Master Document – Audit Program

Activity Code 11510	Information Technology General System Controls
Version 5.9, dated June 2012	
B-1 **Planning Considerations**	
Purpose and Scope	

The major objectives of this audit are to:
• Evaluate the adequacy of and the contractor's compliance with the information technology (IT) system general internal controls.
• Obtain a sufficient understanding of the contractor's IT system internal controls to plan related contract audit effort. This requires that the auditor assess the adequacy of the contractor's IT policies and procedures, whether they have been implemented, and if they are working and being monitored effectively.
• Document the understanding of the IT system general internal control in working papers and permanent files.
• Assess control risk as a basis to identify factors relevant to the design of substantive tests.
• Report on the understanding of the IT system general internal controls and assessment of control risk and the adequacy of the system for performing on Government contracts.
This audit is limited to the examination of the IT system general internal controls for major contractors, non-major contractors where the system is considered significant, and contractors with substantial firm-fixed price contracts. Only those controls directly related to the contractor's IT system and organization, as defined below, will be audited under this assignment. Controls for interrelated audit concerns regarding the adequacy of the contractor's other major systems (i.e., labor, estimating, etc.) will be audited under separate assignments. While the controls for these areas are not part of this audit, the results of all audits of these interrelated controls must be considered in forming an overall audit conclusion on the IT system general internal controls. The results of this audit should also be commented on in reports on related audit areas.
When performing an update or follow-up examination, the steps should be adjusted and tailored accordingly. To the extent possible, prior audit effort should be used as a basis for validating the contractor's internal control.
Before beginning this examination, the auditor should inquire about internal control evaluations performed by the contractor or its external auditors relating to this audit area. In those cases where internal control evaluations have been performed, the auditor should follow guidance contained in CAM 4-1000, Relying Upon the Work of Others.

Before performing any examination of internal controls, the auditor should determine that the system contemplated for examination is material to the Government. Once it is determined that the system is material to the Government, the auditor should reassess the materiality of each section in the internal control audit before performing any audit steps in that section. The scope of any audit depends on individual circumstances. The auditor is expected to exercise professional judgment, considering vulnerability and materiality, in deciding the scope of audit to be performed.

The internal control matrix (see Internal Control Matrix – IT System General Internal Controls) shows the interrelationships among the control objectives, example control activities, and audit procedures used in this audit program. The control objectives and the audit procedures have been fully integrated into this audit; therefore, the matrix is not needed unless it is desirable to see the associated example control activities and the interrelationships in a matrix format.

In cases where this examination covers internal control systems at multi-segment contractors, follow the guidance in CAM 5-103.2 and 5-110e. Auditing internal controls at multi-segment contractors requires effective coordination among cognizant auditors to identify the audit responsibilities at each location to ensure appropriate audit coverage when contractor locations share components of an internal control system, such as policies and procedures, common technologies (e.g., software) or common management. FAOs cognizant of segment locations should initiate assist audits from off-site locations as necessary. FAOs cognizant of off-site locations should not self-initiate audits of internal controls.

References
CAM 3-300, Internal Control Audit Planning Summary (ICAPS)
CAM 5-100, Obtaining an Understanding of a Contractor's Internal Controls and Assessing Control Risk
CAM 5-400, Audit of Information Technology Systems General Internal Controls
CAM 5-1400, Audit of Information Technology Systems Application Internal Controls
CAM 10-400, Audit Reports on Operations and Internal Control (System Audits)

B-1	**Preliminary Steps**	**W/P Reference**
Version 5.9, dated June 2012		
1.	**Research and Planning**	
	a. Review the open MRD's for guidance which may impact the audit and adjust the scope and procedures appropriately. Open MRDs can be identified using the link provided on the DCAA Intranet home page for "MRDs, AGMs, & AMGMs"	

