

# Retired Draft

## Warning Notice

The attached draft document has been RETIRED. NIST has discontinued additional development of this document, which is provided here in its entirety for historical purposes.

**Retired Date** November 01, 2008

**Original Release Date** September 28, 2007

## Retired Document

**Status** Initial Public Draft (IPD)

**Series/Number** NIST Special Publication 800-110

**Title** Information System Security Reference Data Model

**Publication Date** September 2007

**Additional Information** See <https://csrc.nist.gov> for information on NIST cybersecurity publications and programs.

NIST Special Publication 800-110 (Draft)

Information System Security Reference  
Data Model (DRAFT)

**NIST**

**National Institute of  
Standards and Technology**

U.S. Department of Commerce

**Elizabeth Chew  
Kevin Stine  
Marianne Swanson**

INFORMATION SECURITY

**FIRST PUBLIC DRAFT**

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

*September 2007*



**U.S. Department of Commerce**

*Carlos M. Gutierrez, Secretary*

**National Institute of Standards and Technology**

*James M. Turner, Acting Director*

## **Reports on Information Systems Technology**

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of nonnational security-related information in federal information systems. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

## Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

## **Acknowledgements**

The authors, Elizabeth Chew, Kevin Stine, and Marianne Swanson, wish to express their thanks to colleagues who assisted in the development of earlier drafts and reviewed this document. In particular, their appreciation goes to Joan Hash, Elizabeth Lennon, John Abeles, Dan Chandler, Keith Hall, Steve Newburg-Rinn, Steven Senz, Frances Cordero, Salvador Velaquez, James Neidich, Carolyn Quinn, Christina McNemar, and Anne Roudabush.

# Table of Contents

EXECUTIVE SUMMARY .....	VII
1.0 INTRODUCTION .....	1
1.1 Purpose and Scope .....	1
1.2 Audience .....	1
1.3 Document Structure .....	1
2.0 BACKGROUND .....	3
3.0 REFERENCE MODEL .....	5
3.1 Two-Level Reference Model .....	5
3.2 Dependency and Interdependency .....	7
3.3 System Level.....	7
3.3.1 Categorize the Information System .....	8
3.3.2 Select Security Controls.....	9
3.3.3 Supplement Security Controls .....	10
3.3.4 Document Security Controls.....	10
3.3.5 Implement Security Controls .....	11
3.3.6 Assess Security Controls.....	11
3.3.7 Authorize the Information System.....	12
3.3.8 Monitor Security Controls .....	14
4.0 XML TAXONOMY .....	15
APPENDIX A: ABBREVIATIONS AND ACRONYMS .....	A-1
APPENDIX B: INFORMATION SYSTEM SECURITY XML SCHEMA .....	B-1

## List of Figures

Figure 3-1. Interrelationship of Activities .....	5
Figure 3-2. Risk Management Framework .....	8
Figure 3-3. Authorization to Operate (ATO) Process.....	13

## List of Tables

Table 3-1. Program, Integration, and System Security Activities .....	6
Table 4-1. Taxonomy Category Descriptions.....	15
Table 4-2. XML Taxonomy.....	15

## EXECUTIVE SUMMARY

Federal agencies implement information security programs to provide security for the information and systems that support its operations and assets. These programs, based on laws, regulations, standards, and guidelines, are intended to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements. A properly implemented information security program produces certain artifacts throughout its life cycle that are designed to demonstrate its maturity and the security status of its information systems.

The Information System Security (ISS) Reference Data Model was developed on the fundamental premise that information system-specific security activities must be built on a comprehensive security program and that many of the artifacts produced by these activities can be managed through automated tools. This publication, and its associated Extensible Markup Language (XML) taxonomy and schema, is intended to:

- Serve as a guideline for software tool developers and federal agencies that wish to develop an automated process for managing an information security program; and
- Enable greater interoperability between information system security tools, resulting in more practical and cost-effective information security program management.

The XML taxonomy and schema, based on the security controls contained in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, and the Risk Management Framework, provide a mechanism to denote or “tag” information security artifacts and enable Federal Information Security Management Act (FISMA) related software tools to share information through a common nomenclature of data fields found in most information system security software tools. The process of documenting and confirming many of these artifacts can be automated, and this automation can be used to support legislative reporting requirements.



# 1.0 INTRODUCTION

## 1.1 Purpose and Scope

Managing an organization's information security program is complex and resource-intensive. The numerous reports, documents, and day-to-day security-related events that must be handled can keep the most organized information security officer overburdened. Automating many of the programmatic functions involved in information security can aid organizations to spend more time on securing systems, and less time on the required paperwork activities. There are many automated tools available to assist organizations, yet many of the tools cannot share data. This document will assist in managing an information security program by standardizing data fields to depict information systems and the status of information system security controls. A taxonomy and high-level XML schema is provided for software tool developers and federal agencies that wish to develop automated processes to support management of an information security program.

The Information System Security (ISS) Reference Data Model and Extensible Markup Language (XML) schema are centered on the security controls contained in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, to demonstrate the information system security data and artifacts that can be automated. The activities are presented as key components in the NIST Risk Management Framework. Potential interdependencies such as records management, environmental protection, and human resources are also presented. However, it is envisioned that tool developers will be able to build out the XML schema to include additional automated capabilities (e.g., quarterly and annual Federal Information Security Management Act [FISMA] reports, configuration/vulnerability management, system security plans, and privacy impact assessments).

The use of this reference data model and XML schema by tool developers will support effective data sharing between information system security software tools (ex, system security and contingency planning tools, compliance reporting tools). Many agencies use multiple software packages to create and maintain system security documentation and security program reports. The reference data model is intended to enable greater interoperability between these tools, resulting in more practical and cost-effective automation.

## 1.2 Audience

This document is intended to provide software tool developers with an XML taxonomy and schema to efficiently automate the collection of system-specific and security program artifacts. It may also be used by information security program managers and other information security personnel responsible for the procurement, deployment, and integration of software tools. In addition, this document may be used by nongovernmental (private sector) organizations.

## 1.3 Document Structure

This document is divided into four sections: Introduction, Background, Reference Model, and XML Taxonomy. Section 1, Introduction, presents the basic purpose and scope of the document. Section 2, Background, includes references to the legislative drivers, standards, and guidelines that support an information system security program. Section 3, Reference Model, outlines the major activities in implementing the NIST Risk Management Framework. This section also

discusses a variety of programmatic and integration activities that occur to achieve a robust information security program at the organizational and system levels. Section 4, XML Taxonomy, presents the XML taxonomy and naming conventions to be used in creating a checklist that confirms that required security activities and security controls have been established and implemented.

Two appendices include additional information:

Appendix A is a collection of the abbreviations and acronyms used in this document.

Appendix B provides the Information System Security XML schema used to document and report on security control implementation. This can be used by software tool developers to support FISMA reporting requirements.

## 2.0 BACKGROUND

In December 2002, Congress emphasized the importance of information security when it included FISMA as part of Title III of the Electronic Government Act.<sup>1</sup> FISMA reestablished NIST as the agency charged with development of information system security standards and guidelines for unclassified information systems and reauthorized annual reviews of information systems and reporting to the OMB on the progress of meeting mandated security requirements.

NIST has developed a series of Risk Management Framework (RMF) guideline documents to provide assistance in categorizing information systems; evaluating threats; developing risk mitigation strategies; developing management, operational, and technical security controls; conducting assessments to ensure that security controls are in place, operating as intended, and ultimately authorizing information systems to operate; and maintaining a continuous state of security compliance. Federal Information Processing Standards (FIPS) and NIST SPs relevant to the Information System Security Reference Data Model include the following:<sup>2</sup>

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*;
- SP 800-30, *Risk Management Guide for Information Technology Systems*;
- SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*;
- SP 800-53, *Recommended Security Controls for Federal Information Systems*;
- Draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*;
- SP 800-55, *Security Metrics Guide for Information Technology Systems*;
- SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;
- SP 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*; and
- SP 800-100, *Information Security Handbook: A Guide for Managers*.

