1 Overview

The objective of this white paper is to provide a cliff's note guide to meeting FISMA guidelines as outlined in NIST SP 800-53. This paper is relevant to NIST SP800-53 version 4 and below.
This white paper outlines the technical approach and milestones for implementing a NIST SP800-53 based IT Risk Management program. The appendixes also include a list of tools to assist in the developments of the program.
The primary deliverable of this white paper is the process for developing an effective System Security Plan (SSP).

1.1 Background.

When developing a Information Technology Risk Management Program many organizations focus the technical aspects of IT security, primarily;

1. External penetration test
2. Host based security systems
3. Anti-Virus
4. Intrusion Prevention Systems

More mature organizations also include authenticated vulnerability scans, security management tools and automated internal security policies (like Active Directory GPO's, etc.)
These components are typically monitored on a monthly or quarterly basis, or are configured to send alerts when a discrepancy or anomaly is detected.
Several new tools and advances in information Security systems greatly reduce risk mitigation efforts;

1. Next generation firewalls
2. Open Flow (layer 7) network management tools (particularly with wireless systems)
3. Internal, authenticated vulnerability scans
4. Mobile Device Management systems
5. Workspace management tools (with integrated MDM capabilities)

These tools, particularly Open Flow type and workspace management tools are particularly effective in mitigating Zero Day attacks and reducing configuration management efforts, which are both primary vectors of attack to modern information systems

Recent incidents, like the Target data breach, or password data breach of JP Morgan have brought about the new guidelines in NIST SP 800 Rev 4. In many of these recent breaches, these organizations had all of the tools in place, but did not have an effective operational framework to manage the data generated by these tools and channel them into an effective risk mitigation program. The overall message is this;

> For IT Risk Management Frameworks to be effective, they must have policies and procedures integrated into the daily work flow that ensure that potential risk are managed on an ongoing basis. Furthermore, dedicated teams are needed to provide a 1 hour responses or less for critical threats.

The overall objective of the NIST SP 800 family of standards is to develop an Information Technology based risk management program standard to be used for system that host and manage federal data. The FISMA guidelines in NIST SP800-53 provide the operational controls required to reduce the risk associated with the operation and management of IT systems.

SP 800-37 provides an outline of the SP 800-53 objectives. Of particular interest is the discussion on supporting documents that must be in place to create an effective program. Figure 2.2 of SP 800-37 outlines the Risk management Framework that must be in place to support an effective System Security Plan.