b. Become familiar with CAM 5-400, the Information Systems and Auditing Knowledge Base contained on DCAA's intranet	
c. Perform the following steps using the permanent file, if applicable:	
(1) Review prior IT system audit working paper package.	
(2) Identify any IT system deficiency reports issued (review ICRS database, as applicable).	
(3) Determine if there are any reported deficiencies in the other internal control system audits that impact the scope of this IT general internal control system audit (review ICRS database, as applicable).	
(4) Identify the sources for the detailed policies, procedures, charts, etc., called for in steps (a) through (c) below. Document the sources of data by listing the data, its source, and any changes since the last system audit.	
(a) Contractor's written IT policies, procedures and IT system manual.	
(b) IT Organization charts depicting the functional areas responsible for developing and processing IT related data.	
(c) IT system architecture providing a pictorial overview of the IT infrastructure.	
(5) Review audit lead sheets.	
(6) Review other related audits, for example the impact of suspected irregular conduct (SIC) and CAS noncompliances, if applicable.	
(7) Consider the impact of the contractor's financial condition on the IT general internal control system by reviewing prior financial capability assessments or audits – (Activity Code 176XX).	
d. Hold a planning meeting with the audit team (e.g., RAM, Manager, Supervisor, Auditors) to discuss the risk of fraud and other noncompliances with applicable laws and regulations that could have a material effect on the assertion. The discussion should include relevant prior audit experience (e.g., questioned cost, relevant reported estimating or accounting system deficiencies), relevant aspects of the contractor's environment (e.g., the extent of incentives, pressures and opportunities to commit fraud and the propensity to rationalize misstatements), other known risk factors, and the audit team's understanding of relevant internal controls (see W/P B-2). The team should also review and discuss the general and other relevant sections of the IG Handbook on Fraud Indicators for Contractors as well as the	

relevant fraud indicators in CAM Figure 4-7-3. See "Principal Sources of Fraud Indicators" below. Based on the team discussion and other risk assessment procedures the team should document on W/P B, Section 4 the risk factors/indicators identified and design audit procedures to meet the audit objectives and provide reasonable assurance of detecting fraud and other noncompliances with applicable laws and regulations that could have a material effect on the proposal (i.e., tailor (add/delete/modify) the audit steps). GAGAS 6.13(a) Communication among audit team members about the risk of material misstatement due to fraud should continue as needed throughout the audit. Principle Sources of Fraud Indicators: • Handbook on Fraud Indicators for Contract Auditors, Sections I and III, (IGDH 7600.3, APO March 31, 1993) located at: h http://www.dodig.mil/PUBS/igdh7600.doc. • CAM Figure 4-7-3. (To access the fraud handbook, copy and paste the web address shown above into the address block in Internet Explorer.)	
e. Obtain from the contractor a schedule of total dollars processed through the IT system for the past twelve months (or most recently completed fiscal year) and summarize by total dollars and dollars by Government flexibly priced contracts and fixed price contracts in order to determine the materiality of the IT system. Complete the Materiality section of the ICAPS form at W/P A.	
f. Contact the contracting officer to ascertain any known concerns (including risk related to the contractor's financial condition) that will impact the audit and adjust the audit scope and procedures accordingly. If information regarding the contractor's financial condition is not available from the contracting officer, the auditor should perform the procedures addressed in CAM 2-302.1h. If during the course of the audit the auditor becomes aware of unfavorable or adverse financial conditions, they should immediately communicate their concerns to the contracting officer, and appropriately adjust the scope of audit.	
g. Electronically transmit an acknowledgement/notification to the ACO/Buying Command notifying them of the commencement of the risk assessment and that the expected completion date will be provided in the formal acknowledgement/notification once the risk assessment is complete. (CAM 2-303). The acknowledgement/notification process should be within the	

timeframe and in accordance with the procedures in CAM 4-104.	
h. FAOs that have cognizance of contractors with significant classified contracts should coordinate with the Field Detachment to determine the DCAA office responsible for reviewing costs on classified contracts. This coordination should be documented in the W/Ps. FAOs should also coordinate with the Field Detachment on any significant IT system issues.	
i. Close coordination is required at FAOs cognizant of a shared services location and the FAOs cognizant of the segments serviced by the shared services. Document the objectives and procedures to be performed at the shared services location and the segment level. Request assist audits, as applicable.	
j. Determine the extent and results of the contractor's self-governance activities, internal and external audits, and coordinated audits related to the IT General Internal Control system.	
(1) Request the contractor provide a list of completed internal and external audits and determine if any are related to the IT system.	
(2) If applicable, coordinate with the CAC or corporate office auditors to determine if any internal control weaknesses that might impact the IT system were identified in management's internal control report or the independent auditor's attestation on management's assertion included in the annual report filed with the SEC.	
k. The assistance of IT specialists may be required to adequately perform this examination. Determine the need for technical assistance, if any, and document your consideration on W/P B-3. Auditors should contact their regional offices to obtain the necessary expertise.	
2. Entrance Conference and Preparation	
a. Prepare a written memorandum to the contractor requesting an entrance conference covering the areas highlighted in CAM 4-302 and any specific data or pertinent information not yet provided. More specifically, request information related to the following IT control areas. Request the contractor's response during, or preferably prior to, the entrance conference.	
(1) Independent Management Reviews.	
(2) Organizational Structure.	

