

**Master Document – Audit Program**

<b>Activity Code 11510</b>	<b>IT System General Internal Controls</b>
<b>Version 3.0, dated April 2004</b>	
<b>B-1</b>	<b>Planning Considerations</b>
<b>Purpose and Scope</b>	
The major objectives of this audit are to:	
<ul style="list-style-type: none"> <li>• Obtain a sufficient understanding of the contractor’s information technology (IT) system internal control 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 effectively.</li> </ul>	
<ul style="list-style-type: none"> <li>• Document the understanding of the IT System general internal control in working papers and permanent files.</li> </ul>	
<ul style="list-style-type: none"> <li>• Test the operational effectiveness of IT System general internal controls.</li> </ul>	
<ul style="list-style-type: none"> <li>• Assess control risk as a basis to identify factors relevant to the design of substantive tests.</li> </ul>	
<ul style="list-style-type: none"> <li>• Report on the understanding of the IT System general internal control and assessment of control risk.</li> </ul>	
<p>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 negotiated firm-fixed price contracts. Only those controls directly related to the contractor's Information Technology (IT) organization, 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 control. The results of this audit should also be commented on in reports on related audit areas.</p>	
<p>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.</p>	
<p>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.</p>	
<p>The internal control matrix shows the interrelationships among the control objectives, control</p>	

**Master Document – Audit Program**

activities, and audit procedures used in this audit. 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 control activities and the interrelationships in a matrix format.

<b>B-1</b>	<b>Preliminary Steps</b>			<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>				
<b>1. Research and Planning</b>				
a. Become familiar with CAM 5-400 and the Information Systems (IS) Auditing Knowledge Base that is contained on DCAA’s Intranet and any recent Headquarters guidance not incorporated in the CAM.				
b. The assistance of IT specialists may be required to adequately perform this examination. In these cases, auditors should contact their regional offices to obtain the necessary expertise.				
c. Determine the extent and results of the contractor's self-governance activities; e.g., internal and external audits, coordinated audits, etc., related to IT organization. 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. Document your evaluation.				
d. Evaluate the permanent file for:				
(1) Existence of contractor IT policies and procedures.				
(2) Organization charts depicting the various functional elements within the IT organization.				
(3) Contractor furnished documentation that may provide information relative to the adequacy of general internal controls.				
(4) Listings of current Government contracts.				
(5) Previous system audits performed. Check if the system is applicable, and if applicable, determine if it is relevant to the current system audit:				
	<b>System</b>	<b>Applicable?</b>	<b>Relevant?</b>	
	Accounting			
	Billing			
	Budget (Planning)			

**Master Document – Audit Program**

	Compensation			
	IT			
	Estimating			
	Indirect/ODC			
	Labor			
	Material			
	Purchasing			
(6) Audit lead sheets.				
(7) The analysis of the control environment and the results of any other audits, for internal control weaknesses that may impact this examination.				
e. Discuss the planned examination of the IT System general internal controls with the administrative contracting officer and, if appropriate, other customers to identify, understand, and document any concerns they may have and to identify any areas which may require substantive evaluation.				
f. In planning and performing the examination, consider the fraud risk indicators specific to the audit. The principal sources for the applicable fraud risk indicators are:				
<ul style="list-style-type: none"> <li>• Handbook on Fraud Indicators for Contract Auditors, Section II. (IGDH 7600.3, APO March 31 1993) located at <a href="http://www.dodig.osd.mil/PUBS/index.html">www.dodig.osd.mil/PUBS/index.html</a>, and</li> </ul>				
<ul style="list-style-type: none"> <li>• CAM 4-700 and CAM Figure 4-7-3.</li> </ul>				
Document in working paper B any identified fraud risk indicators and your response/actions to the identified risks (either individually, or in combination). This should be done at the planning stage of the audit as well as during the audit if risk indicators are disclosed. If no risk indicators are identified, document this in working paper B.				
<b>2. Entrance Conference and Preparation</b>				
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.				

