THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

11/28/17

FISMA Compliance Handbook

For UAB Researchers and Supporting Staff

UAB ENTERPRISE INFORMATION SECURITY OFFICE
UNIVERSITY OF ALABAMA AT BIRMINGHAM

Document Revision History

Date	Description	Version	Author
6/23/2014	Initial version of the handbook	1.0	UAB Enterprise Information Security Office
9/18/2017	Minor updates to content and links in Appendix A	1.01	UAB Enterprise Information Security Office
11/28/2017	Minor updates to content	1.02	UAB Enterprise Information Security Office

Table of Contents

1. Executive Summary

This handbook serves as a reference document for University of Alabama at Birmingham (UAB) principal investigators (PI) and researchers interested in federally funded research opportunities. It is designed to provide an introduction to the Federal Information Security Management Act (FISMA) of 2002, explain how that law applies to research contracts and grants, and detail the steps that researchers working with federal data must take to meet the FISMA-specific requirements detailed in their grants and contracts.
The key tasks in the process include:

- ❑ Determining whether the contract or grant includes FISMA requirements.
- ❑ Determining whether the sponsoring government agency requires that FISMA compliance must be met.
- ❑ Creating a project plan if compliance is required) and, in that case, determining whether the research organization can achieve FISMA compliance on its own or will require assistance.
- ❑ Budgeting appropriately to develop and implement the required security controls.
- ❑ Following the six-step process detailed in the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) to create a FISMA-compliant environment for the research project.

Achieving FISMA compliance involves implementing both technology-based and procedural controls — it is not just a technical solution. Business processes and procedures, along with security controls, will be developed, evaluated, and documented to create a more secure environment aimed at protecting the research project and its valuable data. The thrust of the documentation that is created and maintained is to provide assurance to both the contracting federal agency and independent auditors that the controls are in place, proper procedures are being followed, and the combination of controls and procedures are effectively protecting the research data.

This handbook is designed to provide a bird's-eye view of the process, from discovery of FISMA language in a contract, through information system and security control design, to auditing, authorization, and continuous monitoring. Appendix A provides references and links to documentation for readers who prefer more in-depth information. Appendix B contains a checklist of deliverable documents tied to the FISMA process. Appendix C details key actions required during each phase of the FISMA process. Appendix D contains a glossary and list of acronyms used in this document.

In addition to the information provided in this handbook, security engineers from the Risk Management and IT Compliance team in the UAB Enterprise Information Security Office (EISO) are available to provide guidance regarding FISMA requirements and compliance. Contact the EISO at 975-0842 or e-mail the Risk Management and IT Compliance team at DSO-RiskMgt@uab.edu.

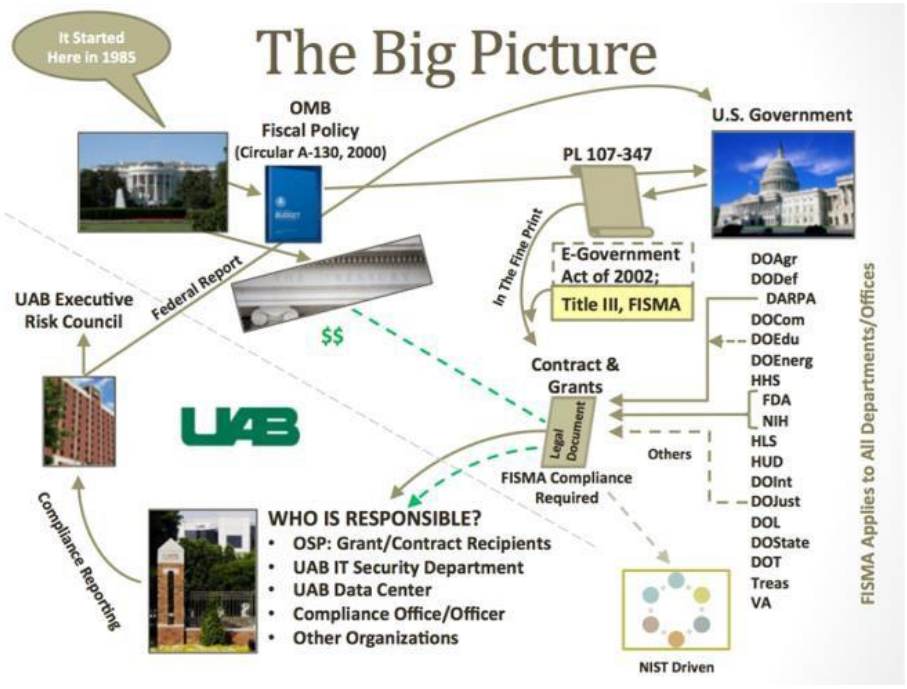

Figure 1: Creating a FISMA-compliant environment requires contributions from numerous sources, both locally and federally.