Confirming that security controls are in place, as well as tracking gaps in current information systems, can be a resource-intensive process. This document provides:

- A description of security activities that manage risk to an acceptable level for information and information systems. Some activities are conducted by organizational entities outside of the information system—these are considered program-level activities and usually involve implementation of enterprise and integration services through common processes and common security controls across the agency. Other activities are conducted at the information system level—these are considered information system-

---

<sup>1</sup> H.R. 2458, December 8, 2002.

<sup>2</sup> Various NIST documents are revised over time. The references below intentionally do not include specific dates to indicate that the reference is the latest version of the named document.

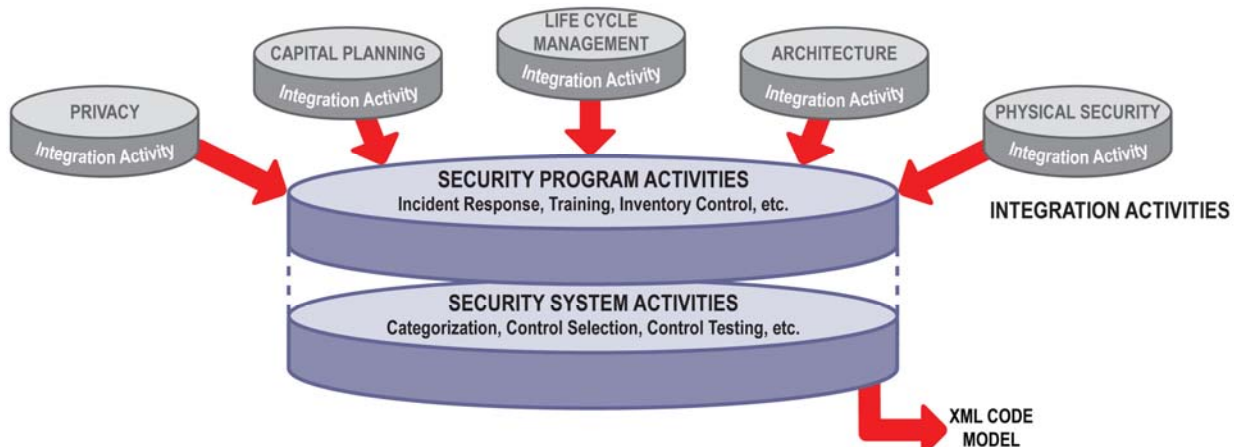
level activities and usually involve implementation of security controls that account for the unique mission and features of the organization providing the service.

- An XML taxonomy foundation and schema which captures the security control-level activities and artifacts which can be used to automate management of an information system security program.

## 3.0 REFERENCE MODEL

### 3.1 Two-Level Reference Model

A variety of programmatic, integration, and information system-specific security activities must occur to achieve information security at the program and system levels. Figure 3-1 depicts the interrelationship of these activities.



**Figure 3-1. Interrelationship of Activities**

The program level includes activities that are institutionalized across an agency to ensure that its information system security program is being consistently managed. These activities are considered to be program security activities and are usually prescriptive in nature. They often include specific procedures that must be followed (e.g., forms to be completed, a series of actions to be followed, or activities that must be accomplished within specific time frames) to ensure a minimum baseline compliance level.

Certain program-level activities play a major role without providing a specific security function. These activities are considered to be integration activities. For example, they may include capital planning, which ensures that funding for security is included in life cycle budget requests, or human resources, which ensures that policies are in place to address employee terminations and violations.

Activities at the program level are usually centrally managed at agency headquarters to ensure that a common interpretation of security requirements is being implemented. These program-level security controls are often called *common security controls*. By centrally managing the development, implementation, and assessment of the common security controls designated by an organization, security costs can be amortized across multiple information systems. Security controls not designated as common security controls are considered *information system-specific security controls* and are the responsibility of the individual information system owner. The taxonomy provided in this document does not differentiate between common security controls and information system-specific security controls.

This document's focus is on a suggested taxonomy that can be utilized to report or document that the required security controls (both common and system-specific) are implemented on information systems, and that these controls are working as intended. This document is designed

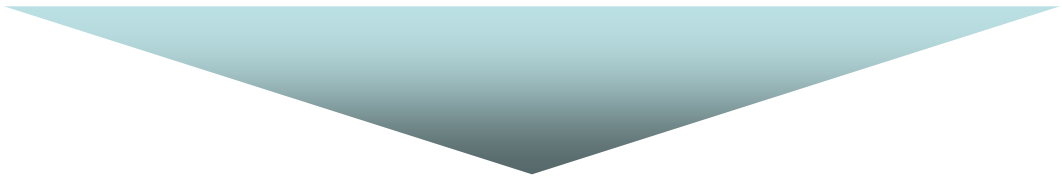
to provide guidelines to tool developers on how to “tag” security control artifacts so an organization’s information security program can be easily managed through automating many of the risk management activities with software tools that are interoperable and share data across many tools used in the program and integration activities (see suggested taxonomy in Section 4.0).

Table 3-1 lists the programmatic, integration, and system security activities that are typically a part of an information security program.

**Table 3-1. Program, Integration, and System Security Activities**

<b>Program Level</b>	
<b>Program Security Activities</b>	<b>Integration Activities</b>
<ul style="list-style-type: none"> <li>• Annual and Quarterly Review and Reporting of Information Security Program</li> <li>• Asset Inventory</li> <li>• Awareness and Specialized Security Training</li> <li>• Continuity of Operations</li> <li>• Incident Response</li> <li>• Periodic Testing and Evaluation</li> <li>• Plan of Action and Milestones</li> <li>• Policies and Procedures</li> <li>• Risk Management</li> </ul>	<ul style="list-style-type: none"> <li>• Business Risk</li> <li>• Capital Planning and Investment Control (CPIC)</li> <li>• Configuration Management</li> <li>• Enterprise Architecture (EA)</li> <li>• Environmental Protection</li> <li>• Human Resources</li> <li>• Personnel Security</li> <li>• Physical Security</li> <li>• Privacy</li> <li>• Records Management</li> <li>• Strategic Plan</li> <li>• System Development Life Cycle (SDLC)</li> </ul>



<b>System Level</b>
<b>System Security Activities</b>
<ul style="list-style-type: none"> <li>• Categorize the Information System</li> <li>• Select Security Controls</li> <li>• Supplement Security Controls</li> <li>• Document Security Controls</li> <li>• Implement Security Controls</li> <li>• Assess Security Controls</li> <li>• Authorize the Information System</li> <li>• Monitor Security Controls</li> </ul>

A variety of programmatic and integration requirements must be in place and operational to provide a structure for these information systems to operate securely. However, the taxonomy and XML provided in this document focuses on system security activities as defined in the Risk Management Framework. It is expected that these activities can be automated, and this

automation can be used to document and report on the status of information system and program security.

## 3.2 Dependency and Interdependency

When designing tools, it is important to note that information system-level security controls cannot be completely developed or applied without considering program-level security controls. For example, if the agency consolidates processing facilities as part of an overall reorganization and one of the sites closed was the backup for the information system being reviewed, closure of this facility must be reflected in the risk assessment, the contingency plan, and the security plan. If more than one tool is used to generate these documents, the taxonomy provided in this document facilitates data sharing among the tools.

The following definitions are used to describe relationships between activities:

- **Interdependency Relationship.** When the activities of A and B are mutually reliant on each other to successfully complete the analysis or implementation.
- **Dependency Relationship.** When activity B cannot be performed without the input from activity A. Failure to receive input from activity A results in incomplete analysis or inadequate implementation of activity B.

