UF Computing Environment for Restricted Data (CERD) System Security Package Handbook for Research Systems

Research Computing

Scott Crowell

Erik Deumens

Brian Parks

David Stricklin

Alicia Turner

Information Security Office

Avi Baumstein

Kurt Kauffman

Office of Internal Audit

Jeff Capehart

Office of Research

Terra Dubois

Published by the University of Florida (February 2018)

Contents

Introduction

The Federal Information Security Modernization Act (FISMA) of 2014 calls for federal organizations, and sub-contractors of federal organizations, to develop and maintain a set of practices and procedures to manage federal information and information systems. The act delegates responsibility for establishing information security guidelines and standards to the National Institute of Standards and Technology (NIST).

NIST developed a comprehensive set of documents, collectively called the Special Publication (SP) 800 series, to document US federal government computer security policies, procedures and guidelines. Although the NIST SP 800 series is written for the federal government, the publications are also used by private sector and academic institutions. The term “FISMA compliance” is often used to describe the process organizations go through to implement the NIST standards and guidelines.

The NIST publications provide recommendations for assessing and documenting system threats and vulnerabilities, and for implementing security measures to minimize the risk of adverse events. While the NIST publications describe best practices, and provide guidelines, they do not prescribe implementation checklists, task lists, or require specific products or features to be FISMA compliant. Thus, many books and consulting agencies are available to help organizations operationalize the NIST standards and guidelines to ensure FISMA compliance.

FISMA is written in a general way with the goal to have well-managed information systems that can be operated in a cost-effective manner to serve the mission of the organization. FISMA compliance is dependent on the organization’s mission, budget, in-house expertise and resources. Differences in these key areas directly impact planning and implementation of the NIST standards and guidelines, thus a FISMA implementation can vary greatly across organizations. For this reason, it is important to develop a “FISMA Handbook” to define the organization’s interpretation and implementation of NIST standards and guidelines. The FISMA Handbook documents the local processes, policies and procedures used to secure and manage information systems based on the organization’s needs.

Once the process for FISMA compliance is in place, the handbook serves as a framework and guide to meet other compliance requirements regarding the management of information systems that hold and process restricted data.

The University of Florida (UF) defines restricted data as data in any format collected, developed, maintained or managed by or on behalf of the university, or within the scope of university activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are

not limited to medical records, social security numbers, credit card numbers, Florida driver licenses, non-directory student records and export controlled technical data.

It is important to maintain secure systems to safeguard data, but it is crucial to have them when they contain restricted data.

The content of the handbook must address the following (Taylor, 2007):

- Background, purpose, scope
    - Mission served by the systems
    - Budget context for that mission
    - Risk analysis of the activities, the data, and the systems
- Overview of the process
- Requirements for secure implementations of the systems
    - Requirements for secure configurations
    - How to build secure systems
    - Security controls
    - Required security tests
    - Security assessment checklists
- Roles and responsibilities
- Threat and risk assessment guidelines
- Reference information
    - Regulatory citations
    - Associated internal security and privacy policies
    - Definitions of key terms and acronyms
    - Information on the requirements for Security Package documents

The initial law (FISMA 2002) and its revision (FISMA 2014) focused on information security requirements for federal agencies, and NIST SP 800-53 is the primary technical guideline for selecting controls that secure federal information systems (Ross, 2013). In 2010, Executive Order 13556 (Nov 4, 2010) established the Controlled Unclassified Information (CUI) program and delegated authority for administering the CUI program to the National Archives and Records Administration (NARA). NARA partnered with NIST to develop guidelines for federal agencies to ensure that sensitive or restricted information remains confidential when stored in nonfederal information systems and organizations, such as academic institutions. On September 14, 2016, NARA issued a regulation setting forth the specific policies and procedures for safeguarding, disseminating, controlling, and marking CUI. The regulation is effective on November 14, 2016. (Federal Registry, 2016) Additional information on NARA, CUI, FAR and DFARS programs can be obtained by visiting the links provided in Appendix A of this document.

As the result of another executive order 13636 (Feb 12, 2013) NIST wrote “Framework for Improving Critical Infrastructure Cybersecurity” https://www.nist.gov/cyberframework. This document provides a higher-level overview of the process of managing security for information systems laid out in the numerous Special Publications 800-series. It clearly states that it is an overarching guide to complement and add to the existing laws like FISMA) and guidelines provided by NIST. It is not an alternative, but rather it hopes to help people and organizations to better and more efficiently implement the existing guidelines and requirements and to integrate the security efforts into a risk management approach. An interesting point is that the executive order,

and as a result the document, make a point that privacy considerations and civil liberties are emphasized. One can think of the NIST Special Publications like 800-53, 800-171, 800-37, etc. as the basic materials for risk and security management. This document provides a general framework to read these and make a plan to implement the recommendations for your organization in a way that fits the mission and budget. As such, it fits between the NIST Special Publications and this handbook.

NIST published SP 800-171 to establish consistent guidelines for protecting federal information collected or stored in nonfederal information systems (Ron Ross P. V., 2015). NIST SP 800-171 follows the 800-53 "tailoring" process to customize the security and privacy requirements for nonfederal organizations to replace 800-53 controls that are not applicable or meaningful for nonfederal organizations with controls that are relevant for nonfederal organizations.

NIST 800-160 (Ron Ross J. C., 2016) provides a detailed framework for architecting and engineering secure systems. The document was written using industry recognized engineering design principles and standards.

The UF FISMA handbook further tailors the requirements in 800-53 and 800-171 within the scope of restricted data for research carried out by UF faculty and their collaborators. Research activities often have limited budgets and a need for rapid change to support innovation. These factors are important considerations for planning a research-centric architecture that is FISMA compliant, and NIST also provides guidance for the process of risk assessment within the context of investment and budget planning (Joan Hash, 2005) (Force, 2012).

The reader must keep in mind that building a secure computing and storage environment for working on restricted data is not a purely technical activity. In addition to technical factors, it involves making choices based on other factors, such as mission, business, and risk. For this reason, it is important that the team charged with building the FISMA-compliant environment involve experts from all these key institutional domains, or equally ensures that representatives from these domains are intimately involved in the process, from initial conception to delivery of the environment and finally, during its operation.

Compliance

The systems that are part of CERD are managed using the process and procedures that closely follow what is mandated by the FISMA acts of 2002 and 2014 for systems owned by and operated for the federal government.

- Data processed by projects set up in CERD is classified following FIPS-199.
- CERD systems are classified according to FIPS-200 to meet data requirements classified at the “moderate” impact level for Confidentiality, Integrity, and/or Availability.
- Controls are implemented and maintained for all systems in CERD as specified in 800-53 Moderate and 800-171.
- A system security plan (SSP) with Plan of Actions and Milestones (POAM) is maintained for all systems in CERD according to NIST 800-18.
- Approval to operate is obtained by the system owner and operator from the appropriate university official.
- The implementation of the controls is assessed by an organization independent of the system owner, UF Information Technology, with annual assessments thereafter.