(3) Software Acquisition Development and Modification.	
(4) Computer Operations.	
(5) Security (Physical & Logical).	
(6) Contingency Plans/Disaster Recovery.	
b. Conduct an entrance conference as outlined in CAM 4-302, with particular emphasis on:	
(1) Requesting the contractor to provide a system orientation briefing or a demonstration of physical and logical controls incorporated within each of the functional areas that comprise the IT organization and applicable user groups.	
(2) Determining any changes implemented in the IT system general internal control environment.	
(3) Obtain documentation on the contractor's risk assessment process. (The documentation will be evaluated under Contractor Risk Assessment, Section D-1.)	
(4) Obtain documentation on the contractor's monitoring process that ensure established manual and computerized controls are functioning as intended. (The documentation will be evaluated under Monitoring, Section F-1.)	
(5) Discussing any identified weaknesses which may have been previously reported and related follow-up actions.	
3. Initial Risk Assessment	
Using the framework and the guidelines in WP B-2, obtain and document an understanding of the contractor's internal controls that are relevant to the audit. With the proper planning auditors should be able to obtain and document a major portion of this understanding during a walk-through of the contractor's assertion.	

C-1	Control Environment	W/P Reference
Version 5.9, dated June 2012		
The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The		

auditor should obtain a sufficient understanding of the control environment to determine the impact that it may have on the overall effectiveness of IT system general internal controls.	
1. Evaluate the most recently completed ICAPS for the Control Environment and Overall Accounting Controls (Activity Code 11070), if the audit was completed within the cycle time. (See CAM 5-103.1.a.) Consider the rationale behind any moderate or high risk assessment ratings and determine the potential impact, if any, on the effectiveness of the IT general internal controls.	
2. If an examination of the control environment has not been performed or has not been completed within the required cycle time (CAM 5-103.1.a.), evaluate all documented prior audit experience with the contractor, including permanent files, relevant audit reports and working papers, suspected irregular conduct (SIC) referrals and discussions with prior auditors. Obtain an understanding of the following factors:	
a. Integrity and ethical values.	
b. Commitment to competence.	
c. Board of directors and/or audit committee participation.	
d. Management's philosophy and operating style.	
e. Organizational structure.	
f. Assignment of authority and responsibility.	
g. Human resource policies and procedures.	
h. Financial capability.	
3. Document your overall understanding of the control environment and the impact that it has on the nature and extent of testing of each control objective (W/Ps G, H, I, J, K, L, and M).	

D-1	Contractor Risk Assessment	W/P Reference
Version 5.9, dated June 2012		
The auditor should develop a sufficient understanding of the risk assessment process currently employed by the contractor in terms of its identification, analysis, and management of risks relevant to the IT organization.		
1. Meet with responsible personnel to obtain an overview of the various risk factors considered by management.		

2. Once the various risk factors are identified, obtain an understanding of how management identifies the risks, estimates the significance of risks, assesses the likelihood of their occurrence, and relates them to contract reporting.	
3. If applicable, obtain an overview of any plans, programs, or actions management may initiate to address specific risks. Keep in mind that, depending on the nature of specific risks, management may elect to accept a given risk due to costs or other considerations.	
4. Document your overall understanding of the contractor's risk assessment practices and the impact that it has on the nature and extent of testing of each control objective (W/Ps G, H, I, J, K, L, and M).	