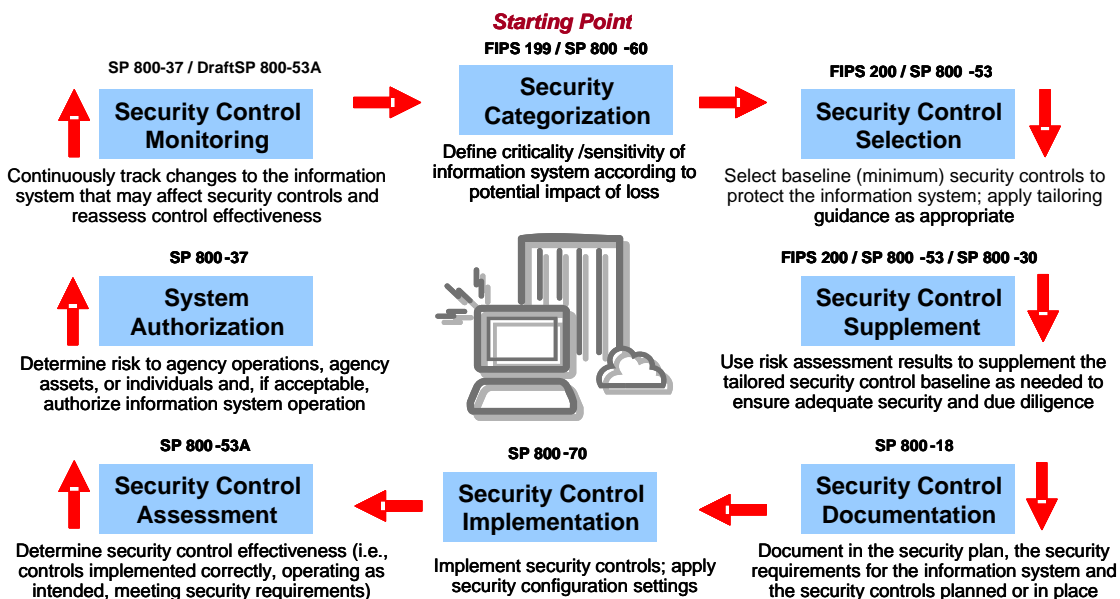
For example, awareness training has an interdependency relationship with the system security plan. Awareness training should not be completed until vulnerabilities to the environment have been identified and security plan(s) have been modified to ensure that the training modules accurately reflect these issues. The system security plan must also ensure that the training modules being prepared reflect the vulnerabilities being faced, or the effectiveness of the security control will be compromised.

Dependency relationships are a little more straightforward—the initial accreditation boundary, which is an information system-level activity, cannot be determined until all assets that constitute the information system have been identified. Determination of the initial accreditation boundary is dependent on asset inventory security control, which is a program-level activity.

This discussion of dependent and interdependent security activities is provided to ensure these relationships between program and system level security activities are considered. The XML taxonomy and schema provided in this document do not capture or represent the specific dependency and interdependency relationships between program and system level security activities.

## 3.3 System Level

The system level encompasses activities that are specifically required within the Risk Management Framework and detailed in NIST Special Publications. As illustrated in Figure 3-2, these activities are part of a cyclical continuous improvement process.



**Figure 3-2. Risk Management Framework**  
*Activities to develop a system-level security defense in depth can be mapped to these guidelines.*

System-level activities result in the implementation of system-specific security controls designed to account for unique environmental considerations, the information being protected, and specific operational (mission) requirements. The degree of flexibility is determined by allowing organizations to selectively define input values for certain parameters associated with the security controls and is achieved through use of assignment and selection operations within the main body of the security control.

System-level activities are the responsibility of the information system owners to implement, institutionalize, and monitor. The Chief Information Officer (CIO) ensures that these activities have been completed through quarterly reporting mechanisms or via specific data calls to provide evidence of compliance.

The following sections outline the major activities in implementing the NIST Risk Management Framework. Each section identifies the steps for completion of each task and provides a tip for automating it.

### 3.3.1 Categorize the Information System

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, should be used as a foundation for initially determining an information system’s security categorization. Final determination should be made based on organizational factors such as risk and the impact of loss to operations.

The business function that the assets support is a critical aspect of information system categorization. Business type will affect the confidentiality, integrity, and availability (CIA) and level of impact to the agency’s mission if the information is compromised. The unique characteristics of the information system or environment must also be considered because they



influence the impact level of the information system. For example, an information system infrastructure housed within the confines of a gated campus with its own power plant may be considered at less risk than an information system infrastructure located in a city building that is dependent on public utilities.

Each step of the security categorization process includes dependent and interdependent functions that must be considered. For example, if the information system being categorized is interconnected to other information system(s), then a Memorandum of Understanding (MOU) needs to be developed and reviewed to ensure that the impact level assigned to this information system does not put the connecting information system at risk or vice versa.

***Automation Tip***

Tool developers can create a taxonomy whereby each asset of an information system is assigned a business function designation and a final impact level within the configuration tables of that asset. An asset management tool can be used to query each device to ensure that the asset is properly grouped into the accreditation boundary that has the most appropriate set of controls (see Section 4, XML Taxonomy).

### **3.3.2 Select Security Controls**

The process of security control selection should be consistently applied to all information and information systems. The initial security categorization will lead to an examination of the prescribed security controls in SP 800-53. Organizations have the flexibility to tailor security control baselines through application of scoping guidance, selection of compensating security controls, and the specification of organization-defined parameters to reflect the operational environment, mission, and risk tolerance of the organization. If a specific security control is not feasible for the organization, compensating security controls from other security control families can be selected to provide a similar level of assurance for the security function. For example, session lock is required for all moderate-impact and high-impact information systems—but if an overarching need requires that session lock not be enabled on a particular information system, the room where the information system is located should remain locked at all times. In this example, the lack of logical access control (no session lock) can be compensated by additional physical access controls (the room remains locked).

***Automation Tip***

Tool developers can augment the taxonomy created in the previous step by tagging each asset with the requisite security control(s) being applied. The asset management tool can be used to query each device to ensure that controls for each asset are properly assigned. The tool would also confirm that assets have security controls only for the accreditation boundary for which they belong.

### 3.3.3 Supplement Security Controls

The tailored security control baseline must be assessed against the level of risk associated with the information system to ensure that residual risks have been appropriately mitigated. If vulnerabilities are still not being adequately addressed, additional security controls must be applied to information systems within the accreditation boundary to supplement the currently selected security controls. Additional security controls can include management, operational, or technical security controls. Enterprise-level common security controls should be considered as part of the total security control set.

The purpose of reviewing the tailored security control baseline with respect to risk assessment is to ensure that all known vulnerabilities are being reduced to an acceptable level as determined by the authorizing official and information system owner. It should be noted that not all security controls will be implemented concurrently. It is the responsibility of the information system owner to track security control implementation progress and update the Plan of Action and Milestones (POA&M) to reflect the current scenario.

#### *Automation Tip*

Tool developers can augment the taxonomy created in the previous step by tagging each asset with the additional security control(s) being added as a result of the supplement process. As the level of risk changes, an extract of the additional controls can be made to determine whether the security controls are still required or sufficient to address the updated risk posture.

### 3.3.4 Document Security Controls

Each accreditation boundary and all information resources contained should be documented in a system security plan as detailed in NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*. Agencies have flexibility in determining what constitutes an information system. If a set of information resources is identified as an information system, the resources should generally be under the same direct management control.

It is also possible for an information system to contain multiple *subsystems*. A subsystem is a major subdivision or component of an information system, consisting of information, information technology, and personnel that perform one or more specific functions. Subsystems typically fall under the same management authority, are included within a single system security plan, and should be identified separately along with the information system owner.

The operational status of the information system should also be identified in the security plan. Roles and responsibilities for all key personnel with security functions should be defined in this document or in supporting documentation that is referenced in the plan. The security plan should also describe how the security control is being implemented (or is expected to be implemented); any scoping guidance that has been applied plus the type of consideration; whether it is a common security control; and who is responsible for the control's implementation.

#### *Automation Tip*

Developers can map assets of the accreditation boundary to a metafile that contains information about the accreditation boundary itself. In this manner, data applying to all assets within an accreditation boundary can be quickly accessed and centrally managed. Developers and agencies that procure these tools need to ensure that there is sufficient flexibility to support a metalanguage, as well as the protocols for accessing accreditation boundary information.

### **3.3.5 Implement Security Controls**

Once each asset is assigned a business function designation and impact level, a configuration baseline setting should be established for each asset (see NIST SP 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklist Users and Developers*). In addition to this implementation of configuration settings, each asset should have a pointer indicating whether an outstanding POA&M item affects its security posture.

Security plan documentation should describe the standard configuration and explain how security controls are to be implemented for the components (devices) that comprise the information systems. In some cases, however, not all security controls can be implemented for all devices because of legacy applications, unique systems, information systems that are maintained but not controlled (e.g., appliance systems), or the information system's life cycle. In these cases, a compensating security control strategy should be implemented. For example, legacy applications may have to be run on information systems located behind dedicated firewalls to keep the vulnerability of the older applications from affecting the rest of the infrastructure.

#### *Automation Tip*

Tool developers need to ensure that taxonomy used to describe security controls in place for an accreditation boundary can support a high-level assessment of the program as well as a detailed assessment of individual security controls within an information system. The XML taxonomy provided in Section 4 offers a framework for tracking these individual security controls.

### **3.3.6 Assess Security Controls**

NIST Draft Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, describes an assessment methodology that determines the overall effectiveness of security controls employed within organizational information systems through evaluating whether a security control is implemented correctly, operating as intended, and providing the desired outcome with respect to meeting the information security requirements of the information system. The assessment methods and procedures from Draft SP 800-53A should be used as a starting point for, and input into, these security control assessment plans.

Organizations should adjust and supplement the assessment procedures from Draft SP 800-53A, taking into consideration platform-specific (i.e., hardware, software, or firmware) dependencies or organizational dependencies resulting from employment of the security controls within the information system.

Selection of appropriate assessment procedures for a particular organizational information system depends on three factors:

1. The FIPS 199 impact level of the information system;
2. The specific security controls selected and employed by the organization to protect the information system; and
3. The assurance or level of confidence that the organization must have in determining effectiveness of the security controls within the information system.

Once methods of assessing security controls have been determined, a security test and evaluation (ST&E) plan can be generated. The ST&E provides evidence that the security controls implemented on an information system properly protect information that the system stores and processes.

Assessment procedures are self-documenting in that the assessor records test results in the plan. The assessment methodology creates a test baseline for the system by testing the baseline and recording baseline results. A technical report that summarizes these test results and provides recommendations for improvement (if applicable) typically concludes the assessment process.

Recommendations for improvement (if any) are discussed with the senior agency information security officer and information system owner. A POA&M is generated for all deficiencies that are to be mitigated. Those that are not mitigated should be added to the residual risk statement for the information system. The ST&E report, risk analysis decisions, security plan, POA&Ms, and accreditation letter are then prepared and presented to the authorizing official.

#### *Automation Tip*

As discussed in Section 3.3.6, tool developers need to ensure that the taxonomy can support a detailed assessment of the individual security controls. The tool should perform a mapping of the security controls to assets within each information system to ensure that all requisite security controls have been implemented. Each security control could be tagged for the type of test(s) (i.e., examine, interview, test from draft SP 800-53A) that would be used to confirm that the control is operating as intended.

### **3.3.7 Authorize the Information System**

All federally operated and contractor-operated federal information systems must obtain an Authorization to Operate (ATO) to process and transmit information. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for the certification and accreditation (C&A) of information systems that support executive agencies of the federal government.

Security certification determines the extent to which the information system security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to

meeting the security requirements for the system. Security accreditation is the official management decision given by a senior agency official (authorizing official) to authorize operation of an information system.

The information system accreditation package documents results of the security certification, and provides the authorizing official with essential information needed to make a credible, risk-based decision on whether to authorize the information system's operation. This package contains the System Security Plan (SSP); the Security Assessment Report (SAR), which includes the applicable ST&E report; and the POA&M. The SSP can reference or contain all supporting documentation (e.g., risk assessment, contingency plan, and asset inventory).

The information system accreditation package is prepared and presented to the authorizing official. The authorizing official then reviews the package in order to ensure the adequacy of the security controls implemented for the information system. Based on the results of this review, the authorizing official makes one of three decisions: to grant the ATO, grant an Interim ATO (IATO), or deny the ATO. This decision-making process is shown in Figure 3-3.



**Figure 3-3. Authorization to Operate (ATO) Process**

The authorizing official, in considering this decision, must also look at the information system relative to the business mission it supports and the organization that owns and operates the information system. The authorizing official must often make a decision on an information system that is currently in use, and the disruption to the organization and its mission may be such that cessation of service is not feasible. In these instances, the authorizing official may grant an IATO for much shorter duration and require periodic progress meetings to ensure that deficiencies are being resolved quickly.

***Automation Tip***

XML tagging can be used for the documentation suite to indicate information such as last review date and version number. XML can also be used for program-level activities, to confirm that dependent and interdependent activities have taken place (e.g., that training reflects the most current cyber issues of concern, or that the configuration benchmark is consistent with the latest recommendations).

### 3.3.8 Monitor Security Controls

All information systems are dynamic in nature—operating systems are patched or upgraded to the next major release, baseline configuration settings may change, new computing devices are added to the network, and new applications and information systems may come online. In addition, interconnection agreements may be established which might require new security controls to be implemented across the infrastructure.

Continuous monitoring is intended to provide oversight of security controls in the information system on an ongoing basis and inform the authorizing official when changes occur that might impact the system's security. These monitoring activities include configuration management and control, security impact analyses of changes to the information system, ongoing assessment of security controls, and status reporting. The organization establishes selection criteria for security control monitoring and selects a subset of the security controls employed within the information system for purposes of continuous monitoring. NIST Special Publications 800-37 and 800-53 provide guidelines on the continuous monitoring process. Draft SP 800-53A provides guidelines on the assessment of security controls.

FISMA requires that each information system be reviewed at least annually. These security control assessments should not be interpreted by organizations as adding additional assessment requirements to requirements already in place. Organizations can satisfy the FISMA requirement by using security control assessment results from any of the following sources, including security certifications conducted as part of a routine information system accreditation or reaccreditation process; ongoing continuous monitoring activities; self or independent assessments; or routine testing and evaluation of the information system as part of the ongoing System Development Life Cycle (SDLC) process and changes approved by configuration management. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program that is capable of producing the data needed to determine the actual security status of the information system.

#### *Automation Tip*

Developers need to ensure that scripting languages for customization of data collection has been designed to enable *open-ended* queries. Collection of data from the information system needs to be optimized to minimize the amount of data collected or monitored to ensure that the configured state has not changed. The tool needs to support data aggregation as well as data summarization to minimize the need to send source data outside the local environment. Finally, the tool selected should be extensible to other asset management tools that may be in use. A robust application program interface (API) to other tool suites should also be required.

## 4.0 XML TAXONOMY

This section describes the XML taxonomy and naming conventions that can be used by tool developers to standardize on the common data fields found in information system security-related tools. This can be used to create a checklist to confirm that required system security activities and security controls have been established and implemented. Table 4-1 provides a brief descriptive overview of the XML taxonomy categories.

**Table 4-1. Taxonomy Category Descriptions**

Category	Description
RMF Activity	Map directly to the NIST Risk Management Framework (RMF) activities
RMF Sub-activity	Security activities that occur within a given RMF activity
Activities/Artifacts	Refer to a specific artifact (e.g., document, metric, action) created or performed in support of the RMF sub-activity.
Data Type	Provide the function's XML data type (e.g., String, Yes/No, Date)
Required	Specify whether the evidence item is a requirement (e.g., Yes, No, Nil)
Comments	Add additional clarification to compliance items

Table 4-2 presents the XML taxonomy and associated system security activities that are specifically required within the Risk Management Framework. This taxonomy maps to the Information System Security XML schema contained in Appendix B. Using this convention will aid in automating the process of documenting and reporting on security control implementation, and this automation can be used to support FISMA reporting requirements.

**Table 4-2. XML Taxonomy**

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
General System Information		System Name	String	Yes	
		System Type	String	Yes	GSS, Major, Minor
		Common Platform Enumeration (CPE) Identifier	CPE <sup>3</sup>	Yes	

<sup>3</sup> The Common Platform Enumeration (CPE) (<http://cpe.mitre.org>) is a standards based dictionary of software product names (e.g., vendor names, product names, version numbers, and editions). CPE is a trademark of The MITRE Corporation. For each CPE identifier, provide the following data:

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
CPE	CPE Identifier	CPE Instances	String	Yes	
		Number of Instances	Int	Yes	

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments	
<b>Categorize the Information System</b>	Identify Accreditation Boundaries	Physical Network Topology Identified	Yes/No	Yes		
		Logical Network Topology Identified	Yes/No	Yes		
	Business Function	Specific Business Function	String	Yes	Business function identified	
		Description of the Business Function	String	Yes	Description provided	
		Specific Business Area Associated With the Business Function Record	String	Yes	Business area identified	
	Perform Impact Assessment	CIA Impact Completed	Date	Yes; value can be nil		
	Determine Rating	System Overall Categorization Determination	String	Yes	Low, Moderate, High (based on high water mark)	
		Confidentiality	String	Yes	Low, Moderate, High	
		Integrity	String	Yes	Low, Moderate, High	
		Availability	String	Yes	Low, Moderate, High	
	<b>Select Security Controls</b>	FIPS 199 Decision	Threat Statement	Date	Yes; value can be nil	
			Initial Risk Assessment	Date	Yes; value can be nil	
			Accreditation Boundary Grouping	Date	Yes; value can be nil	Listing of systems with same risk profile
Baseline Security Control List (per 800-53)		Access Control (AC) Family <sup>4</sup>		No	Required only if a control number is present	

<sup>4</sup> For every security control family, there can be one or many control numbers. As an example, the sub-element is "Access Control." For each security control, provide the following data.

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
Security Control Family	Security Control Number		String	Yes	The control number (XX-NN). 'AC-1' is an example
		In Place	Yes/No	Yes	Based on security categorization rating
		Security Control Name	String	Only if "In Place" is "Yes" and is not an enhancement	Correlates to security control number
		Security Control or Enhancement Description	String	Yes	



<b>RMF Activity</b>	<b>RMF Sub-activity</b>	<b>Activities/Artifacts</b>	<b>Data Type</b>	<b>Required</b>	<b>Comments</b>
<b>Select Security Controls, continued</b>		Awareness and Training (AT) Family		No	
		Audit and Accountability (AU) Family		No	
		Certification and Accreditation (CA) Family		No	
		Configuration Management (CM) Family		No	
		Contingency Planning (CP) Family		No	
		Identification and Authentication (IA) Family		No	
		Incident Response (IR) Family		No	
		Maintenance (MA) Family		No	
		Media Protection (MP) Family		No	
		Physical and Environmental Protection (PE) Family		No	
		Planning (PL) Family		No	
		Personnel Security (PS) Family		No	
		Risk Assessment (RA) Family		No	
		System and Services Acquisition (SA) Family		No	
		System and Information Integrity (SI) Family		No	
		System and Communication Protection (SP) Family		No	
	Initial Security Control Baseline	Gap Analysis of Security Controls Not Incorporated	Yes/No	Yes	Gap analysis complete

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
<b>Select Security Controls, continued</b>	Updated Risk Assessment	Risk Assessment With Gap Analysis	Yes/No	Yes	
	Compensating Security Controls	Security Control Family <sup>5</sup>		No	Is the compensating security control required to address a gap?
	Accept Risk	POA&M Completed	Yes/No	Yes	
<b>Supplement Security Controls</b>	Additional Security Controls – Special Factors	Security Control Family <sup>6</sup>		No	Is the additional security control required to address a critical factor or security enhancement?
<b>Document Security Controls</b>	Document System and Component Accreditation Boundaries	Accreditation Boundaries Documented	Yes/No	Yes	
	Develop Information System Accreditation Boundary Security and Contingency Plans	Security and Contingency Plan Exists for Each Information System Accreditation Boundary	Yes/No	Yes	Per NIST SP 800-18
	Distribute Documentation	Procedures Online or Available for All Responsible Parties to Follow	Yes/No	Yes	Intranet Web portal or policies and procedures physically in all data and system owner offices?
	Update POA&M	Continuous Update with Quarterly Reporting	Date	Yes	Last date of reporting?
		System-level POA&M	Date	Yes; value can be nil	If applicable
		Organizational POA&M	Yes/No	Yes	If applicable

---

<sup>5</sup> Refer to Footnote 4.

<sup>6</sup> Refer to Footnote 4.

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
<b>Implement Security Controls</b>	Determine Level to Implement Each Security Control	Identification of Security Control Authority— CIO/SAISO (CISO)	String	Yes	Agency-level identifier
		Identification of Security Control Authority—Bureau-Component Level	String	Yes	Site-level identifier
		Identification of Security Control Authority—System Owner	String	Yes	System-level identifier
	Security Control Applied	Security Control Family in Place <sup>7</sup>		Yes	Depending on the security control, this can be a database, manual log, plan, report, etc.
		Artifact Evidence	String	Yes	
	Scoping Guidance Applied	Unique Condition Identified	Yes/No	No	
	Compensating Security Control Applied	Unique Condition Identified	Yes/No	No	Risk statement
		Security Control Family in Place <sup>8</sup>		No	
		Artifact Evidence	String	No	
	Additional Security Control Applied	Unique Condition Identified	Yes/No	No	Risk statement
		Security Control Family in Place <sup>9</sup>		No	

<sup>7</sup> For each SP 800-53 control, the following is required:

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
Security Control Family in Place	Control Number		String	Yes	The control number (YY). 'AC-1' is an example
		Security Control Type	String	Yes	Options are Common, System-specific, Hybrid
		Last Date Security Control Assessed	Date	Yes	
		Assessor Name	String	Yes	
		Assessor Independence	String	Yes	Options are Self, Independent
		Assessed Security Control Effectiveness	String	Yes	Options are Satisfied, Partially Satisfied, Not Satisfied
		Assessment Steps Used	String	Yes	
		Assessment Evidence	String	Yes	

<sup>8</sup> Refer to footnote 7.

<sup>9</sup> Refer to footnote 7.

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
<b>Implement Security Controls, continued</b>		Artifact Evidence	String	No	Depending on the security control, this can be a database, manual log, plan, report, etc.
<b>Assess Security Controls</b>	ST&E Plan <sup>10</sup>	ST&E Test Plan	Yes/No	Yes	If yes, indicate date
		ST&E Test Plan—Date Completed	Date	Yes; value can be nil	Date completed
		Rules of Engagement	Yes/No	Yes	If yes, indicate date
		Rules of Engagement—Date Completed	Date	Yes; value can be nil	Date completed
	Evaluate ST&E Results	Security Assessment Report (SAR)	Yes/No	Yes	If yes, indicate date
		SAR—Date Completed	Date	Yes; value can be nil	Date completed
	Document ST&E Results	ST&E Results	Yes/No	Yes	If yes, indicate date
		ST&E Results—Date Completed	Date	Yes; value can be nil	Date completed
		Findings/Corrective Action Report	Yes/No	Yes	If yes, indicate date
		Findings/Corrective Action Report—Date Completed	Date	Yes	Date completed
		Update Risk Assessment	Date	Yes	Date completed
		Update SSP	Date	Yes	Date completed
	Develop POA&M	Findings/Corrective Actions Incorporated	Yes/No	Yes	If yes, indicate date
		Findings/Corrective Actions Incorporated—Date Completed	Date	Yes; value can be nil	Date completed
		Budget Impact Assessment	Yes/No	Yes	CPIC-300, 53, other
<b>Authorize the Information System</b>	Review ST&E Results	Signed SAR Result	Yes/No	Yes	If yes, indicate date

<sup>10</sup> Security control monitoring is done as part of the initial C&A and is an ongoing annual activity throughout the system life cycle. The Monitor Security Controls RMF activity can be found in section 3.3.8.