2. What is FISMA?

FISMA is a federal law that requires the implementation of specific sets of security controls for information systems that process, transmit, or store federal data. This mandate covers government agencies, such as NIH, NASA, the CDC, the EPA, and many more. FISMA compliance also trickles down to the contracting agents or grantees that work on behalf of these government entities. As a major research institution, UAB is awarded such contracts or grants and, as a result, its researchers can fall under the FISMA umbrella. Because it is a federal law, FISMA compliance is mandatory and UAB researchers must meet the minimum security controls prescribed by FISMA if the federal agency and the contract or grant specifies that the researcher must meet those FISMA requirements.

These security controls are designed to protect the confidentiality, integrity, and availability of information systems funded by the federal government. Much like research protocols assure the quality of the research being performed, the FISMA-specific processes are implemented to provide a high degree of assurance that the information systems interacting with federal data are adequately protected and performing properly.

3. FISMA is a Technical Solution, Right?

When one thinks of “information systems” or “information security,” it is easy to focus solely on technology. However, that is just one component of the FISMA equation. A significant portion of the controls is implemented outside of the technical realm. Such controls apply standards that govern how processes and procedures related to the researcher’s mission can be conducted in a more secure, compliant manner. Other non-technical controls govern how physical information system

assets are protected, such as servers being housed in a locked room with backup power supplies attached to them.

There also is a significant amount of FISMA documentation that must be created and updated during the lifecycle of the contract or grant. It is not just an exercise in paperwork, though. There are significant information security benefits to be gained by creating and operating a FISMA-compliant environment.
The primary benefits of these controls include:

- ❑ Helping ensure that a researcher's data remain confidential, which will be necessary if the research data include private health information (PHI), personally identifiable information (PII), intellectual property, proprietary information, and other forms of sensitive information.
- ❑ Creating an environment that protects the integrity of the research data and decreases the chance that the data might be maliciously or accidentally altered, or even lost.
- ❑ Providing assurance that the research data collected are regularly backed up and both the data and the associated information systems themselves will be available when needed.

4. How Difficult is this Going to Be?

Creating a FISMA-compliant environment is not as bad as some people make it out to be. There will be learning curves to tackle during the process, though. A culture change often is required to adapt to a new way of doing business. In fact, the culture change might be the biggest hurdle the organization faces. Also, there is a large amount of work that needs to be done. However, there are resources that can be used to help a PI navigate the road to FISMA compliance. This handbook, for example, is one such resource. UAB's Risk Management and IT Compliance team also can provide a variety of services. Other resources that can provide insight include the Authorizing Official (AO), the Information System Security Officer (ISSO), the Contracting Officer, and the Program Director of the federal agency awarding the contract or grant. These officials can provide more information regarding agency-specific FISMA deadlines, deliverables, and additional tasks that might be required.

In the end, going through the initial process will provide assurance that research data is being protected sufficiently. Also, once the FISMA-compliant system is in place, researchers will have laid a FISMA foundation that only needs to be maintained or updated for future contracts and/or grants.

One thing to keep in mind at the outset of this process is this: The cost of providing ongoing assurance of the confidentiality, integrity, and availability of the researcher's information system is an expensive business that must be planned for and maintained. In fact, early planning and budgeting are key actions that can be taken to define the project's scope and requirements, determine priorities, and create a schedule of tasks, deadlines, and deliverables. Remember, FISMA systems will cost more than non-FISMA systems, so calculate associated expenses early and budget before applying for the contract or grant, if possible.

When evaluating a new research effort or preparing to renew an ongoing effort, please start planning for compliance and factoring it into your budget. There is no good rule of thumb yet at UAB for how much a project costs. That said, if a new effort is similar to an existing effort, UAB will attempt to leverage as much experience between the two projects and common controls to help researchers save costs and implementation time.