DISCLAIMER

The NIST documentation can be applied as best practice and standard for operating any information system owned by and operated for any organization. Because of the possible narrow interpretation that FISMA compliance implies that the system is owned by and operated for the federal government:

- We do not claim that CERD systems are “FISMA complaint”.
- We do not claim that any cloud service that is used as a connected system to any system in CERD is FedRAMP certified.
- We do not claim that CERD is a “cloud service provider (CSP)” that is FedRAMP certified.

Scope

This handbook describes the framework used to design, implement, and operate a FISMA-compliant environment to enable research with restricted data. Although many elements described in this document have broader application, the UF FISMA handbook focuses on secure computing environments that support research projects with the following characteristics:

1. Research conducted at both public and private academic institutions, where researchers often work on multiple projects, and where governance structures tend to be more complex than in private companies or federal agencies.
2. Research funded from various sources, including the Federal Government, state, industry, and local institutions. Each funding source may require special restrictions, therefore a high degree of flexibility in meeting regulatory compliance is needed. The requirements evolve and the system and business processes need to be adaptable to these changes in a cost effective manner.
3. Research projects vary widely in budget, number of people involved, and timeline (from concept, to proposal, to execution, to final report and deliverables). This requires a very flexible environment that can respond nimbly to ad-hoc requests and new needs.
4. The people conducting research have various backgrounds, including citizenship in countries with export restrictions, and often include collaborators at other institutions. This requires a high degree of flexibility to manage personnel and regulatory training requirements, including training on highly customized procedures.

As outlined in the scope above, a significant portion of the challenges associated with architecting this type of environment are not technical. As stated in the FISMA regulation, institutions must develop a business process framework to make appropriate decisions and investments in equipment, human resources, and processes to manage the risk of operating the information system(s).

The current technology era lends itself to state-of-the-art information systems with sophisticated architecture and security measures. Modern technology is very reliable, and best-practices for hardware, software, and system administration are wide-spread to ensure high integrity and availability of data stored, transmitted and processed. What is not widespread is the ability to show to an auditor that all systems are operating consistently and effectively and best practices are in place.

When it comes to handling restricted data, where laws or regulation require audit trails, there is often a gap or deficiency in monitoring and documenting the operation of information systems. This handbook addresses how to fill that gap in a way that is:

1. Technically feasible;
2. Fits within the expected abilities and skills of human resources;
3. Financially affordable;
4. Serves the mission of the institution, and;
5. Mitigates existing and expected risks and threats commensurate with these constraints.

Authority

This section gives the background for building and operating an environment where research on restricted data is conducted in full compliance with all pertinent laws and regulations. It lists the legal authority to justify making the effort to undertake this task. This handbook focuses on federal law. Once a system is in place that meets the federal requirements, it is straightforward to tweak the implementation so that any state law or regulation, or any other policy requirements, can be managed within the same system.

Federal law

Increasing awareness and concern about security has led to more scrutiny of compliance with existing laws and regulations. Before 2015, there was the Federal Information Security Management Act (2002), which was revised in 2014 as the Federal Information Security Modernization Act. Both FISMA 2002 and FISMA 2014 mandate that information security standards and guidelines will be provided by the National Institute for Standards and Technology (NIST). Two key NIST publications, Federal Information Processing Standards (FIPS) 199 and 200, are mandatory security standards required by the FISMA legislation:

- FIPS199 requires federal agencies to assess and assign security categorizations for federal information and information systems based on three objectives (confidentiality, integrity, availability) and impact ratings (low, moderate, high).
- FIPS 200 describes minimum security requirements and a risk-based process for selecting the security controls necessary to satisfy the minimum-security requirements.

NIST Special Publication 800-53 (Ross, 2013) describes in detail the catalogue of security controls available for securing federal information systems. NIST SP 800-53 is often inserted as a contract term or condition, legally obligating the institution to comply with FISMA regulation. Contract language can also specify the NIST publications in Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS). When the academic institution is awarded a federal grant or contract involving restricted data, the NIST publications are usually inserted in the FAR and DFARS clauses, legally obligating the institution to comply with FISMA and NIST standards.

In 2015, the Federal Government proposed a new rule 32 CFR part 2002 to unify the classification of data that is restricted across the Federal Government and its contractors based on Executive order 13556 of 2010 introducing the concept of Controlled Unclassified Information (CUI). CUI is the system that standardizes and simplifies the way the Executive Branch handles unclassified information that requires safeguarding or dissemination controls. (NARA, 2016) This rule became final in September of 2016 and is effective on November 14, 2016. (Federal Registry, 2016)

The National Archive and Records Administration (NARA) is charged to maintain a CUI registry website: https://www.archives.gov/cui/registry/category-list.html. The CUI registry includes, controlled technical information (CTI), export controlled information, protected health information (PHI) covered by HIPAA, as well classes of agricultural information. 32 CFR part 2002 further defines CUI as “specified” or “basic”:

1. Where laws, regulations, or Government-wide policies articulate the requirements for protection of unclassified information, this part accommodates and recognizes those requirements as “CUI Specified.”
2. The CUI Basic standards therefore apply whenever CUI Specified standards do not cover the involved CUI.

3. For categories designated as CUI Specified, employees must also follow the procedures in the underlying laws, regulations, or Government-wide policies that established the specific category or subcategory involved.

The data classification for CUI is "moderate" for confidentiality (FIPS 199), which leads (FIPS 200) to the requirement that information systems used to hold, transmit, and process CUI must meet "moderate" controls as specified in NIST SP 800-53. In partnership with NARA, NIST published 800-171, the guidelines for protecting CUI on information systems outside the immediate control of the federal government and not operated by or for the federal government by a third party. NIST SP 800-171 ensures that sensitive federal information is properly safeguarded when stored in nonfederal information systems and organizations. NIST SP 800-171 is intended for non-federal organizations, like academic institutions, and can be used to tailor the SP 800-53 security controls that are not relevant or applicable for academic institutions.

In December 2015, the Department of Defense (DoD) updated DFARS 252.204-7012 with the stipulation that the CUI rule and corresponding NIST SP 800-171 was effective immediately. The DoD is granting organizations a grace period to implement SP 800-171 requirements, and full implementation of SP 800-171 requirements is required by December 31, 2017 for projects where DFARS 252.204-7012 applies. Additional contractual requirements are expected to follow now that the above CUI rule is in effect as of November 14, 2016.

UF must prepare for the expected increase in contracts involving CUI, which includes:

1. Controlled technical information (CTI)
    a. Not all export controlled information is going to qualify as CTI. The CUI Registry identifies "export control" as its own category, separate from CTI
2. Export Controlled Information
    a. Information subject to the International Traffic in Arms Regulations (ITAR)
    b. Information subject to the Export Administration Regulations (EAR)
3. Protected Health Information (PHI)
    a. HIPAA: Health Insurance Portability and Accountability Act
    b. HITECH: Health Information Technology for Economic and Clinical Health

The UF FISMA-compliant environment will use the CUI rule as the context for system design and specifications, with the understanding that other regulations are also relevant to the institution's research mission. The system must accommodate the additional regulation requirements with minimal redesign.

