INTERNAL CONTROL MATRIX FOR AUDIT OF IT GENERAL SYSTEMS CONTROLS	
Version No. 4.2	September 2007

Control Objectives	Example Control Activities	Audit Procedures
1. INDEPENDENT MANAGEMENT REVIEWS Management should perform periodic independent reviews (including internal and external audits) of IT operations to ensure that policies and procedures have been implemented and are working effectively (refer to CAM-5-407 for additional guidance).	Management establishes a schedule for periodic independent reviews of the IT operations. Management establishes formal follow-up procedures to ensure that identified deficiencies are addressed in a timely manner.	a. Verify that periodic reviews of contractor's policies and procedures are conducted to ensure that (1) polices and procedures have been implemented and are working effectively, and (2) follow-up actions are taken on recommendations resulting from management reviews.
		b. Evaluate the contractor's record of completed internal audits and its current internal audit plan to determine if the billing system is being subjected to periodic reviews in accordance with established policies and procedures.
		c. 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.
		d. 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

Control Objectives	Example Control Activities	Audit Procedures
		to which we can rely on the work performed (see CAM 4-1000).
2. ORGANIZATION 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).	Management assures that duties and responsibilities are segregated within the information systems department to avoid perpetration and concealment of errors.	a. Evaluate organization structure to determine if information technology (IT) department reports at a high enough level to allow it to act independently.
		b. Evaluate organization charts, position descriptions, etc. to determine if they provide for adequate segregation of duties and responsibilities within the information systems department.
		c. Interview selected contractor employees to determine whether duties and responsibilities are performed as established in organization charts, position descriptions, etc.
		d. 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.
3. SOFTWARE ACQUISITION, DEVELOPMENT, AND MODIFICATION System and application software should be consistent with management	Management establishes and maintains a standard development methodology which	a. Evaluate the contractor's software acquisition, development, and

Control Objectives	Example Control Activities	Audit Procedures
objectives, operate within specifications, tested prior to implementation, and not susceptible to unauthorized modification. (refer to CAM 5-409 for additional guidance).	contains the following control elements: • Written requirements/specifications reviewed and approved by application users and management. • Participation of appropriate user, and management personnel throughout all phases of software acquisition, development, and modification. • Documentation for all software programs including purchased software and modifications to existing software. • Validation, verification, and testing by management and Information System personnel to determine that software operates in conformity with design specifications and meets user requirements. • Final written approval from management, users, and information systems personnel prior to implementation.	modification policies and procedures to determine if they provide for a standard development methodology including the following controls: • Definition of Requirements • Participation of Appropriate Personnel • Software Documentation • Validation, Verification, and Testing • Final Management Approval
		b. If the preliminary risk assessment indicates that further audit effort is necessary, look at least one recent major software acquisition, development, or modernization project to determine if: (1.) Written requirements/specifications were reviewed and approved by applicable users and management. (2.) Appropriate IT user and

Control Objectives	Example Control Activities	Audit Procedures
		management personnel participated throughout all phases of the software acquisition, development, or modification. (3.) All software programs including purchased software and modifications to existing software are documented. (4.) Validation, verification, and testing was performed by management, users, and IT personnel to determine that the software operates in conformity with design specifications and meets user requirements. (5.) Final written approval from management, users, and IT personnel was obtained prior to implementation.
		c. 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).
4. COMPUTER OPERATIONS Computer operations should ensure the integrity and reliability of all activities impacting the physical operation of the computer. Such activities include:	Management establishes and maintains an operations environment which contains the following control elements: • System descriptions including	a. Evaluate the contractor's computer operation policies and procedures to determine if they provide for an environment in which:

Control Objectives	Example Control Activities	Audit Procedures
system initiation, operator interaction, help desk assistance, print operations, etc. (refer to CAM 5-410 for additional guidance).	technical points of contact, responsible manager, and recovery procedures. • Guidelines covering critical processes. Emphasis on processes that change/modify sensitive data residing in files, databases, etc. Guidelines to include authorized procedures, persons, and time frames. • Manual and automated logs (audit trails) of application processing, system accesses, and computer performance. • Scheduled hardware maintenance and backup/recovery procedures. • 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.	(1.) System descriptions are maintained. (2.) Critical processes are controlled. (3.) Audit trails are maintained (manual/automated logs) (4.) Backup/recovery procedures are maintained. (5.) Communications are checked/safeguarded.
		b. Examine a current major application system (consider using the system selected in 3.b above) to determine: (1.) System descriptions including technical points of contact, responsible manager, and recovery procedures are available. (2.) Guidelines exist which cover critical processes that change/modify sensitive data residing in files,

Control Objectives	Example Control Activities	Audit Procedures
		databases, etc. Guidelines should include authorized procedures, persons, and time frames. (3.) Manual and automated logs (audit trails) of application processing, system accesses, and computer performance are maintained. (4.) Scheduled hardware maintenance and backup/recovery procedures are defined. (5.) 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.
		c. 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).
5. SECURITY Access to computing resources should be limited to those individuals with a documented and authorized need for such access. Layers of physical, logical, and environmental security should be provided to protect the	Physical Security Measures should be taken to ensure that physical controls have been implemented to protect the computer facility (room or installation), central processor/peripheral/telecommunications	a. Evaluate the contractor's physical security policies and procedures to determine if they are adequate to provide for a physically secure environment in which:

Control Objectives	Example Control Activities	Audit Procedures
department's computing resources against unauthorized use, modification, damage, or loss (refer to CAM 5-411 for additional guidance).	hardware, files, or programs from unauthorized use, modification, damage, or loss. Physical controls should include the following: • Entrances to computer facilities are secured (i.e., keys, badges, cipher locks, etc.) • Authorization of individuals with access to computer resources is controlled and documented. • Visitors are escorted within the computer facility. • Access for employees who quit or are terminated are revoked in a timely manner. • Inventory and accountability records are maintained for data files and tapes. • Sensitive data files, programs, and documentation have been identified. • On-site and off-site storage facilities exist. • Environment is protected against fire, excess humidity, temperature variation, and other environmental hazards.	(1.) Facility security is maintained. (2.) User access is authorized and controlled. (3.) Visitor access is controlled. (4.) Terminated employee's access is revoked. (5.) Inventory and accountability records are maintained. (6.) Sensitive data, software, and documentation is identified and protected. (7.) On-site and off-site storage is maintained. (8.) Environmental protection is maintained.
		b. Evaluate the contractor's implementation of physical security controls to determine if: (1.) Entrances to computer facilities are secured (i.e., keys, badges, cipher locks, etc.).