E-1	Information and Communication	W/P Reference
Version 5.9, dated June 2012		
Information and communication processes consist of the methods and records established to record, process, summarize, and report contract cost data. The auditor should develop a sufficient understanding of the contractor's information and communication processes (relevant to contract cost data) to identify significant classes of transactions and how they are initiated, processed, controlled, and reported.		
1. Since the accounting system is an integral component of information and communication processes, evaluate the most recently completed ICAPS for the Control Environment and Overall Accounting Controls for the rationale behind any moderate or high risk assessment ratings in any accounting application area. Determine the potential impact, if any, on the effectiveness of the contractor's IT system general internal controls.	
2. Evaluate relevant permanent files, prior audit working papers, and any prior contractor demonstrations of the functional areas that makeup the Information Technology organization.	
3. Determine if the contractor has made changes within its IT organization since the last demonstration. Evaluate the changes. If no prior systems demonstration was performed, have the contractor provide one. Contractor representatives providing the demonstration should possess a detailed knowledge of the IT organization and related internal controls. The demonstration provides the auditor an opportunity to query contractor personnel regarding internal controls and how they are monitored. The auditor should ensure that the demonstration addresses the control objectives outlined in CAM 5-400.	

4. Document your confirmed understanding of the contractor's IT organization and obtain a written confirmation from the contractor indicating its agreement with this understanding. This documentation will typically take the form of system flowcharts or narrative descriptions and can be prepared by the auditor or consist of documentation prepared by the contractor (see CAM 5-106). Based on your understanding of the contractor's IT system processes, document the impact that it will have on the nature and extent of testing of each control objective (W/Ps G, H, I, J, K, L, and M).	

F-1	Monitoring	W/P Reference
Version 5.9, dated June 2012		
Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. The auditor should develop a sufficient understanding of the contractor's ongoing monitoring activities and/or separate evaluations related to general internal controls within the IT organization and applicable user groups.		
1. Determine if ongoing monitoring procedures are incorporated into the normal recurring activities of the contractor's organization. These procedures should include regular management and supervisory activities.		
2. Where applicable, determine the extent of internal audit involvement in performing monitoring functions through separate evaluations.		
3. Determine and document the extent of monitoring activities being performed by external parties.		
4. In those cases where internal or external audits have been performed, the auditor should follow the guidance contained in CAM 4-1000, Relying Upon the Work of Others.		
5. Document your overall understanding of the monitoring activity being performed at the contractor's location and the impact it will have on the nature and extent of testing of each of the control objectives (W/Ps G, H, I, J, K, L, and M).		

G-1	Independent Management Review	W/P Reference
Version 5.9, dated June 2012		

The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.	
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment • Information and communications • Monitoring	
2. Verify that periodic reviews of contractor's policies and procedures are conducted to ensure that:	
a. Policies and procedures have been implemented and are working effectively (refer to CAM 5-407 for additional guidance).	
b. Follow-up actions are taken on recommendations resulting from management reviews.	
3. Evaluate the contractor's record of completed internal audits and its current internal audit plan to determine if the IT General Internal Control system is being subjected to periodic reviews in accordance with established policies and procedures.	
4. Identify and selectively evaluate documentary evidence and the frequency of the contractor's management reviews to determine whether the scope of such reviews are appropriate, the conclusions sound, and appropriate follow-up actions were taken.	
5. Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can	

rely on the work performed (see CAM 4-1000).	

H-1	Organizational Structure	W/P Reference
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.		
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment • Information and communications • Monitoring		
2. Duties and responsibilities should be adequately segregated so that no one person can perpetrate and conceal material errors or misstatements (refer to CAM 5-408 for additional guidance). The following audit procedures are designed to gain an understanding of the contractor's control activities (policies and procedures) for the subject control objective. Refer to the Internal Control Matrixes (ICMs) to view the control objective, its associated control activities, and audit procedures in a matrix format. In determining the steps needed to obtain a sufficient understanding of the contractor's control activities, the auditor should utilize knowledge obtained in understanding the other components of the internal control (control environment, contractor risk assessment, information and communications, and monitoring).		