When handling data from the Commission for Medicare and Medicaid Services (CMS), a recent update of their standards to Acceptable Risk Safeguards (ARS) 3.0 adds a number of controls beyond the NIST 800-53 moderate baseline. This is an example where institutions need to make sure that the design of the system and business processes is such that changes can be made in a cost effective manner. It is not feasible to start from scratch when such changes make their way into new contractual obligations.

Similarly, the design of the system should be sufficiently general to accommodate research projects with different levels of requirements, some projects needs HIPAA, others need ARS 3.0, and still others need ITAR/EAR for export control. It is not cost effective to build custom systems for each set of requirements. A single system need to be designed to accommodate the mixture of requirements that comes from the contract research portfolio.

State and local law

In addition to federal laws and regulation, information security requirements from state or other sponsors can also be imposed on academic research that involves restricted data.

- UF maintains policies relevant to the use of information systems and data at the General Counsel web site (Regulations and Policies, 2016).
- UF maintains policies and corresponding standards, such as acceptable use, accessibility, email, identity and passwords, information security, intellectual property, networking, and web-related (UF Information Security Policies, 2016).
- The University of Florida Privacy Policy (Privacy Policy, 2016) lists the relevant State of Florida laws and regulations.
- Under the Florida Information Protection Act of 2014, any covered entity or third-party agent must report breaches to the Florida Department of Legal Affairs and to consumers within 30 days of the breach (FL Laws, 2014).

Process Overview

This section provides an overview of the process to design, build, and operate a FISMA-compliant environment with the scope specified in the previous section. The process results in the following deliverables:

1. An information system authorized by the institution to store restricted data for the institution towards the fulfillment of its mission, i.e. so that researchers can process and analyze restricted data with the required information security controls in place.
2. The documentation and audit processes that prove the information security controls are in place and operational, including the required annual audit process.
3. Business processes to use, provision, and operate the information system.

The collection of documents that describes the information system, monitoring procedures and business processes is called the System Security Package (SSP). The following steps are used to design and implement a FISMA-compliant information system with the corresponding SSP:

Gathering Requirements

When gathering requirements, it is important to consider all inputs. While technical requirements and system specifications are important, there are several other factors that must be discussed and considered:

1. The users of the environment.
2. The regulatory requirements.
3. The institutional mission and budget.
4. The threats and vulnerabilities.

Risk Management

Determine the risk management balance with all stakeholders. From the list of requirements, it is possible to find the optimal, usually not perfect, balance between them. The final decision must involve institutional leadership, since the institution will need to accept the residual risk.

The type of balance can be seen by considering the following: Given the mission of supporting research on restricted data, the aspect of confidentiality of the data has higher priority and poses greater risk to the mission and the institution than availability. Therefore, it is appropriate to dedicate more resources to ensuring confidentiality. NIST 800-171 (Ron Ross P. V., 2015) shows how this can be done within the framework of NIST 800-53 (Ross, 2013) to meet the requirements of CUI.

For scientific research, integrity of data is paramount and is more important than 24/7 availability of the data. However, while scientists can wait for the data to become available, it is not acceptable when data of a certain type is lost.

System and Business Process Specification

With the risk balance between the requirements determined it is possible to specify the system, which here means both the computer system and the business processes. These are:

1. The technical controls in hardware and software.
2. Acquire and implement the system as specified and obtain approval to operate from institutional leadership.
3. The process to analyze projects and set up users in the environment.

4. The process to match the appropriate technical controls to each project and to the personnel working on the project.
5. Training of personnel about the use of the environment and about the regulatory constraints and responsibilities of working with the data.
6. The process to maintain system operation and to generate and review audit logs.
7. The annual review by an independent auditor. This can be a third party assessment organization (3PAO), or the Office of Internal Audit which is legally qualified in universities to perform independent audits of university operations.

Build and Document

The next step is complex and parts of it can be carried out in parallel. From the specification, there are three areas in which work needs to be carried out:

1. Build the standard part of computer systems.
2. Build the logging and audit part of computer systems.
3. Implement the business processes.

With the specifications in place, which include the technical controls associated with the level of confidentiality, integrity, and availability as described in NIST 800-53 (Ross, 2013), a systems architecture and design team can build the computer system and configure it with a systems administration team. These teams need to collaborate closely with the FISMA team in charge of building the environment, but it should be clear that they are executing a given specification, not driving the process. If not they can easily undo the benefit of requirements gathering and risk management by building a system that does not meet all the requirements, but only provides the technical controls.

The not-so-standard, in the academic research information technology context, level of change management, documentation requirements, and detailed logging of system activity must be kept in mind during the architecture, design, and build phase of the computer system. Then the work in the second area is straightforward and can be carried out efficiently and effectively.

The design and implementation of the business processes is often a challenge in academic environments, which for good reason have a complex governance structure with multiple often conflicting levels of authority in charge of different aspects of the mission of the institution. This may require a skilled and experienced individual or set of individuals on the team to negotiate. A few team members with a long institutional history, who know many stakeholders and have their trust, may be an invaluable asset in this part of the process.

Business processes will impact the way people do things, and that is always hard to change. Informational web sites must be created. Training materials need to be developed. A process to analyze, review, and approve new projects for using the restricted data environment must be developed. A chain of authority to gain approval needs to be defined.

The processes must be simple and clear, because the variety of projects in academic research institutions is enormous. For some projects, there is the requirement to develop a custom process and chain of authority with the principal investigator as the final authority within the project.

The main benefit of creating a restricted data research environment is to have infrastructure that is pre-approved and ready to go. Thus, the process for getting on board can be simple and fast. Research projects

often have short timelines of as little as six months from start to finish. It must be possible to get approved and set up in the environment within one week.

The result of this step is the set of three deliverables: the system, the system security package, and the business processes and governing policies.

Initial Review and Authorization

The standards for the SSP created in the build-and-document step that the institution sets, given the regulatory requirements, are described in this handbook. The institutional Office of Internal Audit (OIA), in cooperation with the Information Security Office (ISO), needs to review the SSP and verify that the procedures and controls described are in place. This verification ensures that the responsible department in Information Technology is operating the information system and the various departments and officers throughout the University are carrying out the business processes in accordance with the procedures and controls described in the SSP.

Upon positive recommendation by the Office of Internal Audit and after, or while addressing the concerns raised by the review, the system can be authorized for use by the Vice President and CIO.

It may be of value to carry out an independent assessment of the system and procedures by a third party as the budget permits and the need exists.

The deliverable of this step is a document that clearly states that the institution has verified the operation of the system and business processes and has found that they are compliant. This document can be variously described as an assessment report, a certification report. It is typically signed by the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Privacy Officer, and/or the Compliance Officer. The document is then used by the Office of Research in the process of contract negotiation when the contract requires compliance.

Some terms used in the context of initial approval to operate a system as compliance are

- IV&V (Independent verification and validation), and
- SC&A (System certification and accreditation).

One of the consultants, a 3PAO ExcentiumI, described the IV&V as a process in which a team (such as a 3PAO) is contracted by an agency or institution to review the entire system and produce an authority to operate (ATO) package. So IV&V is a process, not a deliverable.

