skyhigh

FISMA Compliance Cheat Sheet

The Federal Information Security Management Act (FISMA) was signed into law in 2002 as part of the Electronic Government Act. Recognizing that both the national and economic security of United States is grounded on having a robust information security infrastructure, FISMA compels each federal agency to build and implement programs to ensure the security (confidentiality, integrity, and availability) of the agency's information. The law applies to all federal agencies, their contractors, and anyone else that handles the information used to support the operations of the agency.

FISMA relies on the security categorizations and definitions provided by FIPS (199, 200) in order to fulfill its goal of ensuring confidentiality, integrity and availability of federal information.

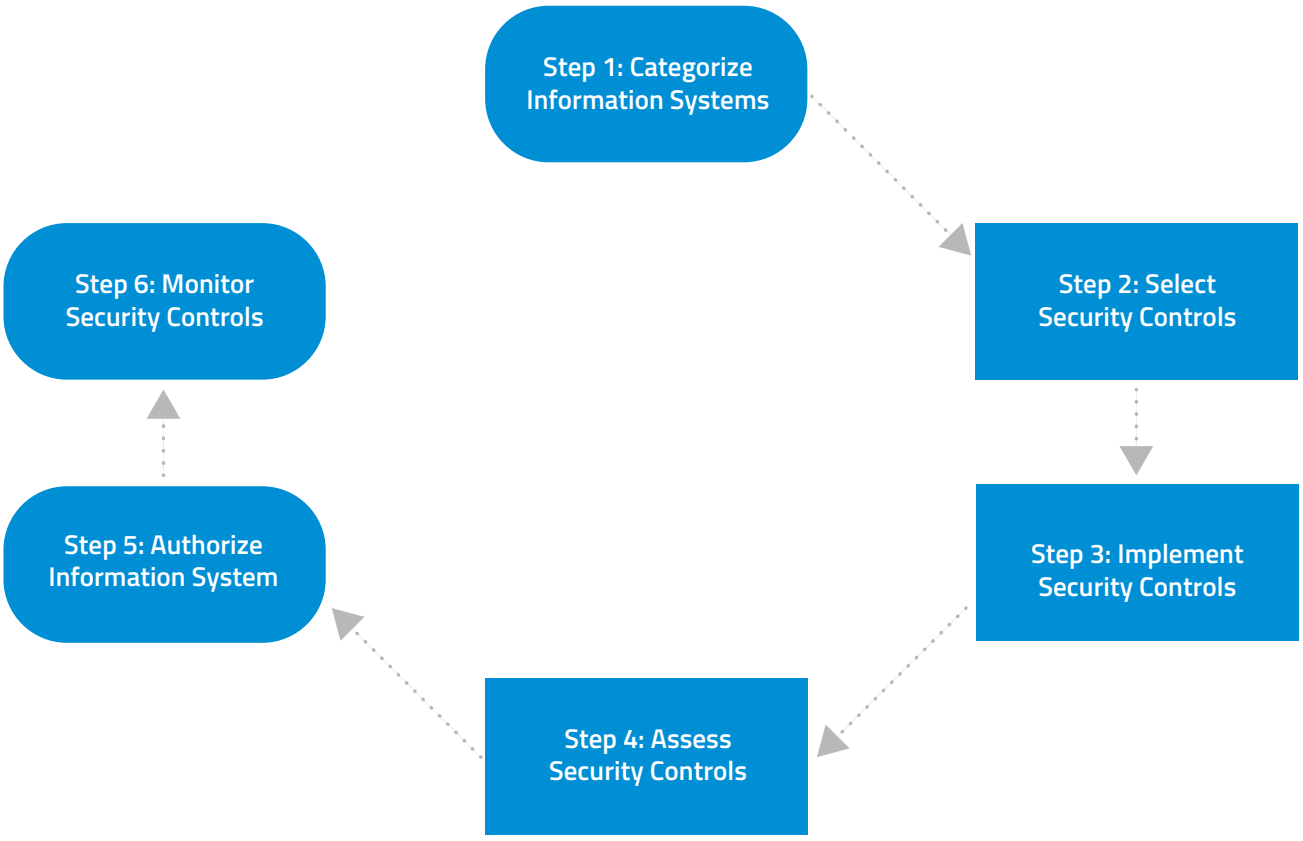
Security Dimension	FISMA Definition	FIPS Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."	"A loss of confidentiality is the unauthorized disclosure of information."
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."	"A loss of integrity is the unauthorized modification or destruction of information."
Availability	"Ensuring timely and reliable access to and use of information."	"A loss of availability is the disruption of access to or use of information or an information system."

The introduction of FISMA gave the National Institute of Standards and Technology (NIST) the authority to develop the necessary guidelines to create programs that ensure acceptable information security and risk management practices. In 2014, FISMA was amended with Public Law 113-283 which made the secretary of the Department of Homeland Security (DHS) responsible for administering the implementation of programs that ensure federal information system security. The amendment to the law also requires, among other things, that agencies notify Congress of major security incidents within seven days of discovering it.

