Global Information Assurance Certification Paper

Type Security Certification and Accreditation in a Nationwide System using NIACAP: An Auditors Perspective

GSNA Practical Version 2.1 (amended 5 July 2002)
Option 2

Author: Windy Elliott
Date: April 1, 2003

Table of Contents

Introduction

This assignment will explain the general certification and accreditation process that is being used by the Federal Government with an emphasis on the NIACAP Methodology. The assignment will be based upon an actual certification project currently being implemented. Due to the sensitive nature of the information, the results will be redacted and generalized and the emphasis will instead be on explaining the process and best practices for completing a certification audit for such a system.

Assignment 1 – Research in Audit, Measurement, Practice and Control will describe certification and its origins as well as explain the methodology in detail. It will include a general description of the system being audited and certified.

Assignment 2 – Create an Audit Checklist will list the security controls that will be tested during the audit of the system. It will include a description of the requirements documents that were used in its creation and how those requirements apply to the system being audited.

Assignment 3 – Audit Report will provide the results of the certification audit in the Security Test and Evaluation Report.

Assignment 1 – Research in Audit, Measurement, Practice and Control

Certification and Accreditation

The Computer Security Act was passed by congress in 1987. This law gave the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines for Federal computer systems, including the security of those systems. This law also established the requirement that all Federal computer systems that contain sensitive information have a security plan and that personnel working on those systems be given annual security training.

In 1996, the Office of Management and Budget (OMB) released their Circular A-130, *Management of Federal Information Resources.* This circular requires federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing prior to operations and, periodically, thereafter but at a minimum of every three years. This authorization by a designated approval authority (DAA) is referred to as *accreditatio*n. The technical and non-technical evaluation of an IT system that produces the necessary information required by the DAA to make a credible, risk-based decision on whether to place the system into operation, is known as *certificatio*n.

While the certification and accreditation (C&A) process focuses on federal IT systems processing, storing, and transmitting sensitive (unclassified) information, the associated tasks and sub-tasks, security controls, and verification techniques and procedures, have been broadly defined so as to be universally applicable to all types of IT systems, including national security or intelligence systems, if so directed by appropriate authorities.

NIST released the Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditatio*n in September 1983. This document was one of the first to refer to the certification and accreditation process, as we understand it today. The document outlines roles and responsibilities, sensitivity levels and evaluation activities.

Since this time there have been many documents and methodologies released on how to complete the certification and accreditation process. Since 2001, the issue of security has become a hot topic and the Federal government has become increasingly aware of our increased dependence on our technological infrastructure as well as its vulnerability.

National Information Assurance Certification and Accreditation Process (NIACAP)

The National Security Telecommunications and Information System Security Committee (NSTISSC) developed the NIACAP process in April of 2000 as an alternative methodology to the DITSCAP process that was being used to secure systems owned by the Defense Department. The NIACAP was designed to certify that a particular IT system meets documented security requirements.

The NIACAP is an attempt to create a national standard for the process, activities, tasks and management of a system certification and accreditation. The process was intended to be highly customizable to fit the requirements and sensitivity of the system being certified. The process was developed to comply with the policies found in OMB Circular A-130, Appendix III was well as guidelines put forth by the National Institute of Standards and Technology (NIST).

The process revolves around a central document referred to as the System Security Authorization Agreement (SSAA). The SSAA documents the system and the security agreements related to the system and to the certification and accreditation. The SSAA also acts as a security baseline document to future certification activities. The SSAA is intended to be a repository of security related documents for a system. Because of this the SSAA can become very large and will not be presented in its entirety for this assignment. Instead, this document will focus on the audit of a system being certified thru the creation of a security checklist and the testing procedures of that checklist.

The minimum roles to complete a NIACAP Certification include the program manager otherwise known as the system owner, the Designated Approval Authority (DAA), and the certifier otherwise known as the auditor. The certifier is the certification expert who documents the certification activities, findings, and remediation required for the system to be recommended for accreditation. If possible, the users of the system should also be included in the certification activities.

There are several different types of certification and accreditation that are standard today. Typically a system accreditation evaluates a major application or general support system. NIST defines major applications as systems that perform clearly defined functions for which there are readily identifiable security considerations and needs, (e.g., an electronic funds transfer system or global command and control system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel).

A general support system is a collection of interconnected information resources or computing environments under the same direct management control, which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or common applications. A general support system, for example, can be a local area network (LAN) including smart terminals that support a branch office, a backbone network (e.g., agency-wide), communications network, departmental data processing center including its operating system and utilities, tactical radio network, office automation and electronic mail services, or shared information processing service organization. A general support system can also host one or more major applications.

A site accreditation evaluates a system at a particular location. A type accreditation evaluates a system that is distributed to various locations. We will be using a type accreditation for this assignment. We will be reviewing the system using the central system components as well as the evaluation of a sample remote implementation. When completing a type accreditation, a representative site is certified and then the certification is distributed to the other facilities. The facilities can then be inspected for compliance and correct implementation without needing to repeat the baselines tests conducted by the initial certification effort.

The NIACAP is composed of several phases: Definition, Verification, Validation, and Post Accreditation. The Definition Phase activities focus on the discovery of

the system components, boundaries to the system being certified, baselines requirements for security, system sensitivity and criticality, and resources required to complete the certification. During this phase the system and its documentation are reviewed and the first draft of the SSAA is created if it does not exist already. Technical Architecture documents, user manuals, configuration management plans, prior risk assessments, and design specifications are gathered and reviewed in order to gain the highest possible understanding of the system being certified. The system owner is interviewed to determine the governing security requirements for the system.

During the review of the system it is important to confirm the scope of the certification activities. This includes reviewing the boundaries to the system. The accreditation boundary is determined by determining the limit of the control of the system owner. The system owner is often defined as the entity that maintains financial control over the system security. Therefore, the boundary of the system would be the point at which the system owner no longer has financial control over the security controls.

For systems that connect with other systems at its boundaries, it is generally recommended that a Memorandum of Understanding (MOU) be created between the system owners. The MOU typically outlines specific security responsibilities between the two systems. The process of signing MOUs with other system owners can also be an educational exercise as it increases the security awareness of both systems as well as find connections that the system owner may not have been aware of.

During this phase the certifier will determine the system sensitivity and criticality. This is determined by reviewing the type of data contained in the system. Refer to the following table for a list of data categories.

Information Categories

Category		Explanation and Examples
#	Name	
1	Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).