3. Document the existence of a functional IT organization with defined organizational responsibilities.	
4. Evaluate organization structure to determine if the IT department reports at a high enough level to allow it to act independently.	
5. Evaluate organization charts, position descriptions, etc. to determine if they provide for adequate segregation of duties and responsibilities within the information systems department.	
6. Interview selected contractor employees to determine whether duties and responsibilities are performed as established in organization charts, position descriptions, etc.	
7. Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

I-1	Computer Operations	W/P Reference
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.		
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment	

• Information and communications • Monitoring	
2. Computer operations should ensure the integrity and reliability of all activities impacting the physical operation of the computer. Such activities include: system initiation, operator interaction, help desk assistance, print operations, etc. (refer to CAM 5-410 for additional guidance).	
3. Obtain a written description of the overall work flow process in the IT organization.	
4. Obtain and evaluate the contractor's IT operations policies and procedures to determine if they provide for an environment in which:	
a. System descriptions are maintained.	
b. Critical processes are controlled.	
c. Audit trails are maintained (manual/computerized logs).	
d. Backup/recovery procedures are maintained.	
e. Communications are checked/safeguarded.	
5. Test a current major application system (consider using the system selected in "Software Acquisition, Development, and Modification"), to determine:	
a. System descriptions including technical points of contact, responsible manager, and recovery procedures are available.	
b. Guidelines exist which cover critical processes that change/ modify sensitive data residing in files, databases, etc. Guidelines should include authorized procedures, personnel, and time frames.	
c. Manual and computerized logs (audit trails) of application processing, system accesses, and computer performance are maintained.	
d. Scheduled hardware maintenance and backup/recovery procedures are defined.	
e. Communication checks/safeguards over data transmitted via wide-area networks (WANs), local area networks (LANs), high-speed inter-mainframe connections, workstation-mainframe connectivity, satellite links, etc. are established.	
6. Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

J-1	Logical Security	W/P Reference
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.		
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment • Information and communications • Monitoring	
2. Access to computing resources should be limited to those individuals with a documented and authorized need for such access. Layers of logical security should be provided to protect computing resources against unauthorized use, modification, damage, or loss (refer to CAM 5-411 for additional guidance).	
3. Test the contractor's logical security policies and procedures for all operating environments (e.g., batch, interactive, and database) to determine if they are adequate to provide for a logically secure environment in which:	
a. User access levels are controlled.	
b. Security software is used.	

c. Security software levels are properly implemented.	
d. Logical access restrictions are controlled by passwords and computerized rules.	
e. Logical access is recorded and monitored.	
4. Evaluate the contractor's implementation of logical security controls for all operating environments to determine if:	
a. User access levels are identified and documented.	
b. Security software is used to control access to computer resources.	
(1) Determine the type of information security software installed on major computer systems.	
(2) Gain a general understanding of the software package(s).	
c. Security software access levels have been properly implemented based on demonstrated need.	
(1) Determine who the contractor has given special system privileges to, such as those that:	
(a) are used to define user and group access authorities	
(b) permit full system access	
(c) are used to monitor system access and access violations	
(2) Determine that the information security software covers all major application areas.	
(3) Obtain a listing of all user/group security authorities for an audit selected critical application.	
(4) Trace a sample of the user/group authorities for the audit selected critical application to specific persons/groups and determine if the authority is reasonable and justifiable.	
(5) Ensure that the systems and application programmers do not have access to production programs and data.	
d. User IDs, passwords, and computerized rules are established and controlled. Determine if:	
(1) IT personnel, when terminated or separated for any reason, are promptly removed from the IT organization spaces in order to safeguard the computer facilities and data files.	
(2) Passwords or other control devices used to access computing resources are changed immediately upon the termination or transfer of the individual employee to whom they are related.	

	(3) Passwords issued by the IT organization are at least 8 characters in length, cannot be easily guessed, and do not contain repeating characters.	
	(4) Passwords are changed periodically and cannot be reused by the same individual.	
	(5) Passwords are not displayed during the logon process, are not printed on output, and are stored by data processing operations in an encrypted file.	
	(6) Users are logged-off automatically if they have not been active for a specific length of time.	
e.	Computer access is recorded and monitored.	
	(1) Determine whether or not the contractor makes use of logs to detect unauthorized accesses to production data. Verify that they evaluate these logs within reasonable timeframes and follow-up on unauthorized access attempts.	
	(2) Interview personnel responsible for information security to determine procedures for monitoring and following up on improper access attempts.	
	(3) Select a sample of improper access attempt reports and follow up on the actions taken by the information security function for reported violations.	
f.	Training is conducted on security procedures and awareness.	
g.	Violation and security activity reports are evaluated regularly to identify and resolve incidents involving unauthorized activity.	
5.	Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