<b>RMF Activity</b>	<b>RMF Sub-activity</b>	<b>Activities/Artifacts</b>	<b>Data Type</b>	<b>Required</b>	<b>Comments</b>
<b>Authorize the Information System, continued</b>		Signed SAR Result—Date Completed	Date	Yes	Date completed
		Signed Findings	Yes/No	Yes	If yes, indicate date
		Signed Findings—Date Completed	Date	Yes; value can be nil	Date completed
		Corrective Action Reports	Yes/No	Yes	If yes, indicate date
		Corrective Action Reports—Date Completed	Date	Yes; value can be nil	Date completed
	Review POA&M Schedule	All Corrective Actions are Scheduled for Completion Within an Acceptable Time Frame	Yes/No	Yes	If no, update risk assessment as needed
	Prepare ATO Justification	Recommendation Letter	Yes/No	Yes	If yes, indicate date
		Recommendation Letter—Date Completed	Date	Yes; value can be nil	Date completed
		Signed ATO	Yes/No	Yes	If yes, indicate date
		Signed ATO—Date Completed	Date	Yes; value can be nil	Date completed
	Grant/Deny ATO	Denial Letter	Yes/No	Yes	If yes, indicate date
		Denial Letter—Date Completed	Date	Yes; value can be nil	Date completed
		Corrective Actions Plan	Yes/No	Yes	If yes, indicate date
		Corrective Actions Plan—Date Completed	Date	Yes; value can be nil	Date completed
<b>Monitor Security Controls</b>	Configuration Management Reviews	Change Impact Assessment	Yes/No	Yes	

RMF Activity	RMF Sub-activity	Activities/Artifacts	Data Type	Required	Comments
<b>Monitor Security Controls, continued</b>	Documentation Revisions	POA&M Quarterly Report—Approval Date	Date	Yes	Approval date
	Periodic and Ongoing Testing/Assessment—Conduct Continuous Monitoring Activities	Periodic and Ongoing Testing Family <sup>11</sup>		Yes	
	Review of ATO Decision	Outstanding POA&M Items <sup>12</sup>	String	Yes	List actual open POA&M items separately
		IG, GAO Report, and Internal/External Assessment Findings <sup>13</sup>	String	Yes	List actual open items
		ATO—Date Completed	Date	Yes	Date completed

---

<sup>11</sup> Reference Footnote 7.

<sup>12</sup> For each outstanding POA&M report/finding, the following are needed:

RMF Activity	RMF Sub-activity	Compliance Items Checklist	Data Type	Required	Comments
POA&M	Report/Finding	Description	String	Yes	
		Date Due	Date	Yes	
		Date Completed	Date	Yes	
		Individual Responsible	String	Yes	
		Individual Verified	String	Yes	
		Comments	String	Yes	

<sup>13</sup> For each Inspector General (IG) Government Accountability Office (GAO) report/finding, refer to the table in Footnote 12.

## APPENDIX A: ABBREVIATIONS AND ACRONYMS

AC	Access Control
API	Application Program Interface
AT	Awareness and Training
ATO	Authorization to Operate
AU	Audit and Accountability
BIA	Business Impact Analysis
CA	Certification, Accreditation, and Security Assessments
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
EA	Enterprise Architecture
E-Gov	Electronic Government
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IATO	Interim Authority to Operate
IG	Inspector General
IR	Incident Response
ISS	Information System Security
IT	Information Technology
MA	Maintenance
MOU	Memorandum of Understanding
MP	Media Protection
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PL	Planning
PMA	President's Management Agenda
POA&M	Plan of Action and Milestones
PS	Personnel Security

RA	Risk Assessment
RMF	Risk Management Framework
SA	System and Services Acquisition
SAISO	Senior Agency Information Security Officer
SAR	Security Assessment Report
SC	System and Communications Protection
SDLC	System Development Life Cycle
SI	System and Information Integrity
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
XML	Extensible Markup Language



## APPENDIX B: INFORMATION SYSTEM SECURITY XML SCHEMA

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:fisma="urn:us:gov:nist:fisma" xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="urn:us:gov:nist:fisma"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.4">
  <xs:element name="System">
    <xs:annotation>
      <xs:documentation> This is the root element for the NIST FISMA System XSD. These models should be used to indicate if the
organization meets NIST's
      interpretation of FISMA. </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element name="GeneralSystemInformation" type="fisma:GeneralSystemInformationType"/>
        <xs:element name="CategorizeTheInformationSystem" type="fisma:CategorizeTheInformationSystemType"/>
        <xs:element name="SelectSecurityControls" type="fisma:SelectSecurityControlsType"/>
        <xs:element name="SupplementSecurityControls" type="fisma:SupplementSecurityControlsType"/>
        <xs:element name="DocumentSecurityControls" type="fisma:DocumentSecurityControlsType"/>
        <xs:element name="ImplementSecurityControls" type="fisma:ImplementSecurityControlsType"/>
        <xs:element name="AssessSecurityControls" type="fisma:AssessSecurityControlsType"/>
        <xs:element name="AuthorizeTheInformationSystem" type="fisma:AuthorizeTheInformationSystemType"/>
        <xs:element name="MonitorSecurityControls" type="fisma:MonitorSecurityControlsType"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <!-- *****-->
  <!--Complex Types-->
  <!-- *****-->
  <!-- General System Information complex types -->
  <xs:complexType name="GeneralSystemInformationType">
    <xs:sequence>
      <!--TODO: Unless these elements are referenced somewhere else, define here rather than ref the type-->
      <xs:element name="SystemName" type="xs:string"/>
      <xs:element name="SystemType" type="fisma:SystemTypeOptions"/>
      <xs:element name="CPEIdentifier" type="fisma:CPEIdentifierType"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="CPEIdentifierType">
    <xs:sequence>
      <xs:element name="CPEInstance" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```

        <xs:element name="NumberOfInstances" type="xs:int"/>
    </xs:sequence>
</xs:complexType>
<!-- Categorize the Information System complex types -->
<xs:complexType name="CategorizeTheInformationSystemType">
    <xs:sequence>
        <xs:element name="IdentifyAccreditationBoundaries" type="fisma:IdentifyAccreditationBoundariesType"/>
        <xs:element name="BusinessFunction" type="fisma:BusinessFunctionType"/>
        <xs:element name="PerformImpactAssessment" type="fisma:PerformImpactAssessmentType"/>
        <xs:element name="DetermineRating" type="fisma:DetermineRatingType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="IdentifyAccreditationBoundariesType">
    <xs:sequence>
        <xs:element name="PhysicalNetworkTopologyIdentified" type="fisma:YesNo"/>
        <xs:element name="LogicalNetworkTopologyIdentified" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="BusinessFunctionType">
    <xs:sequence>
        <xs:element name="SpecificBusinessFunction" type="xs:string"/>
        <xs:element name="DescriptionOfTheBusinessFunction" type="xs:string"/>
        <xs:element name="SpecificBusinessAreaAssociatedWithTheBusinessFunctionRecord" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="PerformImpactAssessmentType">
    <xs:sequence>
        <xs:element name="CIAImpactCompleted" type="xs:date" nillable="true"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="DetermineRatingType">
    <xs:sequence>
        <xs:element name="SystemOverallCategorizationDetermination" type="fisma:RatingOptions"/>
        <xs:element name="Confidentiality" type="fisma:RatingOptions"/>
        <xs:element name="Integrity" type="fisma:RatingOptions"/>
        <xs:element name="Availability" type="fisma:RatingOptions"/>
    </xs:sequence>
</xs:complexType>
<!-- Select Security Controls complex types -->
<xs:complexType name="SelectSecurityControlsType">

```