NIST's Risk Management Framework

One of the primary objectives of FISMA is that the robustness and extent of information security controls should be commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of any information maintained by an agency or a contractor maintaining agency data. This puts a high importance on the ability to accurately implement risk assessment programs. When successful, such application of security controls can be highly efficient and cost effective.

To that end NIST developed the Risk Management Framework, which attempts to define all FISMA-related security standards and guidance to facilitate the creation of a broad and balanced information security program at each agency. Since management of agency-wide risk is a primary component of an information security program, NIST has outlined a 6-step process to effectively assess risk and implement security controls in line with the magnitude of the risk.



1. CATEGORIZE INFORMATION SYSTEMS

Categorization offers a logical means by which to assess the importance and sensitivity of the data being stored, transmitted, and processed by a system. The security category corresponds to the potential damage (worst case) an agency could incur if an incident occurs. Specifically, the risk to the agency's ability to protect its assets and individuals, fulfill its legal responsibilities, and maintain day-to-day functions. An owner (usually the information systems owner) is assigned to the information and information system, who is then responsible for assigning a security impact value (low, medium, high) for the security goals of data privacy, integrity, or availability.

FIPS Publication 199, along with NIST Special Publication 800-60 Volume 1, 2 defines security categories for both information and information systems and provides a guide to mapping the types of information to security categories. Standardizing security categorization provides a common framework for security that encourages better management and oversight of IT security programs.

Once the security impact value is determined, the appropriate set of security controls are selected based on the impact value.

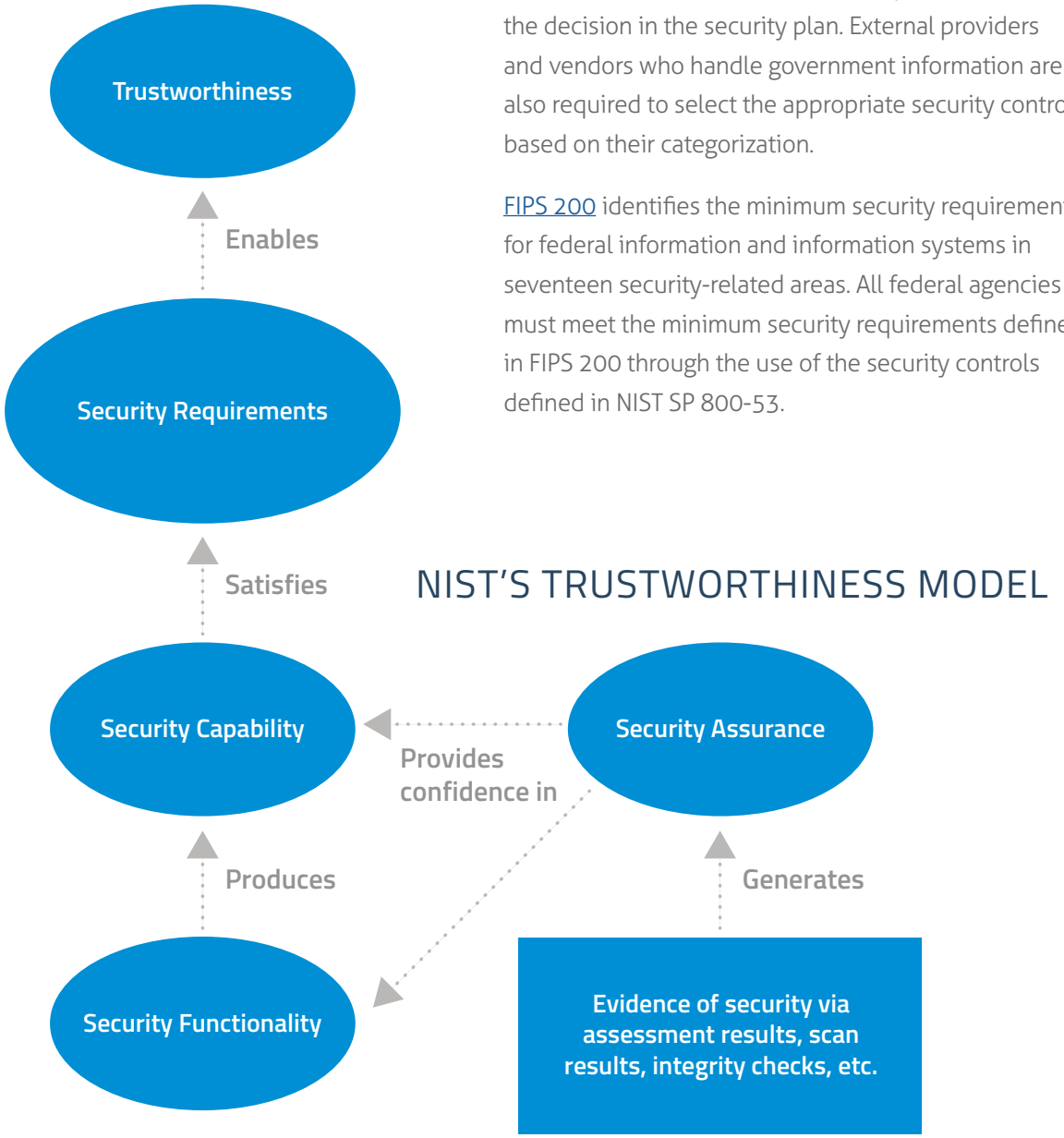
Potential Impact	FIPS 199 Definition
Low	"Any loss of confidentiality, integrity, or availability would have negligible adverse effect, which means 'the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.'"
Medium	"Any loss of confidentiality, integrity or availability would have medium adverse effect, which, according to NIST, means 'the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.'"
High	"Loss of confidentiality, integrity or availability would have high or catastrophic adverse effect if it leads to a 'severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.'"