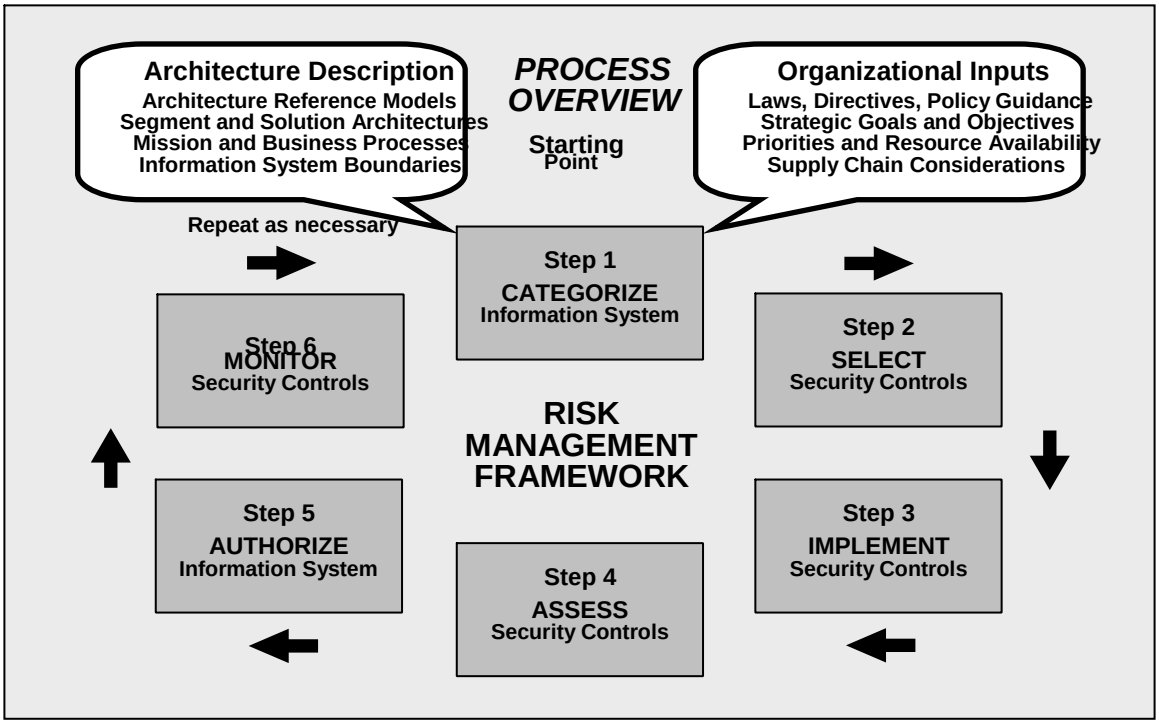


Figure 1 Risk Management Framework

Figure 2.2 outlines the Enterprise Architecture, policies and procedures that need to be in place to build a SSP that meets FISMA standards.

The critical components are to properly categorize the information systems and to put in place a monitoring system that can respond within the appropriate time required by the classification. For example, the SSP security controls AU & IR (monitoring and Incident Reporting) require an almost immediate response to a Level 1 threat on a system classified FIPS 199 as moderate. To meet this objective, an organization would require an automated alert system, a back-up monitoring component and a fully staffed dedicated 24hr NOC to ensure appropriate response.

2 Technical approach

To meet the response times required to meet FISMA Risk Management Framework goals, an integrated process is needed. The Risk Management Framework outlined by NIST guidelines leave a large gap in the approach to the system development lifecycle. Organizational efforts led from within an organization need guidance to rapidly mature their Risk Management Framework efforts and require interaction of Third party Assessment organizations (3PAO's) to meet FISMA guidelines. It resembles a chicken and the egg dilemma in determining where to start.
Our studies and analysis have indicated that key components in the process are the organizations work management and change control system. See figure 2 below.

