SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Transaction Histories/Audit Trails. According to Joint Financial Management Improvement Program guidance, a transaction is recording the data elements involved in a financial event. A financial event is any occurrence having financial consequences to the federal government related to the receipt of appropriations or other financial resources; acquisition of goods or services; payments or collections; recognition of guarantees, benefits to be provided, or other potential liabilities; or other reportable financial activities. Transaction histories and audit trails provide the basis for tracing individual transactions through the system. Transaction histories uniquely identify each transaction input to the system while audit trails allow the tracing of a transaction from the originating supporting document (including changes and corrections) through the system to the subsidiary ledger and/or general ledgers and financial statements. Adequate audit trails are critical to providing support for transactions and balances maintained by the financial system. Financial management systems must: - Provide audit trails to trace transactions from the source documents, original input, changes and corrections, other systems, system generated transactions, and internal assignment transactions through the system. - Provide audit trails to allow tracing of source documents and transactions through successive levels of summarization to the financial statements. A complete audit trail allows all transactions to be traced from the source records and documents (including changes and corrections) to the Subsidiary and General Ledgers and to the financial statements and vice versa. - Provide audit trails to identify changes made to system parameters and tables that affect processing or reprocessing of any financial transactions. - The audit trails should identify the document input, changes, deletions, and approvals by the originator.	Software	Functional OPR & System Lifecycle Manager	Key Accounting Requirement (KAR) 8 and para 020207G, I	Ch 6, pp 43, 44, 49, 50	JFMIP-SR-99-4, pp 20 and FFMSR-0, pp 31	Ch 3, AC-4.1 & Ch 4, AN-2.1

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Transaction Histories/Audit Trails (cont.) Supporting documentation forms the basis of the transaction histories and audit trails. Supporting documentation must be maintained in accordance with legal requirements. AFM 37-139, Records Disposition Schedule, 1 March 1996, contains the Air Force requirement for retaining source documents and transaction data to support financial management and financial statements.						
Electronic Interface Between Systems. The Joint Financial Management Improvement Program *Core Financial System Requirements* requires that data should be entered or input into a financial management system only once. Thus all interfaces between the system of original input and any other system must be electronic and not have any manual intervention. The interfaces between systems must be documented and controlled and the accounting system as a whole must ensure the timely and complete transmission of transactions and financial related data.	Software	Functional OPR & System Lifecycle Manager	para 020202C and para 020207C	Ch 6, pp 47	JFMIP-SR-99-4, pp 7 and FFMSR-0, pp 56	Ch 3, SP-2.1 thru SP-2.2 & SS-1.2
Transaction Controls. Transaction controls consist of input, processing, and output controls to prevent, detect, and correct irregularities that may occur anywhere in the chain of events from transaction authorization to the final reports and financial statement. The controls shall cover the functions of transaction authorization and approval, data preparation and validation, input, communication, processing, storage and output. Transaction controls are used to or detect the following kinds of situations - Failure to record a transaction. - Incorrect or incomplete transaction. - Duplicate transaction - Loss of a transaction	Software	Functional OPR & System Lifecycle Manager	KAR 7	Ch 6, pp 7, 27, 28, 44, 45, 47, 48, 50	JFMIP-SR-99-4, pp 20, 21 and FFMSR-0, pp 62, 68	Ch 4, AN-1, AN-3, CP-1, AY-1 thru AY-3

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Transaction Controls (cont.) - Incorrect default value. - Unauthorized use of programs that bypass normal controls and edits. - Inappropriate use of operating program testing aids to circumvent normal processing control procedures. - Unauthorized entry to system and files. For example, controls to detect above situations include edits. Specifically, system edits should check transaction fields to ensure only proper and correct data is processed. If edits can be bypassed, the system should maintain a record of who is authorized to override the edits and how often the edits have been bypassed. The system should have threshold edits to prevent invalid data from being entered to the system. For example, if the organization only allows depreciation for equipment for a maximum of 120 months is there should be an edit control that prevents depreciation of more than 120 months from being input. Hash and batch totals to separately control groups of transactions should also be present. Transaction controls also include error detection and correction. The system should have the means and procedures to detect and correct errors in a timely manner and within the appropriate processing cycle and fiscal year. Additionally, management should procedures to analyze error reports so that system improvements can be made.						

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Completeness Controls. This directly relates to the financial statement accounting assertion on completeness, which deals with whether all valid transactions are recorded and properly classified. The system should contain procedures that allow management to periodically verify the accuracy of file data. A record of data verification should be maintained. This is normally done in conjunction with the annual FMFIA system manager user review. Likewise, the system should contain procedures to periodically reconcile summarized or general ledger data with subsidiary accounts and/or source records. Regularly scheduled reconciliations of control and subsidiary accounts should be performed at least monthly to substantiate and maintain the completeness and accuracy of account postings and balances by checking the agreement between the sum of the detail in subsidiary accounts and the general ledger control balances.	Procedural	Functional OPR	para 030602C	Ch 6, pp 50, 51	FFMSR-0, pp 25-34	Ch 4, CP-2
Computation Logic. Management should periodically verify the accuracy of computations. Specifically, management should validate that computation algorithms use appropriate data and manipulate that data to achieve the intended result. For example, when depreciating equipment, the correct value (purchase price versus sale price) and date (purchase date versus requisition date) must be used and the correct mathematical depreciation formula should be applied.	Software	Functional OPR & System Lifecycle Manager				

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Access Controls. Management should establish procedures to authorize, control and maintain records of personnel with access to systems. Management should periodically validate access records with supervisors to ensure only active personnel with a "need to know" have access to the system. Further management should periodically validate access records with the system administrator to ensure that only currently valid personnel have access to the system. In addition, the system should contain adequate software access controls. For example, software controls can force users to periodically change their passwords and adhere to corporate password standards (i.e., minimum number of characters, reuse limitations, etc.).	Procedural/ Software	Data Center Manager & System Lifecycle Manager & Functional OPR	KAR 7	Ch 6, pp 22, 24, 45; and App A, pp 50	FFMSR-0, pp 61-62	Ch 3, AC-1 thru AC-4 Ch 4, AN-2

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Separation of Duties. Management should implement controls so that incompatible duties separated among systems and user personnel. For example, -- In the system program office, systems analysis and design personnel should not have access to source programs, the computer itself, or to data conversion facilities. -- Within system operations, application programmers should not have access to the operating system programs or to the data files. In addition, application programmers should not be allowed to load programs into the production region of the computer. A program librarian should do this. -- Operating system programmers should not have access to the database, data base management system or programs, or the application programs. -- Within user operations, users should only have access to data as designated by the functional OPR. Users should not have access to application programs, operating system programs and utilities, or the data base management system and programs. -- Also, within user operations, separation of duties and responsibilities must be maintained for initiating, authorizing, processing, recording, and reviewing transactions.	Procedural	Data Center Manager & System Lifecycle Manager & Functional OPR	KAR 7	Ch 3, pp 4; and Ch 6, pp 42	FFMSR-0, pp 62	Ch 3, SD-1 thru SD-3

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Configuration Management. The configuration management process is a process of applying administrative and technical procedures throughout the software life cycle to: identify and define software items in a system; control modifications and releases of the items; record and report the status of the items and modifications requests; ensure the completeness, consistency, and correctness of the items; and control storage, handling, and delivery of the items (IEEE/EIA 12207.0, para 6.2). Procedures should be established to identify and document configuration items and digital data files. Subsequently, management should formally document all system changes. All proposed system changes should be properly controlled and classified. Users should formally approve system changes before the changed software is migrated to the production region. Procedures should be established to test system changes using predetermined test results by someone other than the software developer and maintenance activity. Test criteria, procedures, and results should be documented and kept on file to facilitate future reviews, evaluations and modifications. All system changes should be independently tested by someone other than the maintenance activity. The appropriate documentation should be updated to reflect system changes as they occur.	Procedural	Data Center Manager & System Lifecycle Manager & Functional OPR		Ch 6, pp 20, 25, 40, 41	FFMSR-0, pp 61, 76, 77	Ch 3, CC-1 thru CC-3

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Documentation. The documentation process is a process for recording information produced by a life cycle process or activity. The process contains the set of activities which plan, design, develop, produce, edit, distribute, and maintain those documents needed by all concerned such as managers, engineers, and users of the system or software product (IEEE/EIA 12207.0, para 6.1). The documentation should be current and cover the system's development and actual operations. The documentation should be of sufficient scope and depth to provide managers, users, systems operators, and software maintenance personnel with an understanding of the design and operation of each component in the system and its integration with and relation to all other components. The system documentation should also provide accounting policies, processes, and procedures. It should describe aspects of the system such as the account structure and definitions; transaction codes; the accounting cycles and procedures; transaction and data flow; and coordination needed with other groups or systems. Documentation should describe, in detail, the effect of all transactions on the Subsidiary or General ledgers. For example, the documentation should clearly show that a sale from the depot decreases the asset balance and increases the corresponding accounts receivable balance.	Procedural	Data Center Manager & System Lifecycle Manager & Functional OPR	KAR 10 & 11	Ch 4, pp 1 thru 6 and Ch 6, pp 36, 37, 25	FFMSR-0, pp 72	
Query Languages. Query languages should be used as query tools only and not used to update or change data. Using query tools to update or change data bypasses normal system transaction controls and, often, does not create an acceptable audit trail.	Software	Data Center Manager & System Lifecycle Manager & Functional OPR	para 030602B	Ch 6, pp 24		Ch 4, AY-2