Category		
2	Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially related systems, and site operating and security expenditures.
3	Internal administration	Information related to the internal administration of Federal Systems. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.
4	Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.
5	Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.
6	New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce.
7	Mission-critical information	Information designated as critical to a business mission, includes vital statistics information for emergency operations.
8	Operational information	Information that requires protection during operations; usually time-critical information.
9	Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).
10	Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.

Category		
11	System configuration Management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at the federal system; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.
12	Public information	Any information that is declared for public consumption by official authorities. This includes information contained in press releases approved by the Office of Public Affairs, Office of Civil Aviation Security or other official source. It also includes Information placed on public access world-wide-web (WWW) servers.

Once the data category is determined, the sensitivity of that category is used to determine the level of protection required from the following table. From that the level of the certification testing will be determined.

Relationship Between Information Categories and *Minimum* Security Levels for IS

Information Category		*Minimum* Security Level		
#		LOW	MEDIUM	HIGH
1	Information about persons		X	
2	Financial, budgetary, commercial, and trade secret information		X	
3	Internal administration		X	
4	Investigation, intelligence-related, and security information			X
5	Other Federal agency information		X	
6	New technology or controlled scientific information		X	
7	Mission-critical information			X
8	Operational information		X	
9	Life-critical information			X
10	Other information	X		
11	System configuration management information		X	
12	Public information	X		

Typically there are 3 levels of system sensitivity for unclassified systems: high, medium, and low. These will dictate to three levels of testing for the certification. These levels are defined in the following table.

Security Levels for Information Systems

Security Level	Impact Description	Explanation
LOW	Moderately serious	Noticeable impact on missions, functions, image, or reputation. A breach of this security level would result in a negative outcome or would result in damage, requiring repairs, to an asset or resource.
MEDIUM	Very serious	Severe impairment to 's missions, functions, image, and reputation. The impact would place at a significant disadvantage; or Would result in MAJOR damage, requiring extensive repairs to assets or resources.
HIGH	Catastrophic	Complete loss of mission capability for an extended period; or Would result in the loss of MAJOR assets or resources and could pose a threat to human life.

These levels will define the effort of the certification activities. A Level 1 system certification will have a low sensitivity level. Certification activities will only include a basic security review such as a checklist that covers the basic requirements for the system. A Level 2 system certification will have a medium sensitivity level and certification activities will include a minimum analysis of the system and may include a technical review of the system. At levels 2 and 3 a test, observation, document review, or interview should test each security control. A Level 3 system certification will have a high sensitivity level and certification activities will include a detailed analysis of the system possibly including a penetration test. The evidence required for certification will be much stricter for this level of testing.

The Verification Phase prepares the system for certification by defining the current level of compliance with the SSAA. The SSAA is usually updated at this point to ensure it is as up to date as possible. Both the technical and non-technical security controls should be addressed and should include change control and risk management. MOUs with interconnecting systems should be signed and collected at this point to ensure that correct procedures are being followed.

The Validation Phase is the testing phase of the certification and will be the focus of this paper. The system is tested and evidence is gathered to support the DAA in his/her decision to accredit the system. Activities during this phase include the Security Test and Evaluation (ST&E), site evaluations, a review of the Disaster Recovery/Contingency Plan and of the system risk management. If the certifier concludes that the required security controls are in place and operating as intended, then recommendations are developed and a certification statement is issued. The certification package is then forwarded to the DAA for accreditation.

The Post Accreditation Phase focuses on mitigation activities that were outlined during the certification process as well as the risk management/configuration management activities that happen in between certifications.

Identify the system to be audited

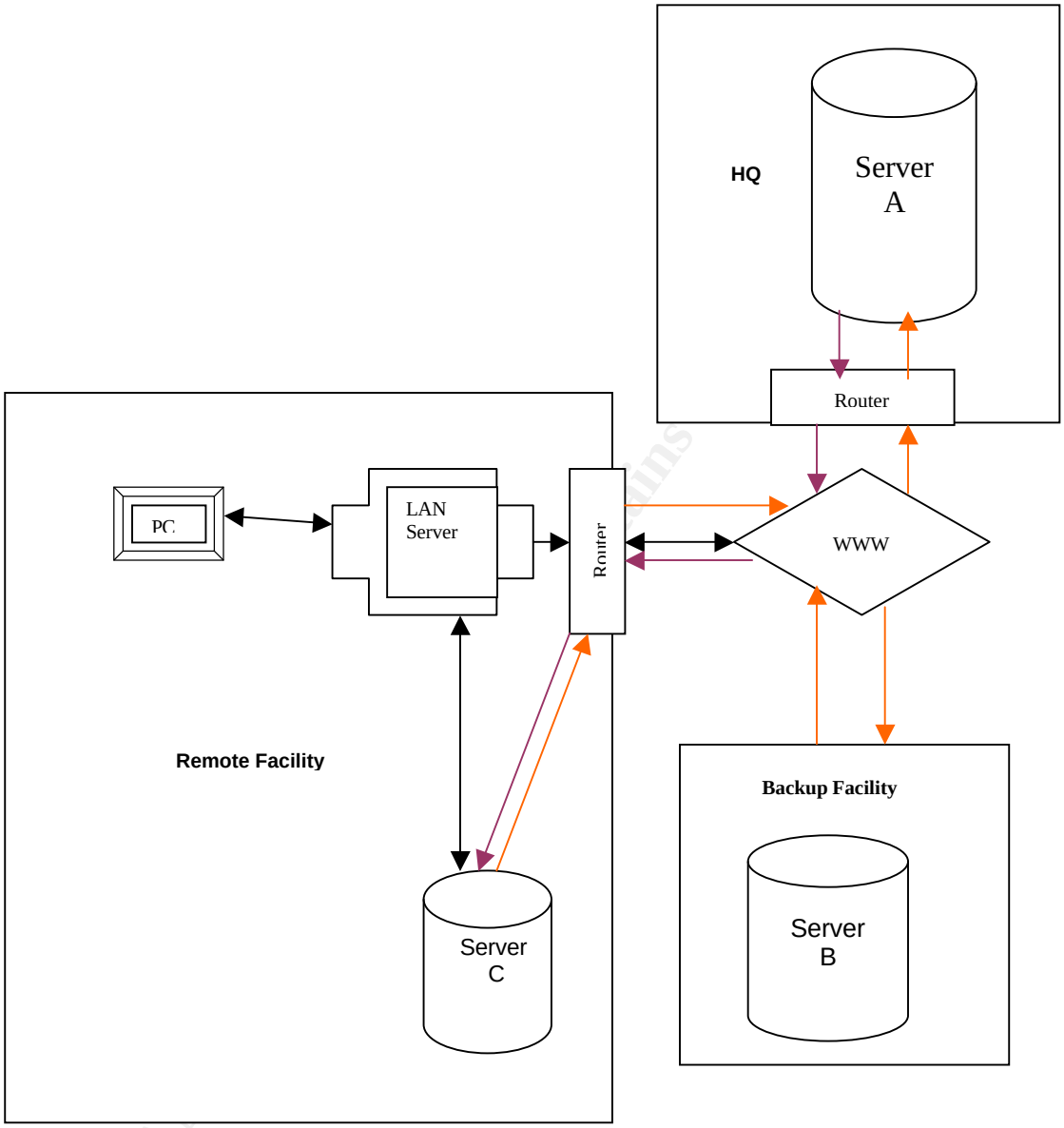
The system being certified is a federal system that was developed by an unnamed federal agency for the purpose of increased efficiency and improved performance for significant business processes within the organization. In order for the system to be certified it must undergo a detailed audit and any deficiencies must be addressed before the system can be approved for connection to other government systems. The system is distributed across the country in over 500 locations with local servers providing the main client interface and a group of central system specific servers located in the region of the program management team.

These central servers maintain a master database that is accessible to everyone on the network. The local servers update the master data continuously, ensuring all users have accurate, up-to-date information. The system servers run Microsoft Windows 2000 operating system. The servers are configured and the operating system is hardened by the organization prior to being placed in production. Oracle is used as the database for the system.

The data on these servers is primarily administrative with some privacy act information. For the purposes of the certification, the federal government has rated this data medium sensitivity and mission critical. Therefore the certification activities will be customized for level two.

Since the system us being certified using a “Type” certification we are defining the system as being the interconnection between the central server (Server A), the backup server (Server B), which is located 26 miles from the central server, and the sample remote facility server (Server C) as outlined in the following diagram.

System Diagram



Evaluate the risk to the system

The system being certified is a sensitive but unclassified system. The data within the application contains both privacy act data as well as agency specific information that could prove harmful if unauthorized individuals were to gain access to it. The agency has a very strong security posture and the facilities that house the remote servers are very well protected from public access. The facilities also make use of firewalls, IDS systems and virus detection, both at the regional level thru the agency backbone, and at the facility and server level with tools installed on site. Much of the potential vulnerabilities seem to revolve around the personnel at the remote facility who manage the server on a daily basis. Also, since these servers all communicate to each other thru the internet, the potential danger of unauthorized access exists.

Assignment 2 – Create an Audit Checklist

Introduction:

The government organization has requested a certification of their system. This certification includes doing an audit of the system. The audit should include all areas of security, including Physical, Environmental, Technical, Operational, and Risk Management. Because many of these items can't be tested thru technology, several other types of tests were included in this audit including visual inspection, interviews with knowledgeable parties, and documentation review.

Any technical testing will be conducted by the network engineer responsible for the design, installation and maintenance of the proposed system. The tests will be observed by the auditor and the report will be given to the auditor for submission in the certification package.

Objectives:

The purpose of this audit is to complete certification of a nationwide government system. Once the system is certified the system will be approved for connection to other government systems.

The audit will show the existing security controls in use for the system as a whole including interconnecting systems that directly impact the system being certified. It will also show any material weaknesses in the system.

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
OMB Circular A-130, III DOT H1350.253		RISK MANAGEMENT		
	Is risk periodically assessed?			
NIST SP 800-18 DOT H1350.253		Is the current system configuration documented, including links to other systems?	-Review Technical Architecture Document	
FISCAM SP-1		Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?	-Review Past Risk Assessments	
FISCAM SP-1		Has data sensitivity and integrity of the data been considered?	-Review Past Risk Assessments	
FISCAM SP-1		Have threat sources, both natural and manmade, been identified?	-Review Past Risk Assessments	
NIST SP 800-30		Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current?	-Review Past Risk Assessments	
NIST SP 800-30 DOT H1350.253		Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	-Review Past System Tests	
	Do program officials understand the risk to systems			

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	under their control and determine the acceptable level of risk?			
FISCAM SP-1		Are final risk determinations and related management approvals documented and maintained on file?	-Review Past Risk Assessments	
NIST SP 800-30		Has a mission/business impact analysis been conducted?	-Review Review analysis	
NIST SP 800-30		Have additional controls been identified to sufficiently mitigate identified risks?	-Review Review Past mitigation reports	
OMB Circular A-130, III FISCAM SP-5 NIST SP 800-18		REVIEW OF SECURITY CONTROLS		
	Have the security controls of the system and interconnected systems been reviewed?			
FISCAM SP-5.1 DOT H1350.253		Has the system and all network boundaries been subjected to periodic reviews?	-Review Assessment reports	
OMB Circular A-130, III FISCAM SP-5.1		Has an independent review been performed when a significant change occurred?	-Review Assessment reports	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18				
NIST SP 800-18		Are routine self-assessments conducted?	-Review Assessment reports	
OMB Circular A-130, 8B3 NIST SP 800-18		Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?	-Review test results	
FISCAM SP 3-4 NIST SP 800-18		Are security alerts and security incidents analyzed and remedial actions taken?	-Incident Response Procedures -Security Plan	
	Does management ensure that corrective actions are effectively implemented?			
FISCAM SP S-1 and 5.2 NIST SP 800-18		Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?	-Incident Response Procedures -Security Plan -Past Audit Reports	
OMB Circular A-130, III FISCAM CC-1.1 DOT H1350.253		LIFE CYCLE		

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	Has a system development life cycle methodology been developed?			
		Initiation Phase		
OMB Circular A-130, III FISCAM AC-1.1 & 1.2 NIST SP 800-18		Is the sensitivity of the system determined?	-Interview Owners and confirm on data sensitivity chart	
Clinger-Cohen		Does the business case document the resources required for adequately securing the system?	-Review Exhibit 53	
Clinger-Cohen		Does the Investment Review Board ensure any investment request includes the security resources needed?	-Review Exhibit 53	
FISCAM CC-1.2		*Are authorizations for software modifications documented and maintained?*	-Change Request Forms	
GISRA		*Does the budget request include the security resources required for the system?*	-Review Budget request	
		Development/Acquisition Phase		
NIST SP 800-18 DOT H1350.253		During the system design, are security requirements identified?	-Interview system developers	
NIST SP 800-30		Was an initial risk assessment performed to determine security requirements?	-Review risk assessment	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		*Is there a written agreement with program officials on the security controls employed and residual risk?*	-Review agreement or sign off sheet	
OMB Circular A-130, 8B3		Are security controls consistent with and an integral part of the IT architecture of the agency?	-Walk thru facility -Interview management	
NIST SP 800-18		Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action?	-Review test procedures	
NIST SP 800-18		Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?	-Review solicitation documents	
NIST SP 800-18		Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented?	-Review solicitation documents	
		Implementation Phase		
	Are changes controlled as programs progress through testing to final approval?			
FISCAM CC-2.1 NIST SP 800-18 DOT H1350.253		Are design reviews and system tests run prior to placing the system in production?	-Review test plans and results	
FISCAM CC-2.1		Are the test results documented?	-Review test results	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18				
NIST SP 800-18		*Is certification testing of security controls conducted and documented?*	-Review test results	
NIST SP 800-18		If security controls were added since development, has the system documentation been modified to include them?	-Review documentation	
FISCAM CC-2.1 NIST SP 800-18		If security controls were added since development, have the security controls been tested and the system recertified?	-Review test results	
NIST SP 800-18 DOT H1350.253		Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	-Review past certification documents	
NIST SP 800-18		Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization?	-Review past certification documents	
		Operation/Maintenance Phase		
OMB Circular A-130, III FISCAM SP 2.1 NIST SP 800-18		Has a system security plan been developed and approved?	-Review Plan	
NIST SP 800-18 DOT		If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems?	-Review MOUs/MOAs	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
H1350.253				
OMB Circular A-130, III FISCAM SP 2.1 NIST SP 800-18		Is the system security plan kept current?	-Review Plan and review sign sheet	
		Disposal Phase		
NIST SP 800-18 DOT H1350.253		Are official electronic records properly disposed/archived?	-Interview management	
FISCAM AC-3.4 NIST SP 800-18 DOT H1350.253		Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere?	-Review Security Plan -Review Disposal Log	
NIST SP 800-18		Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized?	-Review Disposal Log	
OMB Circular A-130, III FIPS 102		AUTHORIZE PROCESSING		
	Has the system been certified/recertified and authorized to process (accredited)?			

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Has a technical and/or security evaluation been completed or conducted when a significant change occurred?	-Review past security evaluations	
NIST SP 800-18		Has a risk assessment been conducted when a significant change occurred?	-Review past risk assessments	
NIST SP 800-18 DOT H1350.253		Have Rules of Behavior been established and signed by users?	-Review Rules of Behavior	
NIST SP 800-18		Has a contingency plan been developed and tested?	-Review contingency plan	
NIST SP 800-18		*Has a system security plan been developed, updated, and reviewed?*	-Review security plan	
NIST SP 800-18		Are in-place controls operating as intended?	-Review test results	
NIST SP 800-18		*Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity?*	-Review test results and mitigation plans	
NIST SP 800-18 DOT H1350.253		*Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)?*	-Review MOUs/MOAs	
	Is the system operating on an interim authority to process in accordance with specified agency procedures?			
NIST SP 800-18		*Has management initiated prompt action to correct deficiencies?*	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
OMB Circular A-130, III FISCAM SP 2.1 NIST SP 800-18		SYSTEM SECURITY PLAN		
	Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?			
FISCAM SP 2.1 NIST SP 800-18		Is the system security plan approved by key affected parties and management?	-Review Security Plan sign sheet	
NIST SP 800-18		*Does the plan contain the topics prescribed in NIST Special Publication 800-18?*	-Review Security Plan	
OMB Circular A-130, III NIST SP 800-18		Is a summary of the plan incorporated into the strategic IRM plan?	-Review IRM Plan	
	Is the plan kept current?			
FISCAM SP 2.1 NIST SP 800-18		Is the plan reviewed periodically and adjusted to reflect current conditions and risks?	-Review Security Plan sign sheet	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
OMB Circular A-130, III		PERSONNEL SECURITY		
	Are duties separated to ensure least privilege and individual accountability?			
FISCAM SD 1.2 NIST SP 800-18 DOT H1350.253		Are all positions reviewed for sensitivity level?	-Review job descriptions and interview management	
FISCAM SD 1.2		*Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?*	-Review job descriptions and interview management	
OMB Circular A-130, III NIST SP 800-18 FISCAM SD-1		Are sensitive functions divided among different individuals?	-Review job descriptions and interview management	
FISCAM SD 1.1		Are distinct systems support functions performed by different individuals?	-Review job descriptions and interview management	
OMB Circular A-130, III FISCAM SD-2 & 3.2		Are mechanisms in place for holding users responsible for their actions?	-Review logs of management reviews	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
DOT H1350.253				
FISCAM SD 1.1 FISCAM SP 4.1		Are regularly scheduled vacations and periodic job/shift rotations required?	-Interview management	
NIST SP 800-18 FISCAM SP-4.1		Are hiring, transfer, and termination procedures established?	-Review procedures -Compare a list of system users to a list of active employees to determine if terminated employees exist.	
NIST SP 800-18 FISCAM SP-4.1		*Is there a process for requesting, establishing, issuing, and closing user accounts?*	-Review Process	
	Is appropriate background screening for assigned positions completed prior to granting access?			
OMB Circular A-130, III FISCAM SP-4.1 DOT H1350.253		Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?	-Review hiring policies	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM SP-4.1		Are confidentiality or security agreements required for employees assigned to work with sensitive information?	-Review confidentiality agreements for a subset of employees	
OMB Circular A-130, III		When controls cannot adequately protect the information, are individuals screened prior to access?	-Review screening process	
NIST SP 800-18 FISCAM AC-2.2		Are there conditions for allowing system access prior to completion of screening?	-Review policies	
		PHYSICAL AND ENVIRONMENT PROTECTION		
		Physical Access Control		
	Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?			
NIST SP 800-18 FISCAM AC-3 DOT H1350.253		Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?	-Observe entries and escort procedures -interview management	
FISCAM AC-3.1 DOT		Does management regularly review the list of persons with physical access to sensitive facilities?	-Review the list with management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
H1350.253				
FISCAM AC-3.1		Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?	-Review log -Review Security Plan	
FISCAM AC-3.1 DOT H1350.253		Are keys or other access devices needed to enter the computer room and tape/media library?	-Interview management -Observe entries and exits	
FISCAM AC-3.1		Are unused keys or other entry devices secured?	-Observe key storage	
FISCAM AC-3.1		Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc?	-Review emergency procedures	
FISCAM AC-3.1		Are visitors to sensitive areas signed in and escorted?	-Review visitor logs -Observe entries and exits	
FISCAM AC-3.1		Are entry codes changed periodically?	-Review logs of changes	
FISCAM AC-4		Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?	-Review information being audited -Review a list of incidents	
FISCAM AC-4.3		Is suspicious access activity investigated and appropriate action taken?	-Interview management about recent violations and how they were handled	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM AC-3.1		Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks?	-Observe verification procedures for visitors	
		Fire Safety Factors		
FISCAM SC-2.2 NIST SP 800-18 DOT H1350.253		Are appropriate fire suppression and prevention devices installed and working?	-Walk thru, visual inspection of the facilities.	
NIST SP 800-18		Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically?	-Interview management	
		Supporting Utilities		
NIST SP 800-18		Are heating and air-conditioning systems regularly maintained?	-Interview management	
FISCAM SC-2.2		Is there a redundant air-cooling system?	-Visual inspection	
FISCAM SC-2.2 NIST SP 800-18 DOT H1350.253		Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure?	-Interview management	
FISCAM SC-2.2 NIST SP 800-18		Are building plumbing lines known and do not endanger system?	-Visual inspection	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM SC-2.2 DOT H1350.253		Has an uninterruptible power supply or backup generator been provided?	-Visual inspection	
FISCAM SC-2.2		Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.?	-Interview management	
		Interception of Data		
	Is data protected from interception?			
NIST SP 800-18		Are computer monitors located to eliminate viewing by unauthorized persons?	-Visual inspection	
NIST SP 800-18 DOT H1350.253		Is physical access to data transmission lines controlled?	-Visual inspection	
		Mobile and Portable Systems		
	Are mobile and portable systems protected?			
NIST SP 800-14 DOT H1350.253		Are sensitive data files encrypted on all portable systems?	-Interview management	
NIST SP 800-14		Are portable systems stored securely?	-Visual inspection	
		PRODUCTION, INPUT/OUTPUT CONTROLS		

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	Is there user support?			
NIST SP 800-18		Is there a help desk or group that offers advice?	-Interview management	
	Are there media controls?			
NIST SP 800-18		Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	-Interview management -Visual inspection	
NIST SP 800-18		Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?	-Review processes	
NIST SP 800-18		Are audit trails used for receipt of sensitive inputs/outputs?	-Review audit trails	
NIST SP 800-18		Are controls in place for transporting or mailing media or printed output?	-Review processes	
NIST SP 800-18 DOT H1350.253		Is there internal/external labeling for sensitivity?	-Interview management	
NIST SP 800-18 DOT H1350.253		Is there external labeling with special handling instructions?	-Interview management	
NIST SP 800-18		Are audit trails kept for inventory management?	-Review audit trails	
NIST SP 800-18 FISCAM AC-3.4		Is media sanitized for reuse?	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Is damaged media stored and /or destroyed?	-Interview management	
NIST SP 800-18		Is hardcopy media shredded or destroyed when no longer needed?	-Interview management	
OMB Circular A-130, III DOT H1350.253		CONTINGENCY PLANNING		
	Have the most critical and sensitive operations and their supporting computer resources been identified?			
FISCAM SC-1.1 & 3.1 NIST SP 800-18 DOT H1350.253		Are critical data files and operations identified and the frequency of file backup documented?	-Review related documents	
FISCAM SC-1.2		Are resources supporting critical operations identified?	-Interview management	
FISCAM SC-1.3		Have processing priorities been established and approved by management?	-Review policies and related documents -Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	Has a comprehensive contingency plan been developed and documented?			
FISCAM SC-3.1		Is the plan approved by key affected parties?	-Review sign-off sheets	
FISCAM SC-3.1		Are responsibilities for recovery assigned?	-Review contingency plan	
FISCAM SC-3.1		Are there detailed instructions for restoring operations?	-Review contingency plan	
FISCAM SC-3.1 NIST SP 800-18		Is there an alternate processing site; if so, is there a contract or interagency agreement in place?	-Review contingency plan	
NIST SP 800-18 DOT H1350.253		Is the location of stored backups identified?	-Review contingency plan	
FISCAM SC-2.1 DOT H1350.253		Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?	-Interview management	
FISCAM SC-2.1		Is system and application documentation maintained at the off-site location?	-Interview management	
FISCAM SC-3.1		Are all system defaults reset after being restored from a backup?	-Interview management	
FISCAM SC-2.1		Are the backup storage site and alternate site geographically removed from the primary site	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
		and physically protected?		
FISCAM SC-3.1		Has the contingency plan been distributed to all appropriate personnel?	-Interview management	
	Are tested contingency/disaster recovery plans in place?			
FISCAM SC-3.1		Is an up-to-date copy of the plan stored securely off-site?	-Interview management	
FISCAM SC-2.3 NIST SP 800-18		Are employees trained in their roles and responsibilities?	-Review training procedures	
FISCAM SC-3.1 NIST SP 800-18		Is the plan periodically tested and readjusted as appropriate?	-Review test plans and results.	
OMB Circular A-130, III DOT H1350.253		HARDWARE AND SYSTEM SOFTWARE MAINTENANCE		
	Is access limited to system software and hardware?			
OMB Circular A-130, III FISCAM SS-3.1 NIST SP 800-		Are restrictions in place on who performs maintenance and repair activities?	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
18				
FISCAM CC-3.2 & 3.3		Is access to all program libraries restricted and controlled?	-Interview management	
NIST SP 800-18		Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?	-Interview management	
FISCAM SS-1.2 DOT H1350.253		Is the operating system configured to prevent circumvention of the security software and application controls?	-Test scan of system	
FISCAM SS-2.1		Are up-to-date procedures in place for using and monitoring use of system utilities?	-Review policies -Interview management	
	Are all new and revised hardware and software authorized, tested and approved before implementation?			
NIST SP 800-18		Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	-Review configuration management plan	
FISCAM SS-3.1, 3.2, & CC-2.1 NIST SP 800-		Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production?	-Review configuration management plan	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
18				
FISCAM CC-1.2 NIST SP 800-18		Are software change request forms used to document requests and related approvals?	-Review configuration management plan -Review change request forms	
FISCAM CC-2.1		Are there detailed system specifications prepared and reviewed by management?	-Review specifications and tests	
NIST SP 800-18		Is the type of test data to be used specified, i.e., live or made up?	-Interview management	
PSN Security Assessment Guidelines		Are default settings of security features set to the most restrictive mode?	-Interview management	
FISCAM CC-2.3		Are there software distribution implementation orders including effective date provided to all locations?	-Review procedures and samples of change	
NIST SP 800-18		Is there version control?	-Interview management	
FISCAM CC-3.1		Are programs labeled and inventoried?	-Interview management	
FISCAM SS-3.2		Are the distribution and implementation of new or revised software documented and reviewed?	-Interview management	
FISCAM CC-2.2		Are emergency change procedures documented and approved by management, either prior to the change or after the fact?	-Review documents	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM SC-2.1 NIST SP 800-18		Are contingency plans and other associated documentation updated to reflect system changes?	-Review contingency plan approval sheet	
NIST SP 800-18		Is the use of copyrighted software or shareware and personally owned software/equipment documented?	-Review policy and documents	
		Are systems managed to reduce vulnerabilities?	-Interview management	
NIST SP 800-18		Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)?	-Test scan of system	
NIST SP 800-18		Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?	-Test scan of system -Review of prior tests	
OMB Circular A-130, 8B3		DATA INTEGRITY		
	Is virus detection and elimination software installed and activated?			
NIST SP 800-18 DOT H1350.253		Are virus signature files routinely updated?	-Interview management	
NIST SP 800-18		Are virus scans automatic?	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
DOT H1350.253				
	Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?			
NIST SP 800-18		Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts?	-Interview management	
FISCAM SS-2.2		Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?	-Interview management -Review related documents	
NIST SP 800-18 DOT H1350.253		Are procedures in place to determine compliance with password policies?	-Test scan of system	
NIST SP 800-18 DOT H1350.253		Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?	-Interview management	
NIST SP 800-18		Are intrusion detection tools installed on the system?	-Interview management -Review IDS report	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly?	-Interview management	
NIST SP 800-18		Is penetration testing performed on the system?	-Interview management	
NIST SP 800-18		Is message authentication used?	-Interview management	
OMB Circular A-130, 8B3		*DOCUMENTATION*		
	Is there sufficient documentation that explains how software/hardware is to be used?			
NIST SP 800-18 DOT H1350.253		Is there vendor-supplied documentation of purchased software?	-Interview management -Review documentation	
NIST SP 800-18		Is there vendor-supplied documentation of purchased hardware?	-Interview management -Review documentation	
NIST SP 800-18		Is there application documentation for in-house applications?	-Interview management -Review documentation	
NIST SP 800-18		Are there network diagrams and documentation on setups of routers and switches?	-Interview management -Review documentation	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Are there software and hardware testing procedures and results?	-Review configuration management plan	
NIST SP 800-18		Are there standard operating procedures for all the topic areas covered in this document?	-Review Security Plan	
NIST SP 800-18		Are there user manuals?	-Review manuals	
NIST SP 800-18		Are there emergency procedures?	-Review procedures	
NIST SP 800-18		Are there backup procedures?	-Review procedures	
	Are there formal security and operational procedures documented?			
OMB Circular A-130, III FISCAM SP-2.1 NIST SP 800-18		Is there a system security plan?	-Review security plan	
NIST SP 800-18 DOT H1350.253		Is there a contingency plan?	-Review contingency plan	
OMB Circular A-130, III NIST SP 800-18 DOT H1350.253		Are there written agreements regarding how data is shared between interconnected systems?	-Review MOUs/MOAs	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Are there risk assessment reports?	-Review risk assessment reports	
NIST SP 800-18		Are there certification and accreditation documents and a statement authorizing the system to process?	-Review documents	
OMB Circular A-130, III DOT H1350.253		SECURITY AWARENESS, TRAINING AND EDUCATION		
	Have employees received adequate training to fulfill their security responsibilities?			
NIST SP 800-18		Have employees received a copy of the Rules of Behavior?	-Review Rules of Behavior	
FISCAM SP-4.2		Are employee training and professional development documented and monitored?	-Review training records and documents	
OMB Circular A-130, III		Is there mandatory annual refresher training?	-Review training procedures	
NIST SP 800-18		Are methods employed to make employees aware of security, i.e., posters, booklets?	-Review training procedures	
NIST SP 800-18		Have employees received a copy of or have easy access to agency security procedures and policies?	-Review training procedures	
OMB Circular A-130, III FISCAM SP-3.4		INCIDENT RESPONSE CAPABILITY		

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18 DOT H1350.253				
	Is there a capability to provide help to users when a security incident occurs in the system?			
FISCAM SP-3.4 NIST SP 800-18		Is a formal incident response capability available?	-Interview management -Review documents	
FISCAM SP-3.4 NIST SP 800-18		Is there a process for reporting incidents?	-Interview management -Review documents	
NIST SP 800-18		Are incidents monitored and tracked until resolved?	-Interview management -Review documents	
FISCAM SP-3.4 NIST SP 800-18		Are personnel trained to recognize and handle incidents?	-Interview management	
NIST SP 800-18		Are alerts/advisories received and responded to?	-Interview management	
NIST SP 800-18		Is there a process to modify incident handling procedures and control techniques after an incident occurs?	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	Is incident related information shared with appropriate organizations?			
OMB Circular A-130, III NIST SP 800-18 DOT H1350.253		Is incident information and common vulnerabilities or threats shared with owners of interconnected systems?	-Interview management -Review MOUs/MOAs	
OMB Circular A-130, III GISRA		Is incident information shared with FedCIRC[3] concerning incidents and common vulnerabilities and threats?	-Interview management	
OMB Circular A-130, III GISRA		Is incident information reported to FedCIRC, NIPC[4], and local law enforcement when necessary?	-Interview management	
OMB Circular A-130, III FISCAM AC-2 NIST SP 800-18 DOT H1350.253		IDENTIFICATION AND AUTHENTICATION		
	Are users individually authenticated via passwords, tokens, or other devices?			

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM AC-2 NIST SP 800-18 DOT H1350.253		Is a current list maintained and approved of authorized users and their access?	-Review list	
NIST SP 800-18		Are digital signatures used and conform to FIPS 186-2?	-Interview management	
NIST SP 800-18 DOT H1350.253		Are access scripts with embedded passwords prohibited?	-Interview management	
FISCAM AC-2.2		Is emergency and temporary access authorized?	-Interview management	
FISCAM AC-3.2		Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?	-Review policies -Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are passwords changed at least every ninety days or earlier if needed?	-Review policies on passwords -Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)?	-Review policies on passwords -Interview management -Review user training	
FISCAM AC-3.2		Are inactive user identifications disabled after a specified period of time?	-Review policies	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
3.2 NIST SP 800-18		specified period of time?		
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are passwords not displayed when entered?	-Review policies on passwords -Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are there procedures in place for handling lost and compromised passwords?	-Review policies on passwords -Interview management	
NIST SP 800-18 DOT H1350.253		Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?	-Review policies on passwords -Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are passwords transmitted and stored using secure protocols/algorithms?	-Review policies on passwords -Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Are vendor-supplied passwords replaced immediately?	-Review policies on passwords -Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Is there a limit to the number of invalid access attempts that may occur for a given user?	-Review policies on passwords -Interview management	
	Are access controls enforcing segregation of duties?			
OMB Circular A-130, III FISCAM SD-2.1 DOT H1350.253		Does the system correlate actions to users?	-Review audit policies	
FISCAM AC-2.1 DOT H1350.253		Do data owners periodically review access authorizations to determine whether they remain appropriate?	-Review access authorization policy -Interview management	
OMB Circular A-130, III FISCAM AC-3.2 NIST SP 800-18		LOGICAL ACCESS CONTROLS		
	Do the logical access controls restrict users to authorized			

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	transactions and functions?			
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Can the security controls detect unauthorized access attempts?	-Review audit policy and IDS systems -Interview management -Test scan of system	
FISCAM AC-3.2 NIST SP 800-18		Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?	-Review audit policy and IDS systems -Interview management -Test scan of system	
FISCAM AC-3.2		Is access to security software restricted to security administrators?	-Interview management	
FISCAM AC-3.2 NIST SP 800-18 DOT H1350.253		Do workstations disconnect or screen savers lock system after a specific period of inactivity?	-Interview management	
FISCAM AC-3.2 NIST SP 800-18		Are inactive users' accounts monitored and removed when not needed?	-Interview management -Test scan of system	
FISCAM AC-3.2		Are internal security labels (naming conventions) used to control access to specific information types or files?	-Interview management	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18 DOT H1350.253		information types or files?		
NIST SP 800-18		If encryption is used, does it meet federal standards?	-Interview management	
NIST SP 800-18		If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	-Interview management	
FISCAM AC-3.2		Is access restricted to files at the logical view or field?	-Interview management	
FISCAM AC-4		Is access monitored to identify apparent security violations and are such events investigated?	-Review policies -Review reports	
	Are there logical controls over network access?			
FISCAM AC-3.2		Has communication software been implemented to restrict access through specific terminals?	-Review policies -Interview management	
PSN Security Assessment Guidelines		Are insecure protocols (e.g., UDP, ftp) disabled?	-Test scan of system	
PSN Security Assessment Guidelines		Have all vendor-supplied default security parameters been reinitialized to more secure settings?	-Test scan of system	
NIST SP 800-18		Are there controls that restrict remote access to the system?	-Test scan of system	
FISCAM AC-3.2		Are network activity logs maintained and reviewed?	-Review logs	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
FISCAM AC-3.2		Does the network connection automatically disconnect at the end of a session?	-Interview management	
PSN Security Assessment Guidelines		Are trust relationships among hosts and external entities appropriately restricted?	-Review MOUs/MOAs	
FISCAM AC-3.2		Is dial-in access monitored?	-Interview management	
FISCAM AC-3.2 DOT H1350.253		Is access to communications hardware or facilities restricted and monitored?	-Interview management	
NIST SP 800-18		Are firewalls or secure gateways installed?	-Interview management	
FISCAM AC-3.2		If firewalls are installed do they comply with firewall policy and rules?	-Interview management	
PSN Security Assessment Guidelines DOT H1350.253		Are guest and anonymous accounts authorized and monitored?		
FISCAM AC-3.2 NIST SP 800-18		Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished?	Review pertinent policies and procedures. View the opening screen seen by telecommunicatio n system users.	
FISCAM AC-3.2 DOT		Are sensitive data transmissions encrypted?	Review parameters set by communications	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
H1350.253			communications software or teleprocessing monitors.	
FISCAM AC-3.2		Is access to tables defining network options, resources, and operator profiles restricted?	Review parameters set by communications software or teleprocessing monitors. Test telecommunications software or teleprocessing monitors.	
	If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?			
OMB 99-18		Is a privacy policy posted on the web site?	Request a copy of what is shown on the web site to people.	
OMB Circular A-130, III FISCAM AC-4.1 NIST SP 800-18		AUDIT TRAILS		

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
	Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?			
NIST SP 800-18 DOT H1350.253		Does the audit trail provide a trace of user actions?	Interview with sys Admin. Sample of the audit trail. Ask for the actual actions that are being audited.	
NIST SP 800-18 DOT H1350.253		Can the audit trail support after-the fact investigations of how, when, and why normal operations ceased?	Interview with sys Admin. Sample of the audit trail. Ask for the actual actions that are being audited	
NIST SP 800-18		Is access to online audit logs strictly controlled?	Interview with sys Admin. Sample of the audit trail. Confirm separation of duties. Ask for the actual actions that are being audited	
NIST SP 800-18		Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?	Interview with sys Admin. Sample of the audit trail. Ask for the actual	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
			actions that are being audited	
NIST SP 800-18		Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?	Interview with sys Admin. Sample of the audit trail. Ask for the actual actions that are being audited. List of sys admin job descriptions. Written policies	
NIST SP 800-18		Are audit trails reviewed frequently?	Interview with sys Admin. Sample of the audit trail. Ask for the actual actions that are being audited. Is there a log when audit trails are reviewed?	
NIST SP 800-18		Are automated tools used to review audit records in real time or near real time?	Interview with sys Admin. Sample of the audit trail. Ask for the actual actions that are being audited.	
FISCAM AC-4.3		Is suspicious activity investigated and appropriate action taken?	Test a selection of security violations to verify that follow-up investigations were performed and to determine what actions were taken against the perpetrator.	

References	Control Objective	Control Techniques	Evidence Requirement	Pass /Fail
NIST SP 800-18		Is keystroke monitoring used? If so, are users notified?	Interview with sys Admin.	

Assignment 3 – Audit Report

Findings

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
Risk Management	X		Reviewed Technical Architecture Document Reviewed two previous Risk Assessments New Risk Assessment in process MOUs in process	Interviewed System Owners and Security Managers to determine the technical security controls in place. Tour of Backup system at the Data Warehouse Interview with Backup personnel	Reviewed previous ISS scan of the system by the IG.	ISS Report Risk Assessment Reports Security Plan Technical Architecture Document, Disaster Recovery Plan MOUs	Passed contingent on continuation of certification activities. Risk Assessment and DRP are in process. Security Plan is in Draft form MOUs in process.
Review of Security Controls	X		MOUs in process New Risk Assessment in process Reviewed change control process in Configuration Management Plan	Tour of Backup system at the Data Warehouse Interview with System personnel	Reviewed previous ISS scan of the system by the IG.	IRM Plan Configuration Management Plan Risk Assessment MOUs	Passed contingent on continuation of certification activities. Recommend that certification activities be added to the current configuration management plan.

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
Life Cycle	X		MOUs in process Reviewed Configuration Management Plan Reviewed Capital Planning Information Risk Assessment in process Reviewed system configuration documents provided by ICS Developed Security Plan	Interview with the system owner to determine the budget process. Interview with the system owner and security manager to discuss disposal procedures. Tour of backup system at the Data Warehouse Interview with Backup personnel	Reviewed previous ISS scan of the system by the IG.	Capital Planning Information Configuration Management Plan Security Plan Risk Assessment Reports	Recommend that certification activities be incorporated into their configuration management plan and system life cycle. Risk Assessment in process. Security Plan should be reviewed on a yearly basis and updated to reflect any change in the security controls. Currently not keeping records of disposals at the Backup facility. Since they are going to implement a plan to do that now, we will pass them based on the fact that the system is new and no disposals have been made.
Authorize Processing	X		Reviewed Rules of Behavior and other policy and procedure documents. Developing Risk Assessment MOUs in process	Discussed the system life cycle, approval process and other risk management requirements to determine the level of management approval. Tour of backup system at the Data Warehouse Interview with Backup personnel	Reviewed previous ISS scan of the system by the IG.	Risk Assessment Report in process Rules of Behavior Disaster Recovery Plan in process Security Plan MOUs	Passed contingent on continuation of certification activities. Recommend that certification activities be added to the current configuration management plan.
System Security Plan	X		Developed system security			Security Plan	Security Plan should be reviewed

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
			plan. Reviewed IRM			IRM Plan	on a yearly basis and updated to reflect any change in the security controls.
Personnel Security	X			Interviews with Backup facility managers regarding physical access controls for personnel including background checks and separation of duties.			All personnel are subject to FAA background investigations. Audit Trails are used within Backup's network to track user activity.
Physical and Environmental Protection	X		The server is located in a locked room that uses video surveillance to monitor access.	Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel		MOUs IRM Plan	Hallon fire suppression system. There is no public access to the data warehouse.
Production, Input/Output Controls		X	User support is provided thru a toll free number if there is a problem with the system. MOUs	Interviewed the facility manager to ensure that proper disposal procedures are followed. Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel	Twofish encryption is used for sending data across the network.	MOUs Audit procedures provided by ICS	Passed contingent on continuation of certification activities. There are no paper reports or media transported in the Government system. Currently not destroying hard drives that are discarded, but they will start now.

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
Contingency Planning	X		Backup backs up the system on a regular basis.	Interview with The System Owner to discuss the process if a server goes down. 24-hour replacement for a server that is completely down. 4-hour response time for maintenance. Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel		Disaster Recovery Plan in process MOUs	Disaster Recovery Plan must be tested before 6-month deadline.
Hardware and System Software Maintenance	X		ICS monitors the server 24/7 to ensure that no unauthorized changes are made to the configuration. All maintenance personnel are escorted. MOUs Reviewed configuration management plan	Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel	Reviewed previous ISS scan of the system by the IG.	MOUs Configuration Management Plan	Passed contingent on continuation of certification activities. Recommend that certification activities be added to the current configuration management plan.

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
Data Integrity	X		ICS monitors the system for intrusion detection. They also handle the incident reporting and escalation.	Password policy was discussed with The System Owner. Several changes were made to the system to ensure that the passwords rules are enforced on the system, such as a minimum length, expiration date and password reusability. Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel	Twofish encryption is used to send sensitive data across the network.	IRM Plan MOUs	
Documentation	X		Reviewed the policy documents. Government supplies user manuals for their application. They were reviewed. Completing Risk Assessment	Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel		Technical Architecture Document Configuration Management Plan User Manuals System Security Plan Disaster Recovery Plan MOUs Risk Assessment Report	Passed contingent on continuation of certification activities.
Security Awareness, Training and Education	X		Rules of behavior are displayed on the screen prior to entering the	Interview with system owner on security		Rules of Behavior MOUs in process	

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
			system.	training procedures of personnel Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel			
Incident Response Capability	X		ICS Monitors the system 24/7. Incidents are tracked and escalated as required. Incidents are shared with connecting system owners.	Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel		IRM Plan	
Identification and Authentication	X		Password enforcement policy was changed on the system to ensure that the passwords are secure, expire every 90 days, are a minimum of 8 characters, and can't be reused. MOUs in process	Interview with The System Owner on the procedures used to transmit and reset passwords Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel	Reviewed previous ISS scan of the system by the IG.	MOUs	Passed contingent on continuation of certification activities.
Logical Access Controls	X		MOUs in process Reviewed system configuration procedures with ICS	Interview with The System Owner on the value of session control and screen savers. Tour of Backup system at the Backup	Twofish encryption is used to send sensitive data across the system. Reviewed previous ISS scan of the system by the IG.	MOUs	

Control Objective	Pass	Fail	Testing Method			Evidence	Notes/ Recommendations
			Demonstration	Inspection	Test		
				Data Warehouse Interview with Backup personnel			
Audit Trails	X		ICS monitors the system audit trails 24/7. Reviewed auditing procedures for system MOUs in process	Tour of Backup system at the Backup Data Warehouse Interview with Backup personnel		MOUs in process IRM Plan	Passed contingent on continuation of certification activities.

Recommendations

References

DOT H 1350.250: Guide to Establishing an Information Systems Protection Program
DOT H 1350.251: Guide to Developing an Information Systems Security Plan
DOT H 1350.252: Guide to Risk Assessments
DOT H 1350.260: Guide to Protecting Information Technology
DOT H 1350.271: Guide to Information Protection for Senior Management
DOT H 1350.272: Guide to Information Protection for Users
DOT H 1370.273: Guide to Information Protection for Contractors
DOT H 1370.275: Federal Information Protection Resources
FAA Order 1370.82, Information Systems Security Program
NIST 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST 800-12: Introduction to Computer Security: The NIST Handbook
NIST 800-18, Guide for Developing Security Plans for Information Technology Systems
NIST 800-26, Security Self-Assessment Guide for Information Technology Systems
OMB A-130, Management of Federal Information Resources
NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000
Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditatio*n, September 1983

Last Updated: July 22nd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**