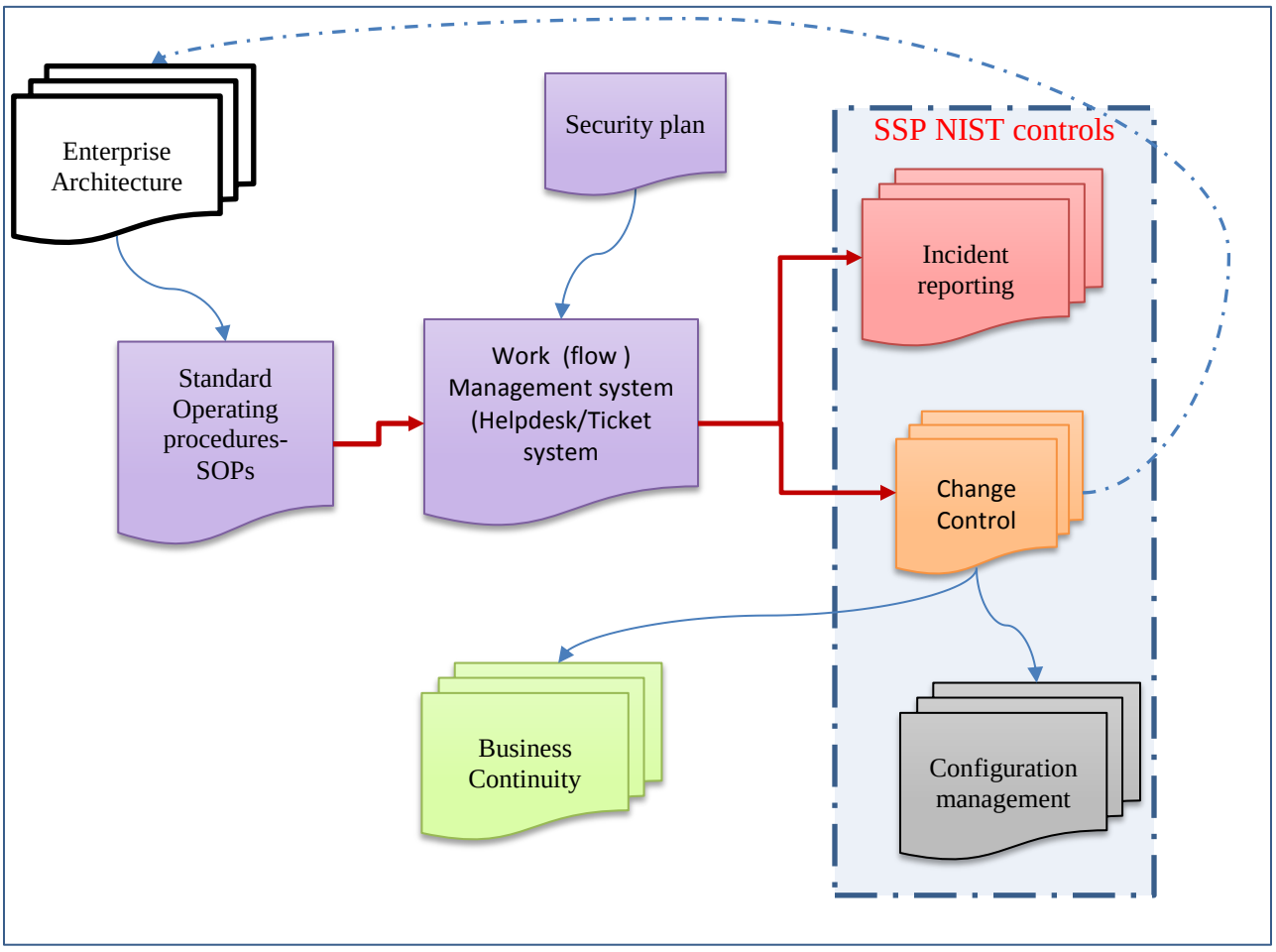


Figure 2 Technology Operational Control lifecycle

Figure 2 outlines the System Security Plan Ecosystem and depicts the central role a Work Management system and Change Control system play in maintaining a System Security Plan.

From these key components, the other components of the SSP ecosystem can be linked and synthesized. The next 3 sections outline critical components and the nature of these key systems, and the resulting implementation plan with these system in place.

2.1 Work Management Systems

The work management system must meet the following requirements;

1. Integrated ITIL capabilities
    a. Embed policies (where possible) outlined in the Enterprise Architecture
2. Have a means of embedding policies and procedures
3. Integrate with change control systems
4. Automate
    a. incident reporting
    b. triggering a change control request
5. Integrated work flows
6. Be managed by a 24 hour operational management team
    a. Be an Integrated Project Team (IPT)
        i. Team with charter to own and resolve Information technology problems
        ii. Have members of critical IT teams (CSO, Business Continuity, operations, etc.)

2.2 Change Management

Change Control is a key component of operational governance of Information Technology (or any system for that matter) systems. If change control is treated as an island, it becomes out of synch with operations and business management. To prevent this, change control must be integrated with the IT work management system(s). All projects must be managed in this system, even if they have separate initiatives. Change management must be governed by one or more Change Control boards. The change management system requires the CIO or representative as a minimum.

2.3 Implementation.

Practice and observation of organizations grappling with Risk Management almost always finds at the core, a poor change management and work management systems. Another critical component is a dynamic monitoring system and process. It is critical to note that process failures are almost always traced back to gaps in the change management and work management protocols. We have found this recipe to work best;

1. Perform business process based system assessment (see our System Assessment worksheet tools).
    a. During the assessment, identify and assess the status of critical governance tools outlined in figure 2.
2. Perform a risk assessment on the systems identified in the systems assessment