The 3PAO described the SC&A as an outdated concept. It provided an extensive review of documentation, testing of controls, interviews of personnel, examination of risks and compensating controls and produced a Security Assessment Report (SAR) that is presented to the Authorizing Official for final decision to allow operating the system as compliant. This process is outdated because of its focus on a single point in time. It has been replaced by continuous monitoring and annual testing of 1/3 of the controls, such as the FedRAMP recommended annual assessment.

The Department of Homeland Security has a document on its website that discusses FISMA 2014 reporting metrics using the terminology introduced by the NIST Cybersecurity Framework (Inspector General, 2016).

Operate and Maintain

The final step in the process is the task that never ends: Operate and maintain the system. The additional burden beyond the standard activities associated with operating and maintaining an information system are the rigorous logging and reporting, on a daily, weekly, monthly, and yearly basis.

Annual Compliance Audit

The annual review is a requirement for compliance. The Office of Internal Audit and the Information Security Office may collaborate with each other and with possible third parties to assess and test the system controls, policies and business processes. They will produce a technical report specifying gaps and needed corrective action as well as a general statement to the institutional leadership, VP and CIO and VP for Research about the state of the FISMA program.

They will again use this handbook, which may have been updated due to regulatory or technology changes, and verify that the system is configured and operated as required by law and as described in the SSP.

Preparing for Implementation

Risk Assessment Process

The business risk assessment enables stakeholders to make informed decisions that support mission critical business processes by defining the mission, identifying potential risks to the mission, calculating the likelihood the adverse events may occur, and estimating the potential impact to the mission if they occur. Business risk assessments allow organizations to focus information system risks on the most highly exposed or mission critical functional areas.

Risks are first examined at the macro level without considering system or IT specifics. Determining business risk first makes it easier to determine system risk. Understanding the organization's mission is the first step to determining risks to the organization. Risk assessments start by analyzing and documenting the mission and the known business processes that support the mission. Answer questions such as:

- What is the service?
- Who is the service for?
- What are the customer requirements viewed in the context of security?
- What is the nature of the data?
- Who is working with the data? How are these people vetted?

Once the mission critical business processes are understood, the next step is documenting the role that information systems play in carrying out the mission (see "Mission Map" on page 205 in Taylor, 2007). Then develop risk statements to identify the threat or vulnerability and estimate the potential impact: "If <this threat occurs>, then <this will be the impact>." Once risk statements are developed, the impact can be forecasted and the likelihood of the potential threat can be determined (see quantitative and qualitative risk assessments, Taylor, 2007).

The result of the business risk assessment should be a risk summary table that includes the risk statement, corresponding risk scores (likelihood, impact, risk exposure) and a decision to accept the risk, transfer the risk or mitigate the risk.

Example 1: Mission and Availability

The following examples demonstrate the level of risk associated with the availability of information systems based on mission critical business processes:

- Research data needs to be available during research work periods. It is acceptable to be down 1 day per year – a 99.7% uptime.
- The UF website cannot be down more than an hour per year – a 99.99% uptime.
- An information system supporting a hospital operating room cannot be down more than a second – a 99.9998% uptime requirement.

Example 2: Physical and Virtual Security

When the data center is broken into, the most serious consequences for the data and systems can result. However, in a city like Gainesville, any criminals are not likely to be organized crime with a complex goal of stealing restricted data from UF computers. If any robber breaks into the data center, they are more likely to take the microwave in the break room or the desktop computers in the work room than to try and get data off the servers. To get into the data center requires more skill and tools than any criminal or criminal organization in

North-Central Florida is likely to have. Thus, while the potential impact is big, the probability is negligibly low. We should not leave the doors open, but the measures that are in place reduce the risk of physical compromise by criminal activity from outsiders too negligible.

If we include attacks by insiders, the risk is a bit higher. There, too, we have measures in place to mitigate insider threats, such as registered key access on doors and video cameras.

The likelihood that we will be subject to attacks over the Internet from various very sophisticated organizations and malware programs is much larger. Hence that is where we should focus the effort and budget resources.

System Security Categorization

To determine the security categorization of an information system, metadata (i.e. variables or field names) are analyzed with respect to three security objectives: confidentiality, integrity, and availability (C-I-A). When federal law or contract/grant terms and conditions require FISMA or NIST compliance, the security categorization is often applied to individual datasets rather than entire information systems. Although the analysis requires inspection of all data contents, the result is a single impact rating of low, moderate, or high (L-M-H) for the dataset or information system in question. Table 2 summarizes the NIST publications that guide the security categorization:

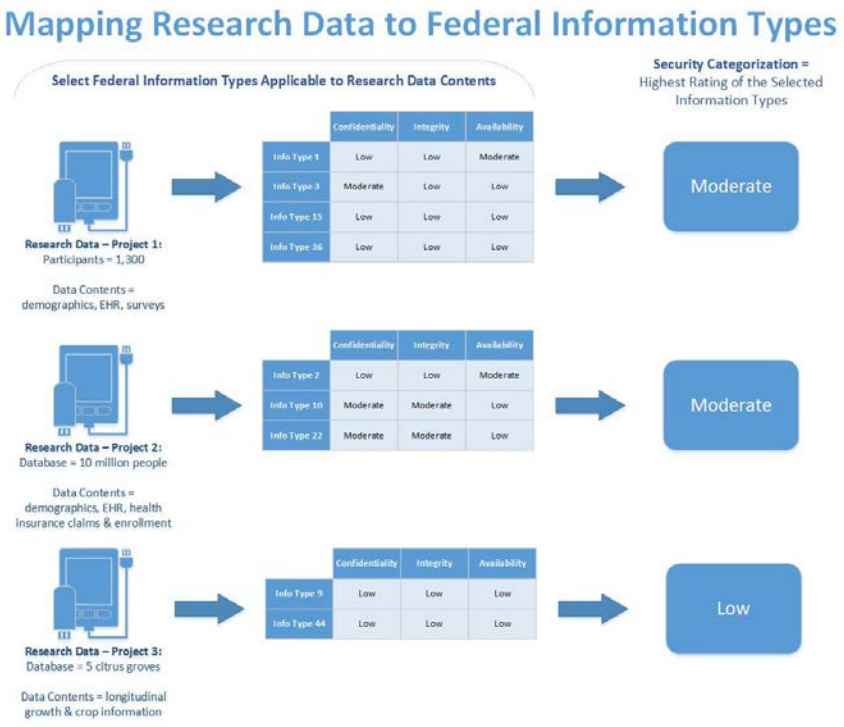
Table 1: NIST Publications for Security Categorization

NIST Publication Number	NIST Publication Title	Key Points
FIPS199 (13 pages)	Standards for Security Categorization of Federal Information and Information Systems	-Defines three security objectives (C-I-A) -Defines three impact levels (L-M-H) -Instructions on documenting security objectives and impact levels for information types and information systems
SP 800-60 vol1 (53 pages)	Guide for Mapping Types of Information and Information Systems to Security Categories	-Section 3 recaps FIPS199 -Section 4 details the step-by-step process for metadata analysis that leads to the single impact rating/security categorization
SP 800-60 vol2 (304 pages)	Appendices	171 federal information types and the corresponding NIST impact ratings for C-I-A are indexed in two categories. These appendices are used as part of the step-by-step process defined in section 4 of SP 800-60 volume 1: • App C: Management and Support (77 info types) • App D: Mission Based (94 info types)

FIPS199 and section 3 of SP 800-60, volume 1, defines the following matrix for analyzing information systems (or research project data) to determine potential impact associated with three primary security objectives:

Security Objective	Potential Impact		
	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

NIST SP 800-60, volume 2, defines 171 specific information types, each with its own impact rating (L-M-H) for the three security objectives (C-I-A). Understanding how research data contents map onto the NIST information types is key for assessing risk to the organization. In collaboration with the Principal Investigator, the Office of Research and applicable IT departments, research project data are mapped to federal information types, and the result is the security categorization, as depicted in the diagram to the right.



While NIST provides a comprehensive list of federal information types, it may be incomplete with respect to academic research data. It is important to note that, when applicable, NIST recommends adjustments to the list of information types or the corresponding impact ratings. Adding or revising information types based on the dataset or information system in question is allowed. In addition to revising information types, the NIST recommended impact ratings may also be adjusted.

Adjustments require proper justification, which must be documented as part of the implementation. Section 4.5 of NIST SP 800-60, volume 1, includes a suggested format for documenting the security categorization process. An example is provided in Table 2 below:

Table 2: Sample Documentation for NIST Security Categorization

Information System Name: <Research Project> <Project ID> <PI Name>			
The objective of this project is to determine the effect of an ED-to-Home Transitional Care Intervention on patients' self-reported quality of life and need for resource intensive, hospital-based care.			
Information Types			
D.14.1 Access to Care	The Health Care Coach is employed by the area Agency for Aging and works with the patient to navigate from the ER department back to their primary care provider.		
D.14.5 Health Care Research and Practitioner Education D.20.1 Research and Development	This is an IRB approved research study to analyze Medicare claims and patient data with intervention data. Researchers will use secondary and primary datasets to understand the intervention effect on complex populations.		
Step 1: Identify Information Types	**Step 2 [Provisional] / Step 3a [Adjustments]** **Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
	Step 3b [Impact Adjustment Justification if applicable]		
D.14.1 Access to Care	L No adjustments	M No adjustments	L No adjustments
D.14.5 Health Care Research and Practitioner Education	L No adjustments	M No adjustments	L No adjustments
D.20.1 Research and Development	L No adjustments	M No adjustments	L No adjustments
Step 4 System: Categorization	**Low**	**Moderate**	**Low**
	Overall Information System Impact: Moderate		

Note that this is a discovery process. One needs to classify all relevant data and show, for example, that no data is classified as High and it least one type of data is classified as Medium. Then the classification is Medium.

Select Security Controls

Once data contents are mapped onto the information types in the categorization process, an overall impact rating (L-M-H) is determined for the dataset or information system. The impact rating drives the security controls selection process. The impact rating determines the minimum number of controls required to safeguard the system and mitigate risk.

NIST SP 800-53 catalogues the 633 controls by control family. Each control is designed to address risk associated with one of the three security objectives (C-I-A). The combination of controls selected is what secures and protects the system at low, moderate or high levels. Table 3 summarizes the NIST publications that guide the selection of controls. Table 4 summarizes the total number of controls defined in each family and the minimum number of controls required for each security categorization, called the baseline. In addition there are 8 families of privacy controls that are relevant in some cases, such as Medicare and Medicaid data as described in CMS ARS 3.0.

Table 3: NIST Publications for Selecting Security Controls

NIST Publication Number	NIST Publication Title	Key Points
FIPS200 (17 pages)	Minimum Security Requirements for Federal Information and Information Systems	-Defines the 18 security control families -Explains how the FIPS199 security categorization (L-M-H) links to SP 800-53 baseline controls

SP 800-53 (462 pages)	Security and Privacy Controls for Federal Information Systems and Organizations	-Section 3 outlines the process to: 1-select a security control baseline, 2-tailor the baseline, 3-document the selection process -Appendix F: Comprehensive catalogue of the 633 controls and control enhancements -Appendix J: 8 families of additional privacy controls.

Table 4: Number of NIST Security Controls by Family (Total and Minimum Number per Security Categorization)

Control Family	Class	Total Controls	Low	Moderate	High
1. Access Control (AC)	Technical	90	11	35	43
2. Audit and Accountability (AU)	Technical	47	10	18	28
3. Awareness and Training (AT)	Operational	8	4	5	5
4. Configuration Management (CM)	Operational	42	8	21	31
5. Contingency Planning (CP)	Operational	46	6	22	35
6. Identification and Authentication (IA)	Technical	33	15	22	24
7. Incident Response (IR)	Operational	21	7	12	16
8. Maintenance (MA)	Operational	23	4	9	13
9. Media Protection (MP)	Operational	19	4	9	12
10. Personnel Security (PS)	Operational	12	8	8	9
11. Physical and Environmental Protection (PE)	Operational	49	10	18	26
12. Planning (PL)	Management	9	3	6	6
13. Program Management (PM)	Management	16	0	0	0
14. Risk Assessment (RA)	Management	14	4	7	8
15. Security Assessment and Authorization (CA)	Management	14	7	10	12
16. System and Communications Protection (SC)	Technical	95	10	24	30
17. System and Information Integrity (SI)	Operational	54	6	21	27
18. System and Services Acquisition (SA)	Management	41	7	14	18
Total Number of Controls		**633**	**124**	**261**	**343**

Implementation

Create the system, set up training and review and audit processes.

Design and Build

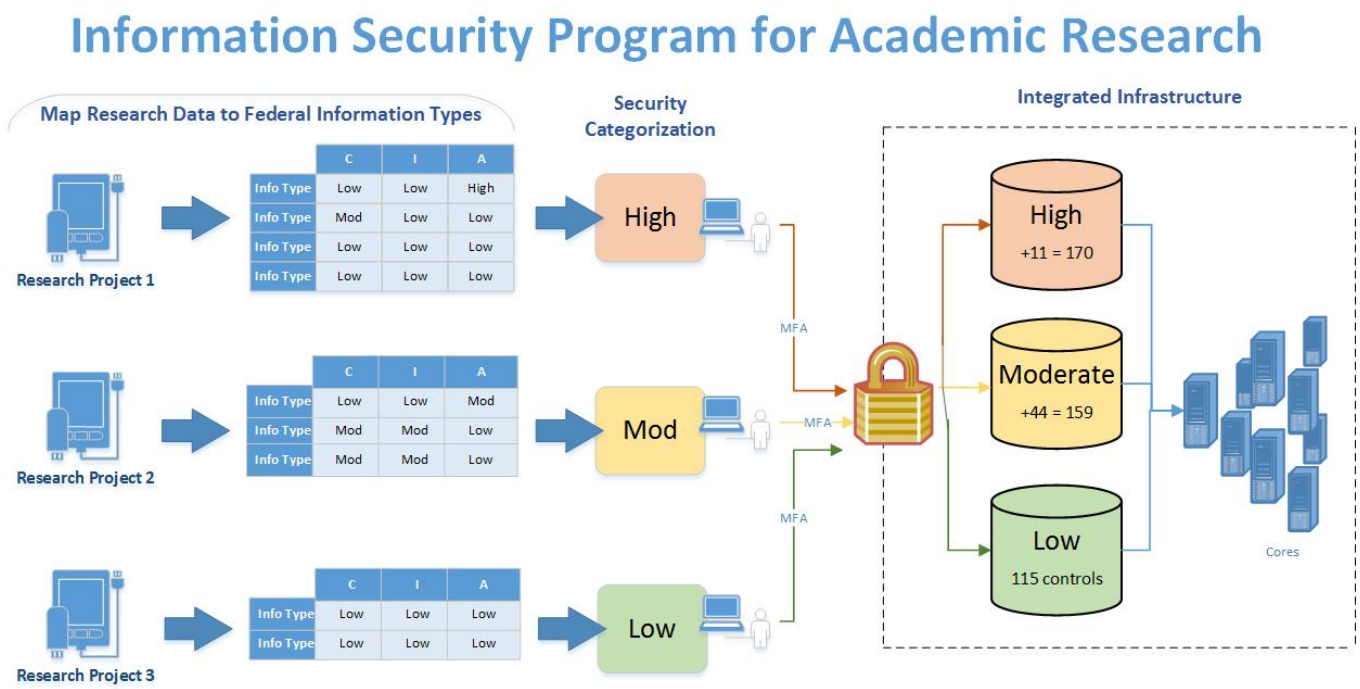
With the business risk assessment, security categorization and controls selection complete, it's time to design the system architecture and implementation plan. The system design is driven by the business needs. Design the system to minimize change or impact on business process and workflow. Answer questions such as:

- Does the system support the business process and requirements?
- What existing systems are in place to leverage reaching the requirements to save in cost?
- What alternatives for implementation exist? Compare them for price, ease of use, simplicity in installation, maintenance, and total-cost of ownership.
- Do all the components work together easily? A complex system built with the best components has a higher risk of failing because of the complexity. People will forget a step and then the great components will not work correctly.
- From that analysis comes a coherent system design and implementation plan.

The number of controls listed in NIST 800-53, or any other specification, is very large. A good system and business process architecture will ensure that a single architectural feature implies many of these controls. That will make implementation simpler as well as the audit process. The system will be secure at a more fundamental level when a small number of features ensure compliance with a large number of controls.

Once the system architecture and design is complete, build the system to the desired specifications. Documenting the research landscape at academic institutions is important for system architecture and design.

Integrated infrastructure for regulated data can be designed to accommodate varying degrees of security and privacy controls. Once the security categorization is complete, academic research projects are easily moved into pre-assessed computing environments, as depicted in the following concept diagram:



System Security Package (SSP)

In addition to designing and building the system, a comprehensive set of documents, called the System Security Package (SSP), must be written to comply with FISMA regulation and to facilitate the annual system evaluation, also known as system assessment or system audit. To facilitate efficient system evaluations, documentation should be provided using standard templates. Several documentation templates exist, such as FedRAMP, or document templates can be developed in-house.

Although the System Security Package includes several complementary documents, each document must be written as a stand-alone section so it makes sense if the document is pulled out of the System Security Package during a system evaluation or audit (Taylor, 2007). To accomplish stand-alone readability for each document, certain content should be repeated in a consistent manner across documents. Instead of copying and pasting content across documents, it's recommended to use a document generation process or content management system to assemble documents from various components.

Documents

A sample list of documents for the System Security Package (SSP) includes:

1. Hardware and software inventory. All the components needed and where to get them so that you can rebuild the system if necessary (see disaster recovery later). This may include a configuration management plan, or that may be separate.
2. System security plan. Gives full overview of the system, who is responsible for what, how it works.
3. Risk analysis. Details of threats and how they affect the system and the mission. Describes how the requirements are balanced to minimize risk within the constraints of the mission, budget, and legal requirements. This document may include the privacy impact assessment and the business impact assessment, or they may be separate.

4. Business continuity plan. This describes details of what will be done when things happen to cause disruption of normal service. It may be split out in several documents: Incident response plan, contingency plan.
5. Training plan. There are two major groups who need training with respect to security and privacy: The people who operate and maintain the system and software, and the people who are using the system and software for their work. Depending on the mission of the organization and the information system there may be considerations of separation of duties that both groups need to understand. Technical controls often can effectively enforce the required separation. The training must address the rules of behavior, including awareness of penalties for actions or activities that are not allowed. Technical controls may prevent many actions and logging may record actions, but the final responsibility lies with people.
6. Independent assessor audit guide. Describes to an independent agent how to go about verifying that the system and business processes work as described.
7. Security assessment report. This describes the findings after testing the technical controls. The auditor can use the report or may create a new one.
8. System operating procedures. Describe the business and system administration processes that are followed to operate and use the information system.

The final deliverable, after implementation is complete, will be the acceptance or authorization document to be signed by the appropriate institutional administrator, for example the CIO, indicating that the institution allows the system to be operated to conduct its business activities that require compliance.

