FISMA Assessment and Authorization (A&A) Guidance

A&A Introduction

Welcome to the NCI Information System Assessment and Authorization (A&A) information and guidance page. The information provided here is intended to supplement guidance provided by the National Institute of Standards and Technology (NIST) and NIH to provide best practices for managing the A&A process (A&A was formerly called security assessment and authorization (SA&A) and certification & accreditation(C&A) before that).

Government project officers are responsible for ensuring their contractor-hosted or cloud-hosted applications are authorized to operate (ATO) in accordance with FISMA. This includes all planning, testing, and continuous monitoring activities associated with the system's life cycle. Most importantly, this means that you are responsible for securing the resources to conduct required security testing, which for moderate impact systems means using an independent third party assessor qualified to conduct FISMA/FedRAMP audits. NCI CBIIT does not develop required FISMA/FedRAMP security documentation (except for assisting with the FIPS-199, e-Authentication, and Privacy Impact Assessment), or conduct any of the security testing for applications that are operated exclusively at contractor locations or hosted in the cloud. The extent of CBIIT's support for exclusively contractor- and cloud-hosted systems is advisory only.

A&A is the methodology by which an organization establishes and then demonstrates sound, risk-based security posture for a specific system. We hope that the information provided on the following pages is useful to a variety of users including NCI information system owners, project officers and mangers, contracting officers, software developers, security officers, and security practitioners. It is intended to help you better understand, plan for, and execute the A&A process as it applies to your situation (i.e., based on your system's operating location), along with the requirements and expectations for completing the A&A. We have also tried to provide you with the tools, templates, and guidance to facilitate the A&A process.

Who is this information intended for?

The following pages are intended for individuals associated with the design, development, implementation, operation, maintenance, and disposition of NCI systems hosted by a third party (e.g., hosting contractor, university, hospital, cloud service provider, etc.). This typically includes, but is not limited to: System owners, business owners, program and project managers, procurement officials, IT contractors (hosting providers), system developers, and security practitioners.

What is a "Federal Information System" (and what isn't)?

Before getting into specific A&A process and guidance, it is first helpful to review exactly what constitutes a "Federal Information System" so you know when FISMA or, perhaps, another federal security assessment frameworks (e.g. FedRAMP, CUI) may apply. The following definitions and clarifications are based on guidance provided by the Office of Management and Budget (OMB) as well as from subsequent interpretations by OMB on the matter.

OMB initially defined in 2001 a Federal Information System as: *A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual* (defined in OMB circular A-130, (6)(q)). OMB later clarified that Federal Information Systems are those that are used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency (44. U.S.C. § 3544(a)(1)(A)).

Since these definitions can be somewhat vague or confusing, many people often assume that a federal information system only includes those that are physically housed and/or operated within a federally-owned or federally-operated facility (i.e., government-owned/government-operated (GOCO)), and that any other information system that is housed elsewhere (i.e., at a contractor's location, at a hosting provider's location, or in the cloud) are not federal information systems. This is not necessarily the case. In fact, a better determination of federal system vs. non-federal can be made by examining accountability for and control of a system's information, and whether the government directed the establishment of the system. For example, if the government has directed or mandated (e.g., through a contractual arrangement or other means of federal support), the creation or operation of an information system, or if the government will have access to the system or will take possession of the data in the system, it is probably a federal information system. Contracting with a non-federal organization to host or operate your system does not exclude the system from federal regulations. If you are uncertain about whether yours is a federal information system, please contact the NCI ISSO's office for clarification.

The following examples are for illustrative purposes and are not exhaustive.

Federal Information System	NOT a Federal Information System
Website(s) used to collect or publish information by or on behalf of the federal government (regardless of the type or sensitivity of information collected, processed, or stored).	Websites operated by third parties, independent from any government organization (e.g., they do not collect, store, or process any information for or on behalf of the federal government).
Web application/N-tiered application used to collect or publish information on behalf of the federal government. This includes client-server architectures where remote access is possible.	Desktop productivity tools (e.g., Microsoft Office tools, WordPerfect, FileMaker Pro desktop version, MS Access)
An enterprise database system (e.g., Oracle, SQL, Postgres) that contains federal government records. Note that even an MS Access or FileMaker Pro database, which is normally considered a desktop tool rather than a system, could be considered an information system if it is not limited to use by a single user and if it provides a remote/web user interface that could allow multiple people to access the data.	A Microsoft Access database operated on a single workstation, and that does not provide a remote access user interface (i.e., it is not web enabled and is only accessible form the local workstation).
A centrally managed and automated system (collection) of Adobe PDF forms that has been web-enabled to allow users remote access and modification of the forms.	Adobe PDF files kept on a local user's desktop computer or on a networked file share drive.

General Support Systems (GSS) (e.g., enterprise network environment, data center, enterprise database system, enterprise e-mail environment, etc.) used to support federal information and federal technology resources.	User files that are kept in a network file share or network attached drive for the purpose of online storage and backup. (Note that you should never store sensitive or patient related information in group or public file shares without first checking the security policy and checking with your information security officer)
Any externally operated system where the federal government has a contractual arrangement or expectation to access or receive the data stored therein. That is, data that is not owned solely by the external organization but is collected on behalf of or for the benefit of the federal government.	Third Party Websites and Applications (TPWA) as defined by HHS and on the approved TPWA list. TPWAs are usually subscription based applications like Facebook, Flickr, GitHub, YouTube, Twitter, IdeaScale, Survey Monkey). To view the full list of currently HHS approved TPWAs, go here.
Any cloud based website or system that that collects, stores, or processes information on behalf of the federal government. Note that cloud systems also must abide by FedRAMP.	