K-1	**Physical Security**	**W/P Reference**
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may		

have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.	
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment • Information and communications • Monitoring	
2. Access to computing resources should be limited to those individuals with a documented and authorized need for such access. Layers of physical security should be provided to protect computing resources against unauthorized use, modification, damage, or loss (refer to CAM 5-411 for additional guidance).	
3. Evaluate the contractor's physical security policies and procedures to determine if they are adequate to provide for a physically secure environment in which:	
a. Facility security is maintained.	
b. User access is authorized and controlled.	
c. Visitor access is controlled.	
d. Terminated employees access is revoked.	
e. Inventory and accountability records are maintained.	
f. Sensitive data, software, and documentation is identified and protected.	
g. On-site and off-site storage is maintained.	
h. Environmental protection is maintained.	
4. Evaluate the contractor's implementation of physical security controls to determine if:	
a. Entrances to computer facilities are secured (i.e., keys, badges, cipher locks, etc.).	

b.	Authorization of individuals with access to computer resources is controlled and documented.	
c.	Visitors are escorted within the computer facility.	
d.	Access for employees who quit or are terminated are revoked in a timely manner.	
e.	Inventory and accountability records are maintained for data files and tapes.	
f.	Sensitive data files, programs and documentation have been identified.	
g.	On-site and off-site storage facilities exist.	
h.	Environment is protected against fire, excess humidity, temperature variations, and other environmental hazards.	
5.	Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

L-1	Software Acquisition, Development and Modification	W/P Reference
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.		
1. In planning the following audit procedures to understand the contractor's control activities, the auditor should recognize the other components of internal control and their impact on the nature and extent of testing to be performed. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows:		

• Control environment	
• Contractor risk assessment	
• Information and communications	
• Monitoring	
2. System and application software should be consistent with management objectives, operate within specifications, tested prior to implementation, and not susceptible to unauthorized modification (refer to CAM 5-409 for additional guidance).	
3. Evaluate the contractor's software acquisition, development, and modification policies and procedures to determine if they provide for a standard development methodology including the following controls:	
a. Definition of Requirements.	
b. Participation of Appropriate Personnel.	
c. Software Documentation.	
d. Validation, Verification and Testing.	
e. Final Management Approval.	
4. If the risk assessment indicates that further audit effort is necessary, evaluate at least one recent major software acquisition, development, or modernization project to determine if:	
a. Written requirements/specifications were reviewed and approved by applicable users and management.	
b. Appropriate IT user and management personnel participated throughout all phases of software acquisition, development, and modification.	
c. All software programs including purchased software and modifications to existing software are documented.	
d. Validation, verification, and testing was performed by management, users, and IT personnel to determine that software operates in conformity with design specifications and meets user requirements.	
e. Final written approval from management, users, and IT personnel was obtained prior to implementation.	
5. Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

M-1	Contingency Plans	W/P Reference
Version 5.9, dated June 2012		
The auditor should obtain an understanding of the contractor's control activities over the functional elements that makeup the IT organization. Control activities are the policies and procedures that help to ensure the organization's control objectives are met. A detailed understanding of the control activities is essential to the assessment of control risk. The IT organization's primary control objectives, as they relate to U.S. Government contracts, examples of control activities the contractor may have implemented to achieve the control objectives, are provided in the Internal Control Matrix – IT System General Internal Controls (see W/P 31). The audit procedures for this control objective are also included in the internal control matrix. If the auditor determines that relevant internal control activities do not exist, or that the effort to perform tests is not justified, no control testing need be performed, and control risk will be assessed as high.		
1. In performing the following audit procedures to understand the contractor's control activities, the auditor should recognize that while obtaining an understanding of the other components of internal control, he/she is also likely to have obtained some level of knowledge about control activities. The auditor should utilize this knowledge in determining the additional time needed to obtain a sufficient understanding of the contractor's control activities. Document the impact of the internal control components on the nature and extent of testing on this control objective. Internal control components are as follows: • Control environment • Contractor risk assessment • Information and communications • Monitoring	
2. Contingency plans should be established to provide for continuance of information processing following a major hardware or software failure (refer to CAM 5-412 for additional guidance). The following audit procedures are designed to gain an understanding of the contractor's control activities (policies and procedures) for the subject control objective. Refer to the Internal Control Matrixes (ICMs) to view the control objective, its associated control activities, and audit procedures in a matrix format. In determining the steps needed to obtain a sufficient understanding of the contractor's control activities, the auditor should utilize knowledge obtained in understanding the other components of the internal control (control environment, contractor	

