NCI CBIIT-Fully-Managed Applications

All federal systems, regardless of where they are hosted or operated, must adhere to the NIST Risk Management Framework (RMF) and business owners must ensure their system is authorized to operate in accordance with OMB A-130 and FISMA law.

This page provides guidance for achieving FISMA compliance and receiving Authorization to Operation (ATO) for the **CBIIT fully-managed hosting environment.**

The RMF comprises 6 key steps as described below. Since your system will be fully managed by CBIIT's application hosting service team, the SA&A activities you need to follow are relatively easy and require the least amount of support and resources when compared to non CBIIT-managed options.

By choosing a fully managed hosting option, your application will inherit the majority of security controls that you might otherwise be responsible for implementing, assessing, and maintaining over the system's lifetime. As the application owner (aka, the business sponsor), you will be asked to support the *Categorize* step by completing the NCI Starter Kit, and you will be required to develop a minimal set of standard operating procedures for your application. You will also be asked to document the limited set of security controls that you partially or fully manage in a system security plan, but the NCI pre-assessment team (PAT) will assist you with your documentation development activities to reduce your burden and provide one-on-one support during the pre-assessment phase. NCI CBIIT Security will also provide the independent assessor who will conduct formal system testing needed to support the authorization decision. As the application owner you will need to demonstrate applicable system-specific controls that you are responsible for. You will do this by participating in interviews, and by providing requested evidence and artifacts (i.e., completed SOPs, screen captures, log files, relevant communications such as email threads, etc.).

The following information will help you further understand and prepare (pre-assessment) for the formal security assessment step and to manage the FISMA assessment, following system authorization. Note that this process does not reflect the process for cloud hosted applications. Please visit the Cloud Hosted Systems SA&A page for more information on conducting an SA&A for a cloud based applications.

Step 1. Categorize the Application

Use the NCI Security Starter Kit for templates and guidance on completing the

- Federal Information Processing Standard (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 of these forms are required to ensure that you properly categorize your application based on its security-impact rating, authentication needs, privacy concerns, and mission criticality. This step is consistent with other types of federal information systems whether hosted internally, externally, or in the cloud.

Step 2. Select Security Controls

Once you have completed Step 1 (Categorization) you can determine which security controls are required for your application. You should refer to two resources to aid in this step.

1. NIST 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* document, which provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations.
2. NCI maintains a Security Control Inheritance Matrix to help you identify the controls needed for your system. The matrix factors in pre-defined common controls (i.e., controls and services provided by NCI CBIIT for all similar systems they host) so you can more easily identify controls that you are responsible for implementing and managing, and those that are partially or fully implemented and managed for you by CBIIT, NCI, or by NIH.

Step 3. Implement Security Controls

As part of the implementation step, you may need to update your application's design requirements to account for new or modified security requirements identified in Step 2. You may also need to implement or develop specific tools, feature, settings, etc. to satisfy these required controls. For example, you may need to configure your application to comply with NIH security policies like password settings. Under the risk-based approach the NIST follows, if the cost of developing or implementing a new security control is impractical or if it is not cost effective when compared to the potential risk of not implementing the control, you can apply for a security waiver to the NIH chief information security officer (CISO). You should discuss any waiver requests with the NCI ISSO first before submitting the request to determine whether it is likely to be approved, and to help appropriately document the waiver. Waivers are never approved when the system can comply but simply chooses not to. There must be extenuating factors the limit or prevent compliance, and there need to be adequate compensating controls in place to reduce risk.

It is in the step that you will also document how you have or plan to implement all of the required and applicable controls. You will document these in the System Security Plan (SSP). Work with the Pre-Assessment Team to ensure you understand how to complete the SSP properly and to ensure you only address the system-specific controls that you will not inherit.

Step 4. Conduct the Security Assessment

Since your system is fully managed by CBIIT, the NCI ISSO will conduct the independent verification of your system's security controls. the NCI ISSO and the Assessment Team will work with you to schedule your SA&A kickoff meeting and assessment, as well as keep you informed of any meetings required to plan for the assessment.

During this phase of the Risk Management Framework, (RMF) a security assessor will evaluate the effectiveness of your application's security controls through interviews, observation, testing, and data gathering. This process must be completed before your application goes into production (i.e., is live with real data being collected, processed, or stored). One of the advantages of having CBIIT fully manage your application is that CBIIT will help defray the cost of SA&A activity. If your application uses another NIH institute or center (IC) or uses an outsourced hosting option, then you will be responsible for most or all of the security assessment and authorization process and costs.

During the SA&A kickoff meeting, your assigned pre-assessment representative will help you identify artifacts that might be required as evidence of successful security-control implementation and operation so that you can prepare or update them in advance of the assessment step.

Your final SA&A package must contain the minimum set of artifacts required by NIH. Please visit the NCI SA&A Package Checklist for more information.

Step 5. Authorize the Application

The designated authorizing official (AO) will review the assessment package to determine whether any identified residual risks are acceptable to the organization before issuing a written authorization to operate (ATO). Approved ATOs are valid for a maximum of three years. The NCI CIO serves as the authorizing official (AO) for all CBIIT fully managed applications.

Step 6. Conduct Continuous Monitoring and Reauthorization

Continuous monitoring (CM) is the sixth and final step in the RMF, and includes both automated and manual security monitoring and remediation activities. Continuous Monitoring really is more of an iterative cycle than a single finite step since it never ends and, if done correctly, can replace the need for a full re-assessment every three years when your ATO expires. The routine security-control monitoring and remediation that occur after an application has been authorized to operate often includes a combination of automated diagnostic services such as vulnerability scanning, patch management, intrusion detection and prevention, and system and application event log collection and analysis. Additionally, every year system owners must conduct an annual assessment (AA) that follows NIH guidance to review approximately 1/3 of the total controls that may apply to a system. System owners are also required to actively manage their plan of action and milestones (POA&M) to remediate weaknesses in a timely manner, and to seek re-authorization every three years.

Annual Assessments

The NIH SA&A policy requires application owners to assess approximately 1/3 of the applicable controls each year. The list of controls is chosen by NIH each year and is available upon request from the NCI ISSO.

Security Impact Reviews

If you make a significant change to your application, you are advised to document the changes and possible impacts to the security posture of the application in a security impact analysis (SIA). Any controls that may be impacted may need to be re-tested to ensure the security posture is not reduced.

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 remediation progress. New findings that are generated from ongoing security assessments and risk impact reviews should be added to the POA&M as it is a living document.

Ongoing Authorization or Reauthorization

The NIH is currently developing its ongoing authorization (OA) model for externally hosted applications. Because of the numerous technical challenges associated with automating security analyses and remediation activities to fully replace manual checks and testing, this process will most likely include a hybrid of automated and manual activities. Please check back in the future for updated information on ongoing authorization.

Re-authorization decisions are made based on performing the required annual assessments, remediating POA&M-identified weaknesses in a timely manner as outlined in the POA&M Milestones, ensuring vulnerabilities in the application are remediated according to the NIH remediation standard, and demonstrating the you have reviewed and updated necessary documentation in accordance with the NIH review time frames.