```

<xs:sequence>
  <xs:element name="FIPS199Decision" type="fisma:FIPS199DecisionType"/>
  <xs:element name="BaselineSecurityControlListFamily" type="fisma:BaselineSecurityControlListType" minOccurs="0"/>
  <xs:element name="InitialSecurityControlBaseline">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="GapAnalysisOfSecurityControlsNotIncorporated" type="fisma:YesNo"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="UpdatedRiskAssessment">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="RiskAssessmentWithGapAnalysis" type="fisma:YesNo"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="CompensatingSecurityControls" minOccurs="0">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SecurityControlFamily" type="fisma:BaselineSecurityControlListType" minOccurs="0" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="AcceptRisk" type="fisma:AcceptRiskType"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="FIPS199DecisionType">
  <xs:sequence>
    <xs:element name="ThreatStatement" type="xs:date" nillable="true"/>
    <xs:element name="InitialRiskAssessment" type="xs:date" nillable="true"/>
    <xs:element name="AccreditationBoundaryGrouping" type="xs:date" nillable="true"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="BaselineSecurityControlListType">
  <xs:sequence>
    <xs:element name="AccessControl" type="fisma:SecurityControlType" minOccurs="0">
      <xs:annotation><xs:documentation>Required only if a Control Number is present.</xs:documentation></xs:annotation>
    </xs:element>
    <xs:element name="AwarenessTraining" type="fisma:SecurityControlType" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

```

```

<xs:element name="AuditAccountability" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="CertificationAccreditation" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="ConfigurationManagement" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="ContingencyPlanning" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="IdentificationAuthentication" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="IncidentResponse" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="Maintenance" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="MediaProtection" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="PhysicalEnvironmentalProtection" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="Planning" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="PersonnelSecurity" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="RiskAssessment" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="SystemServicesAcquisition" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="SystemInformationIntegrity" type="fisma:SecurityControlType" minOccurs="0"/>
<xs:element name="SystemCommunicationProtection" type="fisma:SecurityControlType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="SecurityControlType">
  <xs:sequence>
    <xs:element name="SecurityControl" maxOccurs="unbounded">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="SecurityControlNumber" type="xs:string"/>
          <xs:element name="InPlace" type="fisma:YesNo"/>
          <xs:element name="SecurityControlName" type="xs:string" minOccurs="0"/>
          <xs:element name="SecurityControlEnhancementDescription" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
<!-- Supplement Security Controls complex types -->
<xs:complexType name="SupplementSecurityControlsType">
  <xs:sequence>
    <xs:element name="AdditionalSecurityControls" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="SecurityControlFamily" type="fisma:BaselineSecurityControlListType" minOccurs="0" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```

                </xs:sequence>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="AcceptRiskType">
    <xs:sequence>
        <xs:element name="POAMCompleted" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<!-- Documentation Security Controls complex types -->
<xs:complexType name="DocumentSecurityControlsType">
    <xs:sequence>
        <xs:element name="DocumentSystemAndComponentAccreditationBoundaries"
type="fisma:DocumentSystemAndComponentAccreditationBoundariesType"/>
        <xs:element name="DevelopInformationSystemAccreditationBoundarySecurityAndContingencyPlans"
type="fisma:DevelopInformationSystemAccreditationBoundarySecurityAndContingencyPlansType"/>
        <xs:element name="DistributeDocumentation" type="fisma:DistributeDocumentationType"/>
        <xs:element name="UpdatePOAM" type="fisma:UpdatePOAMType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="DocumentSystemAndComponentAccreditationBoundariesType">
    <xs:sequence>
        <xs:element name="AccreditationBoundariesDocumented" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="DevelopInformationSystemAccreditationBoundarySecurityAndContingencyPlansType">
    <xs:sequence>
        <xs:element name="SecurityAndContingencyPlanExistsForEachInformationSystemAccreditationBoundary" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="DistributeDocumentationType">
    <xs:sequence>
        <xs:element name="ProceduresOnlineOrAvailableForAllResponsiblePartiesToFollow" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="UpdatePOAMType">
    <xs:sequence>
        <xs:element name="ContinuousUpdateWithQuarterlyReporting" type="xs:date"/>
        <xs:element name="SystemLevelPOAM" type="xs:date" nillable="true"/>
    </xs:sequence>
</xs:complexType>

```

```

        <xs:element name="OrganizationalPOAM" type="fisma:YesNo"/>
    </xs:sequence>
</xs:complexType>
<!-- Security Controls Implementation complex types -->
<xs:complexType name="ImplementSecurityControlsType">
    <xs:sequence>
        <xs:element name="DetermineLevelToImplementEachSecurityControl"
type="fisma:DetermineLevelToImplementEachSecurityControlType"/>
        <xs:element name="SecurityControlApplied" type="fisma:SecurityControlAppliedType"/>
        <xs:element name="ScopingGuidanceApplied" minOccurs="0">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="fisma:UniqueConditionIdentified" minOccurs="0"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="CompensatingSecurityControlApplied" type="fisma:SecurityControlStrategyType" minOccurs="0"/>
        <xs:element name="AdditionalSecurityControlApplied" type="fisma:SecurityControlStrategyType" minOccurs="0"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="DetermineLevelToImplementEachSecurityControlType">
    <xs:sequence>
        <xs:element name="IdentificationOfSecurityControlAuthorityCIOSAIO" type="xs:string"/>
        <xs:element name="IdentificationOfSecurityControlAuthorityBureauComponentLevel" type="xs:string"/>
        <xs:element name="IdentificationOfSecurityControlAuthoritySystemOwner" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="SecurityControlAppliedType">
    <xs:sequence>
        <xs:element name="SecurityControlFamilyInPlace" type="fisma:SecurityControlFamilyFor800-53Type"/>
        <xs:element ref="fisma:ArtifactEvidence" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="SecurityControlFamilyFor800-53Type">
    <xs:sequence>
        <xs:element name="AccessControl" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
        <xs:element name="AwarenessTraining" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
        <xs:element name="AuditAccountability" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
        <xs:element name="CertificationAccreditation" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
        <xs:element name="ConfigurationManagement" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    </xs:sequence>

```

```

    <xs:element name="ContingencyPlanning" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="IdentificationAuthentication" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="IncidentResponse" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="Maintenance" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="MediaProtection" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="PhysicalEnvironmentalProtection" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="Planning" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="PersonnelSecurity" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="RiskAssessment" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="SystemServicesAcquisition" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="SystemInformationIntegrity" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
    <xs:element name="SystemCommunicationProtection" type="fisma:SecurityControlFor800-53Type" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="SecurityControlStrategyType">
  <xs:sequence>
    <xs:element ref="fisma:UniqueConditionIdentified" minOccurs="0"/>
    <xs:element name="SecurityControlFamilyInPlace" type="fisma:SecurityControlFamilyFor800-53Type"/>
    <xs:element ref="fisma:ArtifactEvidence" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="SecurityControlFor800-53Type">
  <xs:sequence>
    <xs:element name="SecurityControl" minOccurs="0" maxOccurs="unbounded">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="SecurityControlNumber" type="xs:string"/>
          <xs:element name="SecurityControlType" type="fisma:SecurityControlTypeOptions"/>
          <xs:element name="LastDateSecurityControlAssessed" type="xs:date"/>
          <xs:element name="AssessorName" type="xs:string"/>
          <xs:element name="AssessorIndependence" type="fisma:AssessorIndependenceOptions"/>
          <xs:element name="AssessedSecurityControlEffectiveness"
type="fisma:AssessedSecurityControlEffectivenessOptions"/>
          <xs:element name="AssessmentStepsUsed" type="xs:string"/>
          <xs:element name="AssessmentEvidence" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```