risk assessment, information and communications, and monitoring).	
3. Evaluate the contractor's policies and procedures to determine if they are adequate to provide for processing of critical application systems in the event of a major hardware or software failure. Contingency plans should require:	
a. Identification of critical applications and data files.	
b. Provisions for a backup computer system.	
c. Off-site storage of critical application programs, data and contingency plans.	
d. Tests of contingency plans.	
4. Evaluate the contingency plan and test documentation to determine if established policies and procedures were followed with emphasis in the following areas:	
a. Critical and sensitive applications and data files were identified.	
b. A backup computer site was identified with sufficient systems hardware and software available to commence alternative computer center operations in a timely manner.	
c. Copies of the contingency plan, software documentation, and critical user data are pre-positioned off-site.	
d. Any deficiencies identified during testing were documented and resolved.	
5. Determine the extent of compliance with the Contractor Records Retention requirements as defined in FAR – Part 4, Subpart 4.7.	
6. Identify any reviews which may have an impact on this examination, and evaluate the reports and supporting working papers to determine if any system deficiencies were noted, and the extent to which we can rely on the work performed (see CAM 4-1000).	

A-1	Concluding Steps	W/P Reference
Version 5.9, dated June 2012		
1. **Assessment of Control Risk**		
a. Considering all five components of internal control (control environment, contractor risk assessment, information and communications, monitoring, and control activities) that relate to control objectives, assess control risk for each of the relevant control objectives (independent management review, organizational structure, computer operations, logical security,	

physical security, software acquisition/development/modification, and contingency plans). For each of the objectives, summarize the characteristics which support the assessed level of control risk and specifically identify any internal control weaknesses or system deficiencies.	
b. Determine if the IT system is adequate to reasonably assure proper pricing, administration, and settlement of Government contracts in accordance with applicable laws and regulations.	
c. Based on the assessments above, determine the impact on the scope of other audits.	
d. Complete the ICAPS form at W/P A (see CAM 3-305)	
e. Coordinate the results of audit with the supervisor. The supervisor and the FAO manager should review and initial the ICAPS form at W/P A before the exit conference is performed. If it is determined that additional audit steps are needed, any additional planned audit effort should be accomplished as part of this examination or immediately thereafter. Any delays in completion of this audit effort should be documented and approved by management.	
2. **Summary Steps**	
a. Prepare a draft audit report in accordance with CAM 10-400. If applicable, prepare a separate CAS noncompliance report.	
b. Conduct an exit conference with the contractor in accordance with CAM 4-304.	
c. Finalize the audit report incorporating the contractor's response and audit rejoinder.	
d. If the contractor has EVMS covered contracts, provide comments in the audit report on whether any findings are likely to impact the contractor's EVMS (CAM 10-1204.5b). Discuss findings and recommendations relating to the EVMS with the Contract Administration Office EVMS Monitor prior to issuance of the report. Immediately evaluate the impact of these findings on specific EVMS covered contracts and provide the details in flash EVMS surveillance reports (CAM 11-203.5.b).	
e. Update the permanent file in accordance with CAM 4-405.b (MAAR 3). Retain a copy of the approved W/P A ICAPS form. After the audit report is issued, update the ICRS database using the information on the approved W/P A ICAPS form and file the approved W/P A ICAPS form in the Electronic Contractor Permanent File (ECPF). (The control risk assessment (Section II) and overall system opinion (Section III) in the ICAPS may not be	

updated until the system report supporting the change is issued (CAM 3-306a).)	