



International Civil Aviation Organization and the Directorate General of Air Communication, Indonesia

SIXTH MEETING OF AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) TRANSITION TASK FORCE OF APANPIRG



Bali, Indonesia, 26-30 April 2004

Agenda Item 4: Discussions and Review on ATN Technical Documents - ATN Systems Integrity Issues

SYSTEM INTEGRITY VERIFICATION CHECKLIST

(Prepared by: Vic Patel, US FAA)

SUMMARY

The draft ATN System Integrity Policy requires that the Designated Approval Authority (DAA) in each administration authorize operation of the systems in the administration's domain. The authorization is to be based on a review of the management, operational, and technical controls of the systems. The attached checklist, taken from the US National Institute of Standards publication, "Security Self Assessment Guide for IT Systems (NIST SP 800-26)" may be used as a suitable verification checklist. (Attachment A). The complete document is available at <http://csrc.nist.gov/publications/nistpubs/>. The draft ATN System Integrity Policy presented at the last ACP meeting is also attached.

Appendix A

System Questionnaire

Table of Contents

SYSTEM QUESTIONNAIRE COVER SHEET	A-3
MANAGEMENT CONTROLS.....	A-5
1. RISK MANAGEMENT.....	A-5
2. REVIEW OF SECURITY CONTROLS.....	A-7
3. LIFE CYCLE	A-9
4. AUTHORIZE PROCESSING (CERTIFICATION & ACCREDITATION)	A-14
5. SYSTEM SECURITY PLAN.....	A-16
OPERATIONAL CONTROLS	A-18
6. PERSONNEL SECURITY.....	A-18
7. PHYSICAL AND ENVIRONMENTAL PROTECTION.....	A-21
8. PRODUCTION, INPUT/OUTPUT CONTROLS.....	A-25
9. CONTINGENCY PLANNING	A-27
10. HARDWARE AND SYSTEM SOFTWARE MAINTENANCE.....	A-30
11. DATA INTEGRITY.....	A-34
12. DOCUMENTATION.....	A-36
13. SECURITY AWARENESS, TRAINING, AND EDUCATION	A-38
14. INCIDENT RESPONSE CAPABILITY	A-40
TECHNICAL CONTROLS.....	A-43
15. IDENTIFICATION AND AUTHENTICATION.....	A-43
16. LOGICAL ACCESS CONTROLS	A-46
17. AUDIT TRAILS	A-50

System Name, Title, and Unique Identifier: _____

Major Application _____ **or** **General Support System** _____

Name of Assessors: _____

Date of Evaluation: _____

List of Connected Systems:

<u>Name of System</u>	<u>Are boundary controls effective?</u>	<u>Planned action if not effective</u>
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management <i>OMB Circular A-130, III</i>								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? <i>NIST SP 800-18</i>								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? <i>FISCAM SP-1</i>								
1.1.3 Has data sensitivity and integrity of the data been considered? <i>FISCAM SP-1</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.4 Have threat sources, both natural and manmade, been identified? <i>FISCAM SP-1</i>								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? <i>NIST SP 800-30¹</i>								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? <i>NIST SP 800-30</i>								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? <i>FISCAM SP-1</i>								
1.2.2 Has a mission/business impact analysis been conducted? <i>NIST SP 800-30</i>								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? <i>NIST SP 800-30</i>								

NOTES:

¹ Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

2. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls <i>OMB Circular A-130, III</i> <i>FISCAM SP-5</i> <i>NIST SP 800-18</i>								
2.1. Critical Element: Have the security controls of the system and interconnected systems been reviewed?								
2.1.1 Has the system and all network boundaries been subjected to periodic reviews? <i>FISCAM SP-5.1</i>								
2.1.2 Has an independent review been performed when a significant change occurred? <i>OMB Circular A-130, III</i> <i>FISCAM SP-5.1</i> <i>NIST SP 800-18</i>								
2.1.3 Are routine self-assessments conducted ? <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? <i>OMB Circular A-130, 8B3</i> <i>NIST SP 800-18</i>								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? <i>FISCAM SP 3-4</i> <i>NIST SP 800-18</i>								
2.2. Critical Element: Does management ensure that corrective actions are effectively implemented?								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? <i>FISCAM SP 5-1 and 5.2</i> <i>NIST SP 800-18</i>								

NOTES:

3. Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle <i>OMB Circular A-130, III</i> <i>FISCAM CC-1.1</i>								
3.1. Critical Element: Has a system development life cycle methodology been developed?								
Initiation Phase								
3.1.1 Is the sensitivity of the system determined? <i>OMB Circular A-130, III</i> <i>FISCAM AC-1.1 & 1.2</i> <i>NIST SP 800-18</i>								
3.1.2 Does the business case document the resources required for adequately securing the system? <i>Clinger-Cohen</i>								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? <i>Clinger-Cohen</i>								
3.1.4 Are authorizations for software modifications documented and maintained? <i>FISCAM CC -1.2</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.5 Does the budget request include the security resources required for the system? <i>GISRA</i>								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? <i>NIST SP 800-18</i>								
3.1.7 Was an initial risk assessment performed to determine security requirements? <i>NIST SP 800-30</i>								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? <i>NIST SP 800-18</i>								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? <i>OMB Circular A-130, 8B3</i>								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? <i>NIST SP 800-18</i>								
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? <i>NIST SP 800-18</i>								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								
3.2.1 Are design reviews and system tests run prior to placing the system in production? <i>FISCAM CC-2.1</i> <i>NIST SP 800-18</i>								
3.2.2 Are the test results documented? <i>FISCAM CC-2.1</i> <i>NIST SP 800-18</i>								
3.2.3 Is certification testing of security controls conducted and documented? <i>NIST SP 800-18</i>								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? <i>NIST SP 800-18</i>								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? <i>FISCAM CC-2.1</i> <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? <i>NIST SP 800-18</i>								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? <i>NIST SP 800-18</i>								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? <i>OMB Circular A-130, III</i> <i>FISCAM SP 2-1</i> <i>NIST SP 800-18</i>								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? <i>NIST SP 800-18</i>								
3.2.10 Is the system security plan kept current? <i>OMB Circular A-130, III</i> <i>FISCAM SP 2-1</i> <i>NIST SP 800-18</i>								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? <i>FISCAM AC-3.4</i> <i>NIST SP 800-18</i>								
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? <i>NIST SP 800-18</i>								

NOTES:

4. Authorize Processing (Certification & Accreditation)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) <i>OMB Circular A-130, III</i> <i>FIPS 102</i>								
4.1. Critical Element: Has the system been certified/recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? <i>NIST SP 800-18</i>								
4.1.2 Has a risk assessment been conducted when a significant change occurred? <i>NIST SP 800-18</i>								
4.1.3 Have Rules of Behavior been established and signed by users? <i>NIST SP 800-18</i>								
4.1.4 Has a contingency plan been developed and tested? <i>NIST SP 800-18</i>								
4.1.5 Has a system security plan been developed, updated, and reviewed? <i>NIST SP 800-18</i>								
4.1.6 Are in-place controls operating as intended? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? <i>NIST SP 800-18</i>								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? <i>NIST 800-18</i>								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? <i>NIST SP 800-18</i>								

NOTES:

5. System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan <i>OMB Circular A-130, III</i> <i>NIST SP 800-18</i> <i>FISCAM SP-2.1</i>								
5.1. Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.1.1 Is the system security plan approved by key affected parties and management? <i>FISCAM SP-2.1</i> <i>NIST SP 800-18</i>								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? <i>NIST SP 800-18</i>								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? <i>OMB Circular A-130, III</i> <i>NIST SP 800-18</i>								
5.2. Critical Element: Is the plan kept current?								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? <i>FISCAM SP-2.1</i> <i>NIST SP 800-18</i>								

NOTES:

Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Personnel Security <i>OMB Circular A-130, III</i>								
6.1. Critical Element: Are duties separated to ensure least privilege and individual accountability?								
6.1.1 Are all positions reviewed for sensitivity level? <i>FISCAM SD-1.2</i> <i>NIST SP 800-18</i>								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? <i>FISCAM SD-1.2</i>								
6.1.3 Are sensitive functions divided among different individuals? <i>OMB Circular A-130, III</i> <i>FISCAM SD-1</i> <i>NIST SP 800-18</i>								

	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Specific Control Objectives								
6.1.4 Are distinct systems support functions performed by different individuals? <i>FISCAM SD-1.1</i>								
6.1.5 Are mechanisms in place for holding users responsible for their actions? <i>OMB Circular A-130, III</i> <i>FISCAM SD-2 & 3.2</i>								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? <i>FISCAM SD-1.1</i> <i>FISCAM SP-4.1</i>								
6.1.7 Are hiring, transfer, and termination procedures established? <i>FISCAM SP-4.1</i> <i>NIST SP 800-18</i>								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? <i>FISCAM SP-4.1</i> <i>NIST 800-18</i>								
6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? <i>OMB Circular A-130, III</i> <i>FISCAM SP-4.1</i>								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? <i>FISCAM SP-4.1</i>								

