization package to the AO. The system security plan, privacy and security assessment reports, and the PO&AM comprise the authorization package (Open Control, n.d.). If the SAC is hosted in the FedRAMP infrastructure, a continuous monitoring strategy document is also mandatory (Open Control, n.d.). Any controls provided by external providers must be available and included in the authorization package, and the AO may request additional documents be included in the authorization package as well (NIST, 2018). Completeness is of the utmost importance as the AO will make their determination whether to grant an ATO based on the authorization package.

## ***Risk Analysis and Determination***

The second task in the Authorize step is for the AO to evaluate the authorization package and determine the risk posed by the SAC and its controls (NIST, 2018). The AO will meet with the organization’s senior information security officer and senior privacy officer to collaborate on the analysis. This group may meet with control assessors, the SAC PMO, or other stakeholders for further clarification. The group takes all of the information in the authorization package and any supporting documentation into account when evaluating the SAC. Once finished, the AO makes a risk determination for the SAC.

## ***Risk Response***

The third task in the Authorize step is for the AO to respond to the risk posed by the SAC. The AO can elect to accept risks, mitigate risks, or a combination of both (NIST, 2018). If the AO elects to mitigate a risk, the remediation actions are documented in the PO&AM. Once remediated, the offending controls are assessed to confirm remediation, and the results are placed in the assessment report from the Assess step. If the AO elects to accept a risk, the accepted risk is documented in the assessment report. Only the AO can accept a risk, and the responsibility cannot be delegated.

## ***Authorization Decision***

The fourth task in the Authorize step is for the AO to make an authorization decision for the SAC. If the AO determines that the risk posed by the SAC’s operation is acceptable, then the AO grants the SAC an ATO (NIST, 2018). ATOs may be granted with conditions that must be met in order to renew the ATO once the current one expires. ATOs are generally authorized for three years, and significant changes to the SAC necessitate a new authorization (Bennerson, 2017). However, SACs may be granted a continuous ATO if they have a sufficient continuous monitoring strategy for consistently updating the AO regarding the risk assessment and determination of the SAC (NIST, 2018). The AO is responsible for the risk posed by operating the SAC. If the AO denies the SAC an ATO, the SAC PMO makes the necessary corrections and resubmits for authorization.

## ***Authorization Reporting***

The fifth and final task in the Authorize step is for the AO to report their authorization decision to senior leaders in the organization. Informing senior leaders allows them to update and fully understand the organizational risk with the newly approved SAC (NIST, 2018). This ensures that the organization has a holistic view of the operating environment and accounts for all SACs under their authority. Reports are typically sensitive documents and must be protected in accordance with organizational policy.

# **Monitor**

The last step of the RMF is Monitor, and its purpose, as stated by NIST (2018) in 800-37, is “to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions”. A SAC achieving an ATO is not the end of the road as nothing stays constant in the realm of cybersecurity. The PMO is responsible for creating and implementing a strategy to keep the SAC cyber survivable throughout its deployment.

## ***System and Environment Changes***

The first task in the Monitor step is to monitor the SAC and its operating environment for changes. Changes may be authorized or unauthorized. Authorized changes must be planned and documented to preserve system security and availability (NIST, 2018). Unauthorized changes may be made by adversaries or inadvertently by insiders. Regardless, unauthorized changes must be detected and remediated as soon as possible. Each SAC will have a unique strategy for identifying changes and the subsequent remediation depends on the type and intent of the unauthorized change.

## ***Ongoing Assessments***

The second task in the Monitor step is to conduct control assessments beyond the initial assessment for authorization. The organization determines minimum assessment tempo, but Federal Information Security Management Act (FISMA) requirements dictate that assessments are conducted at least annually (NIST, 2018). SACs may require more frequent assessment but cannot delay assessments longer than FISMA allows. Assessment results may be reused in specific scenarios approved by the organization. Additionally, the SAC’s ATO may stipulate more frequent or specific types of assessments that the SAC PMO is bound to conduct.

## ***Ongoing Risk Response***

The third task in the Monitor step is to remediate findings discovered during ongoing assessments. The AO reviews the assessment results and determines the risk response necessary for remediation (NIST, 2018). Control providers and the PMO may suggest remediations for the AO’s approval as well. Once the AO approves remediations, the control providers and PMO implement the remediations if risk mitigation is pursued and update the SAC PO&AM. The assessors then ensure the corrective action successfully mitigates the findings. The SAC's risk assessment documentation is updated to include the new findings if risk acceptance is pursued.

## ***Authorization Package Updates***

The fourth task in the Monitor step is to document assessment results and update the authorization package components. Security and privacy plans, assessment reports, and the PO&AM are updated at regular intervals as changes are made (NIST, 2018). Like the assessment tempo, the organization determines the update tempo with respect to all applicable laws, policies, and regulations. The PMO may elect to update at a more frequent pace. PMOs are encouraged to update the authorization package as frequently as possible to make submitting for reauthorization easier.