3. Start with P1 controls outlined in NIST SP 800 53 (see our Security controls worksheet tool).
4. Implement a work management system (see section 2.1 above)
5. Establish teams and roles required by system security controls. Representatives of these teams will form the Integrate Project Team (IPT). At a minimum these should be (see SP 800-37 Appendix D):
    a. CEO
    b. CIO/CTO
    c. CSO
    d. Proactive Sustaining team
    e. Change control team/board
    f. Incident response team
    g. Disaster Recovery or COOP team
    h. NOC/Monitoring and Incident Response team Integrated Project Team
6. Complete System Security Plan (by IPT)
7. Develop a Plan of Action (POAM)
8. Perform a 3PAO assessment
9. Implement POAM and monitoring phase
    a. Include re-assessment
    b. This is an iterative process
    c. As the program matures, implement Priority 2 and 3 (P2, P3) controls or ass dictated by FIPS categorizations

3 Cost and Milestones

Major activities/milestones

Table 1 Schedule overview and cost

Activity	Time Frame	Cost ($)	resources
System Assessment	30-90 days	varies	3rd party, CIO
Risk assessment	30days	varies	3rd party, CSO
System Security plan Development	180 days (typical)	$250K (typical)	3rd party, CSO, IT
Work Management system	30-60days	$20K-100K	CIO
Integrated Project Team development	60 days	varies	CIO, CEO
Develop Plan of Action (POAM)	30 days	varies	**CSO**
Third party Assessment (3PAO)	15-30 days	$30k to 200K	**3PAO**
Monitoring and management phases	ongoing	varies	Special tools, 3PAO

4 Summary

The goal of an IT security Plan is to develop an effective Risk Management Framework for information systems that ensures information and systems are protected throughout the system development lifecycle. Although all organization hare different, core information system tools and organizations structures such as comprehensive Work Management tools and IT governance teams such as the IT Operations Integrated Project Team provide the glue that holds together an effective FISMA complaint System Security Plan.

5 About Vigilant

Vigilant Technologies is a Veteran owned technology based company based in Chandler Arizona since 2004. The Vigilant Team has developed and implemented highly available IT infrastructures, Business Continuity programs and systems assessments for clients such as Intel, the City of Phoenix, San Francisco Airport, USACE, Federal Security Agencies and various commercial concerns.
Vigilant Technologies most recently completed the first phase of certification in the FedRAMP Cloud Service Provider Program, an infrastructure and operation certification program based on NIST SP 800-53.

Vigilant Technologies (Chandler Automated Systems, LLC)

25 South Arizona Place, Suite 515

Chandler, Arizona 85225

www.vigilant1.com

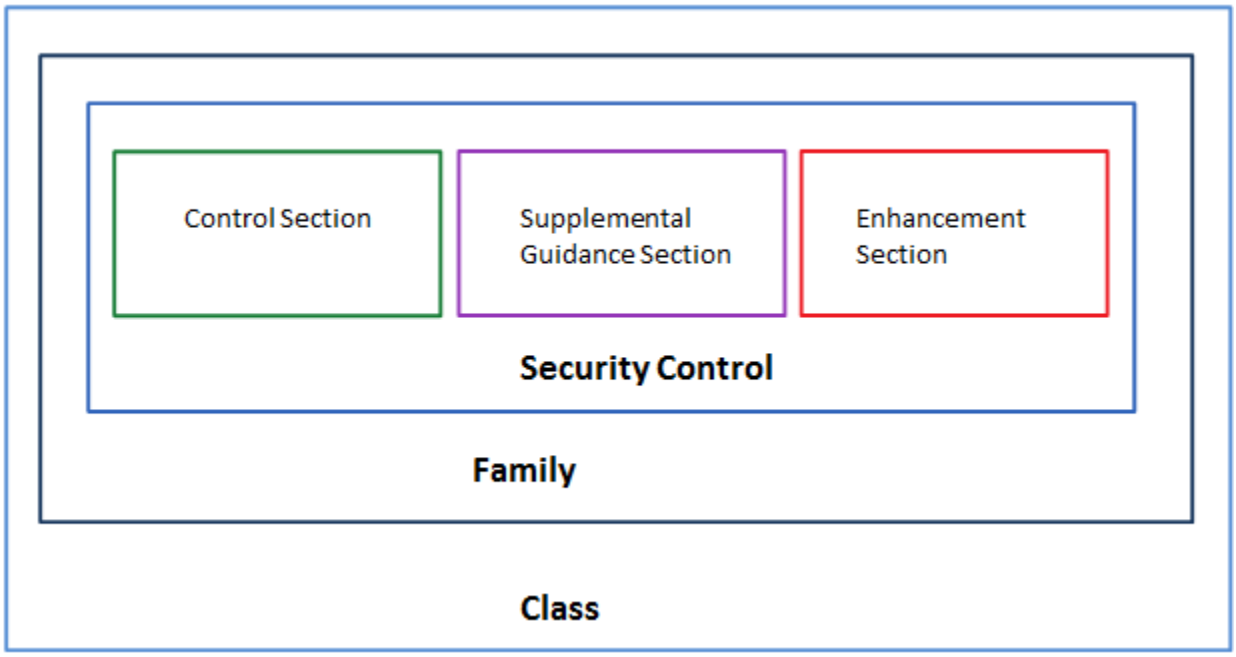
Certifications;
SBA; 8a case number; 303129
SBA 8a, DOT MWBE/DBE, SDVOB
FedRAMP (JAB)-in-process

6 Appendices

6.1 Appendix 1 NIST security controls

6.1.1 Section 1: Families, Security Controls, and Classes Hierarchy

6.1.1.1 Organization of Security Controls



3.1 The 3 Classes

- Management
- Operational
- Technical

3.2 List of Families and Their Identifier Tags

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

3.3

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12
AC-13	Supervision and Review—Access Control	AC-13	AC-13	AC-13 (1)
AC-14	Permitted Actions w/o Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3)	AC-17 (1) (2) (3)
AC-18	Wireless Access Restrictions	Not Selected	AC-18 (1)	AC-18 (1)
AC-19	Access Control for Portable and Mobile Systems	Not Selected	AC-19	AC-19 (1)
AC-20	Personally Owned Information Systems	AC-20	AC-20	AC-20
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2	AU-2
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Audit Processing	AU-5	AU-5	AU-5 (1)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7	AU-7 (1)
AU-8	Time Stamps	Not Selected	AU-8	AU-8
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Retention	AU-11	AU-11	AU-11
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	Not Selected	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4	CA-4
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Sites	Not Selected	CP-6 (1)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Sites	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2	IA-2 (1)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Periodic Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2 (1)
MP-3	Media Labeling	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5	MP-5
MP-6	Media Sanitization	Not Selected	MP-6	MP-6
MP-7	Media Destruction and Disposal	MP-7	MP-7	MP-7
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	Not Selected
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Logs	PE-8	PE-8 (1)	PE-8 (1)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1)	PE-13 (1) (2)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4	SA-4
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Design Principles	Not Selected	SA-8	SA-8
SA-9	Outsourced Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not selected	SC-3
SC-4	Information Remnants	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	SC-6	SC-6
SC-7	Boundary Protection	SC-7	SC-7 (1)	SC-7 (1)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Validated Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2	SI-2
SI-3	Malicious Code Protection	SI-3	SI-3 (1)	SI-3 (1) (2)
SI-4	Intrusion Detection Tools and Techniques	Not Selected	SI-4	SI-4
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5
SI-6	Security Functionality Verification	Not Selected	SI-6	SI-6 (1)
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7
SI-8	Spam and Spyware Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Input Accuracy, Completeness, and Validity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems

6.2 Appendix B

6.2.1 Section 2: Process for NIST Certification[1]

3.1 RMF STEP 1 – Categorize information System
3.2 RMF STEP 2 – Select Security Controls
3.3 RMG STEP 3 – Implement Security Controls
3.4 RMF STEP 4 – Assess Security Controls
3.5 RMF STEP 5 – Authorize Information System
3.6 RMF STEP 6 – Monitor Security Controls

6.3 Appendix C -Tools

6.3.1 System Assessment work sheet

6.3.2 Security Control worksheet

6.3.3 Work Management templates

6.3.4 Risk Assessment work sheet.

6.3.5 Integrated Project Team Charter.

[1] All tasks can be found under Chapter 3 of the NIST SP 800-37 Rev1 document.