Appendix D
References

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? <i>OMB Circular A-130, III</i>								
6.2.4 Are there conditions for allowing system access prior to completion of screening? <i>FISCAM AC-2.2</i> <i>NIST SP 800-18</i>								

NOTES:

7. Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
<i>Physical Access Control</i>								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? <i>FISCAM AC-3</i> <i>NIST SP 800-18</i>								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? <i>FISCAM AC-3.1</i>								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? <i>FISCAM AC-3.1</i>								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? <i>FISCAM AC-3.1</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.5 Are unused keys or other entry devices secured? <i>FISCAM AC-3.1</i>								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? <i>FISCAM AC-3.1</i>								
7.1.7 Are visitors to sensitive areas signed in and escorted? <i>FISCAM AC-3.1</i>								
7.1.8 Are entry codes changed periodically? <i>FISCAM AC-3.1</i>								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? <i>FISCAM AC-4</i>								
7.1.10 Is suspicious access activity investigated and appropriate action taken? <i>FISCAM AC-4.3</i>								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? <i>FISCAM AC-3.1</i>								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? <i>FISCAM SC-2.2</i> <i>NIST SP 800-18</i>								

	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Specific Control Objectives and Techniques								
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? <i>NIST SP 800-18</i>								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? <i>NIST SP 800-18</i>								
7.1.15 Is there a redundant air-cooling system? <i>FISCAM SC-2.2</i>								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? <i>FISCAM SC-2.2</i> <i>NIST SP 800-18</i>								
7.1.17 Are building plumbing lines known and do not endanger system? <i>FISCAM SC-2.2</i> <i>NIST SP 800-18</i>								
7.1.18 Has an uninterruptible power supply or backup generator been provided? <i>FISCAM SC-2.2</i>								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? <i>FISCAM SC-2.2</i>								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? <i>NIST SP 800-18</i>								
7.2.2 Is physical access to data transmission lines controlled? <i>NIST SP 800-18</i>								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? <i>NIST SP 800-14</i>								
7.3.2 Are portable systems stored securely? <i>NIST SP 800-14</i>								

NOTES:

8. Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? <i>NIST SP 800-18</i>								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? <i>NIST SP 800-18</i>								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? <i>NIST SP 800-18</i>								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? <i>NIST SP 800-18</i>								
8.2.4 Are controls in place for transporting or mailing media or printed output? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.5 Is there internal/external labeling for sensitivity? <i>NIST SP 800-18</i>								
8.2.6 Is there external labeling with special handling instructions? <i>NIST SP 800-18</i>								
8.2.7 Are audit trails kept for inventory management? <i>NIST SP 800-18</i>								
8.2.8 Is media sanitized for reuse? <i>FISCAM AC-3.4</i> <i>NIST SP 800-18</i>								
8.2.9 Is damaged media stored and /or destroyed? <i>NIST SP 800-18</i>								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? <i>NIST SP 800-18</i>								

NOTES:

9. Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning <i>OMB Circular A-130, III</i>								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? <i>FISCAM SC- SC-1.1 & 3.1</i> <i>NIST SP 800-18</i>								
9.1.2 Are resources supporting critical operations identified? <i>FISCAM SC-1.2</i>								
9.1.3 Have processing priorities been established and approved by management? <i>FISCAM SC-1.3</i>								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties? <i>FISCAM SC-3.1</i>								
9.2.2 Are responsibilities for recovery assigned? <i>FISCAM SC-3.1</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2.3 Are there detailed instructions for restoring operations? <i>FISCAM SC-3.1</i>								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? <i>FISCAM SC-3.1</i> <i>NIST SP 800-18</i>								
9.2.5 Is the location of stored backups identified? <i>NIST SP 800-18</i>								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? <i>FISCAM SC-2.1</i>								
9.2.7 Is system and application documentation maintained at the off-site location? <i>FISCAM SC-2.1</i>								
9.2.8 Are all system defaults reset after being restored from a backup? <i>FISCAM SC-3.1</i>								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? <i>FISCAM SC-2.1</i>								
9.2.10 Has the contingency plan been distributed to all appropriate personnel? <i>FISCAM SC-3.1</i>								
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? <i>FISCAM SC-3.1</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.3.2 Are employees trained in their roles and responsibilities? <i>FISCAM SC-2.3</i> <i>NIST SP 800-18</i>								
9.3.3 Is the plan periodically tested and readjusted as appropriate? <i>FISCAM SC-3.1</i> <i>NIST SP 800-18</i>								

NOTES:

10. Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance <i>OMB Circular A-130, III</i>								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? <i>OMB Circular A-130, III FISCAM SS-3.1 NIST SP 800-18</i>								
10.1.2 Is access to all program libraries restricted and controlled? <i>FISCAM CC-3.2 & 3.3</i>								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? <i>NIST SP 800-18</i>								
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? <i>FISCAM SS-1.2</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? <i>FISCAM SS-2.1</i>								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 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? <i>NIST SP 800-18</i>								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? <i>FISCAM SS-3.1, 3.2, & CC-2.1</i> <i>NIST SP 800-18</i>								
10.2.3 Are software change request forms used to document requests and related approvals? <i>FISCAM CC-1.2</i> <i>NIST SP 800-18</i>								
10.2.4 Are there detailed system specifications prepared and reviewed by management? <i>FISCAM CC-2.1</i>								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? <i>NIST SP 800-18</i>								
10.2.6 Are default settings of security features set to the most restrictive mode? <i>PSN Security Assessment Guidelines</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? <i>FISCAM CC-2.3</i>								
10.2.8 Is there version control? <i>NIST SP 800-18</i>								
10.2.9 Are programs labeled and inventoried? <i>FISCAM CC-3.1</i>								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? <i>FISCAM SS-3.2</i>								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? <i>FISCAM CC-2.2</i>								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? <i>FISCAM SC-2.1</i> <i>NIST SP 800-18</i>								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? <i>NIST SP 800-18</i>								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? <i>NIST SP 800-18</i>								

NOTES:

11. Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity <i>OMB Circular A-130, 8B3</i>								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? <i>NIST SP 800-18</i>								
11.1.2 Are virus scans automatic? <i>NIST SP 800-18</i>								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? <i>NIST SP 800-18</i>								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? <i>FISCAM SS-2.2</i>								
11.2.3 Are procedures in place to determine compliance with password policies? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? <i>NIST SP 800-18</i>								
11.2.5 Are intrusion detection tools installed on the system? <i>NIST SP 800-18</i>								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? <i>NIST SP 800-18</i>								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? <i>NIST SP 800-18</i>								
11.2.8 Is penetration testing performed on the system? <i>NIST SP 800-18</i>								
11.2.9 Is message authentication used? <i>NIST SP 800-18</i>								

NOTES:

12. Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation <i>OMB Circular A-130, 8B3</i>								
12.1. Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software? <i>NIST SP 800-18</i>								
12.1.2 Is there vendor-supplied documentation of purchased hardware? <i>NIST SP 800-18</i>								
12.1.3 Is there application documentation for in-house applications? <i>NIST SP 800-18</i>								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? <i>NIST SP 800-18</i>								
12.1.5 Are there software and hardware testing procedures and results? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? <i>NIST SP 800-18</i>								
12.1.7 Are there user manuals? <i>NIST SP 800-18</i>								
12.1.8 Are there emergency procedures? <i>NIST SP 800-18</i>								
12.1.9 Are there backup procedures? <i>NIST SP 800-18</i>								
12.2. Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? <i>OMB Circular A-130, III</i> <i>FISCAM SP-2.1</i> <i>NIST SP 800-18</i>								
12.2.2 Is there a contingency plan? <i>NIST SP 800-18</i>								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? <i>OMB A-130, III</i> <i>NIST SP 800-18</i>								
12.2.4 Are there risk assessment reports? <i>NIST SP 800-18</i>								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? <i>NIST SP 800-18</i>								

NOTES:

13. Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education <i>OMB Circular A-130, III</i>								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? <i>NIST SP 800-18</i>								
13.1.2 Are employee training and professional development documented and monitored? <i>FISCAM SP-4.2</i>								
13.1.3 Is there mandatory annual refresher training? <i>OMB Circular A-130, III</i>								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? <i>NIST SP 800-18</i>								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? <i>NIST SP 800-18</i>								

NOTES:

14. Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability <i>OMB Circular A-130, III</i> <i>FISCAM SP-3.4</i> <i>NIST 800-18</i>								
14.1. Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?								
14.1.1 Is a formal incident response capability available? <i>FISCAM SP-3.4</i> <i>NIST SP 800-18</i>								
14.1.2 Is there a process for reporting incidents? <i>FISCAM SP-3.4</i> <i>NIST SP 800-18</i>								
14.1.3 Are incidents monitored and tracked until resolved? <i>NIST SP 800-18</i>								
14.1.4 Are personnel trained to recognize and handle incidents? <i>FISCAM SP-3.4</i> <i>NIST SP 800-18</i>								
14.1.5 Are alerts/advisories received and responded to? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? <i>NIST SP 800-18</i>								
14.2. Critical Element: Is incident related information shared with appropriate organizations?								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? <i>OMB A-130, III NIST SP 800-18</i>								
14.2.2 Is incident information shared with FedCIRC ² concerning incidents and common vulnerabilities and threats? <i>OMB A-130, III GISRA</i>								
14.2.3 Is incident information reported to FedCIRC, NIPC ³ , and local law enforcement when necessary? <i>OMB A-130, III GISRA</i>								

² FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

³ NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

NOTES:

Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication <i>OMB Circular A-130, III</i> <i>FISCAM AC-2</i> <i>NIST SP 800-18</i>								
15.1. Critical Element: Are users individually authenticated via passwords, tokens, or other devices?								
15.1.1 Is a current list maintained and approved of authorized users and their access? <i>FISCAM AC-2</i> <i>NIST SP 800-18</i>								
15.1.2 Are digital signatures used and conform to FIPS 186-2? <i>NIST SP 800-18</i>								
15.1.3 Are access scripts with embedded passwords prohibited? <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.4 Is emergency and temporary access authorized? <i>FISCAM AC-2.2</i>								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? <i>FISCAM AC-3.2</i>								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.8 Are inactive user identifications disabled after a specified period of time? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.9 Are passwords not displayed when entered? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.10 Are there procedures in place for handling lost and compromised passwords? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.13 Are vendor-supplied passwords replaced immediately? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
15.2. Critical Element: Are access controls enforcing segregation of duties?								
15.2.1 Does the system correlate actions to users? <i>OMB A-130, III</i> <i>FISCAM SD-2.1</i>								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? <i>FISCAM AC-2.1</i>								

NOTES:

16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls <i>OMB Circular A-130, III</i> <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.1. Critical Element: Do the logical access controls restrict users to authorized transactions and functions?								
16.1.1 Can the security controls detect unauthorized access attempts? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.1.3 Is access to security software restricted to security administrators? <i>FISCAM AC-3.2</i>								
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.5 Are inactive users' accounts monitored and removed when not needed? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.1.7 If encryption is used, does it meet federal standards? <i>NIST SP 800-18</i>								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? <i>NIST SP 800-18</i>								
16.1.9 Is access restricted to files at the logical view or field? <i>FISCAM AC-3.2</i>								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? <i>FISCAM AC-4</i>								
16.2. Critical Element: Are there logical controls over network access?								
16.2.1 Has communication software been implemented to restrict access through specific terminals? <i>FISCAM AC-3.2</i>								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? <i>PSN Security Assessment Guidelines</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? <i>PSN Security Assessment Guidelines</i>								
16.2.4 Are there controls that restrict remote access to the system? <i>NIST SP 800-18</i>								
16.2.5 Are network activity logs maintained and reviewed? <i>FISCAM AC-3.2</i>								
16.2.6 Does the network connection automatically disconnect at the end of a session? <i>FISCAM AC-3.2</i>								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? <i>PSN Security Assessment Guidelines</i>								
16.2.8 Is dial-in access monitored? <i>FISCAM AC-3.2</i>								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? <i>FISCAM AC-3.2</i>								
16.2.10 Are firewalls or secure gateways installed? <i>NIST SP 800-18</i>								
16.2.11 If firewalls are installed do they comply with firewall policy and rules? <i>FISCAM AC-3.2</i>								
16.2.12 Are guest and anonymous accounts authorized and monitored? <i>PSN Security Assessment Guidelines</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.13 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? <i>FISCAM AC-3.2</i> <i>NIST SP 800-18</i>								
16.2.14 Are sensitive data transmissions encrypted? <i>FISCAM AC-3.2</i>								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? <i>FISCAM AC-3.2</i>								
16.3. Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?								
16.3.1 Is a privacy policy posted on the web site? <i>OMB-99-18</i>								

NOTES:

17. Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails <i>OMB Circular A-130, III</i> <i>FISCAM AC-4.1</i> <i>NIST SP 800-18</i>								
17.1. Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								
17.1.1 Does the audit trail provide a trace of user actions? <i>NIST SP 800-18</i>								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? <i>NIST SP 800-18</i>								
17.1.3 Is access to online audit logs strictly controlled? <i>NIST SP 800-18</i>								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? <i>NIST SP 800-18</i>								

Appendix D
References

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? <i>NIST SP 800-18</i>								
17.1.6 Are audit trails reviewed frequently? <i>NIST SP 800-18</i>								
17.1.7 Are automated tools used to review audit records in real time or near real time? <i>NIST SP 800-18</i>								
17.1.8 Is suspicious activity investigated and appropriate action taken? <i>FISCAM AC-4.3</i>								
17.1.9 Is keystroke monitoring used? If so, are users notified? <i>NIST SP 800-18</i>								

NOTES: