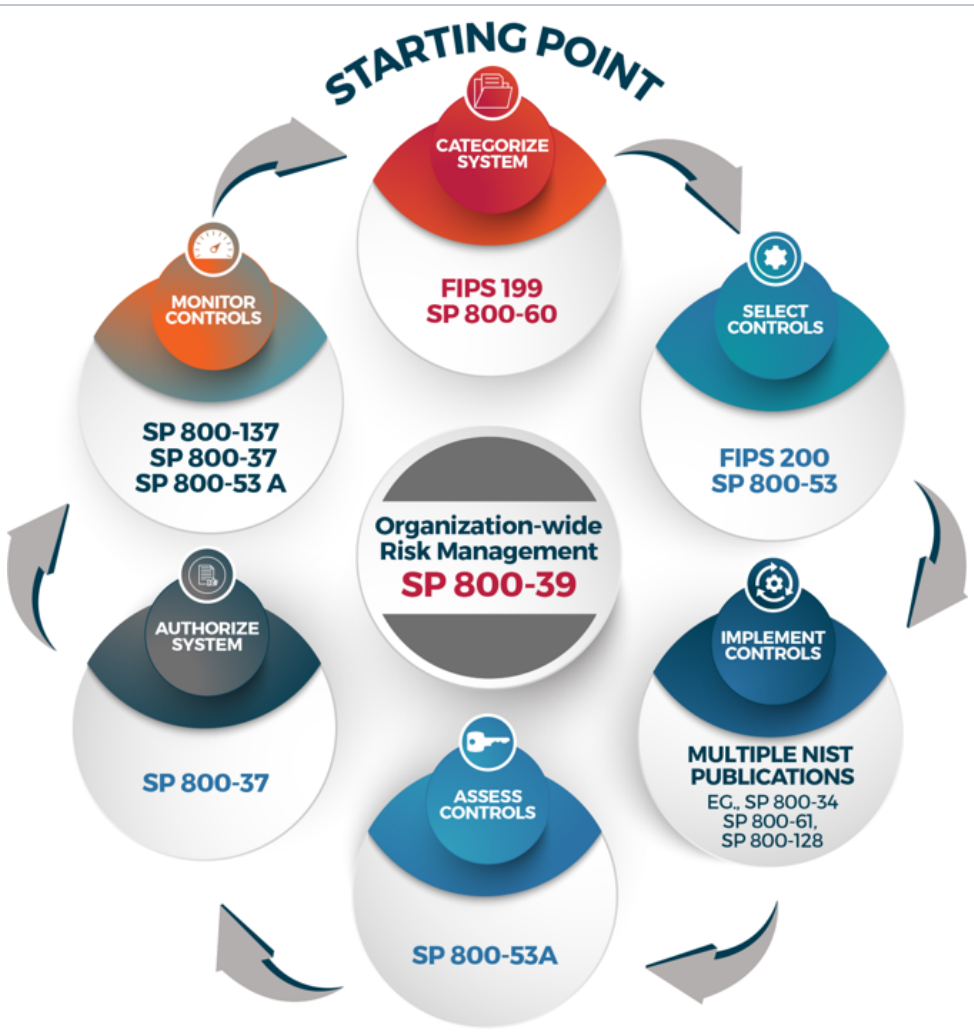
Conducting the FISMA A&A

The Risk Management Framework (RMF) Assessment and Authorization (A&A)

The RMF is the full life cycle approach to managing federal information systems' risk should be followed for all federal information systems. The RMF comprises six (6) phases, with Assessment and Authorization (A&A) being steps four and five in the life cycle. To read more about the RMF, please refer to NIST Special Publication 800-37 rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

1. Categorizing the system;
2. Selecting security controls;
3. Implementing security controls;
4. Assessing controls;
5. Authorizing systems; and
6. Monitoring security controls



The following general information is intended to help you generally understand the risk management framework, and prepare you to conduct the SA&A for your federal information system or application.

Step 1. Categorize the System

Once you have established that yours is a federal information system, the first step is to categorize the information system. Use the NCI Security Starter Kit for templates and guidance on completing the Federal Information Processing Standard 199 (FIPS-199) form, the e-Authentication Threshold and Risk Analysis (eTA/eRA) form, the Privacy Impact Assessment (PIA), and the Business Impact Analysis (BIA). All four forms are required to ensure that you properly define the risk rating for your system, and will allow you to select the proper security controls (from NIST 800-53) for your application and will help you design the application to meet security, privacy, and availability needs. This first step is consistent across all federal information systems whether they are hosted internally, externally, or in the cloud.

Step 2. Select Security Controls

Once you have categorized your application you can determine which security controls apply to your system. Controls are technical, managerial, or operational in nature and help ensure adequate security and assurance for your system. There are three ways controls can be applied and managed:

1. Common controls are those that are fully inherited by a system from a higher-level system or environment (i.e., an organization-wide network or service like email);
2. Hybrid controls are those that are partially inherited from a common control provider but still require the system owner to take some responsibility for implementing and managing; and
3. System-specific controls are entirely the system's or system owner's responsibility to implement, operate, manage, and monitor.

This control selection matrix is a tool that can help you determine which controls to implement (based on your rating) and will help you determine which are common, hybrid, or system-specific.

Step 3. Implement Security Controls

As part of the system's design process, you will need to ensure that system-specific and hybrid portions of controls are properly designed and implemented. By incorporating security control requirements into your overall system design and development process, and continuously throughout the system's life cycle, you should realize cost savings when compared to implementing security to an existing system or retrofitting the application to meet security requirements. You may even find that security ends up driving or altering some of your functional and design requirements, which is why it is best to integrate security early in the system's life cycle instead of later. However, if the cost of developing or implementing a new security control is not possible, causes undue hardship, or is not cost-effective then you may be able to apply for a security waiver to the NIH chief information security officer (CISO). All waiver requests must be vetted first with your Contracting Officer Representative (COR), and then with the NCI ISSO (link sends email). All final waivers must be approved by the NIH CISO.

Step 4. Conduct the Security Assessment

During this phase a qualified – and usually an independent, 3rd party – security assessor will evaluate the effectiveness of your application's security controls. The cost and burden of identifying and paying for the assessor varies based on where the application resides or operates, but the general rules of thumb at NCI are:

- CBIIT-fully-managed applications will be assessed by the internal CBIIT security audit team
- Non-CBIIT-managed applications will be assessed by external security assessors. These assessors are usually hired by and paid for by the system owner (business owner). All packages for externally hosted systems should be provided to the NCI ISSO's office so they can perform a quality assurance review and provide feedback to the authorizing official for the authorization decision.

NOTE: All final A&A packages must contain the minimum set of artifacts required by NIH.

The preliminary package that includes the System Security Plan, Security Assessment Report, and Plan of Action and Milestones must be provided to the AO or her designated reviewing official to assess the quality and completeness of the package, and to review the findings. This gives the system owner and the system operator a chance to correct invalid findings, and to address any that can quickly and easily be closed before the authorization request is made. Once this review has been completed and the business owner is satisfied that the package is ready for review, it is sent to the authorizing official.

Step 5. Authorize the Application (System)

Once the system's security assessment has been completed and the POA&M has been finalized, the final and complete authorization package is submitted to the authorizing official (AO) for a decision. The authorizing official will make the final decision if residual risks are acceptable and if the remediation plan (POA&M) to address them is adequate. The AO varies based on the hosting solution, as follows:

- CBIIT fully managed: NCI CIO
- Non-CBIIT Managed: Business Owner
- Contractor/Third-party hosted: Business Owner
- Cloud: May be the FedRAMP PMO or Agency CIO

Step 6. Conduct Continuous Monitoring and Reauthorization

- Continuous monitoring (CM): CM is the sixth and final step in the RMF, and includes both automated and manual security monitoring and remediation activities. The routine security-control monitoring and remediation that occur after an application has been authorized to operate often includes a combination of automated diagnostics services such as vulnerability management, intrusion detection and prevention, system and application event log collection and analysis, and patch management. Along with these, manual assessment and remediation procedures such as annual assessments (AA), security impact reviews, plan of action and milestones (POA&M) management, and ongoing authorization (OA) or re-authorization must be performed.
- Annual Assessments: The NIH A&A policy requires application owners to assess a set of controls that is roughly 1/3 of the total applicable controls, each year after the ATO has been issued. Each year NIH issues guidance on which controls must be annually assessed. This list is available from the NCI ISSO upon request, or may be provided by your C.O.R. This approach helps owners address the most prevalent security threats on an ongoing basis while maximizing efficiency and supports the system's re-authorization decision every three years. If a system owner fails to keep up with the annual assessments, then every three years the system must be fully re-assessed. These controls need only be assessed to the extent they are not already covered under the FedRAMP inherited controls.
- Security Impact Reviews: When significant changes to your application are proposed (while it is operational and has an active ATO), you must ensure that new security risks are identified, evaluated, and addressed before those changes are implemented. This may require re-testing of any new or modified controls and, possibly, reauthorization of your application. However, if you follow a defined change control process, and if you adequately identify and address potential risks that may result from a proposed significant change, re-authorization may not be required. The idea is to be transparent about such changes, adequately identify and address potential risks, and to keep a record of such assessments. Some changes may be so significant that the system must be re-authorized, such as changing the operating location of a system or a complete re-design of a system. When in doubt about when a re-authorization may be needed, please consult with your ISSO.
- POA&M Management: The Plan of Action and Milestones (POA&M) is a key management tool that lists, prioritizes, and tracks an application's identified weaknesses and progress. Any new security findings that are generated from ongoing security assessment and risk impact reviews should be added to the application specific POA&M and remediated in a timely manner. You should not track the CSPs POA&M items as those will be monitored by the FedRAMP Project Management Office (PMO) or by the agency that sponsored their FedRAMP assessment.
- Ongoing Authorization and Re-authorization: The NIH is currently developing its ongoing authorization (OA) model so we are not using a true ongoing authorization approach at this time. However, by demonstrating that you have conducted annual assessments, applied sound

configuration and change control, scanned for and closed technical and security vulnerabilities, addressed your POA&M items in a timely manner, and patched your systems and applications in accordance with NIH standards, you will be able to seek re-authorization as required every three years and should find the process less time consuming and less expensive than starting from square one.