<!-- Security Controls Assessment complex types -->
<xs:complexType name="AssessSecurityControlsType">
  <xs:sequence>
    <xs:element name="STEPlan" type="fisma:STEPlanType"/>
    <xs:element name="EvaluateSTERResults" type="fisma:EvaluateSTERResultsType"/>
    <xs:element name="DocumentSTERResults" type="fisma:DocumentSTERResultsType"/>
    <xs:element name="DevelopPOAM" type="fisma:DevelopPOAMType"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="STEPlanType">
  <xs:sequence>
    <xs:element name="STETestPlan" type="fisma:YesNo"/>
    <xs:element name="STETestPlanDateCompleted" type="xs:date" nillable="true"/>
    <xs:element name="RulesOfEngagement" type="fisma:YesNo"/>
    <xs:element name="RulesOfEngagementDateCompleted" type="xs:date" nillable="true"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="EvaluateSTERResultsType">
  <xs:sequence>
    <xs:element name="SAR" type="fisma:YesNo"/>
    <xs:element name="SARDateCompleted" type="xs:date" nillable="true"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="DocumentSTERResultsType">
  <xs:sequence>
    <xs:element name="STERResults" type="fisma:YesNo"/>
    <xs:element name="STERResultsDateCompleted" type="xs:date" nillable="true"/>
    <xs:element name="FindingsCorrectiveActionReport" type="fisma:YesNo"/>
    <xs:element name="FindingsCorrectiveActionReportDateCompleted" type="xs:date"/>
    <xs:element name="UpdateRiskAssessment" type="xs:date"/>
    <xs:element name="UpdateSSP" type="xs:date"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="DevelopPOAMType">
  <xs:sequence>
    <xs:element name="FindingsCorrectiveActionsIncorporated" type="fisma:YesNo"/>
    <xs:element name="FindingsCorrectiveActionsIncorporatedDateCompleted" type="xs:date" nillable="true"/>
    <xs:element name="BudgetImpactAssessment" type="fisma:YesNo"/>
  </xs:sequence>
</xs:complexType>

```



```

<!-- Authorize The Information System complex types -->
<xs:complexType name="AuthorizeTheInformationSystemType">
  <xs:sequence>
    <xs:element name="ReviewSTERResults" type="fisma:ReviewSTERResultsType"/>
    <xs:element name="ReviewPOAMSchedule">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="AllCorrectiveActionAreScheduledForCompletionWithinAnAcceptableTimeframe"
type="fisma:YesNo">
            <xs:annotation>
              <xs:documentation>If no, updated risk assessment as needed</xs:documentation>
            </xs:annotation>
          </xs:element>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="PrepareATOJustification" type="fisma:PrepareATOJustificationType"/>
    <xs:element name="GrantDenyATO" type="fisma:GrantDenyATOType"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="ReviewSTERResultsType">
  <xs:sequence>
    <xs:element name="SignedSARResult" type="fisma:YesNo"/>
    <xs:element name="SignedSARResultDateCompleted" type="xs:date"/>
    <xs:element name="SignedFindings" type="fisma:YesNo"/>
    <xs:element name="SignedFindingsDateCompleted" type="xs:date" nillable="true"/>
    <xs:element name="CorrectiveActionReports" type="fisma:YesNo"/>
    <xs:element name="CorrectiveActionReportsDateCompleted" type="xs:date" nillable="true"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="PrepareATOJustificationType">
  <xs:sequence>
    <xs:element name="RecommendationLetter" type="fisma:YesNo"/>
    <xs:element name="RecommendationLetterDateCompleted" type="xs:date" nillable="true"/>
    <xs:element name="SignedATO" type="fisma:YesNo"/>
    <xs:element name="SignedATODateCompleted" type="xs:date" nillable="true"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="GrantDenyATOType">
  <xs:sequence>

```

```

        <xs:element name="DenialLetter" type="fisma:YesNo"/>
        <xs:element name="DenialLetterDateCompleted" type="xs:date" nillable="true"/>
        <xs:element name="CorrectiveActionsPlan" type="fisma:YesNo"/>
        <xs:element name="CorrectiveActionsPlanDateCompleted" type="xs:date" nillable="true"/>
    </xs:sequence>
</xs:complexType>
<!-- Monitor Security Controls complex types -->
<xs:complexType name="MonitorSecurityControlsType">
    <xs:sequence>
        <xs:element name="ConfigurationManagementReviews">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="ChangeImpactAssessment" type="fisma:YesNo"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="DocumentationRevisions">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="POAMQuarterlyReportApprovalDate" type="xs:date"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="PeriodicAndOngoingTestingAssessmentConductContinuousMonitoringActivities">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="PeriodicAndOngoingTestingFamily" type="fisma:SecurityControlFamilyFor800-
53Type"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="ReviewOfATODDecision">
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="OutstandingPOAMItem" type="fisma:IGGAORReportType" maxOccurs="unbounded">
                        <xs:annotation>
                            <xs:documentation>List actual open POA&amp;M items separately</xs:documentation>
                        </xs:annotation>
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="ReviewOfATODDecision">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="OutstandingPOAMItem" type="fisma:IGGAORReportType" maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>List actual open POA&amp;M items separately</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>

```

```

maxOccurs="unbounded"/>
        <xs:element name="IGGAOResultAndInternalExternalAssessmentFinding" type="fisma:IGGAOResultType"
        <xs:element name="ATODateCompleted" type="xs:date"/>
    </xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>

<xs:complexType name="PeriodicAndOngoingTestingType">
    <xs:sequence>
        <xs:element name="ControlNumber" type="fisma:SecurityControlFor800-53Type" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="IGGAOResultType">
    <xs:sequence>
        <xs:element name="Description" type="xs:string"/>
        <xs:element name="DateDue" type="xs:date"/>
        <xs:element name="DateCompleted" type="xs:date"/>
        <xs:element name="IndividualResponsible" type="xs:string"/>
        <xs:element name="IndividualVerified" type="xs:string"/>
        <xs:element name="Comments" type="xs:string"/>
    </xs:sequence>
</xs:complexType>
<!-- ***** -->
<!--Simple Types-->
<xs:simpleType name="YesNo">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Yes"/>
        <xs:enumeration value="No"/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name="RatingOptions">
    <xs:restriction base="xs:string">
        <xs:enumeration value="Low"/>
        <xs:enumeration value="Moderate"/>
        <xs:enumeration value="High"/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name="SecurityControlTypeOptions">

```

```

        <xs:restriction base="xs:string">
            <xs:enumeration value="System-Specific"/>
            <xs:enumeration value="Common"/>
            <xs:enumeration value="Hybrid"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AssessorIndependenceOptions">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Self"/>
            <xs:enumeration value="Independent"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AssessedSecurityControlEffectivenessOptions">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Satisfied"/>
            <xs:enumeration value="Partially Satisfied"/>
            <xs:enumeration value="Not Satisfied"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="SystemTypeOptions">
        <xs:restriction base="xs:string">
            <xs:enumeration value="GSS"/>
            <xs:enumeration value="Major"/>
            <xs:enumeration value="Minor"/>
        </xs:restriction>
    </xs:simpleType>
<!-- ***** -->
<!--Global Element Definitions-->
<!-- ***** -->

<!-- Compensating Security Control Applied-->
<xs:element name="UniqueConditionIdentified" type="fisma:YesNo"/>
<!-- Additional Security Control Applied -->
<xs:element name="ArtifactEvidence" type="xs:string"/>
</xs:schema>

```