## ***Security and Privacy Reporting***

The fifth task in the Monitor step is to document the continuous monitoring activities and inform the AO and other senior stakeholders. The reports inform the AO and senior stakeholders about the security and privacy status of the system, the effectiveness of the continuous monitoring activities, and PO&AM items (NIST, 2018). The PMO should use the report format of their organization, and organizations are granted freedom to create their report formatting standards. Like the assessment and updating tempo, the organization determines the reporting tempo concerning all applicable laws, policies, and regulations. The PMO may elect to report at a more frequent pace. Reports are typically sensitive documents and must be protected per organizational policy.

## ***Ongoing Authorization***

The sixth task in the Monitor step is for the AO to analyze the SAC’s security and privacy posture and determine whether the ATO should remain in effect. Continuous monitoring activity data guides the AO’s analysis, and if the risk posed by the SAC’s operation is too significant, the ATO will be withdrawn (NIST, 2018). If the risk remains acceptable, then the ATO will remain in effect until the next reauthorization period dictated by law and by any ATO stipulations.

## ***System Disposal***

The seventh and final task in the Monitor step is to properly decommission a SAC that has reached its end of life. Data should be archived and or destroyed, records should be retained as dictated by law or organizational policy, and organizational architecture and risk documents should be updated (NIST, n.d.). The PMO should notify SAC users of the system disposal ahead of time, and interconnecting systems should be notified so they may update their architecture diagrams as well.

# **Conclusion**

As shown, the RMF process is an in-depth and comprehensive framework designed to ensure cybersecurity at all stages of the SAC’s life cycle. RMF is mandatory for all federal information systems and while not explicitly recommended for private sector organizations, the general concept of a cybersecurity framework serves a similar purpose. Frameworks allow for a common understanding and prioritization of operational procedures in addition to encouraging transparency and forward-thinking. Implementing the entire RMF increases the cybersecurity effectiveness of both public and private sector organizations. Implementing only some RMF steps has no relationship to organizational cybersecurity effectiveness. The RMF encompasses a SAC’s development, hardening, deployment, maintenance, and decommissioning to cover from the cradle to the grave. Gathering necessary information, gaining situational awareness, choosing security controls, implementing the chosen controls, bringing the SAC online, and continuously monitoring the SAC allows an integrated approach to cybersecurity. The most time-consuming RMF step by far is Select. NIST details over 1,000 security controls ranging from technical, administrative, and physical for organizations to choose from. The security controls selected in this step will form the basis of the SAC’s security posture and authorization package, not to mention protecting the SAC from adversarial threats. Skimping on this step in particular may allow for easier accreditation and authorization, but the time saved will be lost to recovering from damage done to the SAC, the organization, and the user community. All steps should be taken seriously and given the time and energy they deserve. Just as one cog in a machine cannot do anything by itself, one RMF step will not improve organizational cybersecurity effectiveness on its own. Conscious action and proactive planning help prevent most common cybersecurity threats and a sizeable portion of the uncommon ones. By implementing RMF, organizations can sleep easier at night knowing that they have done their due diligence in protecting their SACs.

# **References**

Bennerson, J. (2017). Federal Government's process for IT security: ISACA Journal. Navigating the US Federal Government Agency ATO Process for IT Security Professionals. <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/navigating-the-us-federal-government-agency-ato-process-for-it-security-professionals>

Hess, W. (2021). Enterprise risk management as a measurement of cybersecurity effectiveness: A correlational study [Doctoral dissertation, Capella University]. ProQuest. <https://www.proquest.com/docview/2488603980/2A64D030234240C5PQ/3>

National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy. <https://doi.org/10.6028/NIST.SP.800-37r2>

National Institute of Standards and Technology. (2020). Security and privacy controls for information security systems. <https://doi.org/10.6028/NIST.SP.800-53r5>

National Institute of Standards and Technology. (n.d.). NIST RMF quick start guide: Assess step frequently asked questions (FAQs). <https://csrc.nist.gov/Projects/risk-management/about-rmf/assess-step>

National Institute of Standards and Technology. (n.d.). NIST RMF quick start guide: Monitor step frequently asked questions (FAQs). <https://csrc.nist.gov/Projects/risk-management/about-rmf/monitor-step>

National Institute of Standards and Technology. (n.d.). NIST RMF quick start guide: Prepare step frequently asked questions (FAQs). <https://csrc.nist.gov/Projects/risk-management/about-rmf/prepare-step>

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

Open Control. (n.d.). Steps of the ATO process. <https://atos.open-control.org/steps/>

Ross, R., Pillitteri, V., & Lefkovitz, N. (2020). Selecting security and privacy controls: Choosing the right approach. <https://www.nist.gov/blogs/cybersecurity-insights/selecting-security-and-privacy-controls-choosing-right-approach>