**Master Document – Audit Program**

(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 demonstration of physical and logical controls incorporated within each of the functional areas that comprise the IT organization and applicable user groups.	
(2) Any changes implemented in the IT System general internal control environment, which enhance its effectiveness.	
(3) The contractor’s monitoring process to ensure that established manual and computerized controls are functioning as intended.	
(4) Any identified weaknesses which may have been reported and related follow-up actions taken.	
<b>3. Other Preliminary Steps</b>	
Perform a high level cursory assessment to determine if the following exist:	
(1) A functional organization with defined organizational responsibilities.	
(2) A written description of the overall work flow process in the IT organization.	
(3) Policies and procedures for effectively controlling the IT operations.	
<b>4. Initial Risk Assessment</b>	
Using the information obtained in steps 1, 2, and 3, prepare an initial risk assessment to determine the scope of the examination (W/P B).	

**Master Document – Audit Program**

<b>C-1</b>	<b>Control Environment</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
<p>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.</p>		
<p>1. Obtain a copy of the most recently completed ICAPS for the Control Environment and Overall Accounting Controls. 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.</p>		
<p>2. If an examination of the control environment has not been recently performed, 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:</p>		
<p>a. Integrity and ethical values.</p>		
<p>b. Commitment to competence.</p>		
<p>c. Board of directors and/or audit committee participation.</p>		
<p>d. Management’s philosophy and operating style.</p>		
<p>e. Organizational structure.</p>		
<p>f. Assignment of authority and responsibility.</p>		
<p>g. Human resource policies and procedures.</p>		
<p>3. Document the overall assessment of the contractor control environment and the impact that it will have on the examination of IT System general internal controls.</p>		

<b>D-1</b>	<b>Contractor Risk Assessment</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
<p>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</p>		

**Master Document – Audit Program**

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.	

<b>E-1</b>	<b>Information and Communication</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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, obtain a copy of the most recently completed Internal Control Audit Planning Summary (ICAPS) for the Control Environment and Overall Accounting Controls. Consider 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. Document your assessment.		
2. Evaluate relevant permanent files, prior audit working papers, and any prior contractor demonstrations of the functional areas that makeup the Information Technology organization. Document your evaluation.		
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		

**Master Document – Audit Program**

and how they are monitored. The auditor should ensure that the demonstration addresses the control activities 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 their agreement with this understanding.	

<b>F-1</b>	<b>Monitoring</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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. Document your overall understanding of the monitoring activity being performed at the contractor’s location and determine the impact it will have on our examination of the IT organization.		

<b>G-1</b>	<b>Independent Management Review</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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. The IT organization’s primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.		

**Master Document – Audit Program**

<p>The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).</p>	
<p>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 (control environment, contractor risk assessment, information and communications, and monitoring), 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.</p>	
<p>Management should perform periodic independent reviews (including internal and external audits) of the IT operations to ensure that policies and procedures have been implemented and are working effectively (refer to CAM 5-407 for additional guidance).</p>	
<p>1. Evaluate the contractor's policies and procedures, internal review schedules, etc. to determine if they provide for the periodic independent review of IT operations and follow-up on identified deficiencies.</p>	
<p>2. Evaluate recent independent review activity to determine if established schedules are being followed.</p>	
<p>3. Selectively evaluate working papers of internal audits and other contractor or external auditor related reviews to determine the extent to which we can rely on these reviews of IT operations (see CAM 4-1000).</p>	
<p>4. Selectively evaluate identified deficiencies, if applicable, to determine if follow-up was performed in accordance with established policies and procedures.</p>	

<b>H-1</b>	<b>Organizational Structure</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
<p>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. The IT organization’s primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.</p>		

**Master Document – Audit Program**

<p>The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).</p>	
<p>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 (control environment, contractor risk assessment, information and communications, and monitoring), 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. 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 (control environment, contractor risk assessment, information and communications, and monitoring), 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</p>	
<p>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).</p>	
<p>1. Evaluate organization structure to determine if the IT Department reports at a high enough level to allow it to act independently.</p>	
<p>2. Evaluate organization charts, position descriptions, etc. to determine if they provide for adequate segregation of duties and responsibilities within the information systems department.</p>	
<p>3. Interview selected contractor employees to determine whether duties and responsibilities are performed as established in organization charts, position descriptions, etc.</p>	

