State of Michigan (agency name)
Biennial Evaluation of the Internal Control Structure - Application Specific Controls
As of September 30. 2004

Note: Due to the formation of the Department of Information Technology (DIT), many IT related responsibilities that were formally assumed by agency management has shifted to DIT management. However, agency management is still the business process/application owners, and therefore, still holds the responsibility for managing the application and the application environment.

Application Specific Controls apply to individual computer application systems and may include such controls as data origin, input controls, processing controls, output controls, application access controls, audit train controls, and documentation. They consist of mechanisms in place over each separate computer system that helps to ensure authorized data is processed completely, accurately, and reliably. Business owners/Agencies are primarily responsible for ensuring application specific controls are in place and functioning properly within their organizations.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Define the Information Architecture													
Objective: To optimize the organization of information systems.													
Potential/Likely Risks: Systems are not defined to optimize the use of information.													
Data Classification Scheme													
Has agency management established a general classification framework with regards to placement of data in information classes?	PO 2.3												
Security Levels													
Has agency management defined, implemented and maintained security levels for different classifications of data?	PO 2.4												
Conclusion for this Section (Include All Weaknesses Identified)													
Define the IT Organization and Relationships													
Objective: To deliver the right IT services.													
Potential/Likely Risks: IT needs are not aligned with business and do not help provide effective direction and adequate control.													
Segregation of Duties													
Is there adequate separation of duties between information system users (data entry staff, etc.) and IT staff functions (operations staff, developers, system administrators, network management, security staff, etc.)?	PO 4.10												
Conclusion for this Section (Include All Weaknesses Identified)													

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Identify Automated Solutions													
Objective: To ensure an effective and efficient approach to satisfy the user requirements.													
Potential/Likely Risks: There is not an objective and clear identification and analysis of alternative opportunities measured against user requirements.													
Audit Trails Design													
Are there adequate mechanisms in place to ensure that audit trails are available (or can be developed for systems that are in development)?	AI 1.10												
Do audit trails provide a mechanism that facilitates the tracing of transaction processing and the reconciliation of disrupted data?	AI 1.10												
Are there adequate trails in place to trace transactions through the system (input to output and in reverse)?	AI 1.10												
Are there adequate trails in place to trace transactions from the summary reporting level to the detail level?	AI 1.10												
Do audit trails adequately monitor the security activity that has occurred within the application?	AI 1.10												
Do the audit trails adequately monitor the user activity that has occurred with the application, including file access?	AI 1.10												
Is there an adequate retention period for audit trails?	AI 1.10												
Have procedures defined the methodology to follow for reviewing audit trail records (e.g., frequency of review, level of review, reporting of suspect transactions or security violations, etc.)?	AI 1.10												

Conclusion for this Section (Include All Weaknesses Identified)

Acquire and Maintain Application Software													
Objective: To provide automated functions that effectively support the business process.													
Potential/Likely Risks: Specific statements of functional and operational requirements are not defined. A phased implementation does not identify clear deliverables.													
Definition of Interfaces													
What is the quality of the application documentation (should include system and program flowcharts, decision tables, file layouts, data element definitions, narratives, source program listings, record of changes, etc.)?	AI 2.8												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
User References and Support Materials													
What is the quality of the application operations documentation (should include job and system flowcharts, input and output descriptions, job frequency and sequence of operation, job restart/recovery procedures, file backup requirements and procedures, error messages and file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, data capture instructions)?	AI 2.16												
What is the quality of end-user documentation (should include a description of the system, description of source documents and procedures for their preparation, input mechanisms, job submission procedures, control procedures, error identification and correction procedures, description of output reports and their use, etc.)?	AS 2.16												

Conclusion for this Section (Include All Weaknesses Identified)

Develop and Maintain Procedures

Objective: To ensure the proper use of the applications and the technological solutions put in place.

Potential/Likely Risks: There is not a structured approach to the development of user and operations procedures manuals, service requirements, and training manuals.

User Procedures Manual													
Are adequate user procedure manuals prepared and refreshed as part of every information system development, implementation, or modification project?	AI 4.2												

Conclusion for this Section (Include All Weaknesses Identified)

Install and Accredit Systems

Objective: To verify and confirm that the solution is fit for the intended purpose.

Potential/Likely Risks: There is no well formalized installation migration, conversion, and acceptance plan.