**Please note that even if yours is not an IT system, federal privacy and OMB regulations may still apply, especially if you are collecting information from private citizens or contractors, including, for example, through online or paper surveys, via clinical trials, etc. You should always consult the OMB clearance office and the NCI Privacy Coordinator for additional guidance.*

Overview of FISMA and A&A

The Federal Information Security Modernization Act (FISMA) of 2014 mandates that all federal information systems — including all NCI information systems — must be formally assessed and authorized to operate (ATO) using the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). The RMF is the model used to conduct federal system assessment and authorizations (A&A), so the terms RMF and A&A may be used interchangeably. NIST documented the RMF in Special Publication 800-37 rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. The RMF is also supported by several additional NIST special publications (SP) guides that are designed to work in conjunction with 800-37 rev. 2. To further help system owners implement the RMF, NIH and NCI have also developed agency-specific A&A guidance, templates, and sample materials, which are discussed in the following A&A process guidance pages.

NIST Risk Management Framework

NIST's Risk Management Framework (RMF) is the security risk assessment model that all federal agencies (with a few exceptions) follow to ensure they comply with FISMA. The RMF is formally documented in NIST's special publication 800-37 (SP 800-37) and describes a model for continuous security assessment and improvement throughout a system's life cycle. The RMF comprises six (6) steps as outlined below.

Step 1 — Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis. FIPS-199 provides security categorization guidance for non-national security systems (CNSS Instruction 1253 provides similar guidance for national security systems). NIH also requires in this step the completion of the e-Authentication Risk Assessment (eRA) and the Privacy Impact Analysis. Together, these three documents define the security baseline for the system, determine what level and type of identity and access controls are needed to protect the system, and determine if any information in the system falls under the Privacy Act (as amended) regulations.

Step 2 — Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions. NIST Special Publication 800-53 provides security control selection guidance for non-national security systems. CNSS Instruction 1253 provides similar guidance for national security systems.

NIST 800-53 groups security controls by families (e.g., Access Control (AC), Auditing (AU), Risk Assessment (RA), etc.) as well as by impact classification (e.g., Low, Moderate, and High) to help identify the proper controls required for each system.

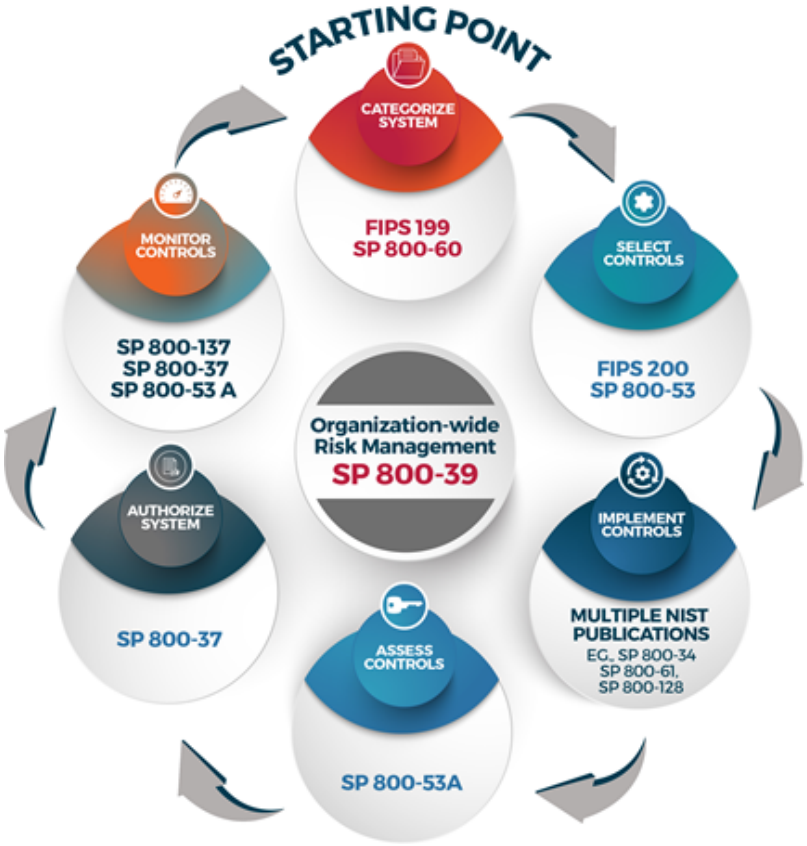
Many of the controls found in 800-53 can also be tailored with organization-specific guidance such as specific password policies, access control policies, and the like. In order to assist system owners with the security control identification and selection process, NCI has developed multiple security control inheritance guides based on hosting environments (i.e., CBIIT hosted, third party hosted, other NIHnet hosted, etc.) to help owners select controls for their system.

Step 3 — Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

Step 4 — Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Step 5 — Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Step 6 — Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.



One of the fundamental tenets of NIST's risk based approach to security throughout the life cycle is that system owners must balance the requirement to protect agency information and assets (i.e., its federal systems and data) against the cost/benefit of implementing and maintaining appropriate security controls when compared to not implementing such controls and strategies. In other words risk management should be cost-effective. This is an important concept to keep in mind when you are faced with tough decisions about when and how to implement certain security controls. Whenever you have a question about such choices, the NCI ISSO and the Information Resource Management (IRM) team are here to help you make the appropriate choices and provide the necessary guidance.