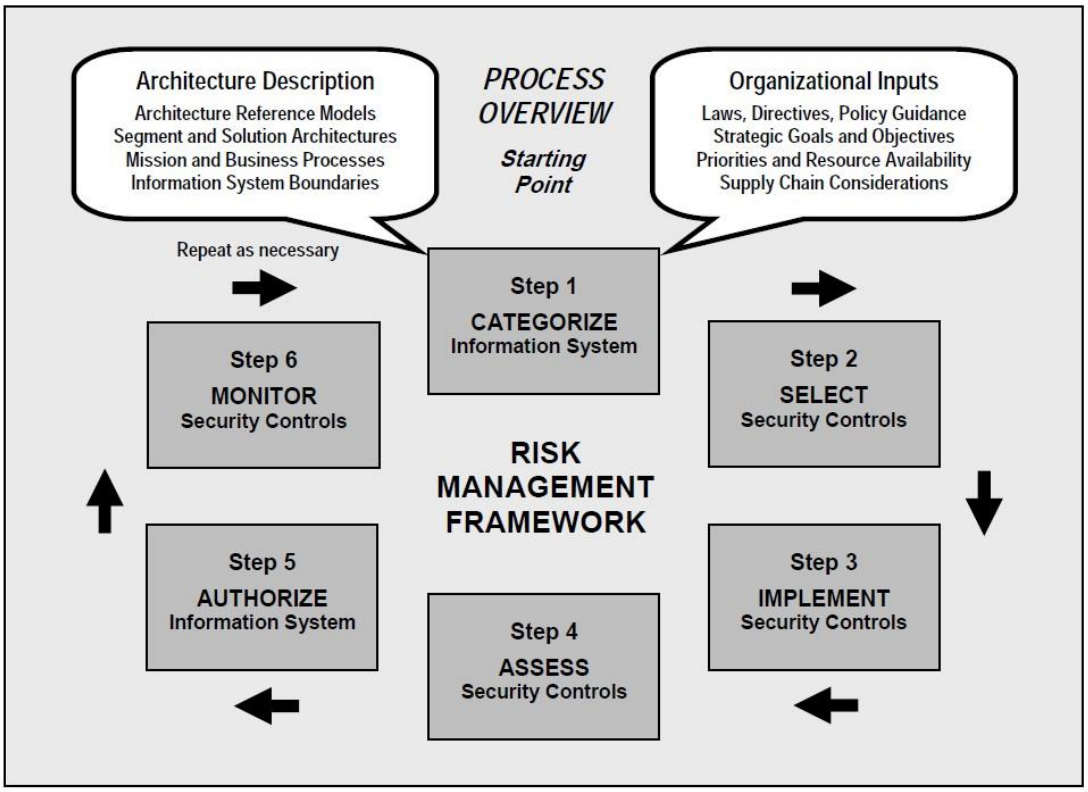

Figure 2: The FISMA process, as defined by the National Institute of Standards and Technology (NIST), is a six-step process.

5. The FISMA Process

The FISMA process is based on the Risk Management Framework (RMF) defined by NIST. This framework, illustrated above, is designed to create a repeatable process that accomplishes the following tasks:

1) Categorize the sensitivity of the researcher's data and the information system, followed by the enumeration of risks that may compromise the confidentiality, integrity, and availability of both the data and the information system.
2) Select a specific set of security controls based on the sensitivity of the data and implement these controls while architecting the information system during the software/system development life cycle (SDLC).
3) Implement and test the security controls as the information system is built.
4) Assess the performance and effectiveness of both the information system and the security controls to provide assurance that they are working as intended.
5) Gain authorization and approval from the contracting/granting agency for the information system to begin processing, transmitting, and storing federal data to accomplish the research mission.
6) Continuously monitor the security controls to ensure they are effective during the life cycle of the information system.

The risk management tasks should begin early in the SDLC. Identification of security requirements early in the system design will provide the opportunity to implement the controls during the construction of the system, which is much more cost effective than trying to "bolt" security on to the information system during later stages. The cost to redesign and implement security controls later in the life cycle is much more expensive, less effective, and might place more constraints on users of the system.

For more on the RMF, refer to NIST Special Publication 800-37 in Appendix A.

6. Where Do I Begin?

When evaluating a new research effort or preparing to renew an ongoing effort, start by discovering whether FISMA-specific language is included in the terms of the federal contract or grant. Such FISMA-specific language often appears in the special contract requirements or security requirements sections of those documents. Look for references such as the following:

- ❑ IT Security Plan or System Security Plan (IT-SP or SSP)
- ❑ IT Risk Assessment (IT-RA or RA)
- ❑ FIPS 199 and FIPS 200 Standards
- ❑ NIST Special Publications (SP) 800-26, 800-30, 800-37, and/or 800-53
- ❑ Federal Information Security Management Act (FISMA)

If you find references to one or more of these topics, your research project might require FISMA compliance, but it's not a guarantee that compliance is mandatory. Some government agencies write overly broad contracts/grants that include FISMA language even though it is not applicable to the contractor/grantee. For example, FISMA compliance is required if federal data is being stored, processed, and/or transmitted by a contractor/grantee. If your research project does not store, process and/or transmit federally owned data, you likely will not be required to meet FISMA information security requirements even if your contract/grant includes FISMA-specific language.

If you discover FISMA requirements in your contract or grant, the best course of action to determine whether compliance applies to your research project is to reach out to your primary contact at the sponsoring government agency tied to the contact or grant. Ask him/her for clarification regarding how the FISMA language should be interpreted. If FISMA compliance is required, you can contact UAB's Enterprise Information Security Office (EISO) at 975-0842 or DSO-RiskMgt@uab.edu and request additional guidance in meeting FISMA's information security requirements.

Security engineers from UAB's Risk Management and IT Compliance team are available to provide guidance regarding the following:

- ❑ Meeting FISMA requirements.
- ❑ Planning and executing the project.
- ❑ Helping ensure that the proper security controls are incorporated during the SDLC.
- ❑ Providing examples of the deliverables required by the contract.
- ❑ Serving as subject matter experts to answer questions a PI might have.

Seeking input from these security engineers early in the planning process can eliminate confusion and potential wasted effort on the part of the research organization. Such input also can help narrow the scope of the project, aid in the creation of a project plan to follow, and lead to a reduction in costs due to wasted time or resources.

As for the initial planning aspect of the project, the contract or grant will provide deadlines for specific deliverables and milestones. These deadlines also should be enumerated in the "Special Contract Requirements" section of the contract, likely using terms similar to the following:

An IT Risk Assessment (IT-RA) and FIPS 199 Assessment shall be due within 30 days after the contract is awarded. The IT Security Certification and Accreditation (IT-SC&A) shall be due within 3 months after the contract is awarded.

If FISMA requirements must be met and deadlines are set, an extension to the deadlines can and should be negotiated by the PI. This may occur before the contract's terms and conditions are settled and the contract is signed. Alternatively, a PI may simply rely on the change order process to extend a deadline, or deadlines. This second option is viable, but it provides no guarantee that the federal agency will approve the request for a deadline extension.

If FISMA requirements don't apply to the contract or grant, that does not mean there aren't any information security requirements at all. Your research project must still follow all UAB policies, standards, and rules related to information security and the protection of UAB-owned resources and data. For example, if your research project involves identifiable patient data, you also would have to abide by the security and privacy mandates derived from the Health Insurance Portability and Accountability Act (HIPAA). You also have to abide by all pertinent UAB policies, standards, and rules that apply to HIPAA. Finally, some government agencies include information security requirements that are specific to them and have nothing to do with FISMA. The National Institute of Health (NIH), for example, often requires that contractors and their staff complete annual security awareness training provided by NIH. Therefore, even if the sponsoring government agency informs you that FISMA is not required, there will be other information security requirements that must be met.

7. Titles, Roles, and Responsibilities

Before beginning the six-step process defined in the NIST RMF, take time to assign the roles detailed below to departmental or research staff members. FISMA requires that specific roles and responsibilities must be designated to ensure that specific security- and information assurance-related tasks are completed properly. The minimum roles that should be assigned are:

- **System Owner (SO):** The official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
- **Information System Security Officer (ISSO):** The individual who is assigned responsibility for maintaining the operational security posture for an information system or program.
- **System Administrators (SA):** Individuals assigned to design and operate the information system that will be storing, transmitting, and/or processing federal data.

A fourth role that will be referred to often is that of the Authorizing Official (AO), which is defined by NIST as a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations. This official will be a member of the federal agency that awards the research contract or grant. In essence, the AO is responsible for approving or denying the opportunity for a research organization's information system to manage federal data under the terms of the contract. This will be discussed in more depth later.

A key fact to remember is that some roles exist at both the federal and the local levels. For example, UAB Research Department A is awarded a grant from Federal Agency X. UAB Research Department should select an SO and ISSO from its department or research staff. These UAB staff members will coordinate with Federal Agency X's ISSO during the course of developing the researcher's FISMA-compliant information system.

8. Tasks, Deliverables, and Timetables

Step 1: Categorize the System

Once the roles have been assigned, Step 1 of the RMF can begin. According to NIST SP 800-37, this phase includes the following steps:

- ❑ Categorize the sensitivity of the data (Low, Moderate, or High) using FIPS Publication 199; for more on FIPS 199 and this process, refer to Appendix A.
- ❑ Use the data categorization to determine the information system security level (Low, Moderate, or High) using FIPS Publication 200; for more on FIPS 200 and this process, refer to Appendix A.
- ❑ Conduct a business impact analysis based on NIST SP 800-34, Rev. 1, and a risk assessment based on SP 800-30; for more on SPs 800-30, 800-34, and this process, refer to Appendix A.
- ❑ Gather requirements regarding how the information system will serve the research mission.
- ❑ Create an information system description (this process is detailed in SP 800-37).
- ❑ Begin drafting a System Security Plan (SSP) based on the sensitivity of the data and the information system security level determined by the steps taken via FIPS 199 and 200.
- ❑ Begin the SDLC by designing the information system, keeping in mind that security controls should be incorporated throughout the SDLC process.

Examples of how research data might be classified are given below:

RISK LEVEL	EXAMPLE DATA	RECOMMENDATION
Low	De-identified datasets, research on public information	Low and Moderate represent the broadest set of data classifications. UAB is targeting them for compliant environments. UAB's Data Classification Rule defines Sensitive and Restricted data as Low and Moderate, respectively.
Moderate	Social Security numbers, identified data sets, patient health info	
High	Schedule I controlled substances	Researchers with High data should identify a compliance research partner to host and provide all IT services for such projects.

Table 1: Examples of Data Classification

This step of the RMF determines the security requirements by considering the legislation, policies, directives, regulations, standards and organizational mission/business/operational requirements that apply to the data and the information system. This step also should be performed as part of the system design phase, where the requirements are determined. The system design should define both the system architecture and the information system boundaries that are within the scope of the project.