Training													
Is application training available for end users and is this training adequate, current, and available for new people?	AI 5.1												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		

Conclusion for this Section (Document Any Material Weaknesses)

Ensure Systems Security													
Objective: To safeguard information against unauthorized use, disclosure or modification, damage or loss.													
Potential/Likely Risks: Logical access controls do not ensure that access to systems, data, and programs is restricted to authorized users.													
Manage Security Measures													
Is IT security managed so that security measures are in line with business requirements, including the following? • Translating risk assessment information to the IT security plans • Implementing the IT security plan • Updating the IT security plan to reflect changes in the IT configuration • Assessing the impact of change requests on IT security • Monitoring the implementation of the IT security plan • Aligning IT security procedures to other policies and procedures	DS 5.1												
Identification, Authentication and Access													
Has an adequate authentication mechanism of identified users and resources (associated with access rules) been implemented that restricts the logical access to and use of the information services function's computing resources?	DS 5.2												
Are there standards for password configuration including password length, periodic password changes, password composition, password aging, invalid password attempts, password encryption, etc.?	DS 5.2												
Is access to key data files, tables, log, and program files restricted to only those users requiring access to perform their job functions?	DS 5.2												
Are passwords required for all users? Are user access control reports periodically reviewed for accuracy, completeness, and appropriate access levels by user management?	DS 5.2												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Security of Online Access to Data													
In an on-line IT environment, have procedures been implemented in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change, or delete data?	DS 5.3												
User Account Management													
Do access request forms require proper approvals for the requested access?	DS 5.4												
Are there formal procedures in place related to requesting, establishing, issuing, suspending, and closing user accounts and monitoring of application access (including the data or system owner granting the access privileges)?	DS 5.4												
Do procedures define the methods for timely deletion/disabling of user IDs (e.g., staff turnover, changes in responsibility, extended absence, etc.)?	DS 5.4												
Have administrative and/or privileged accounts been restricted to only appropriate individuals?	DS 5.4												
Management Review of User Accounts													
Are periodic reviews of user access completed to ensure users are active and have been limited to what is required to complete their job responsibilities?	DS 5.5												
User Control of User Accounts													
Do users review information for normal activity in addition to being alerted to unusual activity?	DS 5.6												
Security Surveillance **Violation and Security Activity Reports** **Incident Handling**													
Is violation of security policy and security activity logged, reported, reviewed, and appropriately escalated on a regular and timely basis to identify and resolve incidents involving unauthorized activity?	DS 5.7 DS 5.10 DS 5.11												
Data Classification													
Has data been classified into a security category by its ownership and have access rules for the categories been defined?	DS 5.8												
Has agency management defined security levels for each of the data classifications that represent the appropriate (minimum) set of security and control	DS 5.8												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
measures for each of the classifications?													
Central Identification and Access Rights Management													
Are controls in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner?	DS 5.9												
Do procedures exist to ensure that unique user IDs are assigned to system users and shared user IDs are not allowed?	DS 5.9												
Reaccredidation													
Are reaccreditations of security periodically performed to keep the formally approved security level and acceptance of residual risk up-to-date?	DS 5.12												
Counterparty Trust **Transaction Authorization**													
Do organizational policy, procedures and protocol ensure that, where appropriate, controls are implemented to provide authenticity of transactions (i.e., cryptographic techniques for signing and verifying transactions, etc.) and to provide against unauthorized access, modification and misaddressing during transmission and transport?	DS 5.13 DS 5.14												
Non-Repudiation													
Does organizational policy ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions, (e.g., use of digital signatures, time stamping, trusted third parties, etc.)?	DS 5.15												
Trusted Path													
Does policy ensure that sensitive transaction data, security information, passwords, cryptographic keys, etc. is only exchanged over a trusted path?	DS 5.16												
Protection of Security Functions													
Is security-related hardware and software protected against tampering?	DS 5.17												
Protection of Electronic Value													
Are all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information protected?	DS 5.21												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		

Conclusion for this Section (Include All Weaknesses Identified)

Manage Projects													
Objective: To ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence.													
Potential/Likely Risks: There is not a problem management system which records and progresses all incidents.													
Manage Problems and Incidents													
Are emergency and temporary access authorizations documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function and automatically terminated after a predetermined period?	DS 10.4												
Have emergency processing priorities been established, documented and approved by appropriate program and IT management?	DS 10.5												

Conclusion for this Section (Include All Weaknesses Identified)