**Master Document – Audit Program**

I-1	Computer Operations	WP Reference
<b>Version 3.0, dated April 2004</b>		
<p>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. The IT organization's primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.</p>		
<p>The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).</p>		
<p>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 (control environment, contractor risk assessment, information and communications, and monitoring), 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.</p>		
<p>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).</p>		
<p>1. Evaluate the contractor's computer operations policies and procedures to determine if they provide for an environment in which:</p>		
<p>a. System descriptions are maintained.</p>		
<p>b. Critical processes are controlled.</p>		
<p>c. Audit trails are maintained (manual/computerized logs).</p>		
<p>d. Backup/recovery procedures are maintained.</p>		
<p>e. Communications are checked/ safeguarded.</p>		
<p>2. Test a current major application system (consider using the system selected in "Software Acquisition, Development, and Modification"), to determine:</p>		
<p>a. System descriptions including technical points of contact, responsible manager, and recovery procedures are available.</p>		
<p>b. Guidelines exist which cover critical processes that change/ modify sensitive data residing in files, databases, etc. Guidelines</p>		

**Master Document – Audit Program**

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.	

<b>J-1</b>	<b>Logical Security</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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. The IT organization's primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.		
The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).		
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 (control environment, contractor risk assessment, information and communications, and monitoring), 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		
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).		
1. 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		

## Master Document – Audit Program

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.	
2. 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	

**Master Document – Audit Program**

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.	

<b>K-1</b>	<b>Physical Security</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
<p>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. The IT organization's primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.</p>		

## Master Document – Audit Program

<p>The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).</p>	
<p>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 (control environment, contractor risk assessment, information and communications, and monitoring), 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.</p>	
<p>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).</p>	
<p>1. Evaluate the contractor's physical security policies and procedures to determine if they are adequate to provide for a physically secure environment in which:</p>	
<p>a. Facility security is maintained.</p>	
<p>b. User access is authorized and controlled.</p>	
<p>c. Visitor access is controlled.</p>	
<p>d. Terminated employees access is revoked.</p>	
<p>e. Inventory and accountability records are maintained.</p>	
<p>f. Sensitive data, software, and documentation is identified and protected.</p>	
<p>g. On-site and off-site storage is maintained.</p>	
<p>h. Environmental protection is maintained.</p>	
<p>2. Evaluate the contractor's implementation of physical security controls to determine if:</p>	
<p>a. Entrances to computer facilities are secured (Keys, badges, cipher locks, etc.).</p>	
<p>b. Authorization of individuals with access to computer resources is controlled and documented.</p>	
<p>c. Visitors are escorted within the computer facility.</p>	
<p>d. Access for employees who quit or are terminated are revoked in a timely manner.</p>	
<p>e. Inventory and accountability records are maintained for data files</p>	

**Master Document – Audit Program**

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.	

<b>L-1</b>	<b>Software Acquisition, Development and Modification</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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. The IT organization's primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.		
The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).		
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 (control environment, contractor risk assessment, information and communications, and monitoring), 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.		
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).		
1. 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.		

**Master Document – Audit Program**

d. Validation, Verification and Testing.	
e. Final Management Approval.	
2. 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.	

<b>M-1</b>	<b>Contingency Plans</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		
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. The IT organization's primary control objectives and examples of control activities, as they relate to U.S. Government contracts, are provided in the Internal Control Matrix (ICM-ITG). The audit procedures associated with section G, H, I, J, K, L and M (control objective), are also included in the matrix.		
The auditor should evaluate contractor internal and/or external audits to determine if any control activities have already been evaluated and if reliance can be placed on such evaluations (see CAM 4-1000).		
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 (control environment, contractor risk assessment, information and communications, and monitoring), 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		

**Master Document – Audit Program**

a sufficient understanding of the contractor’s control activities.	
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).	
1. 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 contingency plans.	
d. Tests of contingency plans.	
2. 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.	
3. Determine the extent of compliance with the Contractor Records Retention requirements as defined in FAR – Part 4, Subpart 4.7.	

<b>A-1</b>	<b>Concluding Steps</b>	<b>WP Reference</b>
<b>Version 3.0, dated April 2004</b>		

**Master Document – Audit Program**

<b>1. Assessment Of Control Risk</b>	
a. Considering all five components of internal control, assess control risk for each of the relevant control objectives. 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 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. Update the Internal Control Audit Planning Summary (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 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.	
<b>2. Summary Steps</b>	
a. Prepare a draft audit report in accordance with CAM 10-400.	
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 11-209.2.e).	
e. Update the permanent file in accordance with CAM 4-405.1.b (MAAR #3).	

**Master Document – Audit Program**

<b>3. Closing Actions</b>	
<p>Closing actions should be performed in accordance with FAO procedures. These procedures may require either auditors or administrative personnel to perform various closing steps. Completion of these closing actions should be documented (e.g., by initials and date on the CD or working paper folder, etc.) and should include:</p>	
<p>a. The title, author, and keywords fields of the file properties in the audit report must be completed (for the audit report only) prior to final filing.</p>	
<p>b. Review the APPS exe file for size. APPS-generated executable files that are over 10 megabytes in size should be reviewed to ensure that the format and content justify the size. Supervisors are responsible for reviewing or designating someone to review these files for content and format.</p>	
<p>c. Review the APPS exe file for temporary files. These files can be recognized by the “~\$” or “~WRL” at the beginning of the file name. Once the APPS exe file is complete and there is NO ACTIVITY to be completed on any of the files contained within the exe file, any temporary files should be deleted so there are no unintentional versions of working papers and/or reports. NOTE: This should be done prior to invoking the Export/Archive Option in APPS.</p>	
<p>d. Once an audit report is signed, the electronic document should immediately be modified to indicate who signed it, and it should be password protected. The electronic file should then be renamed according to the convention “01 DCAA Report [RORG-ASSIGNMENT NO.] – Final.doc” and changed to a read-only file. Only this file should be stored, transmitted, or otherwise used for official purposes. For Memorandums the word “Report” would be replaced by “MFF” or “MFR” in the naming convention as appropriate.</p>	
<p>e. When the audit report is transmitted electronically to the requestor, the transmission email should be saved as a txt file (this will ensure the attachments are not saved again). Saving delivery or read receipts is optional. If saved, the naming convention should distinguish them from transmittal emails.</p>	
<p>f. Once the report is signed, the signature page of the audit report must be scanned in accordance with Agency standard scanning instructions. For audit packages, the scanned signature page file should be named the same as the audit report (see above) with</p>	

**Master Document – Audit Program**

<p>“-sig” added (i.e., 01 DCAA Report 01101-2002X10100389-Final-sig.pdf). There is no requirement to make the file a part of the APPS generated executable file and it must be included separately in the iRIMS folder. There is no need to scan the signature page of a Memorandum unless it is distributed outside of DCAA.</p>	
<p>g. Ensure an electronic copy of the final draft audit report containing the supervisory auditor’s initials and date, cross-referenced to the working papers, is included in the working paper package. The final draft report should include all substantive changes made to the original draft, with cross-referencing updated as necessary. It should differ from the final report only due to minor administrative changes (spelling, format, etc.) made during final processing.</p>	
<p>h. Ensure all working paper files are "read only" and, if necessary, compressed for final storage. Generally, current Agency software should be used to automatically modify all electronic files for storage.</p>	
<p>i. Two complete sets of electronic working papers should be filed. One set (official) will be filed in iRIMS. A second set (backup) will be stored on removable media in the hard copy working paper folder. The new APPS naming convention (ex: 01701-2003A10100001_Archive_093003.exe) will be used for both. If there will be a short-term need to access the working papers, a third, or "working" set should be stored so as to be available for reference, generally on the LAN. This set should be deleted when no longer needed.</p>	
<p>j. Verify using a separate machine, that electronic files stored on removable media are not corrupted and can be unarchived. Indicate the test was successful by placing tester initials and date prominently on the CD label.</p>	
<p>k. Securely enclose the “backup” set of electronic files (CD) and any “official” set of hard copy in the hard copy folder.</p>	
<p>l. File the “official” set of electronic files in iRIMS (see iRIMS User Guide).</p>	
<p>m. <b><u>Do Not File Sensitive Audits in iRIMS:</u></b> Sensitive audits include but are not limited to classified work, suspected irregular conduct, hotline or DCAA Form 2000 related files. These audits should not be filed in iRIMS at this time. See CAM 4-407f for filing instructions.</p>	