Step 2: Select Security Controls

Once the data sensitivity and information system security level are determined in Step 1, the appropriate security controls must be selected and added to the SSP. The controls are comprised of 19 families that provide security or information assurance. Those families are:

CODE	CONTROL FAMILY	CLASS	LEVEL IMPLEMENTED
AC	Access Control	Technical	Organizational*
AT	Awareness and Training	Operational	Organizational*
AU	Audit and Accountability	Technical	Organizational*
CA	Security Assessment and Authorization	Management	Organizational*
CM	Configuration Management	Operational	Organizational*
CP	Contingency Planning	Operational	Organizational*
IA	Identification and Authentication	Technical	Organizational*
IR	Incident Response	Operational	Organizational*
MA	Maintenance	Operational	Organizational*
MP	Media Protection	Operational	Organizational*
PE	Physical and Environmental Protection	Operational	Organizational*
PL	Planning	Management	Organizational*
PS	Personnel Security	Operational	Organizational*
RA	Risk Assessment	Management	Organizational*
SA	System and Services Acquisition	Management	Organizational*
SC	System and Communications Protection	Technical	Organizational*
SI	System and Information Integrity	Operational	Organizational*
PM	Program Management	Management	Institutional**
AP, AR, DI, DM, IP, SE, TR, UL	Privacy	Management	Institutional**

Table 2: FISMA Control Families

**Research organizations are only responsible for implementing controls from these families.*

*** UAB executives are responsible for implementing Institutional controls. Research organizations are not responsible for these.*

NIST Special Publication 800-53, Revision 4, groups the security controls above into three different frameworks that match the data and system security categorizations determined in Step 1 (Low, Moderate, or High). All of the families are represented in the Low, Moderate, and High frameworks.

Each of these frameworks represents the minimum controls that are required according to the Low, Moderate or High category that was determined in the first step. For example, if it is determined

that a project will be categorized with a Low standing, the FISMA-Low security controls detailed in SP 800-53 must be incorporated into the design of the information system. A FISMA-Moderate categorization, however, will include more controls and numerous "enhancements" to FISMA-Low controls in order to better protect the information system and its associated data.

Notice in the paragraph above that each of the Low, Moderate, and High set of controls is referred to as the "minimum controls that are required" for each level. Does this mean that a FISMA-Low information system might require more controls than what is considered the Low baseline set of controls? Yes. A system might be considered Low but, due to regulatory governance or contractual obligation, additional controls might be incorporated with the Low control set.

For example, if a project includes medical devices that fall under the Federal Drug Administration regulations and contain patient data, that project also needs to comply with FDA and HIPAA regulations. The good news is many of the controls are the same, but may have specific privacy enhancements or other documentation requirements in order to provide the required assurance. In this example, the system might adopt the FISMA-Low controls with "overlays" that provide extra controls that pertain to FDA and HIPAA requirements.

When a control set is adopted, that set is added in the project's SSP, along with details regarding how all of the various controls will be implemented and enforced. So, if a System and Information Integrity control requires the use of anti-virus protection, that requirement would be added to the project SSP. Accompanying it would be an explanation that all desktop workstations, laptops, and servers used by the project are required to have anti-virus software than scans at least once a day.

Once all the controls have been added to the SSP, along with the proposed methods to enforce them, the organization has completed a first draft of the SSP that can be submitted to the federal agency's AO or ISSO for review. This provides two benefits to the research organization:

- ❑ It provides proof of a good-faith effort that the organization is making strides toward the goal of being FISMA compliant.
- ❑ It gives the federal official a chance to review how the controls are enforced. The official may provide feedback regarding potential changes to proposed controls early in the SDLC process. Making early changes is much more cost effective than making them late in the process.

UAB has SSP templates that were developed by the EISO and used to aid researchers in meeting their FISMA requirements. These templates can be used as a model and likely will speed up the process of developing an SSP. However, there are two pitfalls that must be avoided:

- ❑ Even though using SSP templates might speed up the creation of a new project's SSP, the development of the plan for a new project will take a significant amount of time. There are no shortcuts to be taken.
- ❑ There might be a temptation to simply copy and paste numerous elements from an example SSP into the SSP being written for a new project. This is a recipe for failure because the SSP must reflect the reality of how a specific information system is designed and controlled. An auditor assessing the information system will quickly realize when an SSP does not match reality, which might jeopardize whether a project is approved by an AO. This could kill the research mission.

Step 3: Implement Controls

By now, a draft of the SSP has been sent to the federal agency, the methods of enforcing the FISMA controls have been determined, and the design of the information system includes the way the technical controls will be incorporated. The information system itself is being built at this point.