Manage Data													
Objective: To ensure that data remains complete, accurate and valid during its input update and storage.													
Potential/Likely Risks: The combination of application and general controls over IT operations is ineffective.													
Data Preparation Procedures **Source Document Error Handling**													
Do error-handling procedures during data origination reasonably ensure that errors and irregularities are detected, reported, and corrected?	DS 11.1 DS 11.4												
Does the design of source documents contribute to the accuracy and efficiency of the input?	DS 11.1												
Source Document Authorization Procedures													
Are transactions appropriately authorized when required, prior to data input?	DS 11.2												
Is there an adequate separation of duties regarding the origination and approval of source documents?	DS 11.2												
Source Document Data Collection **Data Processing Validation and Editing**													
Is data entry conducted within a short time after the source document is created?	DS 11.3 DS 11.10												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
After source documents are entered into the application, are they marked or signed in some way to indicate they were entered, reducing the risk of accidental duplication or reuse of the document?	DS 11.3												
Is manually prepared input, recorded on source documents or entered via terminal, reviewed for accuracy and completeness?	DS 11.3												
Source Document Error Handling													
Do the rejected transactions or suspense files produce follow-up messages and report the status of uncorrected transactions on a regular basis?	DS 11.4												
Source Document Retention													
Are source documents retained for an effective period of time?	DS 11.5												
Data Input Authorization Procedures													
Have procedures been established to ensure only authorized staff performs data input?	DS 11.6												
Do data input procedures allow anyone to override or bypass data validation and error editing routines?	DS 11.6												
Accuracy, Completeness and Authorization Checks													
Are formatted and interactive screens used to ensure data is recorded in the proper field?	DS 11.7												
Does the design of input screens inhibit the omission of data and prevent the acceptance of invalid data (on-line validation and editing routines)?	DS 11.7												
Do online edit routines identify inaccurate data as early as possible and prevent the entry of invalid, duplicate, out-of-period data into the system?	DS 11.7												
Are there controls in place to ensure completeness and accuracy of processing (run-to-run totals, control totals, duplicate processing, reconciliations, etc.)?	DS 11.7												
Data Input Error Handling													
Are there controls in place to ensure that data rejected from the system is corrected and resubmitted on a timely basis (such as an automated suspense file)?	DS 11.8												
Do documented procedures explain the process to ensure that rejected transactions are corrected and re-entered promptly?	DS 11.8												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Are corrected transactions subject to the same edit and balancing controls as the original transactions?	DS 11.8												
Data Processing Integrity													
Source Document Error Handling													
Are data entry procedures and controls effective to ensure complete and accurate input of data?	DS 11.9												
Is there appropriate separation of duties between those who input the source documents and those who approve the source documents for input?	DS 11.9												
Is there adequate separation of duties between individuals that input the data and individuals responsible for verifying the accuracy and completeness of data output?	DS 11.9												
Are effective controls established over input through the use of control totals, hash totals, or record counts?	DS 11.9												
Is there an I/O processing control group that performs such activities as balancing the record counts, batch counts, and control totals (where applicable) for data processed?	DS 11.9												
Are file labels used to ensure that only the correct file is being assessed and processed?	DS 11.9												
Data Processing Validation and Editing													
Are limit tests used that check the values in particular fields to see if their amounts have exceeded a present limit?	DS 11.10												
Are processing results edited against parameters of reasonability (appropriate ranges for data)?	DS 11.10												
Are key computations fully documented to explain calculation sequence, rounding, truncation, decimal positioning, etc.?	DS 11.10												
Do processing controls ensure that transactions are processed and recorded in the correct time period to provide accurate cut off for reporting periods?	DS 11.10												
Data Processing Error Handling													
Are any significant problems not reflected on the problem reports?	DS 11.11												
How are duplicate transactions prevented or identified?	DS 11.11												
Do data processing error handling procedures enable erroneous transactions to be identified without being processed and without undue	DS 11.11												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
disruption of processing other valid transactions?													
Is invalid data properly rejected during subsequent processing of data input?	DS 11.11												
Do IT problem reports identify problems related to the application system?	DS 11.11												
Output Handling and Retention													
Do procedures cover the handling of negotiable instruments, if applicable, and other output?	DS 11.12												
Output Distribution													
Are there documented procedures that address the distribution of data processing output, including critical or sensitive reports awaiting distribution?	DS 11.13												
Is output distributed on a timely basis only to authorized personnel and is restricted output properly labeled?	DS 11.13												
Output Balancing and Reconciliation													
Does the generation of reports permit transactions to be traced forward to the final output and backward to the original source data entries?	DS 11.14												
Are documented balancing and reconciling procedures in place to ensure that out of balance conditions are resolved on a timely basis?	DS 11.14												
For systems that process revenue or expenditures, are there proper user procedures for reconciling the reports and/or system to MAIN?	DS 11.14												
Output Review and Error Handling													
Is there a control group or individual that is responsible for reviewing all output reports for their general acceptability and completeness?	DS 11.15												
Are there totals and other data included in the selected reports verified by the user department to ensure report accuracy?	DS 11.15												
Are production problems identified and resolved on a timely basis?	DS 11.15												
Security Provision for Output Reports **Protection of Disposed Sensitive Information**													
Are there controls in place over the on-line access of reports that prevent the unauthorized from reading, copying, deleting, or redirecting of output?	DS 11.16 DS 11.18												
Protection of Sensitive Information During Transmission and Transport													
In systems where data is received electronically, do controls exist to ensure all data was received	DS 11.17												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
completely?													
Storage Management													
Are there procedures for data storage that consider retrieval requirements, and cost effectiveness and security policy?	DS 11.19												
Retention Periods and Storage Terms													
Is there an appropriate retention period defined for all reports?	DS 11.20												
Protection of Sensitive Messages													
Regarding data transmission over the Internet or any other public network, has management defined and implemented procedures and protocols to be used to ensure integrity, confidentiality and non-repudiation of sensitive messages?	DS 11.27												
Authentication and Integrity													
Is the authentication and integrity of information originated outside the organization, whether received by telephone, voicemail, paper document, fax or email, appropriately checked before potentially critical action is taken?	DS 11.28												
Electronic Transaction Integrity													
Have appropriate procedures and practices for sensitive and critical electronic transactions been defined and implemented, ensuring integrity and authenticity of: • atomicity (indivisible unit of work, all of its actions succeed or they all fail)? • consistency (if the transaction cannot achieve a stable end state, it must return the system to its initial state)? • isolation (a transaction's behavior is not affected by other transactions that execute concurrently)? • durability (transaction's effects are permanent after it commits, its changes should survive system failures)?	DS 11.29												