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Report Utility. Management should have controls to ensure that reports meet management and legal requirements and are provided in a timely manner. Additionally, management must institute controls that ensure that reports that contain sensitive or Privacy Act information are secured and properly destroyed when no longer needed.	Procedural	Functional OPR & System Lifecycle Manager	KAR 12	Ch 6, pp 50, 51		Ch 4, AY-4
Physical Security. Management should provide adequate physical safeguards for the computer facility. For example, backup power and communications should be available. In addition, appropriate physical access controls should be in place. Appropriate documentation should be prepared, maintained and available for inspection.	Procedural	Functional OPR & Data Center Manager		Ch 6, pp 11, 13, 16, 18		CH 3, SC-1 thru SC-4

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Internal Control	Type of Control	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
System Software. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some system software can change data and program code on files without leaving an audit trail. Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. The software should be comprehensively tested prior to release for production. System software controls fall into the following categories: operating systems, system utilities, security software, program library systems, file maintenance systems, data communication systems, data base management systems, and system software change controls. The control concerns for system software are similar to access control issues. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. For this reason, auditors generally treat this segment of a controls review separately.	Software/ Procedural	Functional OPR & Data Center Manager	KAR 11	Ch 6, pp 18, 19		Ch 3, SS-1 thru SS-3
Certification and Accreditation. The system should be certified and accredited for operational use. The completed certification and accreditation process should include a risk assessment, security testing, contingency planning, and a vulnerability assessment. Appropriate documentation should be prepared, maintained and available for inspection. Additional references: DoDI 5200.40[6], and AFSSI 5024, Vol I, II, III, & IV[7]	Procedural	Designated Approving Authority		Ch 3, pp 2, 3, 4; Ch 4, pp 4; and Ch 5		

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

The two processes listed below, although not system controls, require management attention. Reviews of systems in operation is a legal requirement applicable to all financial management systems in use (i.e., this requirement does not apply during system development). Conversely, double entry accounting applies only to those systems producing subsidiary or general ledger entries. If double entry accounting is required but not properly implemented, there could be serious ramifications to the financial statements.

Process	Type of Process	Responsible Organization	DoD 7000.14 Vol 1 [1]	DoD 7740.1-G[2]	JFMIP-SR-99-4[3]/ FFMSR[4]	FISCAM[5]
Reviews of Systems in Operation. Annual evaluations should be performed to determine whether accounting systems conform to principles and standards prescribed by the Comptroller General. The review should include transaction testing of the critical aspects of the system. The transaction test should cover the entire flow of transactions from initial authorization through processing and reporting.	Procedural	Functional OPR & System Lifecycle Manager	KAR 11 and para 030602C	Ch 3, pp 4		
Double Entry Accounting. A basic control in a financial management and accounting system is double entry accounting. Double entry accounting requires that for every debit/credit entry to a subsidiary ledger or general ledger account there must be a corresponding credit/debit entry to a subsidiary ledger and/or general ledger account. The control is realized because all debits must equal credits	Procedural	Functional OPR	KAR 1 and para 020207D			

SYSTEM CONTROL REQUIREMENTS

As of 7 December 1999

Notes:

[1]Department of Defense, Financial Management Regulation, 7000.14-R, Volume 1, May 1993

[2]Department of Defense, ADP Internal Control Guideline, 7740.1-G, July 1988

[3]Joint Financial Management Improvement Program, Core Financial System Requirements, JFMIP-SR-99-4, February 1999

[4]Joint Financial Management Improvement Program, Federal Financial Management System Requirements (FFMSRs) Framework for Federal Financial Management Systems, FFMSR-0, January 1995

[5]U.S. General Accounting Office, Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6 (NOTE: Chapter 4 of this document is still in draft.)

[6]DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoDI 5200.40, 30 December 1997

[7]Air Force System Security Instruction 5024, Volume I, The Certification and Accreditation Process (1 September 1997); Volume II, The Certifying Official's Handbook (1 September 1997), Volume III, The Designated Approving Authority's Guide (1 March 1999), and Volume IV, Type Accreditation (1 March 1999)

Disclaimers:

--This list does not address the accounting functionality that applies to a system (based on the system's objectives [e.g., inventory control]).

--This list is not all-inclusive as to applicable guidance (i.e., laws and regulations).