Roles and Responsibilities

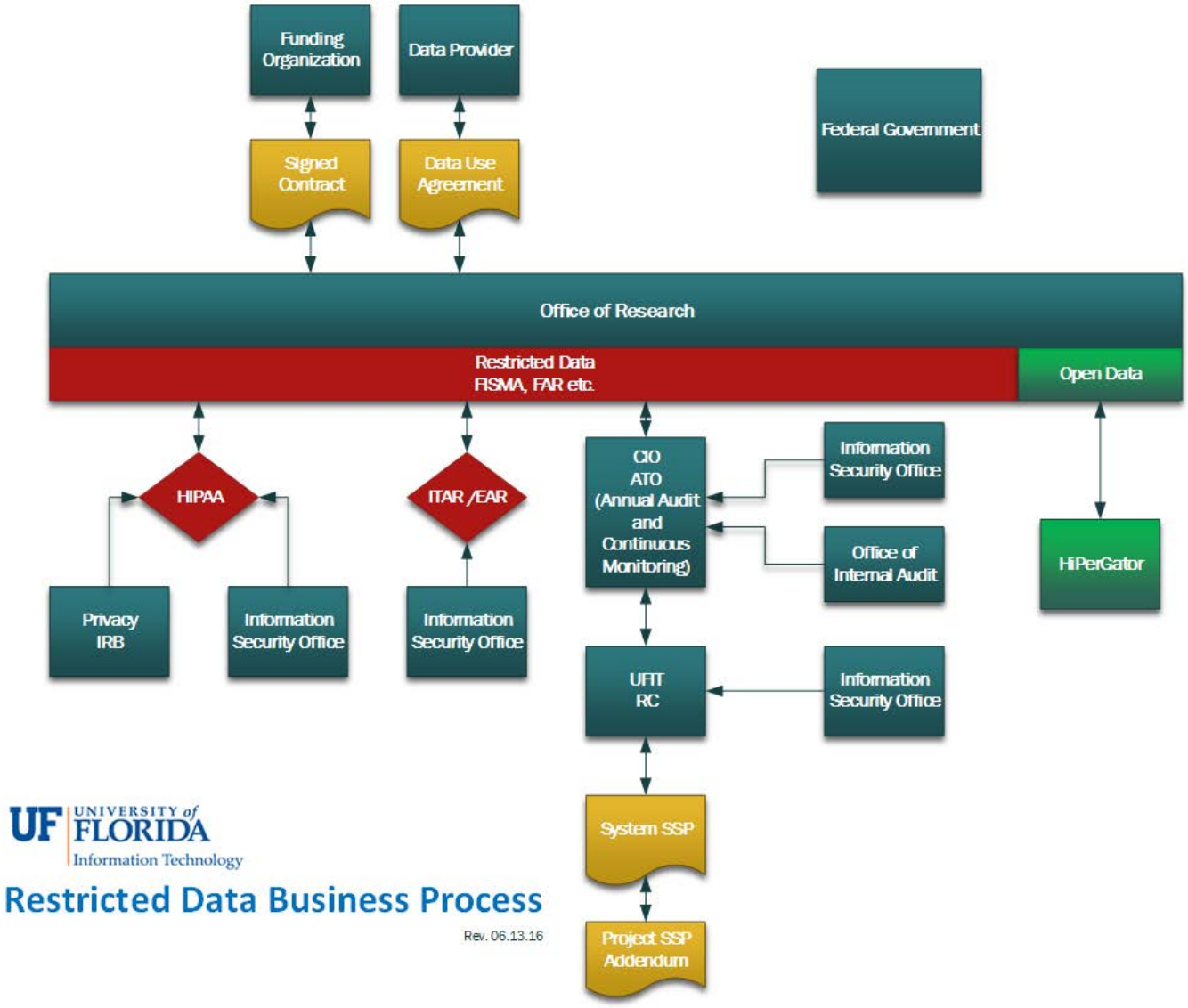
Key Roles

- **Authorizing Official** CIO does not do the work, but has the responsibility to decide on a carefully prepared recommendation
- **Authorizing Official Designated Representative**[1] CISO prepares the recommendation to the CIO so he can decide with all facts known; CISO does not do the paperwork himself either, that is done by the team in ISO, RC, and OIA.
- **Chief Information Officer** (CIO)
- **Senior Agency/Institution Information Security Officer** (CISO)
- **Information System Owner** Director of Research Computing
- **Information System Security Officer** Staff in Research Computing
- **Certification Agent** Office of Internal Audit head does not do the work either, but provides authority and independence for certification to hand to the Designated Representative
- **User Representatives**

Other Supporting Roles

- **Information Owner** Specific researchers
- **Operations Manager** Research Computing staff F
- **Facilities Manager** Data center staff
- **System Administrator** Research Computing staff

[1] This is the one role that may be most difficult to assign.


Funding Organization
Data Provider
Federal Government
Signed Contract
Data Use Agreement
Office of Research
Restricted Data
FISMA, FAR etc.
Open Data
HIPAA
ITAR /EAR
CIO
ATO
(Annual Audit and Continuous Monitoring)
Information Security Office
Office of Internal Audit
HiPerGator
Privacy IRB
Information Security Office
Information Security Office
UFIT RC
Information Security Office
System SSP
Project SSP Addendum
UF UNIVERSITY of FLORIDA
Information Technology
Restricted Data Business Process
Rev. 06.13.16

Information Security Awareness and Training Plan

Overview

Developing an information security training and awareness plan is an important part of FISMA compliance programs. Information security awareness and training is referenced throughout the FISMA regulation and OMB Circular A-130 Revised, specific excerpts include:

- FISMA: *"…security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of – (A) information security risks associated with their activities; and (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks…"*
- OMB Circular A-130 Revised:
    - *"…users of Federal information resources must have skills, knowledge, and training to manage information resources…"*
    - *"…agencies will provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities…"*
    - *"…establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems…"*

In the above we need to read "federal agency" as "institution" and "federal information system" as "university information system". The CUI program seeks to establish consistency for safeguarding data everywhere is flows.

The information security awareness and training plan should advise users about the organization's expectations, policies and procedures related to working with restricted or regulated data. Although large data breaches often make headline news, daily, people are usually unaware of the constant threats to information systems. It's important to explain the various threats and vulnerabilities, not only to generate awareness of the need to protect information, but also to empower users to take ownership of protecting the data and information system. Generating awareness and empowering users to protect information and information systems also enables the organization to hold users accountable for following policies and procedures.

It is important to note the difference between awareness and training (Taylor, 2007). Communication campaigns that market and promote information security are designed to generate awareness about securing and protecting information and information systems. Training programs include formal coursework or curriculum designed to teach people about institutional policies and procedures.

Creating Awareness and Training Programs

Most organizations with Information Security Offices already have cybersecurity awareness and training programs in place. Information security awareness and training plans specific to FISMA-compliant systems can leverage content, curriculum and processes from the central office. Content of FISMA-specific training courses should focus on protecting the confidentiality, integrity and availability of covered information and information systems. FISMA training should be required for all users, including cross-institution collaborators, such as faculty or consultants.

It is important to tailor training content to various audiences.

Normal users will need training on the basic use of the system and an understanding of the security requirements and programs that may apply to their data. These may include HIPAA, ITAR and others based on data types described in their DUA.

Privileged users such as system administrators that manage the FISMA compliant system and routinely handle incidents. Training for this group would be much more rigorous and include a thorough knowledge of the various security requirements.

Business process administrators including representation from Compliance, Privacy, ISO and the contract team. It is important for this group to understand the process and know who to ask when questions arise.

NIST wrote special publication (SP) 800-50 as a guideline for developing security awareness and training programs. A template for writing the plan is included in Appendix C, NIST SP 800-50. In addition to describing the training program and related processes, the plan should also document and archive training records. Resources available to assist with developing the awareness and training plan include:

- NIST SP 800-50 provides an overview of the steps involved to design, develop, implement and measure the plan:
    - Designing an awareness and training program
        - How to structure the awareness and training activity
        - How to conduct a needs assessment
        - How to develop an awareness and training plan
        - How to establish priorities
        - How to properly "set the bar" or level of complexity
        - How to fund the awareness/training program
    - Develop materials
        - Awareness: what behavior should be reinforced?
        - Training: what skills should the audience learn and apply?
    - Implement the plan
        - Communicating the plan
        - Techniques for delivering awareness
        - Techniques for delivering training
    - Post implementation
        - Monitoring compliance
        - Evaluation and feedback (also see Taylor, 2007 for a sample course evaluation)
        - Managing change
        - Ongoing improvement
        - Program success indicators
    - Samples and templates
        - Needs assessment questionnaire
        - Awareness and training metric
        - Awareness and training program metric
        - Awareness posters
- Taylor provides a security awareness and training checklist on page 85 of the FISMA Compliance Handbook:
    - Is the frequency of the training noted?
    - Is specialized training for security personnel described?
    - Are training classes for basic users described?
    - Are instructors for the training classes noted?

- Is it noted that security training is tracked and logged?
- Is it noted that all courses are evaluated by the users?
- Are roles and responsibilities for security awareness noted?
- Are roles and responsibilities for security training noted?
- Does the plan indicate that a record is kept of user training participation?
- Does the plan indicate that users are assessed for their security knowledge after they undergo training?