Conclusion for this Section (Include All Weaknesses Identified)

Manage Operations

Objective: To ensure that important IT support functions are performed regularly and in an orderly fashion.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		

Potential/Likely Risks: There is not a schedule of support activities to report and clear for the accomplishment of all activities.

Safeguard Special Forms and Output Devices

Are there appropriate physical safeguards over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management?	DS 13.7												

Conclusion for this Section (Include All Weaknesses Identified)

Monitoring the Processes

Objective: To ensure the achievement of the performance objectives set for the IT processes.

Potential/Likely Risks: Relevant performance indicators or reporting structures are not defined so deviations can be acted upon promptly.

Assessing Performance

What does end user management perceive to be the risks, exposures, and limitations associated with the system?	M 1.2												

Assessing Customer Satisfaction

What is the attitude of end user management regarding the quality and effectiveness of the system?	M 1.3												
What is the attitude of end users regarding the quality and effectiveness of the system?	M 1.3												

Conclusion for this Section (Include All Weaknesses Identified)

Overall Conclusion of Strengths and Weaknesses

As (job title) of the (office) of (department), I am cognizant of the importance of internal controls. I have taken necessary measures to ensure that the evaluation of the internal control structure has been conducted in a reasonable and prudent manner, in accordance with the General Framework for the Evaluation of Internal Controls, issued by the Department of Management and Budget, Office of Financial Management, in consultation with the Auditor General.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (Non-DIT) Responsible for IT Process and Related Controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		

Objectives of the internal control structure are to provide reasonable assurance that measures are being used to safeguard assets, check the accuracy and reliability of accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. The concept of reasonable assurance recognizes that the cost of internal control should not exceed benefits to be derived therefrom, and that benefits consist of reductions in risks of failing to achieve stated objectives.

The results of the evaluation indicate that the internal control structure in effect for the two-year period ended September 30, 2004, complies with the requirement to provide reasonable assurance that the aforementioned objectives were achieved, unless otherwise indicated below.

Material Weaknesses Identified: _____ Yes _____ No (If yes, attach to this letter a list of material weaknesses identified.)

Activity Level Manager Signature

Date

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments column.