2. SELECT SECURITY CONTROLS

Once an information system has been categorized, the federal agency is then required to procure/build appropriate security controls based on the results of the previous step. The security controls should provide reasonable assurance that the information systems will be protected from compromise. The right security controls will ensure the continuation of the day-to-day agency activities so that the agency can fulfill its mission and security controls should be cost-effective. In other words, the controls should be tightly related to the information system category and the impact score.

NIST's Risk Management Framework defines the concept of an information system owner and an information system architect. The system owner is the person who selects and supplements the security controls as needed as well as obtains approval for the selection. The system architect is responsible for making sure that the selected security controls is consistent with the architecture, including "reference models and segment and solutions architectures." In general, the information system owner and the information system architect will work together to select the appropriate security controls and document the selection process and justify the decision in the security plan. External providers and vendors who handle government information are also required to select the appropriate security controls based on their categorization.

FIPS 200 identifies the minimum security requirements for federal information and information systems in seventeen security-related areas. All federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls defined in NIST SP 800-53.



NIST'S TRUSTWORTHINESS MODEL

NIST Special Publication 800-53 provides guidelines for selecting security controls. This document also defines the risk assessment, security assessments, physical and environmental security, maintenance, access control, accountability, audit, etc. NIST uses the "Trustworthiness" model to satisfy the security requirements of the controls.

3. IMPLEMENT SECURITY CONTROLS

The effectiveness of the security control depends, in large part, on whether they are implemented correctly. For this reason, agencies are required to document the design, development, and implementation details of the controls. The selected security controls should utilize common controls when appropriate and agencies should look to use best practices when implementing the security controls within the information system including system and software engineering methodologies, security engineering principles, and secure coding techniques while staying consistent with the agency's enterprise architecture and information security architecture.

4. ASSESS SECURITY CONTROLS

This step is intended to validate whether the security controls implemented in the previous step are adequate in accomplishing their intended goals and whether they're implemented as such.

Federal agencies should use the NITS Special Publication 800-53A to create an assessment process and procedure, which should be derived from:

- The security categorization of the information system
- The required assurances the agency needs to find the security controls adequate
- The selected security controls

The information that is gained from the assessment process should then be used to:

- Pinpoint potential problems with the implementation or selection of the security controls
- Identify weakness in the information systems
- Inform capital investment and resource allocation

IMPLEMENTATION TIPS

1. The implementation of common security controls (controls that when implemented correctly, can be inherited by other information systems within the agency) are most effective when done organization-wide with involvement from senior leadership (CIO, CISO, risk executives) whose collective knowledge of the agency architecture can lead to a successful implementation.
2. When implementing common controls, realize the inherent risk from using the same technology across multiple information systems and understand a vulnerability or breach in one system could mean multiple systems would also be exposed to compromise.
3. Providers of common controls must keep the underlying technology up to date and must have the capability to rapidly propagate changes to the common controls across all the information systems using it.

Before the assessment process begins, agencies must ensure that a set of policies that will guide the security assessment process are in place, all the steps within the Risk Management Framework have been completed and approved that come before the assessment step, and a specific objective and scope for the assessment have been determined.

5. AUTHORIZE INFORMATION SYSTEM

Once the assessment step has been completed, a plan of action must be created based on the findings of the security controls assessment. The plan of action will include specific tasks intended to correct the weaknesses or inconsistencies discovered during the assessment step.

In cases where weakness are remediated during the assessment step, a plan of action may not be necessary. The plan of action must take into account:

- The security categorization of the information system
- The weakness or shortcoming in the security controls
- The impact of the weakness

Agencies must create an authorization package, which contains 1) the security plan, 2) the assessment results, and 3) the plan of action derived from the assessment result. Authorizing officials must make risk-based authorization decisions based on this package. The official will determine the risk to the agency and the information system and either accept the risk or reject it and propose additional changes.

6. MONITOR SECURITY CONTROLS

Since an agency's technology and security stack is in a constant flux, agencies must adopt a continuous monitoring mindset. This means both monitoring the security controls and systems, as well as documenting proposed or actual changes and subsequently assessing and authorizing the changes needed, thus creating a feedback loop that restarts the Risk Management Framework at step one.

Agencies must conduct ongoing remediation actions based on the results of their continuous monitoring and the assessment activities. As the need for remediation arises, agencies must revisit their security plan, security assessment reports, and generate new plan of action documents.

Monitoring security controls must also include regular security status reports generated by the primary information system owner and supported by the information system security officer, whose primary role is to support the information system owner to complete security responsibilities and participate in the formal configuration management process.