UF Information Security Awareness & Training

The UFIT Information Security Office (ISO) is responsible for developing security awareness and training for UF staff, faculty and students. In additional to formal training courses with evaluations, information is also provided in other formats, such as education guides, pamphlets, and tutorials. Throughout the year, ISO hosts a number of speakers, presentations, and events to generate awareness and incorporate changing regulation and standards in UF policy and practices. Several examples of UF ISO awareness and training, both FISMA and general are included below:

- UFIT Research Computing training examples: https://www.rc.ufl.edu/documentation/hipergator-rv/hipergator-rv-training/
- General UFIT ISO training examples:
  - Cyber Self Defense Course
  - General Awareness Training
  - EduGuides
  - Security Refresher Course
- General UFIT ISO posters and web banners:

Audit

The system, the operational and business processes associated with operating, maintaining, and using it for the organization must be reviewed annually by an independent auditor. The auditor must be independent of the organization that operates and supports the system and the users of the system. In a large organization like UF, the Office of Internal Audit http://www.oia.ufl.edu/ is considered independent of UFIT Research Computing and the researcher community and thus can perform this duty. Per Florida Statute, the UF Office of Internal Audit is authorized as the Inspector General for the University of Florida. To assist them the independent assessor audit guide is created and maintained.

The Office of Internal Audit may call on UFIT staff, for example data security specialists and network engineers, to carry out technical tasks like scanning the environment. They can hire an external organization, but given the significant expertise on campus they are likely to find the necessary assistance for whom there is no conflict of interest to carry out the required tasks. The cost savings can be significant.

Operation

Operations is responsible for the day to day operating of the FISMA environment. This includes but not limited to:

- User provisioning, this includes on-boarding new users and insuring correct roles and permissions are assigned.
- Tenant hardware and software provisioning, insuring the environment meets the work flow needs of the tenant.
- Continuous monitoring, an essential component to ensure that the environment meets all security and performance requirements.
- Documentation that includes process descriptions, training, asset management, physical and logical system diagrams and maintenance of all system logs for compliance reporting.
- Provide any needed documentation to the Office of Internal Audit of the University to facilitate the annual audit and verify that the system and business processes are operating in compliance with FISMA requirements.
- Act on any findings of non-compliance.
- Participate in the ITSM incident and change control process to ensure all changes are approved and documented.

Operations is a key component and is the focal point for all FISMA activities. Management activities include scheduling daily, weekly and monthly compliance activities that seek to minimize risk associated with the storage of data to ensure that the system is managed effectively.

Daily compliance activities:

- Review of all user generated incident and service requests.
- Review of all continuous monitoring generated alerts to insure there has not been any compromise of the system.
- Configuration integrity monitoring which checks for unauthorized system level changes.
- Review of backup and recovery metrics to ensure the system remains recoverable.
- Review of all security alerts including, detection of malware and policy violations from intrusion detection systems.
- A team review of the above activities to ensure any incidents are properly managed within the compliance team.
- Communication with users of any pending changes that may interrupt or affect their normal business process.

Weekly compliance activities:

Participating in the weekly change control meeting to ensure that any FISMA changes are properly documented and approved. If any changes potentially could impact end users, they are notified in advance.

Monthly compliance activities:

Publish and distribute detailed metrics for the environment that includes all required control families. A typical monthly report package for the UF FISMA environment includes the following reports.

- Backup Logs (Success, Failure)
- Antivirus scan reports
- ITSM (Change Management/Incident) Reports
- Citrix Patching
- Credentialed Scans
- Managed File Transfers and DLP (Files moved in/out of FISMA environment))
- MFA (DUO logs)
- Storage reports (In-use and available)
- IAM (User authentication)
- Security and system logs (LogRhythm)
- System management (Nagios)
- Vulnerability scans (Nessus)
- VM management (vCenter)
- Windows Patching
- Physical Access (FISMA Racks in Data Center)

Annual compliance activities:

Conduct the annual audit with the Office of Internal Audit or 3PAO. Develop the Security Assessment Plan (SAP) by listing the controls that will be tested in one given year. The recommended process tests one third of all controls in one review, so that the entire system is reviewed every three years.

Then the operations team assists the auditor to carry out the assessment.

The auditor then produces the Security Assessment Report (SAR) which lists the deficiencies found. A Plan of Action and Milestones (POAM) is then developed to fix the deficiencies.

Then the auditor submits a summary of the SAR and POAM to the Authorizing Official so that the institution can authorize continued operation of the system as a compliant system.

References

Federal Registry. (2016, Sep 14). Retrieved from 32 CFR Part 2002 Controlled Unclassified Information: https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

FL Laws. (2014). Retrieved from http://laws.flrules.org/2014/189

Force, J. T. (2012). *Guide for Comnducting Risk Assessments (NIST 800-30).* Gaithersburg, MD: NIST.

Inspector General. (2016, 9 26). *FISMA 2014 Reporting Metrics*. Retrieved from Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/FY%202016%20IG%20FISMA%20Metrics%20508%20compliant%20.pdf

Joan Hash, N. B. (2005). *Integrating IT Security into the Captical Planning and Investment Control Process (NIST 800-65).* Gaithersburg, MD: NIST.

NARA. (2016). Retrieved from CUI FAQ: https://www.archive.gov/cui/faqs.html

Privacy Policy. (2016). Retrieved from University of Florida Privacy Office: http://privacy.ufl.edu/wp-content/uploads/2012/08/UF-InfoPrivacy-PolProc-11-1-2014.docx

Regulations and Policies. (2016). Retrieved from Legal Counsel: http://generalcounsel.ufl.edu/regulations-and-policies/

Ron Ross, J. C. (2016). *Systems Security Engineering: An integrated Approach to Building Trustworthy Resilient Systems (NISt SP 800-160).* Gaithersburg, MD: NIST.

Ron Ross, P. V. (2015). *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (SP 800-171).* Gaithersburg, MD: NIST.

Ross, R. S. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 revision 4).* Gaithersburg, MD.

Taylor, L. P. (2007). *FISMA Compliance Handbook.* Amsterdam: Elsevier.

UF Information Security Policies. (2016). Retrieved from http://www.it.ufl.edu/policies/

Appendix A: Resources and Quick Links

- University of Florida
  - UF Information Technology
  - UF Privacy Office
  - UF General Counsel
  - Privacy training requirements
  - Operational Guidelines for Health Information
- NIST standards and guidelines
  - Federal Information Processing Standards (FIPS)
  - Special Publications (SP)
    - SP 800-series – Computer Security
    - SP 1800-series – Cybersecurity Practice Guides
    - SP 500-series – Computer Systems Technology
  - NIST Internal/Interagency Reports (NISTIR)
  - Information Technology Laboratory Bulletins (ITL Bulletins)
- Security Technical Implementation Guides
- CERT Advisories
- Regulations
  - HIPAA
  - FISMA
  - FERPA
  - GLBA
  - ITAR
  - Privacy Act
  - PCI-DSS
  - E-Government Act
  - OMB memorandum
  - FAR
  - DFARS
  - NARA: CUI