However, remember that Section 3 explained that FISMA compliance isn't just a technical implementation of controls. At this point, the management and operational controls must be developed and implemented. That involves the writing of standards and procedures that create and enforce the management and operational controls detailed in the SSP.

The standard is the over-arching document that states the "who" and the "why" related to creating a control family. The procedures detail the "what" and the "how" in regard to how the standard will be implemented. For instance, a research organization will write a Risk Assessment Standard that will state the organization must annually examine the threats and vulnerabilities associated with the information system, along with the likelihood of adverse events happening and what the impact of such an event might be. Once the standard is in place, the organization must create step-by-step procedures detailing how that risk assessment will be carried out and what actions will be taken based on the results of the assessment.

Odds are, management and operational controls will be more difficult to implement than technical controls. Management and operational controls often go hand-in-hand with a significant culture change tied to business processes and user behavior. These changes stress compliance instead of convenience.

The key deliverables at this stage include the following:

- ❑ Deployment of the information system in an operational state that includes implementation of the technical controls in the production environment.
- ❑ A completed SSP that has been updated and reviewed since the initial draft was submitted to the federal agency in Step 2.
- ❑ Standards and procedures for the 17 control families highlighted in Table 2.
- ❑ Documents supporting the SSP and the standards and procedures (ex. — network diagrams, data flow diagrams, inventory lists of approved hardware, software, vendors, etc.)

All documents must be reviewed for accuracy to make sure they appropriately detail and enforce the required controls. Technical controls must be tested internally to ensure that they are working as intended. New processes/procedures must be followed. All controls must be monitored continuously to ensure they are effective and meeting their design objective. The evidence of the existence and operation of each control is used for the audit and verification phase that occurs in Step 4.

Step 4: Assess Controls

Once the first three steps of the RMF process are complete, an independent third party must audit the information system before it begins the research mission. This assessment is conducted to provide independent proof that all of the required FISMA controls have been implemented in accordance with the SSP and its associated standards and procedures. If the assessor finds any weaknesses in the controls, or a lack of controls in some areas, these findings will be documented so

that these problems can be addressed.

The auditor begins by first reviewing the organization's SSP, standards, procedures, and operations, and then tests the controls. Interviews are conducted with the SO, ISSO, and others that use or operate the information system. The auditor's assessment is documented in a Security Assessment Report (SAR).

Gaps or deficiencies that are identified in the SAR are detailed by the SO in a Plan of Action and Milestones (POA&M), which explains when and how the deficiencies will be corrected. This document must reflect staffing, budget commitments, and other factors required to provide a detailed plan focused on addressing weak or non-existent controls.

This independent assessment must be conducted every three years in order to verify to the federal agency that the researcher is accomplishing two important tasks:

- ❑ The quality of the controls is being upheld (or improved) during the lifetimes of both the contract/grant and the associated information system.
- ❑ Gaps or deficiencies are being addressed in order to improve the quality of the controls employed in the information system.

Conducting these assessments every three years is a double-edged sword. On one hand, much of the work performed for the initial assessment can be used for subsequent assessments. On the other hand, the research organization must keep detailed evidence that the controls have been enforced or improved since the previous audit three years ago. Letting things slide until three months before the next major assessment is due is a recipe for disaster. Strategies for addressing this potential pitfall are addressed in Step 6.

Step 5: Authorize System

The conclusion of Steps 3 and 4 will produce three key documents:

- ❑ The System Security Plan
- ❑ The Security Assessment Report
- ❑ The Plan of Action and Milestones

These three documents, along with a letter requesting an Authorization to Operate (ATO), must be submitted to the federal agency's AO for review. The AO will examine the quality of the controls in place, the independent assessment of the information system, and determine whether the remaining risk to the information system and the federal data is acceptable. If so, the agency will send an ATO letter to the research team to approve the operation of the system.

If the AO determines the risk currently is too high but can be reasonably reduced to lower levels, the research organization might be issued an interim ATO. In essence, this is a short-term ATO that allows the organization to operate while working to improve and/or implement additional controls to further reduce the risk to a level that is acceptable to the AO.

Finally, an AO might determine that insufficient controls create too great a risk to the federal data managed by the information system. In this case, the AO will not grant an ATO to the research organization, which likely will kill the research mission. Without an ATO, information systems are forbidden to use federal data while operating.

Step 6: Monitor Controls

At this point, an ATO has been granted, the information system has begun operating, and the research mission is underway. A common pitfall now is for the team to take a collective deep breath and say, "Whew, this FISMA stuff is over for a while." Actually, it's not.

There are a number of tasks that must be conducted by the SO, ISSO, and SA(s) during the three-year period between assessments. Examples of these tasks include, but are not limited to, the following:

- ❑ The security controls must be continuously monitored to ensure they are operating as intended.
- ❑ Weaknesses discovered and detailed in the SAR and POA&M must be addressed.
- ❑ Changes to the information system or its associated procedures must be documented.