Control Objectives	Example Control Activities	Audit Procedures
		(2.) Authorization of individuals with access to computer resources is controlled and documented. (3.) Visitors to the computer facility are escorted. (4.) Access for employees who quit or are terminated is revoked in a timely manner. (5.) Inventory and accountability records are maintained for data files and tapes. (6.) Sensitive data files, programs, and documentation have been identified. (7.) On-site and off-site storage facilities exist. (8.) Environment is protected against fire, excess humidity, temperature variation, and other environmental hazards.
		c. 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).
	Logical Security Logical access to software and data files should be limited through the use of security software, which define authorized users and level of access. Logical controls	a. Evaluate the contractor's logical security policies and procedures for all operating environments (e.g., batch, interactive, and database) to determine if they are adequate

Control Objectives	Example Control Activities	Audit Procedures
	should include the following: • User access levels are identified and documented. • Security software is used to control access to computer resources. • Security software access levels have been properly implemented. • User IDs and passwords are established and controlled. • Computer access is recorded and monitored.	to provide for a logically secure environment in which: (1.) User access levels are controlled. (2.) Security software is used. (3.) Security software levels are properly implemented. (4.) Logical access restrictions are controlled by passwords and automated rules. (5.) Logical access is recorded and monitored.
		b. Evaluate the contractor's implementation of logical security controls for all operating environments to determine if: (1.) User access levels are identified and documented. (2.) Security software is used to control access to computer resources. (a) Determine the type of information security software installed on major computer systems. (b) Gain a general understanding of the software package(s). (3.) Security software access levels have been properly implemented based on demonstrated need. (a) Determine who the contractor has given special system privileges to, such as those that:

Control Objectives	Example Control Activities	Audit Procedures
		• are used to define user and group access authorities • permit full system access • are used to monitor system access and access violations (b) Determine that the information security software covers all major application areas, especially those which generate reports on which DCAA relies. (c) Obtain a listing of all user/group security authorities for an audit selected critical application. (d) 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. (e) Ensure that the systems and application programmers do not have access to production programs and data. (4.) User IDs, passwords and automated rules are established and controlled. Determine if: (a) IT personnel, when terminated or separated for any reason, are promptly removed from the IT organization spaces in order to safeguard the computer facilities

Control Objectives	Example Control Activities	Audit Procedures
		and data files. (b) Passwords or other control devices used to gain access to computing resources are changed immediately upon the termination or transfer of the individual employee to whom they are related. (c) The passwords issued by the IT organization are at least e characters in length, cannot be easily guessed, and do not contain repeating characters. (d) Passwords are changed periodically and cannot be reused by the same individual. (e) Passwords are not displayed during the logon process, are not printed on output, and are stored by data processing operations in an encrypted file. (f) Users are logged-off automatically if they have not been active for a specific length of time. (5.) Computer access is recorded /monitored. (a) Determine whether the contractor makes use of logs to detect unauthorized accesses to production data. Verify that they

Control Objectives	Example Control Activities	Audit Procedures
		review these logs within reasonable timeframes and follow-up on unauthorized access attempts. (b) Interview personnel responsible for information security to determine procedures for monitoring and following up on improper access attempts. (c) Select a sample of improper access attempt reports and follow up on the actions taken by the information security function for reported violations. (6.) Training is conducted on security procedures and awareness. (7.) Violation and security activity reports are reviewed regularly to identify and resolve incidents involving unauthorized activity.
		c. 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).
6. CONTINGENCY PLANS Contingency plans should be established to provide for continuance of information processing following a	Management establishes and maintains a contingency plan for processing critical application systems in the event of a major	a. Evaluate the contractor's policies and procedures to determine if they are adequate to provide for the processing

Control Objectives	Example Control Activities	Audit Procedures
major hardware or software failure.	hardware or software failure. Contingency plans should include the following controls: • Critical or sensitive application software and data files are identified. • Provisions for backup site and computer hardware and software have been made. • Copies of the contingency plan are stored offsite. • Tests of the contingency plan are required and performed.	of critical application systems in the event of a major hardware or software failure. Contingency plans should require: • Identification of critical applications and data files. • Provisions for backup computer system. • Off-site storage of contingency plans. • Tests of contingency plans.
		b. Evaluate contingency plans and test documentation to determine if established policies and procedures are followed with emphasis in the following areas: • Critical or sensitive applications and data files are identified. • A backup computer site was identified with sufficient systems hardware and software available to commence alternative computer center operations in a timely manner. • Copies of the contingency plan, software documentation, and critical user data are pre-positioned off-site. • Any deficiencies identified during testing were documented and resolved.

CONTROL OBJECTIVES CONTROL ACTIVITIES AUDIT PROCEDURES

Control Objectives	Example Control Activities	Audit Procedures
		c. Determine the extent of compliance with the Contractor Records Retention requirements as defined in FAR – Part 4, Subpart 4.7.
		d. 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).