The first question that might occur is, "Why do I have to do all of this? This sounds like a lot of work." It is a lot of work, but diligently monitoring the controls and changes to the information system provides three key benefits:

- ❑ The continuous monitoring activities provide assurance that the controls are effective (or even improving), and that the data and information system are being adequately protected.
- ❑ These activities provide evidence to both the federal agency and future assessors/auditors that the risk associated with the operation of the information system remains at an acceptable level.
- ❑ Successfully conducting the continuous monitoring phase translates into a significant reduction in the amount of work required for future assessments. This is both the greatest benefit and greatest motivator for diligently conducting continuous monitoring activities.

Here are key strategies that can be implemented during the continuous monitoring phase:

- ❑ Immediately update all associated documentation when changes are made to:
    - The information system
    - Standards and procedures that govern the FISMA project
    - Any supporting inventories of components or rosters of employees
- ❑ Review the documentation every three to six months to ensure that it reflects reality (for example, make sure that an employee who transferred to another project two months ago no longer has access to the FISMA information system and is no longer on the roster of approved users for the FISMA project).
- ❑ Review the POA&M on a quarterly basis to determine whether weaknesses discovered during the assessment phase are being remediated.
- ❑ Review the SSP on an annual basis to determine if the controls it details still provide an appropriate level of information assurance. If not, improve existing controls or implement new ones designed to provide the appropriate level of information assurance.
- ❑ Annually conduct in-house self-assessments that mimic the three-year assessment/auditing process. This measure can be used to determine how well the organization would do if an audit was conducted, and should reveal any control gaps. Such gaps can be addressed well before the next official third-party assessment, which will be needed to renew an ATO.

9. Can My Department Do This Alone?

Creating a FISMA-compliant information system and environment without outside aid is possible, but the required resources and time are likely cost-prohibitive for most research teams. However, there are solutions that can be developed by leveraging UAB resources and/or third-party service providers.

For example, UAB's Risk Management and IT Compliance security engineers can provide insight and guidance through every step of the FISMA process. These engineers also can examine proposed strategies or help develop roadmaps aimed at creating a FISMA-compliant environment for a research project.

Common strategies that are adopted by some organizations are:

- **The Solo approach:** The organization itself creates all of the documentation, designs and builds the controls and the information system, and conducts the continuous monitoring activities itself.
- **The Hybrid approach:** The organization itself creates all of the documentation, designs and builds the controls and the information system that are specific to its mission. The organization then secures a third-party to host the information system and provide additional controls. (For example, an organization designs and builds a research application and then has a FISMA-compliant third-party cloud provider securely host the application. In this scenario, the research department develops controls specifically for the application and inherits FISMA-compliant controls implemented by the cloud provider). Any third-party cloud provider must be approved in advance by UAB's Vice President of Information Technology.

As discussed earlier in this Handbook, gaining FISMA compliance requires a lot of work. However, there are significant benefits and researchers are not alone in their trek toward meeting a FISMA mandate.

UAB's Risk Management and IT Compliance team can provide assistance during this trek. For more information about FISMA compliance strategies and solutions, please contact UAB's Risk Management and IT Compliance team at 975-0842 or DSO-RiskMgt@uab.edu.

Appendix A: FIPS and NIST Documents

The table below provides links to the relevant FIPS and NIST PDF documents that are cited in this handbook or are helpful in developing FISMA artifacts.

DOCUMENT	TITLE	LINK
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	Link to NIST FIPS 199 Guidance
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	Link to NIST FIPS 200 Guidance
NIST SP 800-30	Guide for Conducting Risk Assessments	Link to NIST SP 800-30 Guidance
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems	Link to NIST SP 800-34 Guidance
NIST SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems	Link to NIST SP 800-37 Guidance
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program	Link to NIST SP 800-50 Guidance
NIST SP 800-53, Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations	Link to NIST SP 800-53 Rev. 4 Guidance
NIST SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans	Link to NIST SP 800-53A Guidance
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	Link to NIST SP 800-60 Guidance
NIST SP 800-61	Computer Security Incident Handling Guide	Link to NIST SP 800-61 Guidance
NIST SP 800-64, Rev. 2	Security Considerations in the System Development Life Cycle	Link to NIST SP 800-64 Guidance
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems	Link to NIST SP 800-128 Guidance
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	Link to NIST SP 800-137 Guidance

Appendix B: Checklist of Deliverables

The checklists below enumerate the various documents that must be created:

DOCUMENTS TO BE SUBMITTED TO THE AO		
❑ System Security Plan	❑ Security Assessment Report	❑ Plan of Action and Milestones

PRIMARY STANDARDS AND PROCEDURES DOCUMENTS	
❑ Access Control Standard and Procedures	❑ Maintenance Standard and Procedures
❑ Awareness and Training Standard and Procedures	❑ Media Protection Standard and Procedures
❑ Audit and Accountability Standard and Procedures	❑ Physical and Environmental Standard and Procedures
❑ Security Assessment and Authorization Standard and Procedures	❑ Planning Standard and Procedures
❑ Configuration Management Standard and Procedures	❑ Personnel Security Standard and Procedures
❑ Contingency Planning Standard and Procedures	❑ Risk Assessment Standard and Procedures
❑ Identification and Authentication Standard and Procedures	❑ System and Services Acquisition Standard and Procedures
❑ Incident Response Standard and Procedures	❑ System and Communications Protection Standard and Procedures
❑ System and Information Integrity Standard and Procedures	

SUPPORTING DOCUMENTATION	
❑ FIPS 199 and 200 Assessments	❑ Risk Assessment and Business Impact Analysis
❑ ISSO Appointment Letter	❑ System Interconnection Agreement Template
❑ Configuration Control Board (CCB) Charter	❑ List of Approved System Interconnections
❑ CCB Minutes Template	❑ System Inventory List
❑ Change Request Form Template	❑ List of Approved Hardware
❑ Security Impact Analysis Template	❑ List of Approved Software
❑ Network Diagram	❑ List of Approved Ports, Protocols and Services
❑ Data Flow Diagram	❑ List of Approved Vendors
❑ Media Transport/Destruction Form	❑ List of Approved Users
❑ Rules of Behavior for Users	❑ ATO Request Letter

Appendix C: Key Tasks for Each FISMA Phase

PHASE	TASKS
Initial Planning	• Determine whether FISMA language is included in the contract/grant • Contact UAB Enterprise Information Security and the federal agency's ISSO, Contracting Officer, Program Director, and/or AO for guidance and to determine whether FISMA compliance is required for the project • If possible, negotiate with the federal agency to set FISMA deadlines • Begin planning for compliance and factoring it into your budget • Assign SO, ISSO, and SA roles to staff members
RMF Step 1: Categorize the System	• Categorize the data and the information system (Low, Moderate, High) using FIPS 199 and 200 • Conduct the risk assessment and business impact analysis • Determine project requirements • Create an information system description and begin drafting an SSP • Begin the SDLC process by designing the information system and determining ways to protect the federal data it will use
RMF Step 2: Select Security Controls	• Select the appropriate security controls detailed in NIST SP 800-53 (Low, Moderate, or High) and add them to the SSP • Detail in the SSP how all of the controls will be implemented • Finalize a rough draft of the SSP and submit it to the federal agency's AO for review • Continue designing and building the information system; incorporate methods to enforce the controls into the system architecture
RMF Step 3: Implement Controls	• Write a rough draft of the standard and procedures for each of the 17 FISMA control families • Test the procedures to determine their effectiveness and update them, if required • Approve and adopt the final drafts of the standards and procedures • Complete the build process for the information system and its associated technical controls; Conduct internal testing of the information system and technical controls • Complete a final version of the SSP • Create the required supporting documents detailed in Appendix B • Review all documents and controls to ensure they are ready to be examined by a third-party assessor/auditor
RMF Step 4: Assess Controls	• Have a third-party assessor/auditor evaluate the effectiveness of the information system's controls • Develop a SAR and POA&M
RMF Step 5: Authorize System	• Draft an ATO Request Letter • Submit the SSP, SAR, POA&M, and ATO Request Letter to the federal agency's AO for review • If an ATO is granted, the research mission can begin
RMF Step 6: Monitor Controls	• Continually review the effectiveness of the controls • Address deficiencies detailed in the SAR and POA&M • Regularly update and review documentation • Conduct annual self-assessments of the controls • Undergo a third-party assessment every three years in order to renew an ATO

Appendix D: Glossary and Acronyms

This is a list of acronyms and FISMA-specific terms used in this handbook. The FISMA-specific terms are derived from NIST Special Publication documentation.

Assurance (or Information Assurance): Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediate and enforces the security policy.

Authorization to Operate (ATO): The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. An ATO must be issued to a research organization before it can begin working with federal data associated with a grant or contract.

Authorizing Official (AO): A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Availability: Ensuring the timely and reliable access and use of information.

Business Impact Analysis: An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control Board (CCB): A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.

EISO: UAB's Enterprise Information Security Office

FIPS: Federal Information Processing Standard

FISMA: Federal Information Security Management Act

Information: Any communication or representation of knowledge, such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Security Officer (ISSO): Individual who is assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Integrity: Guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity.

IT-SP: Information Technology Security Plan; see System Security Plan

NIST: National Institute of Standards and Technology

Personally Identifiable Information (PII): Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Plan of Action & Milestones (POA&M): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment (RA): The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Management Framework (RMF): A six-step process created by the National Institute of Standards and Technology, detailed in NIST Special Publication 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems*.

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

SSP: See System Security Plan

Security Assessment Report (SAR): This deliverable is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information from the assessor/auditor that is necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings.

Security Control: A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

System Owner (SO): Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

System Security Plan (SSP): Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.